Reflected XSS Vulnerability Testing Report - DVWA

Date: 11 June 2025

Objective:

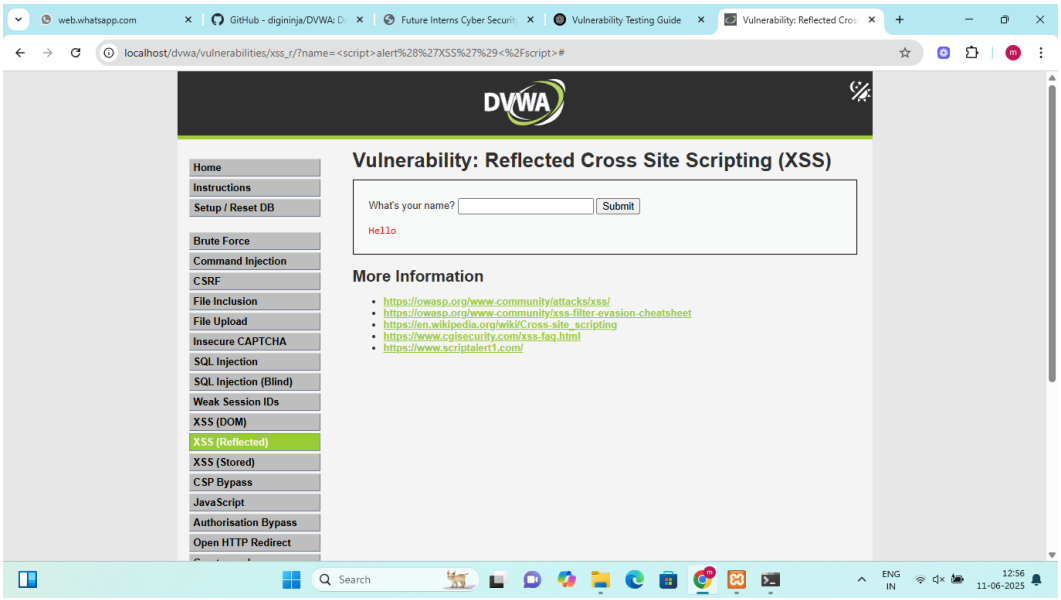
To test and understand how reflected XSS vulnerabilities behave in DVWA under different security levels and confirm whether inputs are properly sanitized or executed.

Test Details:

Payload 1:

<script>alert('XSS')</script>

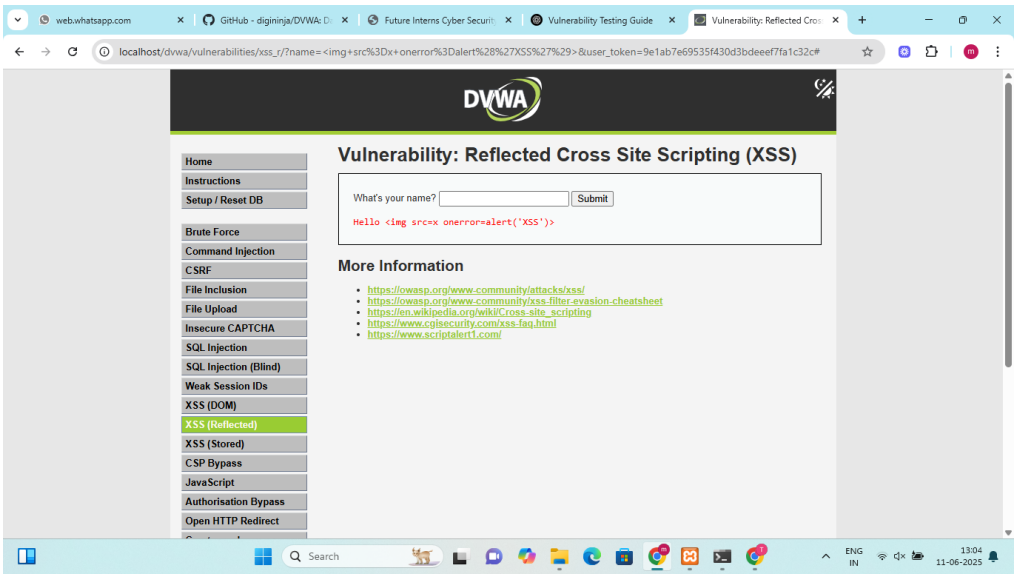
Result: Successfully triggered alert box on Low security level. Screenshot



Payload 2:

<img src=x onerror=alert('XSS')>

Result: Successfully triggered alert box on Low, Medium, and High security levels.



DVWA Security Levels Behavior:

Low: No input sanitization - XSS Successful

Medium: Partial filtering - XSS Successful High:

Stricter filtering - XSS Successful

Impossible: Strong validation and output encoding - XSS Blocked

Technical Analysis:

- Vulnerability Type: Reflected XSS

- Vector: Unsanitized user input reflected in response

- Impact: Arbitrary JS execution

- Parameter: name (GET method)

Recommendations:

- Use output encoding (e.g., htmlspecialchars in PHP)

- Validate and sanitize user input

- Apply CSP headers

- Use frameworks that auto-escape input

- Enable Web Application Firewalls (WAF)

Conclusion:

DVWA XSS (Reflected) module effectively demonstrates vulnerability impact across different security levels.

Your test confirms that reflected XSS can be exploited unless strong sanitization is implemented.