

Vulnerability Assessment Report

Target: DVWA (Damn Vulnerable Web Application)

Date: October 17 2026

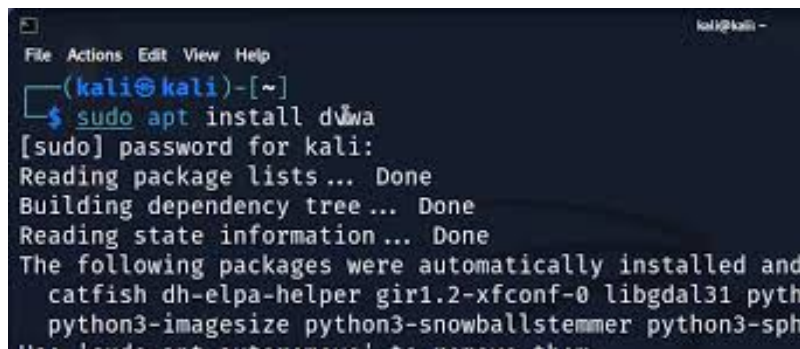
Author: Sahil Punia

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.

A terminal window with a dark background and light blue text. The prompt is '(kali@kali)-[~]'. The user enters '\$ sudo apt install dvwa'. The terminal shows the password prompt '[sudo] password for kali:', followed by 'Reading package lists ... Done', 'Building dependency tree ... Done', and 'Reading state information ... Done'. It then lists several packages that were automatically installed along with dvwa: catfish, dh-elpa-helper, gir1.2-xfconf-0, libgdal31, python3-catfish, python3-dh-elpa-helper, python3-gir1.2-xfconf-0, python3-libgdal31, python3-pyxdg, python3-snowballstemmer, and python3-sphinx. The text is partially cut off at the bottom.

```
(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 python3-
python3-imagesize python3-snowballstemmer python3-sph
```

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:

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.