Vulnerability Assessment Report

Target: DVWA (Damn Vulnerable Web Application)

Date: October 17 2026

Author: Sahil Punia

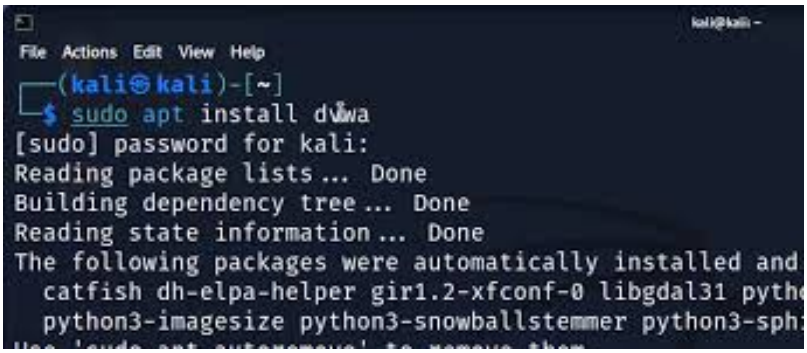
---

1. Introduction

This report details the findings of a security assessment conducted on the Damn Vulnerable Web Application (DVWA). The assessment aimed to identify common web vulnerabilities such as Cross-Site Scripting (XSS). The environment was set up locally for controlled testing.

2. Setup Environment

For this assessment, DVWA was installed on a local virtual machine running Linux. This provided a sandboxed environment to perform penetration testing without affecting production systems.



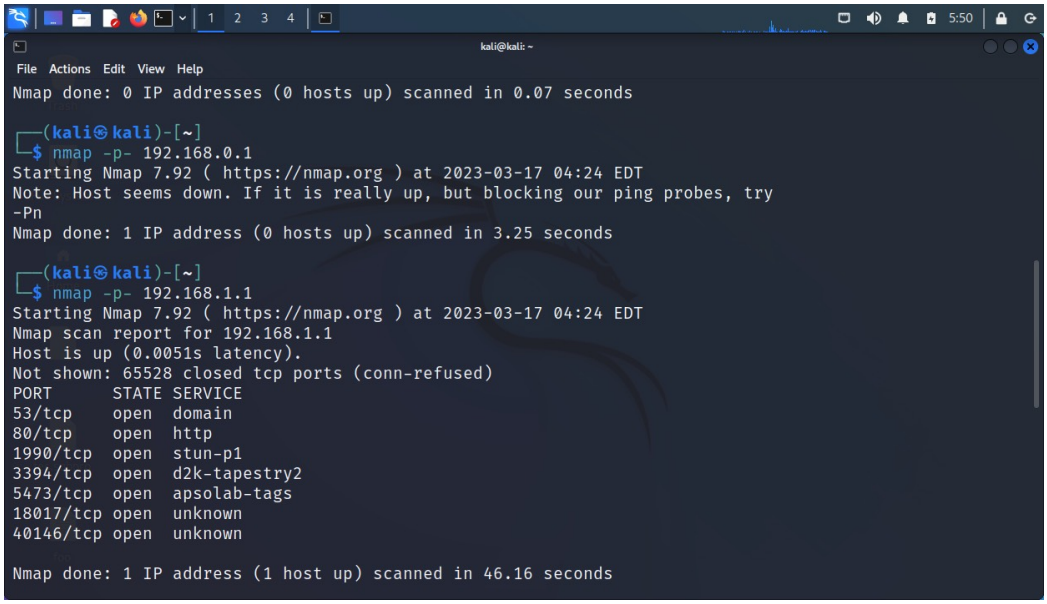
3. Reconnaissance

Initial reconnaissance involved enumerating subdomains (if applicable for a more complex target) and services running on the DVWA instance. For a local setup like DVWA, the focus was primarily on port scanning and identifying accessible services.

Tools Used:

- **Nmap:** For port scanning and service detection.

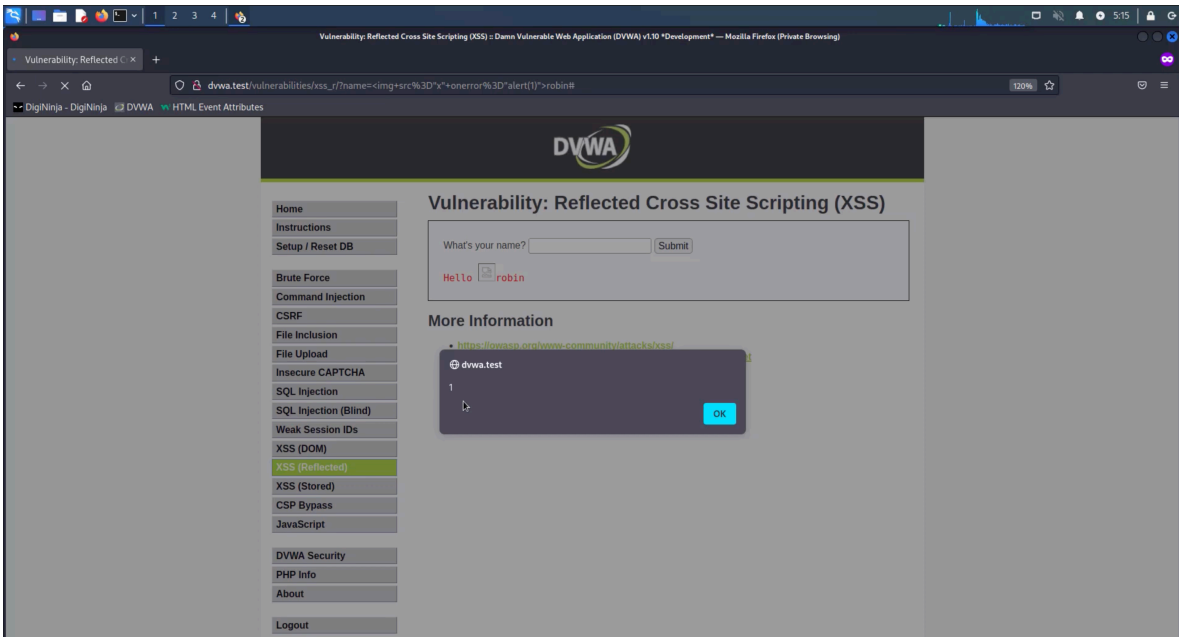
Nmap Scan Output:



4.1 Cross-Site Scripting (XSS)

Description: XSS vulnerabilities allow attackers to inject client-side scripts into web pages viewed by other users. This can lead to session hijacking, defacement, or redirection to malicious sites.

Vulnerable Endpoint: `http://dvwa.test/vulnerabilities/xss_r/`



Proof of Concept (PoC):

Reflected XSS Payload: `<script>alert('1');</script>`

Reproduction Steps:

1. Navigate to the XSS (Reflected) page in DVWA.
2. Enter the reflected XSS payload into the input field.
3. Observe the JavaScript alert box.
4. The alert box will appear immediately, and for subsequent visitors to that page.