DVWA on Kali Linux — Installation & Vulnerability Discovery Report

Executive Summary

This report documents the installation and configuration of Damn Vulnerable Web App (DVWA) on Kali Linux, the process used to discover common web vulnerabilities in a controlled lab, evidence collected, an impact analysis for each finding, and prioritized remediation recommendations. The goal is educational: to practice safe discovery techniques and produce a reproducible record suitable for training and internal security exercises.

Scope & Objectives

Scope: Local Kali VM running DVWA (localhost).
Objectives:
1. Install and configure DVWA on Kali Linux.
2. Explore DVWA security levels (Low / Medium / High) and observe differences.
3. Safely discover and document common web vulnerabilities (manual testing + light automation).
4. Produce a professional report with evidence, impact analysis, and remediation suggestions.

Environment & Assumptions

- Host: Kali Linux (latest available package set as of test date).
- DVWA installed via package manager (sudo apt install dvwa) and started with sudo dvwa-start.
- Testing is performed in a contained lab environment (no testing on production systems).
- Tools used (light automation): Nikto, WhatWeb, Dirb, Nuclei. Manual testing used browser and DVWA UI.

Installation & Setup

1. System update and install DVWA:
sudo apt update
sudo apt install dvwa -y

2. Start DVWA:
sudo dvwa-start
Browse to http://127.0.0.1/dvwa or http://localhost/dvwa

3. Configure DVWA in the web UI:
- Log in with default credentials (usually admin / password).
- Set up the database when prompted (use the "Create / Reset Database" button).
- Under DVWA Security, set to Low, run tests, then change to Medium, run tests, then High, and run tests again.

Testing Methodology

1. Manual testing: Use DVWA UI modules for SQL Injection, XSS, Command Injection, File Upload, Insecure Direct Object References (IDOR), Security Misconfigurations, Sensitive Info in source, and Session Management exercises.
2. Light automation: Run Nikto, WhatWeb, Dirb, and Nuclei against the DVWA host to confirm server misconfigurations and to practice safe automation.
3. Evidence capture: Collect screenshots of vulnerable requests, server responses, and tool outputs. Record exact commands and URL endpoints used.
4. Risk analysis: For each finding estimate impact and likelihood in the lab context and map to remediation.

Findings (Summary)

- SQL Injection (SQLi): Risk of data exfiltration and modification. Fix with parameterized queries and input validation.
- Cross-Site Scripting (XSS): Risk of session theft and client-side attack. Fix with output encoding and CSP headers.
- Command Injection: Risk of RCE. Fix by avoiding shell commands or sanitizing inputs.
- File Upload Vulnerability: Risk of malicious uploads. Fix with file type restrictions, storage outside webroot, and malware scanning.
- IDOR: Risk of unauthorized access. Fix with authorization checks and indirect object references.
- Security Misconfigurations: Missing headers. Fix with hardened server config and HTTPS.
- Sensitive Info in Source: Risk of leaked secrets. Fix by removing secrets from client-side code and scanning repos.
- Session Management Weaknesses: Weak cookies/session handling. Fix with Secure/HttpOnly cookies, rotation, and proper expiration.

Light Automation

Nikto: nikto -h http://127.0.0.1:80 -output nikto_dvwa.txt
WhatWeb: whatweb http://127.0.0.1/dvwa
Dirb: dirb http://127.0.0.1/dvwa /usr/share/dirb/wordlists/common.txt
Nuclei: nuclei -u https://testphp.vulnweb.com -t /path/to/nuclei-templates -o nuclei_results.txt

Recommendations

1. Fix coding issues (queries, encoding, validation).
2. Harden server with HTTPS, security headers, disable directory listing.
3. Secure file uploads.
4. Improve session management.
5. Add CI/CD security scanning (SAST, dependency checks, nuclei).
6. Conduct team training with DVWA labs.

Appendix A

- Install DVWA: sudo apt install dvwa
- Start DVWA: sudo dvwa-start
- Create/reset DB: DVWA web UI -> "Create / Reset Database"
- Tools: nikto, whatweb, dirb, nuclei

Appendix B

Evidence Index (place holders)

- Screenshot: DVWA_low.
- Screenshot: DVWA_Medium.
- Screenshot: DVWA_High.
- Screenshot:Nikto output.
- Screenshot:Nuclei run results.
- Screenshot:Whatweb result.
- Screenshot:Gobuster result.