

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

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

```
(marie@math)-[~/home/marie]
$ nikto -h http://127.0.0.1:42001/
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port:    42001
+ Start Time:    2025-12-20 17:39:24 (GMT-5)

+ Server: nginx/1.28.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:        2025-12-20 17:39:34 (GMT-5) (10 seconds)

+ 1 host(s) tested
```

## BWAPP

```
(root@math)-[~/home/marie]
# nikto -h http://localhost/bWAPP/
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:    2025-12-22 13:22:22 (GMT-5)

+ Server: Apache/2.4.65 (Debian)
+ /bWAPP/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /bWAPP/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /bWAPP/ redirects to: portal.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/admin/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /bWAPP/documents/: Directory indexing found.
+ /bWAPP/images/: Directory indexing found.
+ /robots.txt: Entry '/documents/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /bWAPP/images/: Directory indexing found.
+ /robots.txt: Entry '/images/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /bWAPP/passwords/: Directory indexing found.
+ /robots.txt: Entry '/passwords/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.1.1". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /bWAPP/login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /bWAPP/web.config: ASP config file is accessible.
+ /bWAPP/test.php%3CSCRIPT%3Ealert('Vulnerable')%3C%2FSCRIPT%3E=x: OmniHTTPD's test.php is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1455
```

```

+ /bWAPP/phpinfo.php: Output from the phpinfo() function was found.
+ /bWAPP/admin/: This might be interesting.
+ /bWAPP/apps/: Directory indexing found.
+ /bWAPP/apps/: This might be interesting.
+ /bWAPP/db/: Directory indexing found.
+ /bWAPP/db/: This might be interesting.
+ /bWAPP/passwords/: This might be interesting.
+ /bWAPP/stylesheets/: Directory indexing found.
+ /bWAPP/stylesheets/: This might be interesting.
+ /bWAPP/admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /bWAPP/phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /bWAPP/admin/phpinfo.php: Output from the phpinfo() function was found.
+ /bWAPP/admin/phpinfo.php: Immobilier allows phpinfo() to be run. See: https://vulners.com/osvdb/OSVDB:35877
+ /bWAPP/config.inc: DotBr 0.1 configuration file includes usernames and passwords. See: OSVDB-5092
+ /bWAPP/install.php: install.php file found.
+ /bWAPP/login.php: Admin login page/section found.
+ /bWAPP/test.php: This might be interesting.
+ 7854 requests: 0 error(s) and 32 item(s) reported on remote host
+ End Time: 2025-12-22 13:22:37 (GMT-5) (15 seconds)

+ 1 host(s) tested

```

## 4. Comparison of Vulnerabilities

Vulnerability	DVWA Presence	bWAPP Presence	Severity
<b>Directory Indexing</b>	Not Detected	Critical (Extensive)	High
<b>Sensitive File Exposure</b>	php.ini, robots.txt	config.inc, web.config	High
<b>Information Disclosure</b>	phpinfo.php (Redirected)	phpinfo.php (Accessible)	Medium
<b>Service Versioning</b>	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.