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/

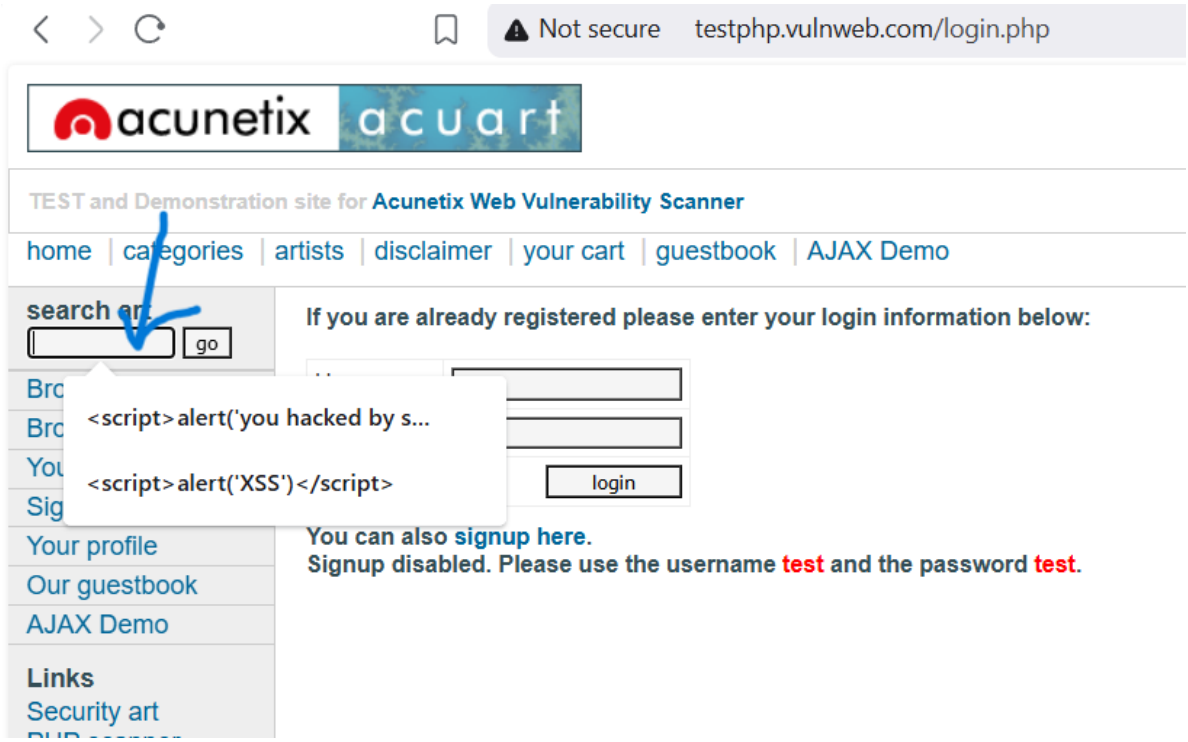
Payload : <script>alert('you hacked by stranger')</script>

Proof Of Concept : (POC)

1 Go TO [http://**testphp.vulnweb**.com/](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

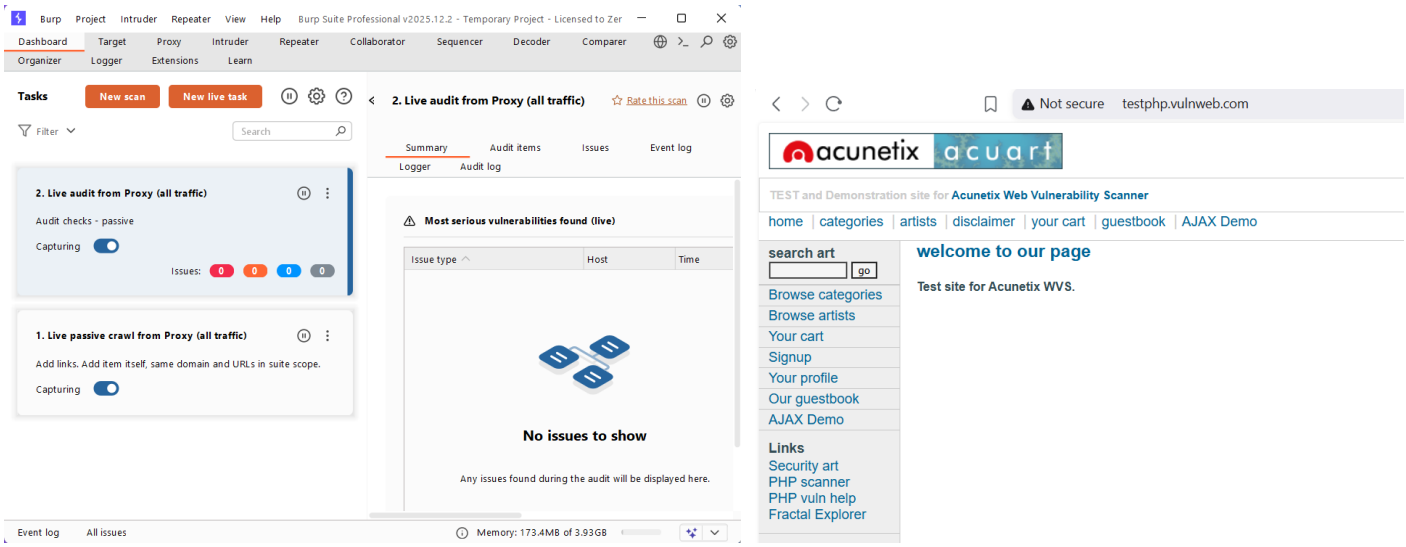
The **test.php** login page is vulnerable to **brute force attacks**, allowing an attacker to repeatedly attempt username and password combinations from a wordlist without restriction.

URL : http://**testphp.vulnweb**.com/

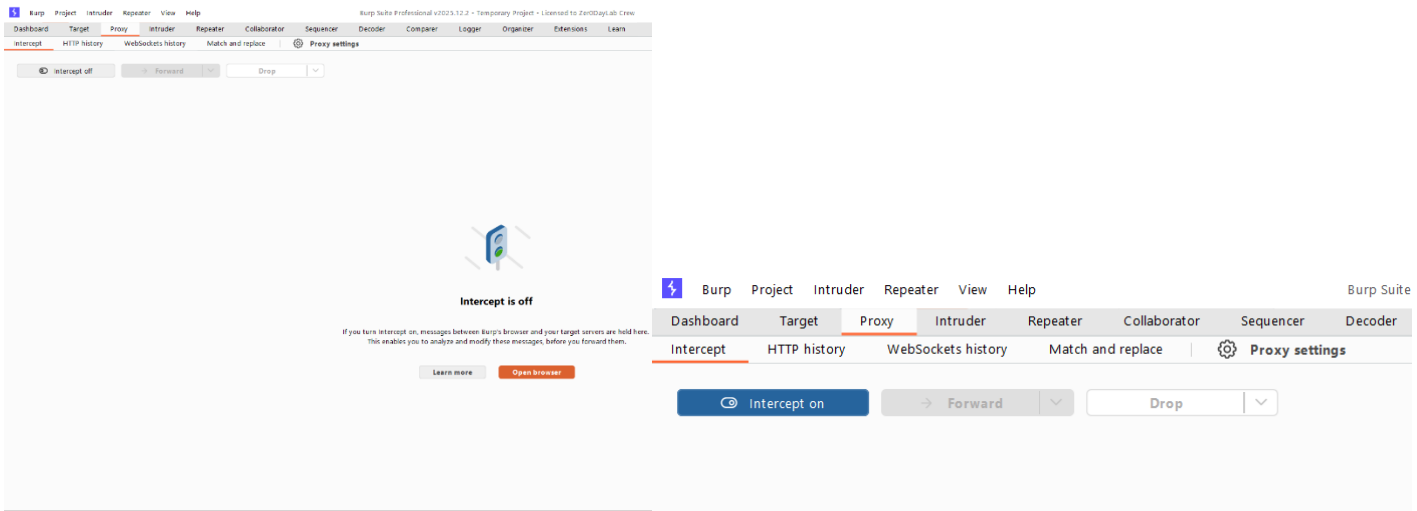
Requirements : Target Website , Burp Suite, Wordlists

Proof Of Concept : (POC)

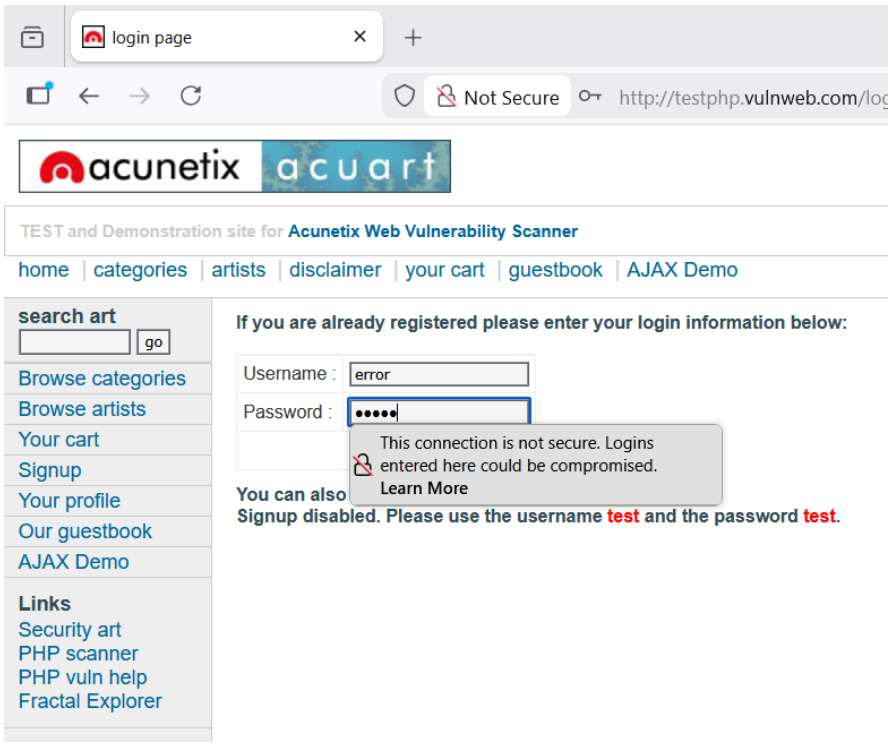
1. open Burp Suite and open http://**testphp.vulnweb**.com/ site in Burp Suite Browser



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

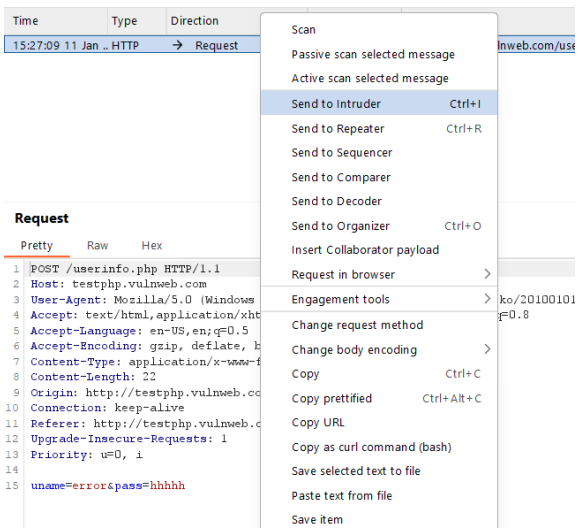


3. Entered an incorrect username or password to capture the login request in Burp Suite.

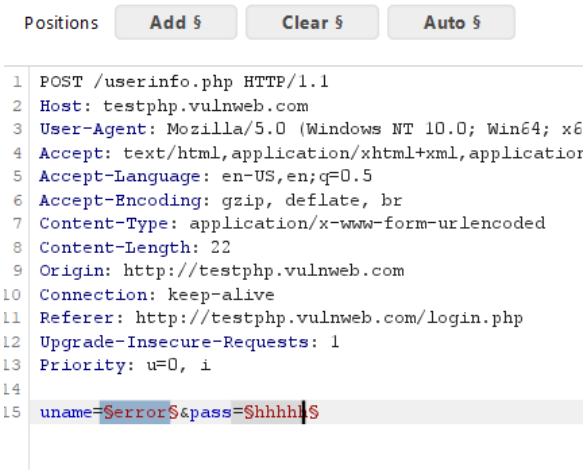


4. Captured the login request containing the username and password in Burp Suite.

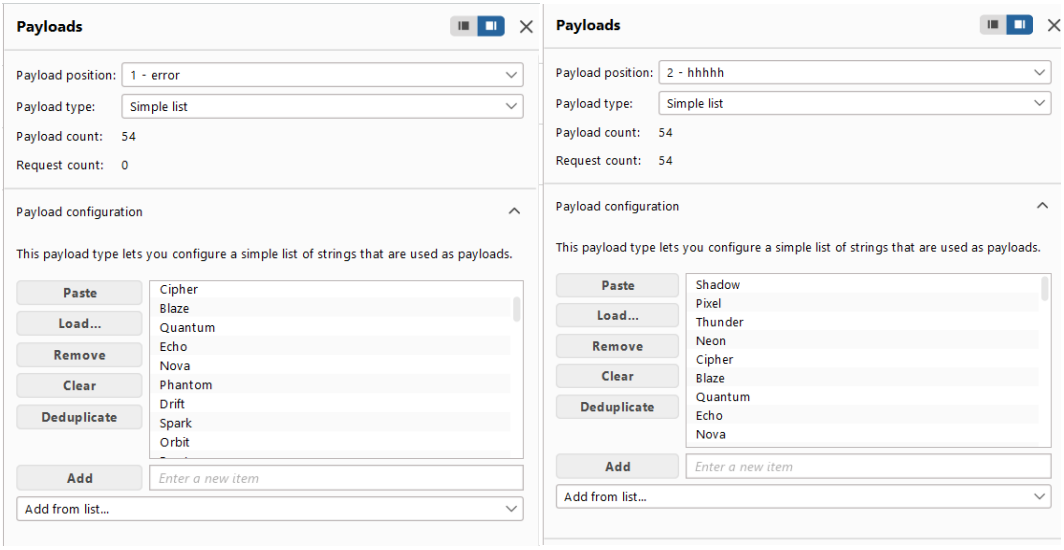
5. Send to **Intruder** Captured login request for modify the request.



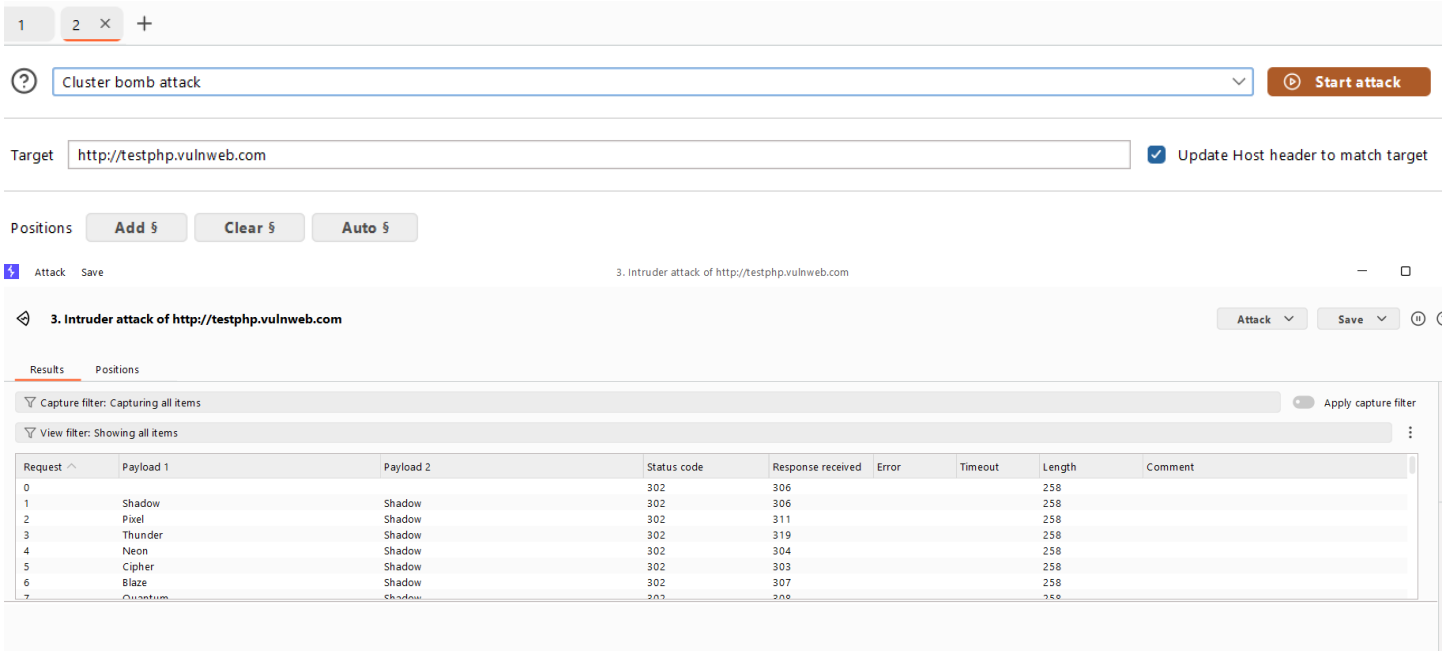
5. Added **$** symbols to the username and password parameters to define payload positions for brute force testing.



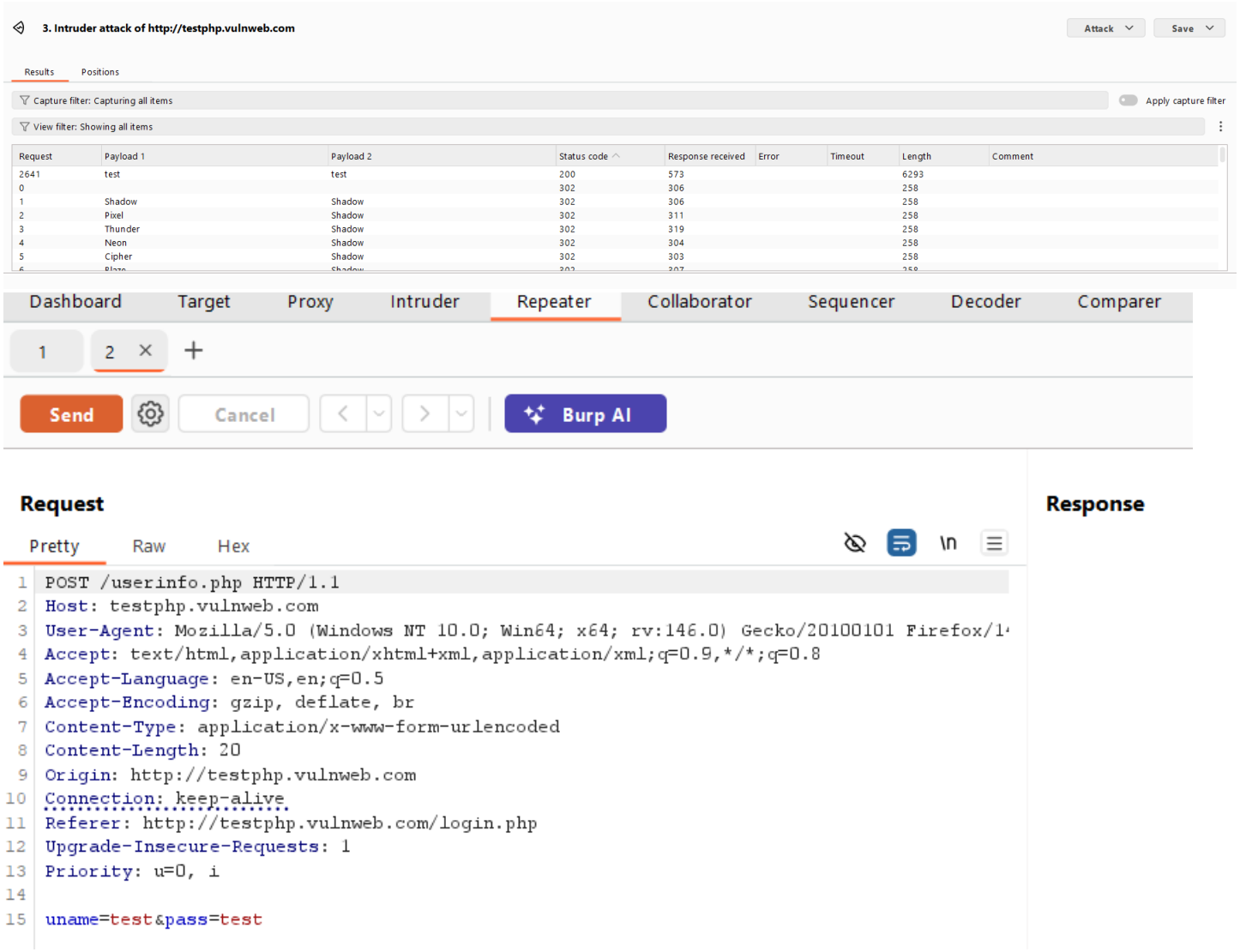
6. Selected **Payload 1** for the username and **Payload 2** for the password and loaded wordlists for both.



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



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



Impact

* Account Takeover

* Unauthorized Access

* Data Breach

Thank you