Penetration Testing Report - DVWA

Date

July 23, 2025

Target

http://127.0.0.1:42001

Test Type

Local Web Application Penetration Test

1. Introduction

DVWA (Damn Vulnerable Web Application) is an intentionally vulnerable PHP/MySQL web application designed for security professionals to practice penetration testing techniques in a safe environment. This assessment aims to simulate an attacker's behavior using common tools to identify weaknesses.

2. Tools & Methodology

Nikto - Scans the web server for known vulnerabilities

WhatWeb - Identifies web technologies and headers

Dirb - Performs dictionary-based discovery of hidden directories

Gobuster - Brute-force scanner for web paths

Snort - Intrusion Detection System to monitor traffic

3. Results Summary

3.1 Nikto:

- Missing X-Frame-Options header (Clickjacking risk)
- Missing X-Content-Type-Options header (MIME-sniffing risk)
- Found /login.php admin login page

3.2 WhatWeb:

- Server: nginx/1.26.3
- Technologies: DVWA, HTML5
- Cookies: PHPSESSID, security (HttpOnly)
- Redirect: / ? /login.php

3.3 Dirb & Gobuster:

- Directories: /config/, /database/, /docs/, /external/
- Files: /php.ini, /phpinfo.php, /robots.txt
- High risk: configuration files publicly accessible

3.4 Snort:

- 2079 packets analyzed, 8 alerts
- Detected port scans, ARP spoofing, back orifice packets

4. Vulnerability Analysis

Clickjacking - Medium

MIME Sniffing - Low

Exposed Config Files - High

Unrestricted Login Path - Medium

Directory Access - High

5. Security Recommendations

- Set headers: X-Frame-Options, X-Content-Type-Options
- Remove or restrict: php.ini, phpinfo.php
- Secure folders: /config/, /database/
- Add rate limiting / CAPTCHA on login
- Deploy WAF and continuous monitoring

- Do NOT deploy DVWA in production

6. Conclusion

This test demonstrated how basic tools can reveal misconfigurations and vulnerabilities. Exposed files and insecure headers pose real threats. Snort effectively detected scanning behavior. DVWA should only be used for testing and not deployed publicly.