This penetration test report documents the security assessment of two vulnerable environments: **Damn Vulnerable Web Application (DVWA)** and **buggy Web Application (bWAPP)**.

---

1. Executive Summary

The assessment involved targeted reconnaissance and vulnerability scanning to identify security weaknesses in two distinct web environments. Both applications were found to be highly vulnerable to information disclosure and configuration weaknesses. **DVWA** exhibited a more hardened directory structure despite being vulnerable , while **bWAPP** suffered from severe **Directory Indexing** issues, exposing sensitive paths such as /passwords/ and /admin/ to the public internet

2. Methodology & Tools

The following industry-standard tools were used during the engagement:

- **Nmap:** Used for network service discovery and version fingerprinting.
- **DIRB:** Utilized for directory brute-forcing and mapping hidden web structures.
- **Nikto:** Deployed for comprehensive web server configuration auditing and vulnerability identification.

3. Technical Findings

3.1 Network Reconnaissance (Nmap)

Nmap was used to identify open ports and service versions for both targets. Scanning revealed the following active services:

- **Target 1 (DVWA):** Detected **nginx 1.28.0** on port 42001. Port 3306 was open, identifying a **MariaDB** database backend through service fingerprinting.

- **Target 2 (bWAPP/General):** Port 80 was active for web traffic. Additionally, port 53 (DNS) was identified as open, running **ISC BIND**

DVWA

```
┌──(marie㉿math)-[/home/marie]
└─PS> nmap -sV -p- 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-20 21:05 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?
42001/tcp open  http    nginx 1.28.0
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.95%I=7%D=12/20%Time=694755F6%P=x86_64-pc-linux-gnu%r(N
SF:ULL,67,"c\0\0\0\n11\.8\.3-MariaDB-1\+b1\x20from\x20Debian\0\xf6\x01\0\0
SF:tV3;k-9x\0\xfe\xff-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\0rT,~X\|\)RB5\$Q
SF:\0mysql_native_password\0")%r(GenericLines,9F,"c\0\0\0\n11\.8\.3-MariaD
SF:B-1\+b1\x20from\x20Debian\0\xf6\x01\0\0tV3;k-9x\0\xfe\xff-\x02\0\xff\x8
SF:1\x15\0\0\0\0\0\0=\0\0\0rT,~X\|\)RB5\$Q\0mysql_native_password\x004\0\0
SF:\x01\xffj\x04#HY000Proxy\x20header\x20is\x20not\x20accepted\x20from\x20
SF:127\.0\.0\.1")%r(LDAPBindReq,67,"c\0\0\0\n11\.8\.3-MariaDB-1\+b1\x20fro
SF:m\x20Debian\0\x07\x02\0\0Q'ja,Q6X\0\xfe\xff-\x02\0\xff\x81\x15\0\0\0\0\
SF:0\0=\0\0\x009Rri6oP\"Vk9v\0mysql_native_password\0")%r(afp,67,"c\0\0\0\
SF:n11\.8\.3-MariaDB-1\+b1\x20from\x20Debian\0\x11\x02\0\0elokJme7\0\xfe\x
SF:ff-\x02\0\xff\x81\x15\0\0\0\0\0\0=\0\0\0\"@\\0×0!Tf\"uJ\0mysql_native_p
SF:assword\0");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.14 seconds
```

BWAPP

```
┌──(root㉿math)-[/home/marie]
└─# nmap -sV -p 53 64.71.255.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-22 13:12 EST
Nmap scan report for dns.cp.net.rogers.com (64.71.255.204)
Host is up (0.0040s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
```

Feature	**DVWA (Target: 127.0.0.1:42001)**	**bWAPP (Target: localhost)**
Web Server	nginx 1.28.0	Apache 2.4.65
Open Ports	3306 (MySQL), 42001 (HTTP)	80 (HTTP), 53 (DNS/Domain)
Database	MariaDB (detected via fingerprint)	MySQL (via Apache/PHP integration)

3.2 Web Directory Discovery (DIRB)

- **DVWA:** Identified standard directories including /config/, /database/, and /docs/. A php.ini file was found with a HTTP 200 status, which could leak server configuration details.
- **bWAPP:** Multiple directories were found to be **LISTABLE**, meaning any user can view the file contents of the folder. This included high-risk directories: /apps/, /db/, /documents/, /passwords/, and /soap/.

DVWA

```
┌──(marie㉿math)-[/home/marie]
└─PS> dirb http://127.0.0.1:42001/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Dec 20 17:42:45 2025
URL_BASE: http://127.0.0.1:42001/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://127.0.0.1:42001/ ----
==> DIRECTORY: http://127.0.0.1:42001/config/
==> DIRECTORY: http://127.0.0.1:42001/database/
==> DIRECTORY: http://127.0.0.1:42001/docs/
==> DIRECTORY: http://127.0.0.1:42001/external/
+ http://127.0.0.1:42001/favicon.ico (CODE:200|SIZE:1406)
+ http://127.0.0.1:42001/index.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/php.ini (CODE:200|SIZE:154)
+ http://127.0.0.1:42001/phpinfo.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/robots.txt (CODE:200|SIZE:25)

---- Entering directory: http://127.0.0.1:42001/config/ ----

---- Entering directory: http://127.0.0.1:42001/database/ ----
```

```
---- Entering directory: http://127.0.0.1:42001/docs/ ----
+ http://127.0.0.1:42001/docs/copyright (CODE:200|SIZE:1085)
==> DIRECTORY: http://127.0.0.1:42001/docs/graphics/

---- Entering directory: http://127.0.0.1:42001/external/ ----

---- Entering directory: http://127.0.0.1:42001/docs/graphics/ ----

-----------------
END_TIME: Sat Dec 20 17:42:50 2025
DOWNLOADED: 27672 - FOUND: 6
```

BWAPP

```
┌──(root㉿math)-[/home/marie]
└─# dirb http://localhost/bWAPP/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Dec 22 13:16:41 2025
URL_BASE: http://localhost/bWAPP/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://localhost/bWAPP/ ----
==> DIRECTORY: http://localhost/bWAPP/admin/
==> DIRECTORY: http://localhost/bWAPP/apps/
==> DIRECTORY: http://localhost/bWAPP/db/
==> DIRECTORY: http://localhost/bWAPP/documents/
==> DIRECTORY: http://localhost/bWAPP/fonts/
==> DIRECTORY: http://localhost/bWAPP/images/
+ http://localhost/bWAPP/index.php (CODE:302|SIZE:0)
+ http://localhost/bWAPP/info.php (CODE:200|SIZE:3426)
==> DIRECTORY: http://localhost/bWAPP/js/
==> DIRECTORY: http://localhost/bWAPP/passwords/
+ http://localhost/bWAPP/phpinfo.php (CODE:200|SIZE:76375)
+ http://localhost/bWAPP/robots.txt (CODE:200|SIZE:167)
```

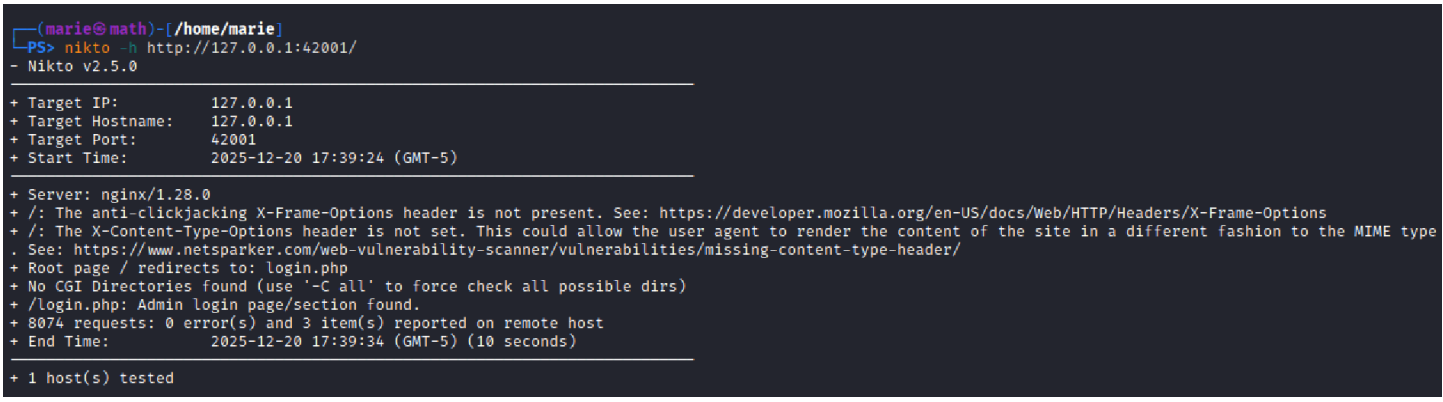
```
==> DIRECTORY: http://localhost/bWAPP/soap/
==> DIRECTORY: http://localhost/bWAPP/stylesheets/
+ http://localhost/bWAPP/web.config (CODE:200|SIZE:7556)

---- Entering directory: http://localhost/bWAPP/admin/ ----
+ http://localhost/bWAPP/admin/index.php (CODE:200|SIZE:3160)
+ http://localhost/bWAPP/admin/phpinfo.php (CODE:200|SIZE:76423)

---- Entering directory: http://localhost/bWAPP/apps/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://localhost/bWAPP/db/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://localhost/bWAPP/documents/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://localhost/bWAPP/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://localhost/bWAPP/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://localhost/bWAPP/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

```
---- Entering directory: http://localhost/bWAPP/passwords/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://localhost/bWAPP/soap/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://localhost/bWAPP/stylesheets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Dec 22 13:16:50 2025
DOWNLOADED: 9224 - FOUND: 7
```

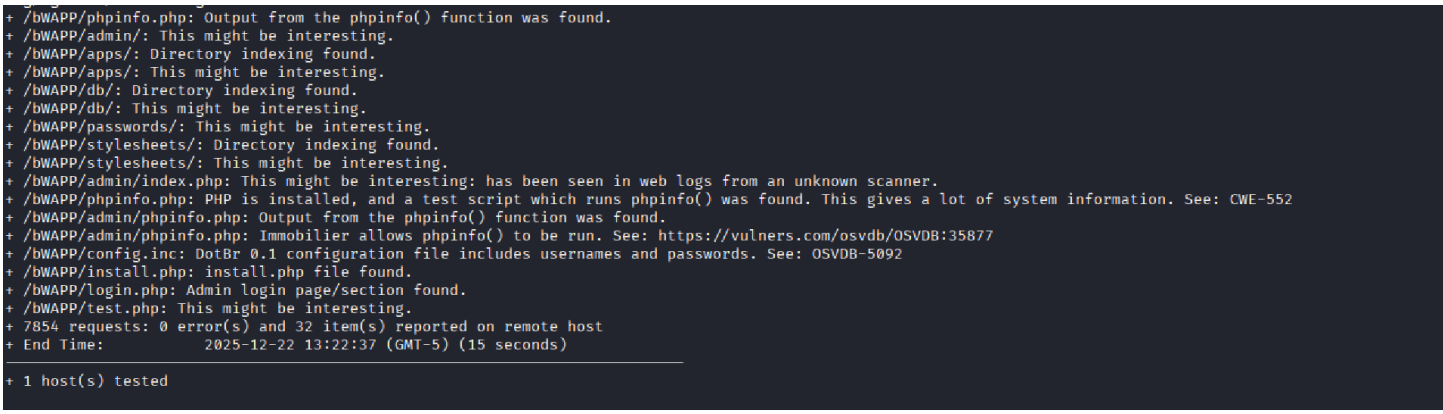
3.3 Vulnerability Scanning (Nikto)

- **Missing Security Headers:** Both targets lack X-Frame-Options (increasing Clickjacking risk) and X-Content-Type-Options (allowing MIME-sniffing).
- **Information Leakage:** bWAPP revealed its internal IP (127.0.1.1) in the HTTP Location header.
- **Cross-Site Scripting (XSS):** bWAPP's test.php script was confirmed to be vulnerable to XSS (CVE-2002-1455).
- **Sensitive Files:** The config.inc file in bWAPP was flagged as containing potential usernames and passwords.

DVWA



BWAPP



4. Comparison of Vulnerabilities

Vulnerability	DVWA Presence	bWAPP Presence	Severity
Directory Indexing	Not Detected	**Critical** (Extensive)	High
Sensitive File Exposure	php.ini, robots.txt	config.inc, web.config	High
Information Disclosure	phpinfo.php (Redirected)	phpinfo.php (Accessible)	Medium
Service Versioning	Nginx 1.28.0	Apache 2.4.65	Low

5. Remediation Plan

1.Disable Directory Listings: Modify server configurations (Apache/Nginx) to prevent users from viewing the contents of directories. In Apache, this is done by removing Indexes from the Options directive.

2.Secure Configuration Files: Restrict access to config.inc, php.ini, and other system files so they are not reachable via a web browser.

3.Implement Security Headers: Configure the web server to include X-Frame-Options and X-Content-Type-Options in all HTTP responses.

4.Patch and Update: Address known vulnerabilities such as the XSS flaw in test.php and ensure the ISC BIND service on port 53 is up to date and necessary for the environment.