

Vulnerability Assessment Report

Target: DVWA (Damn Vulnerable Web Application)

Date: October 17 2026

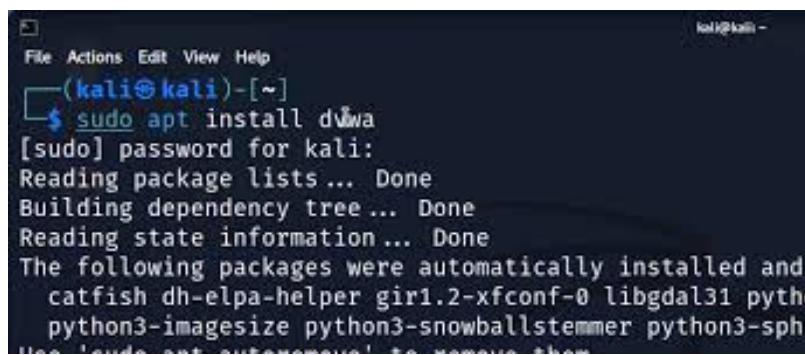
Author: Sahil Punia

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.



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install dvwa
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and
  catfish dh-elpa-helper gir1.2-xfconf-0 libgdal31 python
  python3-imaging python3-snowballstemmer python3-sph
Use 'sudo apt autoremove' to remove them.
```

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:

```

kali㉿kali:[~]
$ nmap -p- 192.168.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-17 04:24 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.25 seconds

kali㉿kali:[~]
$ nmap -p- 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-17 04:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
1990/tcp  open  stun-p1
3394/tcp  open  d2k-tapestry2
5473/tcp  open  apsolab-tags
18017/tcp open  unknown
40146/tcp open  unknown

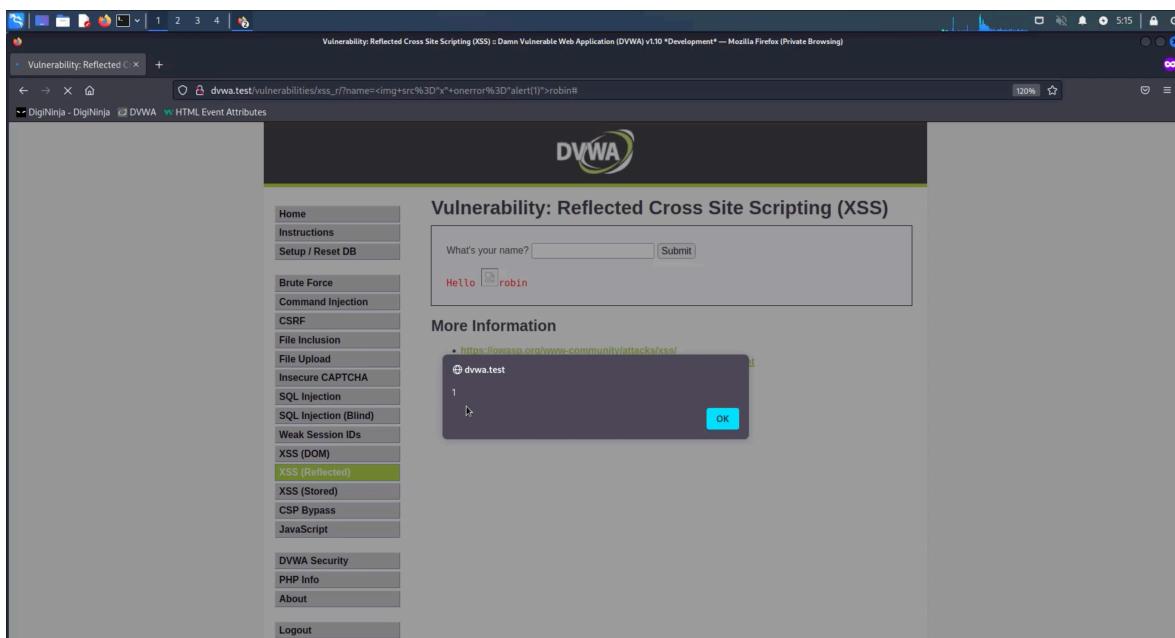
Nmap done: 1 IP address (1 host up) scanned in 46.16 seconds

```

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.