

Vulnerability Report

Reported by: Gopi Kumar

Email: gimgopi21@gmail.com

Organization: DROP Organization

Position: Cyber Security Intern

Date: 19/01/2026

Vulnerability : Cross Site Scripting (XSS)

Severity Risk : High

Description

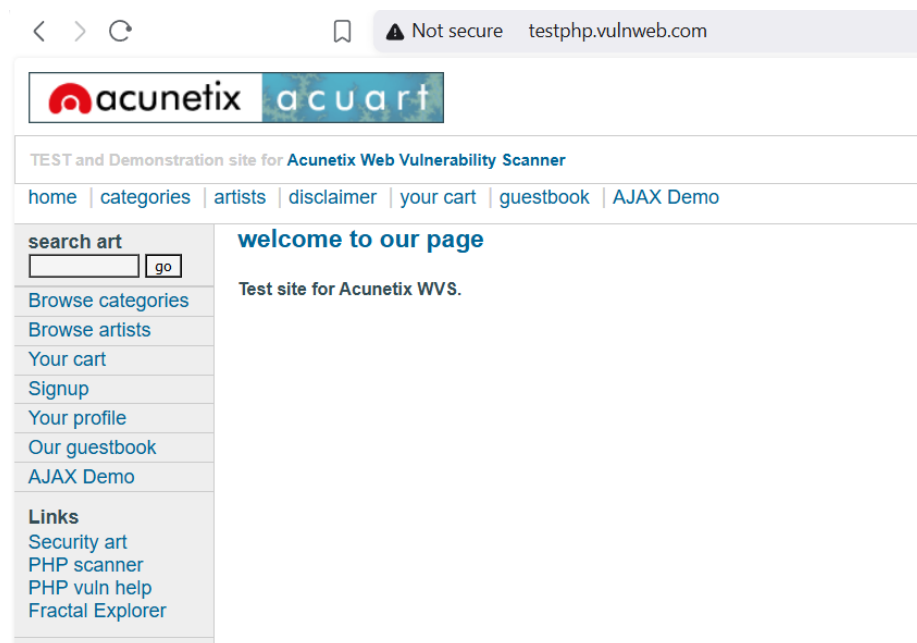
XSS (Cross-Site Scripting) is a web security vulnerability where an attacker injects **malicious JavaScript code** into a website. When other users visit the affected page, the script runs in their browser.

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

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

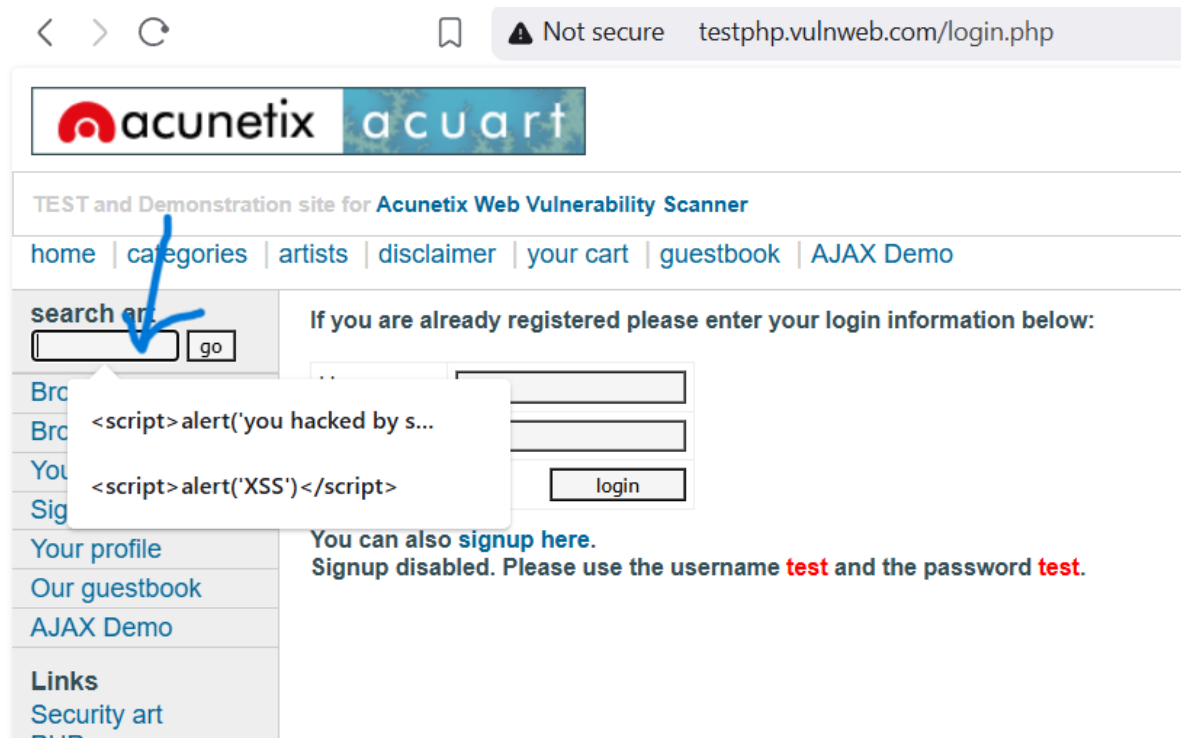
Proof Of Concept : (POC)

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

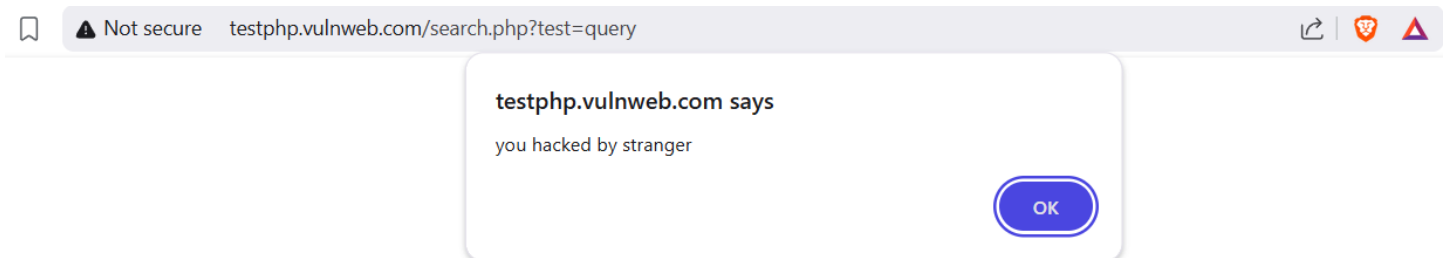


2 Insert the Payload in Search Box

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



3. Check the Response



Impact

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

Vulnerability : Authentication Using Burp Suite

Severity Risk : High

Description

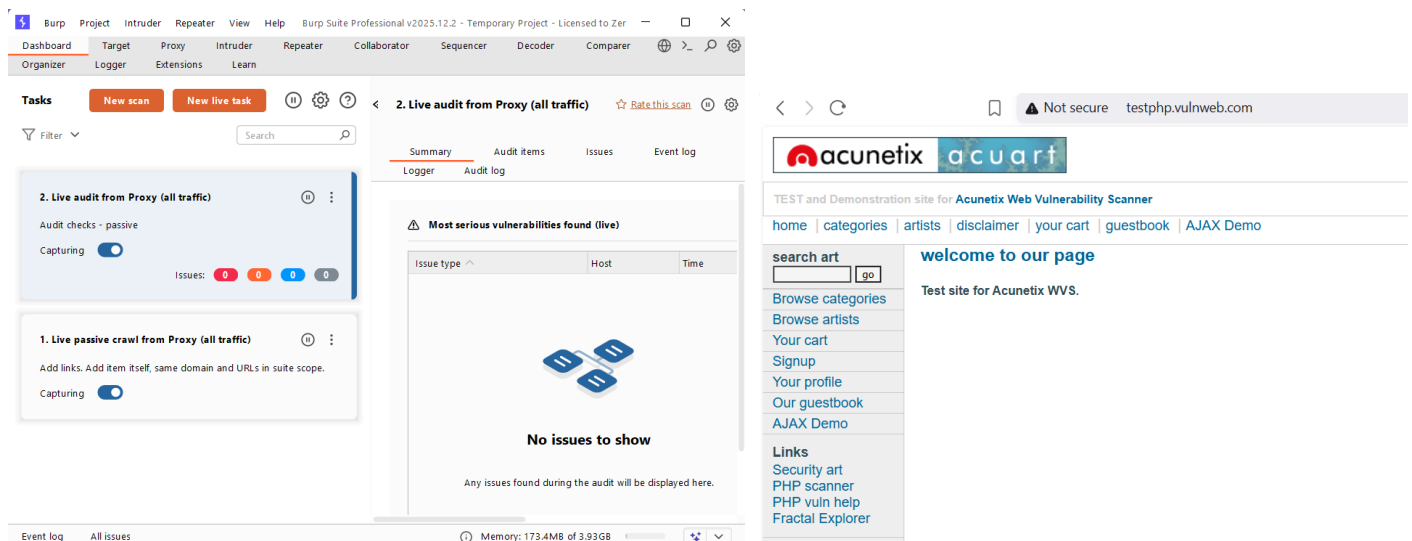
The **test.php** login page is vulnerable to **brute force attacks**, allowing an attacker to repeatedly attempt username and password combinations from a wordlist without restriction.

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

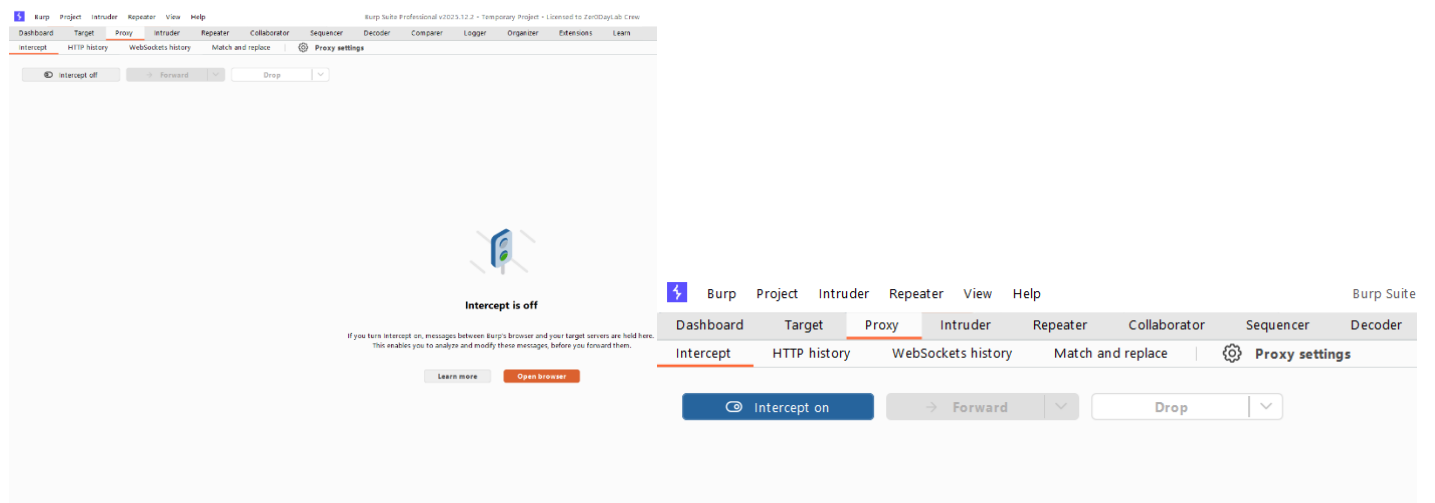
Requirements : Target Website , Burp Suite, Wordlists

Proof Of Concept : (POC)

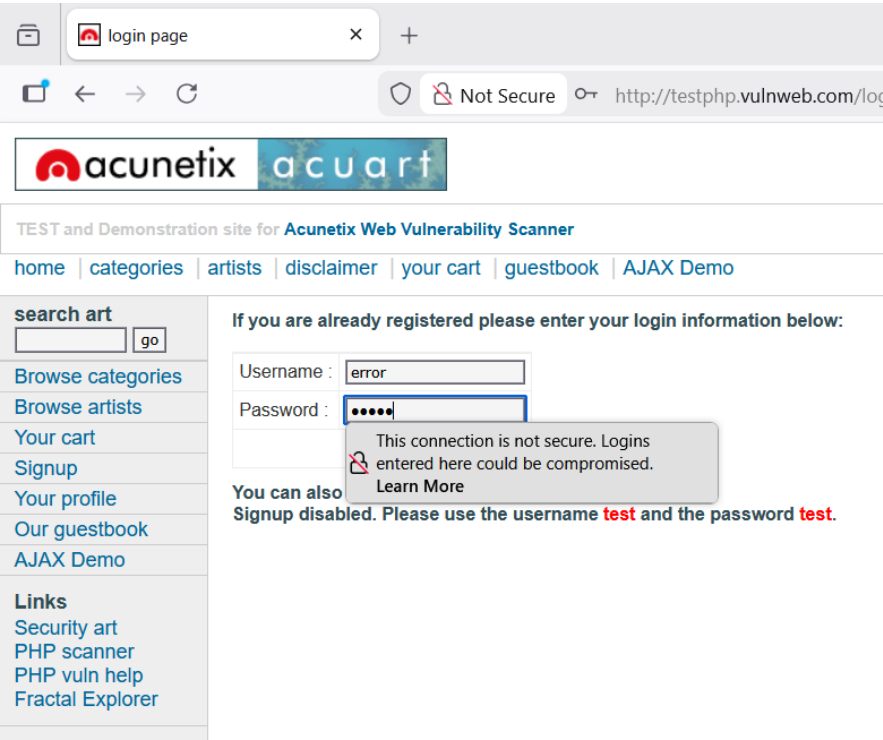
1. open Burp Suite and open <http://testphp.vulnweb.com/> site in Burp Suite Browser



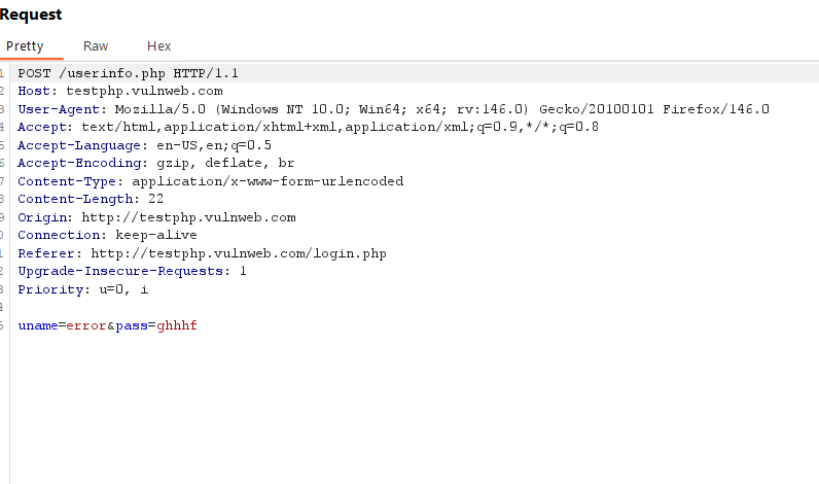
2. Go to **Proxy -> Intercept** -> Turn on **Intercept**



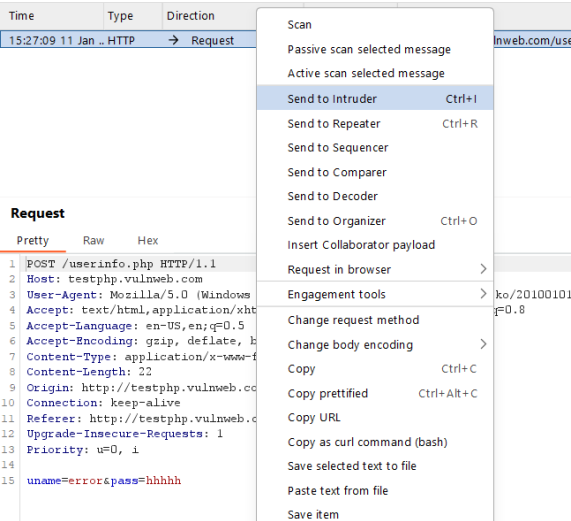
3. Entered an incorrect username or password to capture the login request in Burp Suite.



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



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



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; x6
4 Accept: text/html,application/xhtml+xml,application
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

Load...

Remove

Clear

Deduplicate

Add

Add from list...

Cipher

Blaze

Quantum

Echo

Nova

Phantom

Drift

Spark

Orbit

Enter a new item

Payloads

Payload position: 2 - hhhhh

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

Load...

Remove

Clear

Deduplicate

Add

Add from list...

Shadow

Pixel

Thunder

Neon

Cipher

Blaze

Quantum

Echo

Nova

Enter a new item

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

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	308			258	

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

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

Attack Save

ResultsPositions

Capture filter: Capturing all itemsApply capture filter

View filter: Showing all items

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	
6	Blaze	Shadow	302	307			258	

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparer

12x+

SendCancel<>Burp AI

Request

PrettyRawHex

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/1

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: 20

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=test&pass=test

Response

Impact

- * Account Takeover
- * Unauthorized Access
- * Data Breach