Acunetix
by Invicti

Affected Items Report

Acunetix Security Audit

2024-06-09

Generated by Acunetix

Scan of testphp.vulnweb.com

Scan details

Scan information	
Start time	2024-06-07T23:21:45.483039+07:00
Start url	http://testphp.vulnweb.com/
Host	testphp.vulnweb.com
Scan time	45 minutes, 47 seconds
Profile	Full Scan
Server information	nginx/1.19.0
Responsive	True
Server OS	Unknown
Server technologies	PHP
Application build	24.4.240514098

Threat level

Acunetix Threat Level 4

One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	74
Critical	19
High	23
Medium	14
Low	11
Informational	7

Affected items

Web Server	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	Path Fragment input **/<s>/<s>-[*].html** was set to **1AcuStart504489'"257418AcuEnd**

```
GET /Mod_Rewrite_Shop/RateProduct-1AcuStart504489'"257418AcuEnd.html HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/AJAX/infoartist.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded GET input **id** was set to **1AcuStart334118'"026944AcuEnd**

```
GET /AJAX/infoartist.php?id=1AcuStart334118'"026944AcuEnd HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Cookie: mycookie=3

Accept: */*

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/AJAX/infocateg.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded GET input **id** was set to **1AcuStart866553'"098844AcuEnd**

```
GET /AJAX/infocateg.php?id=1AcuStart866553'"098844AcuEnd HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Cookie: mycookie=3

Accept: */*

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/AJAX/infotitle.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **id** was set to **1AcuStart099151'"196189AcuEnd**

```
POST /AJAX/infotitle.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Cookie: mycookie=3

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

Accept: */*

Content-Length: 32

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



id=1AcuStart099151'"196189AcuEnd
```

/artists.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded GET input **artist** was set to **1AcuStart586434'"602672AcuEnd**

```
GET /artists.php?artist=1AcuStart586434'"602672AcuEnd HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/listproducts.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded GET input **artist** was set to **1AcuStart908144'"539217AcuEnd**

```
GET /listproducts.php?artist=1AcuStart908144'"539217AcuEnd HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/listproducts.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded GET input **cat** was set to **1AcuStart068184'"777805AcuEnd**

```
GET /listproducts.php?cat=1AcuStart068184'"777805AcuEnd HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/Mod_Rewrite_Shop/BuyProduct-1/	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	

```
GET /Mod_Rewrite_Shop/BuyProduct-1/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/Mod_Rewrite_Shop/BuyProduct-2/	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	

```
GET /Mod_Rewrite_Shop/BuyProduct-2/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/Mod_Rewrite_Shop/BuyProduct-3/	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	

```
GET /Mod_Rewrite_Shop/BuyProduct-3/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/Mod_Rewrite_Shop/Details/color-printer/3/	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	

```
GET /Mod_Rewrite_Shop/Details/color-printer/3/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/	
Alert group	**SQL Injection**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	Error message found: `Warning: mysql_fetch_array() expects parameter 1 to be resource, boo`

```
GET /Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/?id=1'"1000 HTTP/1.1

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	

```
GET /Mod_Rewrite_Shop/Details/web-camera-a4tech/2/?id=1ACUSTART'"ACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

User-Agent: 1'"2000

referer: 1'"3000

client-ip: 1'"4000

x-forwarded-for: 1'"5000

accept-language: 1'"6000

via: 1'"7000

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/product.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded GET input **pic** was set to **1AcuStart524939'"572254AcuEnd**

```
GET /product.php?pic=1AcuStart524939'"572254AcuEnd HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/search.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **searchFor** was set to **1AcuStart493480'"347966AcuEnd**

```
POST /search.php?test=query HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 49

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



goButton=&searchFor=1AcuStart493480'"347966AcuEnd
```

/search.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded GET input **test** was set to **1AcuStart091814'"065525AcuEnd**

```
POST /search.php?test=1AcuStart091814'"065525AcuEnd HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 23

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



goButton=&searchFor=the
```

/secured/newuser.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **uuname** was set to **1AcuStart935086"'384793AcuEnd**

```
POST /secured/newuser.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 196

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww
6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-
0606&urname=pHqghUme&uuname=1AcuStart935086'"384793AcuEnd
```

/userinfo.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **pass** was set to **1AcuStart196449'"592850AcuEnd**

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 49

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



pass=1AcuStart196449'"592850AcuEnd&uname=pHqghUme
```

/userinfo.php	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **uname** was set to **1AcuStart158588"'461313AcuEnd**

```
POST /userinfo.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 57

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



pass=u]H[ww6KrA9F.x-F&uname=1AcuStart158588'"461313AcuEnd
```

/index.bak	
Alert group	**[Possible] Backup Source Code Detected**
Severity	High
Description	A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
Recommendations	Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.
Alert variants	

Details	This file was found using the pattern **${fileName}.bak**. Original filename: **index.php** Pattern found:

```
<?PHP require_once("database_connect.php"); ?>
<!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.
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>Home of WASP Art</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")&&(pars
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresiz
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_p
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
  <h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vul
  <div id="globalNav">
    <a href="index.php">home</a> | <a href="categories.php">categori
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="ca
        <a href="guestbook.php">guestbook</a>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        <h2 id="pageName">welcome to our page</h2>
          <div class="story">
                <h3>Test site for WASP.</h3>
          </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
          <li><a href="userinfo.php">Your profile</a></li>
          <li><a href="guestbook.php">Our guestbook</a></li>
          <?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../l
```

```
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
          <li><a href="http://www.eclectasy.com/Fractal-Explorer/ind
    </ul>
  </div>
  <div id="advert">
    <p><img src="images/add.jpg" alt="" width="107" height="66"></p>
  </div>
</div>

<!--end navbar -->
<div id="siteInfo">  <a href="http://www.acunetix.com">About Us</a>
  Map</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mail
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></html>
```

```
GET /index.bak HTTP/1.1

Range: bytes=0-99999

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/index.zip	
Alert group	**[Possible] Backup Source Code Detected**
Severity	High
Description	A possible backup file was found on your web-server. These files are usually created by developers to backup their work.
Recommendations	Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.
Alert variants	
Details	This file was found using the pattern **${fileName}.zip**. Original filename: **index.php**

```
GET /index.zip HTTP/1.1

Range: bytes=0-99999

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Cross-site Scripting**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URI was set to **1<ScRiPt>0Klb(9196)</ScRiPt>** The input is reflected inside a text element.

```
GET /404.php?1<ScRiPt>0Klb(9196)</ScRiPt> HTTP/1.1

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/AJAX/showxml.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page

Alert variants	
Details	Cookie input **mycookie** was set to **3'"()&%<zzz><ScRiPt >rTtR(9467)</ScRiPt>**

```
POST /AJAX/showxml.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: https://www.google.com/search?hl=en&q=testing

Cookie: mycookie=3'"()&%<zzz><ScRiPt%20>rTtR(9467)</ScRiPt>

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Content-Length: 0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/comment.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **name** was set to **<your name here>'"()&%<zzz><ScRiPt >Sjn1(9187)</ScRiPt>**

```
POST /comment.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 132

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



Submit=Submit&comment=555&name=<your%20name%20here>'"()%26%25<zzz><ScRiPt%20>Sjn1(9187)
</ScRiPt>&phpaction=echo%20%24_POST[comment];
```

/guestbook.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **name** was set to **anonymous user'"()&%<zzz><ScRiPt >kWLT(9823)</ScRiPt>**

```
POST /guestbook.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 96

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



name=anonymous%20user'"()%26%25<zzz><ScRiPt%20>kWLT(9823)
</ScRiPt>&submit=add%20message&text=555
```

/guestbook.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **text** was set to **555'"()&%<zzz><ScRiPt >kWLT(9788)</ScRiPt>**

```
POST /guestbook.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 96

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



name=anonymous%20user&submit=add%20message&text=555'"()%26%25<zzz><ScRiPt%20>kWLT(9788)
</ScRiPt>
```

/hpp/	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded GET input **pp** was set to **12'"()&%<zzz><ScRiPt >DxjJ(9637)</ScRiPt>**

```
GET /hpp/?pp=12'"()%26%25<zzz><ScRiPt%20>DxjJ(9637)</ScRiPt> HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/hpp/params.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded GET input **p** was set to **1'"()&%<zzz><ScRiPt >G8ia(9756)</ScRiPt>**

```
GET /hpp/params.php?p=1'"()%26%25<zzz><ScRiPt%20>G8ia(9756)</ScRiPt> HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/hpp/params.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded GET input **pp** was set to **12'"()&%<zzz><ScRiPt >gCAE(9399)</ScRiPt>**

```
GET /hpp/params.php?p=valid&pp=12'"()%26%25<zzz><ScRiPt%20>gCAE(9399)</ScRiPt> HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/listproducts.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded GET input **artist** was set to **1'"()&%<zzz><ScRiPt >VePC(9317)</ScRiPt>**

```
GET /listproducts.php?artist=1'"()%26%25<zzz><ScRiPt%20>VePC(9317)</ScRiPt> HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/listproducts.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded GET input **cat** was set to **1'"()&%<zzz><ScRiPt >Fq4l(9504)</ScRiPt>**

```
GET /listproducts.php?cat=1'"()%26%25<zzz><ScRiPt%20>Fq4l(9504)</ScRiPt> HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/search.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **searchFor** was set to **the'"()&%<zzz><ScRiPt >2v4d(9919) </ScRiPt>**

```
POST /search.php?test=query HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 68

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



goButton=&searchFor=the'"()%26%25<zzz><ScRiPt%20>2v4d(9919)</ScRiPt>
```

/secured/newuser.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **uaddress** was set to **555'"()&%<zzz><ScRiPt >g9ZY(9913) </ScRiPt>**

```
POST /secured/newuser.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 220

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



signup=signup&uaddress=555'"()%26%25<zzz><ScRiPt%20>g9ZY(9913)
</ScRiPt>&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww6KrA9F.x-
F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606&urname=pHqghUme&uuname=pHqghUme
```

/secured/newuser.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **uemail** was set to **'"()&%<zzz><ScRiPt >g9ZY(9005)</ScRiPt>**

```
POST /secured/newuser.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 199

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



signup=signup&uaddress=555&ucc=4111111111111111&uemail='"()%26%25<zzz>
<ScRiPt%20>g9ZY(9005)</ScRiPt>&upass=u]H[ww6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-
666-0606&urname=pHqghUme&uuname=pHqghUme
```

/secured/newuser.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **uphone** was set to **555-666-0606'"()&%<zzz><ScRiPt >g9ZY(9159)</ScRiPt>**

```
POST /secured/newuser.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 220

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww
6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606'"()%26%25<zzz>
<ScRiPt%20>g9ZY(9159)</ScRiPt>&urname=pHqghUme&uuname=pHqghUme
```

/secured/newuser.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **urname** was set to **pHqghUme'"()&%<zzz><ScRiPt >g9ZY(9491)</ScRiPt>**

```
POST /secured/newuser.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 220

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww
6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606&urname=pHqghUme'"()%26%25<zzz>
<ScRiPt%20>g9ZY(9491)</ScRiPt>&uuname=pHqghUme
```

/secured/newuser.php	
Alert group	**Cross-site Scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **uuname** was set to **pHqghUme'"()&%<zzz><ScRiPt >g9ZY(9132)</ScRiPt>**

```
POST /secured/newuser.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

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

Content-Length: 220

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



signup=signup&uaddress=555&ucc=4111111111111111&uemail=testing%40example.com&upass=u]H[ww
6KrA9F.x-F&upass2=u]H[ww6KrA9F.x-F&uphone=555-666-0606&urname=pHqghUme&uuname=pHqghUme'"
()%26%25<zzz><ScRiPt%20>g9ZY(9132)</ScRiPt>
```

/listproducts.php	
Alert group	**Cross-site Scripting (DOM based)**
Severity	High
Description	This script is possibly vulnerable to Cross Site Scripting (XSS) attacks. Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser. While a traditional cross-site scripting vulnerability occurs on the server-side code, document object model based cross-site scripting is a type of vulnerability which affects the script code in the client's browser.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	

Details	*Source:* `window.location` *Execution Sink:* `set HTML code` *Location:* `http://testphp.vulnweb.com/listproducts.php?artist=javascript%3AdomxssExecutionSink%281%2C%22%27%5C%22%3E%3Cxsstag%3E%28%29locxss%22%29&cat=javascript%3AdomxssExecutionSink%281%2C%22%27%5C%22%3E%3Cxsstag%3E%28%29locxss%22%29&pic=javascript%3AdomxssExecutionSink%281%2C%22%27%5C%22%3E%3Cxsstag%3E%28%29locxss%22%29&wvstest=javascript%3AdomxssExecutionSink%281%2C%22%27%5C%22%3E%3Cxsstag%3E%28%29locxss%22%29#javascript:domxssExecutionSink(1,"'\"><xsstag>()hashxss")` *HTML code set:* `yntax to use near ':domxssExecutionSink(1,"'/"><xsstag>()locxss")' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74 </xsstag></div>`

/showimage.php	
Alert group	**Directory traversal (verified)**
Severity	High
Description	This script is possibly vulnerable to directory traversal attacks. Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	URL encoded GET input **file** was set to **1884428/../../xxx\..\..\003250**

```
GET /showimage.php?file=1884428/../../xxx%5C..%5C..%5C003250 HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/showimage.php	
Alert group	**Local File Inclusion**
Severity	High

Description	This script is possibly vulnerable to file inclusion attacks. It seems that this script includes a file which name is determined using user-supplied data. This data is not properly validated before being passed to the include function.
Recommendations	Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list. For PHP, the option **allow_url_fopen** would normally allow a programmer to open, include or otherwise use a remote file using a URL rather than a local file path. It is recommended to disable this option from php.ini.
Alert variants	

Details	URL encoded GET input **file** was set to **showimage.php**
	
	Pattern found:
	
	`<?php`
	`// header("Content-Length: 1" /*. filesize($name)*/);`
	`if( isset($_GET["file"]) && !isset($_GET["size"]) ){`
	`// open the file in a binary mode`
	`header("Content-Type: image/jpeg");`
	`$name = $_GET["file"];`
	`// restrict urls`
	`if (filter_var($name, FILTER_VALIDATE_URL)) {`
	`exit();`
	`}`
	`$fp = fopen($name, 'rb');`
	`// send the right headers`
	`header("Content-Type: image/jpeg");`
	`// dump the picture and stop the script`
	`...`

```
GET /showimage.php?file=showimage.php HTTP/1.1

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/admin/create.sql	
Alert group	**Possible database backup**
Severity	High
Description	Manual confirmation is required for this alert. One or more possible database backups were identified. A database backup contains a record of the table structure and/or the data from a database and is usually in the form of a list of SQL statements. A database backup is most often used for backing up a database so that its contents can be restored in the event of data loss. This information is highly sensitive and should never be found on a production system.
Recommendations	Sensitive files such as database backups should never be stored in a directory that is accessible to the web server. As a workaround, you could restrict access to these file(s).
Alert variants	
Details	Pages with possible database backups: •

```
GET /admin/create.sql HTTP/1.1

Range: bytes=0-99999

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/vendor/installed.json	
Alert group	**Vulnerable package dependencies [high]**
Severity	High

Description	One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.
Recommendations	It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.
Alert variants	

Details	List of vulnerable **composer** packages: **Package:** phpmailer/phpmailer **Version:** 6.1.8.0 **CVE:** CVE-2021-34551 **Title:** Unrestricted Upload of File with Dangerous Type **Description:** PHPMailer before 6.5.0 on Windows allows remote code execution if lang_path is untrusted data and has a UNC pathname. **CVSS V2:** AV:N/AC:H/Au:N/C:P/I:P/A:P **CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H **CWE:** CWE-434 **References:** • https://github.com/PHPMailer/PHPMailer/blob/master/SECURITY.md • https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/FJYSOFCUBS67J3TKR74SD3C454N7VTYM/ • https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3YRMWGA4VTMXFB22KICMB7YMFZNFV3EJ/ **Package:** phpmailer/phpmailer **Version:** 6.1.8.0 **CVE:** CVE-2021-3603 **Title:** Inclusion of Functionality from Untrusted Control Sphere **Description:** PHPMailer 6.4.1 and earlier contain a vulnerability that can result in untrusted code being called (if such code is injected into the host project's scope by other means). If the $patternselect parameter to validateAddress() is set to 'php' (the default, defined by PHPMailer::$validator), and the global namespace contains a function called php, it will be called in preference to the built-in validator of the same name. Mitigated in PHPMailer 6.5.0 by denying the use of simple strings as validator function names. **CVSS V2:** AV:N/AC:M/Au:N/C:P/I:P/A:P **CVSS V3:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H **CWE:** CWE-829 **References:** • https://github.com/PHPMailer/PHPMailer/commit/45f3c18dc6a2de1cb1bf49b9b249a9ee36a5f7f3 • https://www.huntr.dev/bounties/1-PHPMailer/PHPMailer/ • https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/FJYSOFCUBS67J3TKR74SD3C454N7VTYM/ • https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3YRMWGA4VTMXFB22KICMB7YMFZNFV3EJ/ **Package:** phpmailer/phpmailer **Version:** 6.1.8.0 **CVE:** CVE-2020-36326 **Title:** Deserialization of Untrusted Data **Description:** PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation. **CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P **CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **CWE:** CWE-502 **References:**

- https://github.com/PHPMailer/PHPMailer/commit/e2e07a355ee8ff36aba21d0242c5950c56e4c6f9
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/KPU66INRFY5BQ3ESVPRUXJR4DXQAFJVT/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/3B5WDPGUFNPG4NAZ6G4BZX43BKLAVA5B/

Package: phpunit/phpunit
Version: 5.6.2.0
CVE: CVE-2017-9841
Title: Improper Control of Generation of Code ('Code Injection')
Description: Util/PHP/eval-stdin.php in PHPUnit before 4.8.28 and 5.x before 5.6.3 allows remote attackers to execute arbitrary PHP code via HTTP POST data beginning with a "<? php " substring, as demonstrated by an attack on a site with an exposed /vendor folder, i.e., external access to the /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php URI.
CVSS V2: AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-94
References:
- https://github.com/sebastianbergmann/phpunit/pull/1956
- https://github.com/sebastianbergmann/phpunit/commit/284a69fb88a2d0845d23f42974a583d8f59bf5a5
- http://www.securityfocus.com/bid/101798
- http://www.securitytracker.com/id/1039812
- https://security.gentoo.org/glsa/201711-15
- http://web.archive.org/web/20170701212357/http://phpunit.vulnbusters.com/
- https://www.oracle.com/security-alerts/cpuoct2021.html

Package: smarty/smarty
Version: 4.0.0.0
CVE: CVE-2021-21408
Title: Improper Input Validation
Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.43 and 4.0.3, template authors could run restricted static php methods. Users should upgrade to version 3.1.43 or 4.0.3 to receive a patch.
CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-20
References:
- https://github.com/smarty-php/smarty/commit/19ae410bf56007a5ef24441cdc6414619cfaf664
- https://github.com/smarty-php/smarty/releases/tag/v3.1.43
- https://github.com/smarty-php/smarty/security/advisories/GHSA-4h9c-v5vg-5m6m
- https://github.com/smarty-php/smarty/releases/tag/v4.0.3
- https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html
- https://www.debian.org/security/2022/dsa-5151
- https://security.gentoo.org/glsa/202209-09
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/

Package: smarty/smarty
Version: 4.0.0.0
CVE: CVE-2021-29454
Title: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.42 and 4.0.2, template authors could run arbitrary PHP code by crafting a malicious math string. If a math string was passed through as user provided data to the math function, external users could run arbitrary PHP code by crafting a malicious math string. Users should upgrade to version 3.1.42 or 4.0.2 to receive a patch.
CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-74
References:
- https://github.com/smarty-php/smarty/commit/215d81a9fa3cd63d82fb3ab56ecaf97cf1e7db71
- https://github.com/smarty-php/smarty/security/advisories/GHSA-29gp-2c3m-3j6m
- https://packagist.org/packages/smarty/smarty
- https://github.com/smarty-php/smarty/releases/tag/v3.1.42
- https://www.smarty.net/docs/en/language.function.math.tpl
- https://github.com/smarty-php/smarty/releases/tag/v4.0.2
- https://lists.debian.org/debian-lts-announce/2022/05/msg00005.html
- https://www.debian.org/security/2022/dsa-5151
- https://security.gentoo.org/glsa/202209-09
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/

Package: smarty/smarty
Version: 4.0.0.0
CVE: CVE-2022-29221
Title: Improper Control of Generation of Code ('Code Injection')
Description: Smarty is a template engine for PHP, facilitating the separation of presentation (HTML/CSS) from application logic. Prior to versions 3.1.45 and 4.1.1, template authors could inject php code by choosing a malicious {block} name or {include} file name. Sites that cannot fully trust template authors should upgrade to versions 3.1.45 or 4.1.1 to receive a patch for this issue. There are currently no known workarounds.
CVSS V2: AV:N/AC:L/Au:S/C:P/I:P/A:P
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-94
References:
- https://github.com/smarty-php/smarty/releases/tag/v3.1.45
- https://github.com/smarty-php/smarty/security/advisories/GHSA-634x-pc3q-cf4c
- https://github.com/smarty-php/smarty/commit/64ad6442ca1da31cefdab5c9874262b702cccddd
- https://github.com/smarty-php/smarty/releases/tag/v4.1.1
- https://www.debian.org/security/2022/dsa-5151
- https://lists.debian.org/debian-lts-announce/2022/05/msg00044.html
- https://security.gentoo.org/glsa/202209-09
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/L777JIBIWJV34HS7LXPIDWASG7TT4LNI/
- https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/BRAJVDRGCIY5UZ2PQHKDTT7RMKG6WJQQ/

Package: verot/class.upload.php

	Version: 2.0.1.0 **CVE:** CVE-2019-19576 **Title:** Unrestricted Upload of File with Dangerous Type **Description:** class.upload.php in verot.net class.upload before 1.0.3 and 2.x before 2.0.4, as used in the K2 extension for Joomla! and other products, omits .phar from the set of dangerous file extensions. **CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P **CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **CWE:** CWE-434 **References:** • https://github.com/verot/class.upload.php/compare/1.0.2...1.0.3 • https://github.com/getk2/k2/commit/d1344706c4b74c2ae7659b286b5a066117155124 • https://www.verot.net/php_class_upload.htm • https://github.com/verot/class.upload.php/commit/db1b4fe50c1754696970d8b437f07e7b94a7ebf2 • https://github.com/verot/class.upload.php/compare/2.0.3...2.0.4 • https://github.com/verot/class.upload.php/commit/5a7505ddec956fdc9e9c071ae5089865559174f1 • https://www.verot.net • https://github.com/jra89/CVE-2019-19576 • http://packetstormsecurity.com/files/155577/Verot-2.0.3-Remote-Code-Execution.html • https://medium.com/%40jra8908/cve-2019-19576-e9da712b779 **Package:** verot/class.upload.php **Version:** 2.0.1.0 **CVE:** CVE-2019-19634 **Title:** Unrestricted Upload of File with Dangerous Type **Description:** class.upload.php in verot.net class.upload through 1.0.3 and 2.x through 2.0.4, as used in the K2 extension for Joomla! and other products, omits .pht from the set of dangerous file extensions, a similar issue to CVE-2019-19576. **CVSS V2:** AV:N/AC:L/Au:N/C:P/I:P/A:P **CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **CWE:** CWE-434 **References:** • https://github.com/jra89/CVE-2019-19634 • https://github.com/verot/class.upload.php/blob/2.0.4/src/class.upload.php#L3068 • https://medium.com/%40jra8908/cve-2019-19634-arbitrary-file-upload-in-class-upload-php-ccaf9e13875e

Web Server	
Alert group	**Basic authentication over HTTP (verified)**
Severity	Medium
Description	In the context of an HTTP transaction, basic access authentication is a method for an HTTP user agent to provide a user name and password when making a request. One or more directories are protected using Basic Authentication over an HTTP connection. With Basic Authentication the user credentials are sent as cleartext and because HTTPS is not used, they are vulnerable to packet sniffing.
Recommendations	Use Basic Authentication over an HTTPS connection.
Alert variants	

Details	Pages with basic authentication over HTTP: • http://testphp.vulnweb.com/clearguestbook.php

```
GET /clearguestbook.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Directory listings (verified)**
Severity	Medium
Description	Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.
Recommendations	You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.
Alert variants	
Details	Folders with directory listing enabled: • http://testphp.vulnweb.com/wvstests/ • http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/ • http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/ • http://testphp.vulnweb.com/.idea/ • http://testphp.vulnweb.com/.idea/scopes/ • http://testphp.vulnweb.com/Flash/ • http://testphp.vulnweb.com/CVS/ • http://testphp.vulnweb.com/Connections/ • http://testphp.vulnweb.com/Templates/ • http://testphp.vulnweb.com/_mmServerScripts/ • http://testphp.vulnweb.com/admin/ • http://testphp.vulnweb.com/pictures/ • http://testphp.vulnweb.com/vendor/ • http://testphp.vulnweb.com/images/ • http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/

```
GET /wvstests/ HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/redir.php	
Alert group	**HTTP Header Injection (verified)**
Severity	Medium
Description	This script is possibly vulnerable to CRLF injection attacks. HTTP headers have the structure "Key: Value", where each line is separated by the CRLF combination. If the user input is injected into the value section without properly escaping/removing CRLF characters it is possible to alter the HTTP headers structure. HTTP Response Splitting is a new application attack technique which enables various new attacks such as web cache poisoning, cross user defacement, hijacking pages with sensitive user information and cross-site scripting (XSS). The attacker sends a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response.
Recommendations	You need to restrict CR(0x13) and LF(0x10) from the user input or properly encode the output in order to prevent the injection of custom HTTP headers.
Alert variants	
Details	URL encoded GET input **r** was set to **ACUSTART ACUEND**

```
GET /redir.php?r=ACUSTART%0D%0AACUEND HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/hpp/	
Alert group	**HTTP parameter pollution**
Severity	Medium
Description	This script is possibly vulnerable to HTTP Parameter Pollution attacks. HPP attacks consist of injecting encoded query string delimiters into other existing parameters. If the web application does not properly sanitize the user input, a malicious user can compromise the logic of the application to perform either clientside or server-side attacks.
Recommendations	The application should properly sanitize user input (URL encode) to protect against this vulnerability.
Alert variants	
Details	URL encoded GET input **pp** was set to **12&n916132=v980262** Parameter precedence: **last occurrence** Affected link: **params.php?p=valid&pp=12&n916132=v980262** Affected parameter: **p=valid**

```
GET /hpp/?pp=12%26n916132=v980262 HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/crossdomain.xml	
Alert group	**Insecure crossdomain.xml policy**
Severity	Medium

Description	The browser security model normally prevents web content from one domain from accessing data from another domain. This is commonly known as the "same origin policy". URL policy files grant cross-domain permissions for reading data. They permit operations that are not permitted by default. The URL policy file is located, by default, in the root directory of the target server, with the name crossdomain.xml (for example, at www.example.com/crossdomain.xml).
	
	When a domain is specified in crossdomain.xml file, the site declares that it is willing to allow the operators of any servers in that domain to obtain any document on the server where the policy file resides. The crossdomain.xml file deployed on this website opens the server to all domains (use of a single asterisk "*" as a pure wildcard is supported) like so:
	
	`<cross-domain-policy>`
	`<allow-access-from domain="*" />`
	`<allow-http-request-headers-from domain="*" />`
	`</cross-domain-policy>`
	
	This practice is suitable for public servers, but should not be used for sites located behind a firewall because it could permit access to protected areas. It should not be used for sites that require authentication in the form of passwords or cookies. Sites that use the common practice of authentication based on cookies to access private or user-specific data should be especially careful when using cross-domain policy files.

Recommendations	Carefully evaluate which sites will be allowed to make cross-domain calls. Consider network topology and any authentication mechanisms that will be affected by the configuration or implementation of the cross-domain policy.
Alert variants	
Details	The following issues were detected: • **/crossdomain.xml:** Element "allow-access-from" has attribute "domain" set to "*" • **/crossdomain.xml:** Element "allow-access-from" has attribute "secure" set to "false"

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: filelist;aspectalerts;packages

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Insecure HTTP Usage**
Severity	Medium

Description	It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.
Recommendations	It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information
Alert variants	
Details	

```
GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**JetBrains .idea project directory**
Severity	Medium
Description	The .idea directory contains a set of configuration files (.xml) for your project. These configuration files contain information core to the project itself, such as names and locations of its component modules, compiler settings, etc. If you've defined a data source the file dataSources.ids contains information for connecting to the database and credentials. The workspace.xml file stores personal settings such as placement and positions of your windows, your VCS and History settings, and other data pertaining to the development environment. It also contains a list of changed files and other sensitive information. These files should not be present on a production system.

Recommendations	Remove these files from production systems or restrict access to the .idea directory. To deny access to all the .idea folders you need to add the following lines in the appropriate context (either global config, or vhost/directory, or from .htaccess):
	
	`<Directory ~ "\.idea">`
	`Order allow,deny`
	`Deny from all`
	`</Directory>`

Alert variants	
Details	workspace.xml project file found at : /.idea/workspace.xml Pattern found: `<project version="4">`

```
GET /.idea/workspace.xml HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/redir.php	
Alert group	**Open Redirection**
Severity	Medium
Description	This script is possibly vulnerable to URL redirection attacks. URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.
Recommendations	Your script should properly sanitize user input.
Alert variants	
Details	URL encoded GET input **r** was set to **http://xfs.bxss.me?vulnweb.com**

```
GET /redir.php?r=http://xfs.bxss.me%3Fvulnweb.com HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Password transmitted over HTTP**
Severity	Medium
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
Recommendations	Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).
Alert variants	

Details	Forms with credentials sent in clear text:
	• http://testphp.vulnweb.com/login.php
	`Form name: loginform`
	`Form action: userinfo.php`
	`Form method: POST`
	`Password input: pass`
	• http://testphp.vulnweb.com/signup.php
	`Form name: form1`
	`Form action: /secured/newuser.php`
	`Form method: POST`
	`Password input: upass`

```
GET /login.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**PHP errors enabled (verified)**
Severity	Medium
Description	Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. Acunetix AcuSensor found that the PHP `display_errors` directive is enabled.
Recommendations	Adjust `php.ini` or `.htaccess` (`mod_php` with Apache HTTP Server) to disable `display_errors` (refer to 'Detailed information' section).
Alert variants	
Details	Current setting is : **display_errors =** `1`

/secured/phpinfo.php	
Alert group	**PHP session.use_only_cookies Is Disabled (verified)**

Severity	Medium
Description	When use_only_cookies is disabled, PHP will pass the session ID via the URL. This makes the application more vulnerable to session hijacking attacks. Session hijacking is basically a form of identity theft wherein a hacker impersonates a legitimate user by stealing his session ID. When the session token is transmitted in a cookie, and the request is made on a secure channel (that is, it uses SSL), the token is secure.
Recommendations	You can enabled session.use_only_cookies from php.ini or .htaccess. **php.ini** session.use_only_cookies = 'on' **.htaccess** php_flag session.use_only_cookies on
Alert variants	
Details	This vulnerability was detected using the information from phpinfo() page. session.use_only_cookies: On

```
GET /secured/phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**PHPinfo pages**
Severity	Medium
Description	One or more **phpinfo()** pages were found. The **phpinfo()** function exposes a large amount of information about the PHP configuration and that of its environment. This includes information about PHP compilation options and extensions, the PHP version, server information, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.
Recommendations	Remove either the call to the phpinfo() function from the file(s), or the file(s) itself.
Alert variants	
Details	PHPinfo pages found: • /secured/phpinfo.php **<title>phpinfo()</title>**

```
GET /secured/phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**SSL/TLS Not Implemented (verified)**
Severity	Medium
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/vendor/installed.json	
Alert group	**Vulnerable package dependencies [medium]**
Severity	Medium

Description	One or more packages that are used in your web application are affected by known vulnerabilities. Please consult the details section for more information about each affected package.
Recommendations	It's recommended to update the vulnerable packages to the latest version (if a fix exists). If a fix does not exist, you may want to suggest changes that address the vulnerability to the package maintainer or remove the package from your dependency tree.
Alert variants	

Details	List of vulnerable **composer** packages: **Package:** smarty/smarty **Version:** 4.0.0.0 **CVE:** CVE-2018-25047 **Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **Description:** In Smarty before 3.1.47 and 4.x before 4.2.1, libs/plugins/function.mailto.php allows XSS. A web page that uses smarty_function_mailto, and that could be parameterized using GET or POST input parameters, could allow injection of JavaScript code by a user. **CVSS V2:** **CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N **CWE:** CWE-79 **References:** • https://github.com/smarty-php/smarty/releases/tag/v4.2.1 • https://github.com/smarty-php/smarty/releases/tag/v3.1.47 • https://bugs.gentoo.org/870100 • https://github.com/smarty-php/smarty/issues/454 • https://security.gentoo.org/glsa/202209-09 • https://lists.debian.org/debian-lts-announce/2023/01/msg00002.html **Package:** smarty/smarty **Version:** 4.0.0.0 **CVE:** CVE-2023-28447 **Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **Description:** Smarty is a template engine for PHP. In affected versions smarty did not properly escape javascript code. An attacker could exploit this vulnerability to execute arbitrary JavaScript code in the context of the user's browser session. This may lead to unauthorized access to sensitive user data, manipulation of the web application's behavior, or unauthorized actions performed on behalf of the user. Users are advised to upgrade to either version 3.1.48 or to 4.3.1 to resolve this issue. There are no known workarounds for this vulnerability. **CVSS V2:** **CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N **CWE:** CWE-79 **References:** • https://github.com/smarty-php/smarty/security/advisories/GHSA-7j98-h7fp-4vwj • https://github.com/smarty-php/smarty/commit/685662466f653597428966d75a661073104d713d • https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/HSAUM3YHWHO4UCJXRGRLQGPJAO3MFOZZ/ • https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/JBB35GLYTL6JL6EOM6BOZNYP47JKNNHT/ • https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/P7O7SKTATM6GAP45S64QFXNLWIY5I7HP/ **Package:** tinymce/tinymce **Version:** 5.2.0.0 **CVE:** CVE-2019-1010091 **Title:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') **Description:** tinymce 4.7.11, 4.7.12 is affected by: CWE-79: Improper Neutralization of Input During Web Page Generation. The impact is: JavaScript code execution. The component is: Media element. The attack vector is: The victim must paste malicious content to media element's embed tab. **CVSS V2:** AV:N/AC:M/Au:N/C:N/I:P/A:N **CVSS V3:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N **CWE:** CWE-79 **References:**

- https://github.com/tinymce/tinymce/issues/4394

Package: tinymce/tinymce
Version: 5.2.0.0
CVE: CVE-2020-12648
Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Description: A cross-site scripting (XSS) vulnerability in TinyMCE 5.2.1 and earlier allows remote attackers to inject arbitrary web script when configured in classic editing mode.
CVSS V2: AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CWE: CWE-79
References:
- https://labs.bishopfox.com/advisories/tinymce-version-5.2.1

Package: tinymce/tinymce
Version: 5.2.0.0
CVE: CVE-2022-23494
Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Description: tinymce is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in the alert and confirm dialogs when these dialogs were provided with malicious HTML content. This can occur in plugins that use the alert or confirm dialogs, such as in the `image` plugin, which presents these dialogs when certain errors occur. The vulnerability allowed arbitrary JavaScript execution when an alert presented in the TinyMCE UI for the current user. This vulnerability has been patched in TinyMCE 5.10.7 and TinyMCE 6.3.1 by ensuring HTML sanitization was still performed after unwrapping invalid elements. Users are advised to upgrade to either 5.10.7 or 6.3.1. Users unable to upgrade may ensure the the `images_upload_handler` returns a valid value as per the images_upload_handler documentation.
CVSS V2:
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CWE: CWE-79
References:
- https://github.com/tinymce/tinymce/commit/6923d85eba6de3e08ebc9c5a387b5abdaa21150e
- https://www.tiny.cloud/docs/tinymce/6/file-image-upload/#images_upload_handler
- https://www.tiny.cloud/docs/release-notes/release-notes5107/#securityfixes
- https://github.com/tinymce/tinymce/commit/8bb2d2646d4e1a718fce61a775fa22e9d317b32d
- https://github.com/tinymce/tinymce/security/advisories/GHSA-gg8r-xjwq-4w92
- https://www.tiny.cloud/docs/tinymce/6/6.3-release-notes/#security-fixes

Package: tinymce/tinymce
Version: 5.2.0.0
CVE: CVE-2023-45818
Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Description: TinyMCE is an open source rich text editor. A mutation cross-site scripting (mXSS) vulnerability was discovered in TinyMCEâ□□s core undo and redo functionality. When a carefully-crafted HTML snippet passes the XSS sanitisation layer, it is manipulated as a string by internal trimming functions before being stored in the undo stack. If the HTML snippet is restored from the undo stack, the combination of the string manipulation and reparative parsing by either the browser's native [DOMParser API] (https://developer.mozilla.org/en-US/docs/Web/API/DOMParser) (TinyMCE 6) or the SaxParser API (TinyMCE 5) mutates the HTML maliciously, allowing an XSS payload to be executed. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring HTML is trimmed using node-level manipulation instead of string manipulation. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVSS V2:

CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CWE: CWE-79
References:
- https://github.com/tinymce/tinymce/security/advisories/GHSA-v65r-p3vv-jjfv
- https://tiny.cloud/docs/release-notes/release-notes5108/#securityfixes
- https://researchgate.net/publication/266654651_mXSS_attacks_Attacking_well-secured_web-applications_by_using_innerHTML_mutations
- https://tiny.cloud/docs/tinymce/6/6.7.1-release-notes/#security-fixes
- https://www.tiny.cloud/docs/api/tinymce.html/tinymce.html.saxparser/

Package: tinymce/tinymce
Version: 5.2.0.0
CVE: CVE-2023-45819
Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Description: TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCEâ□□s Notification Manager API. The vulnerability exploits TinyMCE's unfiltered notification system, which is used in error handling. The conditions for this exploit requires carefully crafted malicious content to have been inserted into the editor and a notification to have been triggered. When a notification was opened, the HTML within the text argument was displayed unfiltered in the notification. The vulnerability allowed arbitrary JavaScript execution when an notification presented in the TinyMCE UI for the current user. This issue could also be exploited by any integration which uses a TinyMCE notification to display unfiltered HTML content. This vulnerability has been patched in TinyMCE 5.10.8 and TinyMCE 6.7.1 by ensuring that the HTML displayed in the notification is sanitized, preventing the exploit. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVSS V2:
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CWE: CWE-79
References:
- https://github.com/tinymce/tinymce/security/advisories/GHSA-hgqx-r2hp-jr38

Package: tinymce/tinymce
Version: 5.2.0.0
CVE: CVE-2023-48219
Title: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Description: TinyMCE is an open source rich text editor. A mutation cross-site scripting (mXSS) vulnerability was discovered in TinyMCEâ□□s core undo/redo functionality and other APIs and plugins. Text nodes within specific parents are not escaped upon serialization according to the HTML standard. If such text nodes contain a special character reserved as an internal marker, they can be combined with other HTML patterns to form malicious snippets. These snippets pass the initial sanitisation layer when the content is parsed into the editor body, but can trigger XSS when the special internal marker is removed from the content and re-parsed. his vulnerability has been patched in TinyMCE versions 6.7.3 and 5.10.9. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVSS V2:
CVSS V3: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CWE: CWE-79
References:
- https://github.com/tinymce/tinymce/security/advisories/GHSA-v626-r774-j7f8
- https://tiny.cloud/docs/release-notes/release-notes5109/
- https://tiny.cloud/docs/tinymce/6/6.7.3-release-notes/

Web Server	
Alert group	**[Possible] Internal IP Address Disclosure**

Severity	Low
Description	One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks. The significance of this finding should be confirmed manually.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pages with internal IPs: • http://testphp.vulnweb.com/404.php **192.168.0.28** • http://testphp.vulnweb.com/secured/phpinfo.php **192.168.0.5** • http://testphp.vulnweb.com/pictures/ipaddresses.txt **192.168.0.26**

```
GET /404.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Cookies Not Marked as HttpOnly (verified)**
Severity	Low
Description	One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HttpOnly flag for these cookies.
Alert variants	

Details	Cookies without HttpOnly flag set: • http://testphp.vulnweb.com/logout.php `Set-Cookie: login=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT`

```
GET /logout.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Cookies with missing, inconsistent or contradictory properties (verified)**
Severity	Low
Description	At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.
Recommendations	Ensure that the cookies configuration complies with the applicable standards.
Alert variants	

Details	List of cookies with missing, inconsistent or contradictory properties:
	• http://testphp.vulnweb.com/logout.php
	Cookie was set with:
	`Set-Cookie: login=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT`
	This cookie has the following issues:
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`

```
GET /logout.php HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Possible sensitive files**
Severity	Low
Description	A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
Recommendations	Restrict access to this file or remove it from the website.
Alert variants	
Details	Possible sensitive files: • http://testphp.vulnweb.com/hpp/**test.php**

```
GET /hpp/test.php HTTP/1.1

Accept: osjvzbyf/jakv

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Possible username or password disclosure**
Severity	Low
Description	One or more credential pairs (username+password) were found. This information could be sensitive. This alert may be a false positive, manual confirmation is required.
Recommendations	Remove these file(s) from your website or change its permissions to remove access.
Alert variants	
Details	Pages containing credentials: • http://testphp.vulnweb.com/pictures/credentials.txt **username=test** **password=something**

```
GET /pictures/credentials.txt HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Programming Error Messages**
Severity	Low
Description	This alert requires manual confirmation Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. These messages may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page(s).
Recommendations	Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.
Alert variants	

Details	Application error messages: • http://testphp.vulnweb.com/search.php **Warning: mysql_connect(): Connection refused in /hj/var/www//search.php on line 2 ** • http://testphp.vulnweb.com/showimage.php **Warning: fopen(): Filename cannot be empty in /hj/var/www/showimage.php on line 13** • http://testphp.vulnweb.com/search.php **Warning: mysql_connect(): Connection refused in /hj/var/www/database_connect.php on line 2** • http://testphp.vulnweb.com/listproducts.php **You have an error in your SQL syntax** • http://testphp.vulnweb.com/bxss/adminPan3l/index.php **Warning: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in /hj/var/www//bxss/adminPan3l/index.php on line 2 ** • http://testphp.vulnweb.com/showimage.php **Warning: fopen(): Filename cannot be empty in /hj/var/www/showimage.php on line 31** • http://testphp.vulnweb.com/Connections/DB_Connection.php **Fatal error** • http://testphp.vulnweb.com/Connections/DB_Connection.php **Warning: mysql_pconnect(): Access denied for user 'root'@'localhost' in /hj/var/www//Connections/DB_Connection.php on line 9 ** • http://testphp.vulnweb.com/secured/database_connect.php **Warning: mysql_connect(): The server requested authentication method unknown to the client [caching_sha2_password] in /hj/var/www//secured/database_connect.php on line 2 ** • http://testphp.vulnweb.com/secured/newuser.php **You have an error in your SQL syntax** • http://testphp.vulnweb.com/database_connect.php **Warning: mysql_connect(): Connection refused in /hj/var/www//database_connect.php on line 2 ** • http://testphp.vulnweb.com/product.php **Warning: mysql_connect(): Connection refused in /hj/var/www//product.php on line 2 ** • http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php **Warning: mysql_connect(): Connection refused in /hj/var/www//Mod_Rewrite_Shop/details.php on line 2 ** • http://testphp.vulnweb.com/listproducts.php **Warning: mysql_connect(): Connection refused in /hj/var/www//listproducts.php on line 2 ** • http://testphp.vulnweb.com/bxss/cleanDatabase.php **Warning: mysql_connect(): No such file or directory in /hj/var/www//bxss/cleanDatabase.php on line 2 **

- http://testphp.vulnweb.com/artists.php
  **Warning: mysql_connect(): Connection refused in /hj/var/www//artists.php on line 2
**

- http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
  **Warning: Sablotron error on line 1: XML parser error 3: no element found in /usr/local/etc/httpd/htdocs2/destination-ce/destinationce/system/class/xsltTransform.class.php on line 70
**

- http://testphp.vulnweb.com/listproducts.php
  **Warning: mysql_fetch_array() expects parameter 1 to be resource, null given in /hj/var/www//listproducts.php on line 74
**

- http://testphp.vulnweb.com/bxss/vuln.php
  **Warning: mysql_connect(): Access denied for user 'bxss'@'localhost' (using password: YES) in /hj/var/www//bxss/vuln.php on line 2
**

- http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
  **Warning: mysql_connect(): Connection refused in /hj/var/www//Mod_Rewrite_Shop/details.php on line 2
**

- http://testphp.vulnweb.com/bxss/vuln.php
  **Warning: mysql_connect(): The server requested authentication method unknown to the client [caching_sha2_password] in /hj/var/www//bxss/vuln.php on line 2
**

```
POST /search.php?test=query HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

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

Content-Length: 23

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive



goButton=&searchFor=the
```

/secured/phpinfo.php	
Alert group	**PHP allow_url_fopen Is Enabled (verified)**
Severity	Low
Description	The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering. allow_url_fopen is enabled by default.
Recommendations	You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4). **php.ini** allow_url_fopen = 'off' **.htaccess** php_flag allow_url_fopen off
Alert variants	
Details	This vulnerability was detected using the information from phpinfo() page. allow_url_fopen: On

```
GET /secured/phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**PHP allow_url_fopen Is Enabled (verified)**
Severity	Low
Description	The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering. allow_url_fopen is enabled by default.
Recommendations	You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4). **php.ini** allow_url_fopen = 'off' **.htaccess** php_flag allow_url_fopen off
Alert variants	

Details	Current setting is : **allow_url_fopen =** `on`

/secured/phpinfo.php	
Alert group	**PHP display_errors Is Enabled (verified)**
Severity	Low
Description	Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. Acunetix found that the PHP `display_errors` directive is enabled.
Recommendations	Adjust `php.ini` or `.htaccess` (`mod_php` with Apache HTTP Server) to disable `display_errors` (refer to 'Detailed information' section).
Alert variants	
Details	This vulnerability was detected using the information from phpinfo() page. display_errors: On

```
GET /secured/phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/secured/phpinfo.php	
Alert group	**PHP open_basedir Is Not Configured (verified)**
Severity	Low
Description	The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.
Recommendations	You can set open_basedir from php.ini **php.ini** open_basedir = your_application_directory
Alert variants	
Details	This vulnerability was detected using the information from phpinfo() page. open_basedir: no value

```
GET /secured/phpinfo.php HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Version Disclosure (PHP)**
Severity	Low
Description	The web server is sending the X-Powered-By: response headers, revealing the PHP version.
Recommendations	Configure your web server to prevent information leakage from its HTTP response.
Alert variants	
Details	Version detected: **PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1**.

/Mod_Rewrite_Shop/	
Alert group	**.htaccess File Detected (verified)**
Severity	Informational
Description	This directory contains an **.htaccess** file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.
Recommendations	Restrict access to the .htaccess file by adjusting the web server configuration.
Alert variants	
Details	

```
GET /Mod_Rewrite_Shop/.htaccess HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	

Alert group	[Possible] Internal Path Disclosure (*nix)
Severity	Informational
Description	One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks. This alert may be a false positive, manual confirmation is required.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pages with paths being disclosed: • http://testphp.vulnweb.com/pictures/path-disclosure-unix.html **>/usr/local/etc/httpd/htdocs2/destination** • http://testphp.vulnweb.com/secured/phpinfo.php **:/usr/obj/usr/src/sys/GENERIC**

```
GET /pictures/path-disclosure-unix.html HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**[Possible] Internal Path Disclosure (Windows)**
Severity	Informational
Description	One or more fully qualified path names were been found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks. This alert may be a false positive, manual confirmation is required.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	

Details	Pages with paths being disclosed: • http://testphp.vulnweb.com/pictures/path-disclosure-win.html **C:\Inetpub\wwwroot\comparatii.php**

```
GET /pictures/path-disclosure-win.html HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

/pictures/WS_FTP.LOG	
Alert group	**[Possible] WS_FTP Log File Detected (verified)**
Severity	Informational
Description	WS_FTP is a popular FTP client. This application creates a log file named WS_FTP.LOG. This file contains sensitive data such as file source/destination and file name, date/time of upload etc.
Recommendations	Remove this file from your website or change its permissions to remove access.
Alert variants	
Details	Pattern found: `103.05.06 13:17`

```
GET /pictures/WS_FTP.LOG HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Content Security Policy (CSP) Not Implemented**
Severity	Informational

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.
	
	Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:
	
	`Content-Security-Policy:`
	`default-src 'self';`
	`script-src 'self' https://code.jquery.com;`
	
	It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	

Details	Paths without CSP header: • http://testphp.vulnweb.com/ • http://testphp.vulnweb.com/AJAX/index.php • http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php • http://testphp.vulnweb.com/artists.php • http://testphp.vulnweb.com/listproducts.php • http://testphp.vulnweb.com/bxss/adminPan3l/index.php • http://testphp.vulnweb.com/product.php • http://testphp.vulnweb.com/comment.php • http://testphp.vulnweb.com/Connections/DB_Connection.php • http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php • http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php • http://testphp.vulnweb.com/hpp/params.php • http://testphp.vulnweb.com/secured/database_connect.php • http://testphp.vulnweb.com/categories.php • http://testphp.vulnweb.com/disclaimer.php • http://testphp.vulnweb.com/guestbook.php • http://testphp.vulnweb.com/index.php • http://testphp.vulnweb.com/login.php • http://testphp.vulnweb.com/privacy.php • http://testphp.vulnweb.com/signup.php • http://testphp.vulnweb.com/images/

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Generic Email Address Disclosure**
Severity	Informational
Description	One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	

Details	Emails found: • http://testphp.vulnweb.com/ **wvs@acunetix.com** • http://testphp.vulnweb.com/search.php **wvs@acunetix.com** • http://testphp.vulnweb.com/artists.php **wvs@acunetix.com** • http://testphp.vulnweb.com/listproducts.php **wvs@acunetix.com** • http://testphp.vulnweb.com/product.php **wvs@acunetix.com** • http://testphp.vulnweb.com/cart.php **wvs@acunetix.com** • http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php **wvs@acunetix.com** • http://testphp.vulnweb.com/categories.php **wvs@acunetix.com** • http://testphp.vulnweb.com/disclaimer.php **wvs@acunetix.com** • http://testphp.vulnweb.com/guestbook.php **wvs@acunetix.com** • http://testphp.vulnweb.com/index.php **wvs@acunetix.com** • http://testphp.vulnweb.com/login.php **wvs@acunetix.com** • http://testphp.vulnweb.com/signup.php **wvs@acunetix.com** • http://testphp.vulnweb.com/404.php **wvs@acunetix.com** • http://testphp.vulnweb.com/logout.php **wvs@acunetix.com**

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: filelist;aspectalerts;packages

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Web Server	
Alert group	**Permissions-Policy header not implemented**

Severity	Informational
Description	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.
Recommendations	
Alert variants	
Details	Locations without Permissions-Policy header: • http://testphp.vulnweb.com/ • http://testphp.vulnweb.com/search.php • http://testphp.vulnweb.com/AJAX/index.php • http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php • http://testphp.vulnweb.com/AJAX/showxml.php • http://testphp.vulnweb.com/artists.php • http://testphp.vulnweb.com/listproducts.php • http://testphp.vulnweb.com/bxss/adminPan3l/index.php • http://testphp.vulnweb.com/product.php • http://testphp.vulnweb.com/comment.php • http://testphp.vulnweb.com/cart.php • http://testphp.vulnweb.com/Connections/DB_Connection.php • http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php • http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php • http://testphp.vulnweb.com/hpp/params.php • http://testphp.vulnweb.com/secured/database_connect.php • http://testphp.vulnweb.com/categories.php • http://testphp.vulnweb.com/disclaimer.php • http://testphp.vulnweb.com/guestbook.php • http://testphp.vulnweb.com/index.php • http://testphp.vulnweb.com/login.php

```
GET / HTTP/1.1

Acunetix-Aspect: enabled

Acunetix-Aspect-Password: 082119f75623eb7abd7bf357698ff66c

Acunetix-Aspect-ScanID: 13510882192354823921

Acunetix-Aspect-Queries: filelist;packages;aspectalerts;routes

Referer: http://testphp.vulnweb.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36

Host: testphp.vulnweb.com

Connection: Keep-alive
```

Scanned items (coverage report)

http://testphp.vulnweb.com/
http://testphp.vulnweb.com/.idea/
http://testphp.vulnweb.com/.idea/.name
http://testphp.vulnweb.com/.idea/acuart.iml
http://testphp.vulnweb.com/.idea/encodings.xml
http://testphp.vulnweb.com/.idea/misc.xml
http://testphp.vulnweb.com/.idea/modules.xml
http://testphp.vulnweb.com/.idea/scopes/
http://testphp.vulnweb.com/.idea/scopes/scope_settings.xml
http://testphp.vulnweb.com/.idea/vcs.xml
http://testphp.vulnweb.com/.idea/workspace.xml
http://testphp.vulnweb.com/_mmServerScripts/
http://testphp.vulnweb.com/_mmServerScripts/MMHTTPDB.php
http://testphp.vulnweb.com/_mmServerScripts/mysql.php
http://testphp.vulnweb.com/404.php
http://testphp.vulnweb.com/admin/
http://testphp.vulnweb.com/admin/create.sql
http://testphp.vulnweb.com/AJAX/
http://testphp.vulnweb.com/AJAX/artists.php
http://testphp.vulnweb.com/AJAX/categories.php
http://testphp.vulnweb.com/AJAX/htaccess.conf
http://testphp.vulnweb.com/AJAX/index.php
http://testphp.vulnweb.com/AJAX/infoartist.php
http://testphp.vulnweb.com/AJAX/infocateg.php
http://testphp.vulnweb.com/AJAX/infotitle.php
http://testphp.vulnweb.com/AJAX/showxml.php
http://testphp.vulnweb.com/AJAX/styles.css
http://testphp.vulnweb.com/AJAX/titles.php
http://testphp.vulnweb.com/artists.php
http://testphp.vulnweb.com/bxss/
http://testphp.vulnweb.com/bxss/adminPan3l/
http://testphp.vulnweb.com/bxss/adminPan3l/index.php
http://testphp.vulnweb.com/bxss/adminPan3l/style.css
http://testphp.vulnweb.com/bxss/cleanDatabase.php
http://testphp.vulnweb.com/bxss/database_connect.php
http://testphp.vulnweb.com/bxss/index.php
http://testphp.vulnweb.com/bxss/test.js
http://testphp.vulnweb.com/bxss/vuln.php
http://testphp.vulnweb.com/cart.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/clearguestbook.php
http://testphp.vulnweb.com/clientaccesspolicy.xml
http://testphp.vulnweb.com/comment.php
http://testphp.vulnweb.com/Connections/
http://testphp.vulnweb.com/Connections/DB_Connection.php
http://testphp.vulnweb.com/crossdomain.xml
http://testphp.vulnweb.com/CVS/
http://testphp.vulnweb.com/CVS/Entries
http://testphp.vulnweb.com/CVS/Entries.Log
http://testphp.vulnweb.com/CVS/Repository
http://testphp.vulnweb.com/CVS/Root
http://testphp.vulnweb.com/database_connect.php
http://testphp.vulnweb.com/disclaimer.php
http://testphp.vulnweb.com/Flash/
http://testphp.vulnweb.com/Flash/add.swf
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/hpp/
http://testphp.vulnweb.com/hpp/index.php
http://testphp.vulnweb.com/hpp/params.php

http://testphp.vulnweb.com/hpp/test.php
http://testphp.vulnweb.com/images/
http://testphp.vulnweb.com/index.bak
http://testphp.vulnweb.com/index.php
http://testphp.vulnweb.com/index.zip
http://testphp.vulnweb.com/listproducts.php
http://testphp.vulnweb.com/logout.php
http://testphp.vulnweb.com/login.php
http://testphp.vulnweb.com/medias/
http://testphp.vulnweb.com/medias/css/
http://testphp.vulnweb.com/medias/css/main.css
http://testphp.vulnweb.com/medias/img/
http://testphp.vulnweb.com/medias/js/
http://testphp.vulnweb.com/medias/js/common_functions.js
http://testphp.vulnweb.com/Mod_Rewrite_Shop/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/.htaccess
http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/
http://testphp.vulnweb.com/Mod_Rewrite_Shop/index.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
http://testphp.vulnweb.com/pictures/
http://testphp.vulnweb.com/pictures/1.jpg.tn
http://testphp.vulnweb.com/pictures/2.jpg.tn
http://testphp.vulnweb.com/pictures/3.jpg.tn
http://testphp.vulnweb.com/pictures/4.jpg.tn
http://testphp.vulnweb.com/pictures/5.jpg.tn
http://testphp.vulnweb.com/pictures/6.jpg.tn
http://testphp.vulnweb.com/pictures/7.jpg.tn
http://testphp.vulnweb.com/pictures/8.jpg.tn
http://testphp.vulnweb.com/pictures/credentials.txt
http://testphp.vulnweb.com/pictures/ipaddresses.txt
http://testphp.vulnweb.com/pictures/path-disclosure-unix.html
http://testphp.vulnweb.com/pictures/path-disclosure-win.html
http://testphp.vulnweb.com/pictures/wp-config.bak
http://testphp.vulnweb.com/pictures/WS_FTP.LOG
http://testphp.vulnweb.com/privacy.php
http://testphp.vulnweb.com/product.php
http://testphp.vulnweb.com/redir.php
http://testphp.vulnweb.com/search.php
http://testphp.vulnweb.com/secured/
http://testphp.vulnweb.com/secured/database_connect.php
http://testphp.vulnweb.com/secured/index.php
http://testphp.vulnweb.com/secured/newuser.php
http://testphp.vulnweb.com/secured/office.htm
http://testphp.vulnweb.com/secured/office_files/
http://testphp.vulnweb.com/secured/office_files/filelist.xml
http://testphp.vulnweb.com/secured/phpinfo.php

http://testphp.vulnweb.com/secured/style.css
http://testphp.vulnweb.com/sendcommand.php
http://testphp.vulnweb.com/showimage.php
http://testphp.vulnweb.com/signup.php
http://testphp.vulnweb.com/style.css
http://testphp.vulnweb.com/Templates/
http://testphp.vulnweb.com/Templates/main_dynamic_template.dwt.php
http://testphp.vulnweb.com/userinfo.php
http://testphp.vulnweb.com/vendor/
http://testphp.vulnweb.com/vendor/installed.json
http://testphp.vulnweb.com/wvstests/
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/
http://testphp.vulnweb.com/wvstests/pmwiki_2_1_19/scripts/version.php