BUG BOUNTY REPORT

Reflected Cross-Site Scripting (XSS)

Submitted By: Tooba Zainab

---

1. Basic Information

Project Name: Bounty Hunt 101 – Recon to Report
Target Application: DVWA (Damn Vulnerable Web Application)
Application URL: http://localhost/DVWA
Vulnerability Type: Reflected Cross-Site Scripting (XSS)
Severity Level: Medium
Test Environment:

- Kali Linux
- DVWA (Local Lab)
- Apache, PHP, MariaDB

---

2. Vulnerability Summary

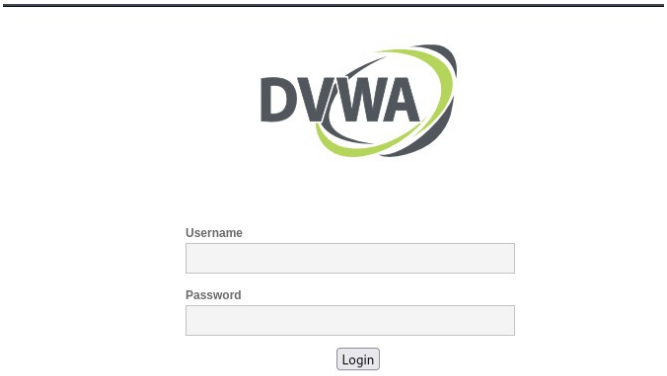
A **Reflected Cross-Site Scripting (XSS)** vulnerability was discovered in the DVWA application under the **XSS (Reflected)** module.
This vulnerability allows an attacker to inject and execute malicious JavaScript code in the victim's browser.

The issue occurs due to **lack of proper input validation and output encoding**.

---

3. Environment Setup Confirmation

The DVWA application was successfully installed and configured on Kali Linux.
The application was accessible via browser and the database was initialized correctly.



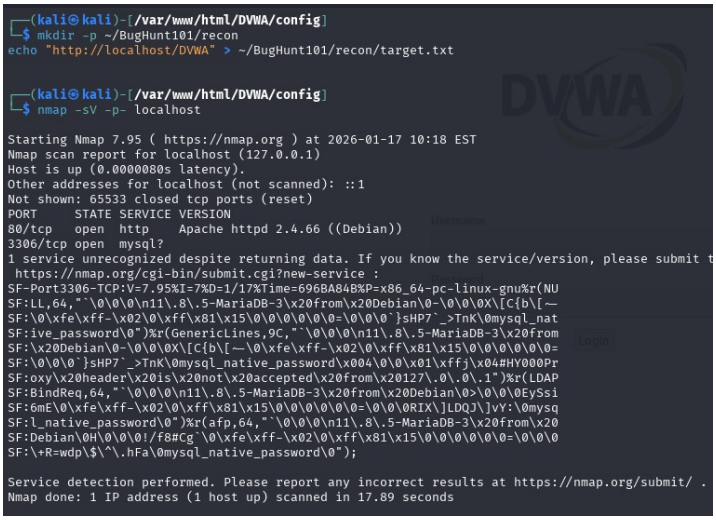
4. Reconnaissance Performed

An Nmap scan was performed on the target system to identify open ports and running services.

Tool Used: Nmap
Command Used:

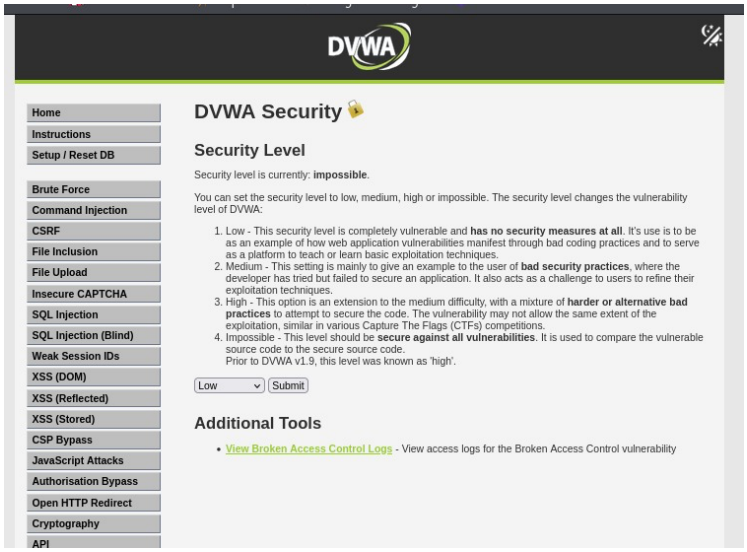
nmap -sV -p- localhost

The scan revealed active services such as Apache web server and MySQL database, confirming a valid web attack surface.



5. Security Configuration

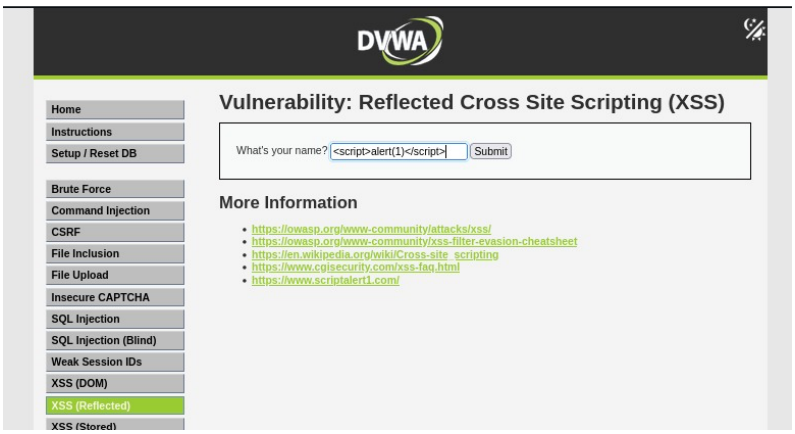
Before testing, the DVWA security level was set to **Low** to simulate a vulnerable application environment.

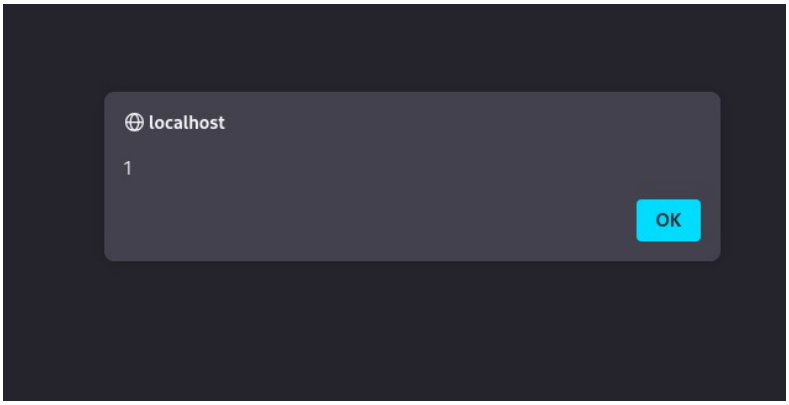


---

6. Steps to Reproduce the Vulnerability

1. Login to DVWA using default credentials:
    - Username: admin
    - Password: password
2. Navigate to **DVWA Security** and set the security level to **Low**.
3. Click on **XSS (Reflected)** from the left menu.
4. Enter the following payload into the input field:
5. <script>alert(1)</script>
6. Click the **Submit** button.





---

7. Proof of Concept (PoC)

Payload Used

<script>alert(document.cookie)</script>

Result

A JavaScript alert popup appeared displaying session cookies, confirming successful execution of injected JavaScript code.

---

8. Impact Analysis

If exploited in a real-world application, this vulnerability could allow an attacker to:

- Steal session cookies
- Hijack user sessions
- Perform phishing attacks

- Execute malicious scripts in the user's browser
- Potentially gain unauthorized access to user accounts

---

9. Evidence Summary

The following evidence was collected during testing:

- DVWA running successfully
- Security level set to Low
- XSS alert popup
- Cookie disclosure popup

---

10. Recommendations

To mitigate this vulnerability, the following actions are recommended:

- Validate and sanitize all user inputs
- Encode output before rendering it in the browser
- Implement Content Security Policy (CSP)
- Avoid directly reflecting user input in responses

---

11. Conclusion

This report demonstrates a successfully identified and exploited **Reflected XSS vulnerability** in a controlled lab environment.
The vulnerability highlights the importance of secure input handling and output encoding in web applications.

All testing was performed **ethically and within scope** for educational purposes only.

---

12. Tester Declaration

This vulnerability assessment was conducted solely for academic learning in a safe lab environment and did not target any real-world systems.