

- **Remediation:** Disable directory listing with Options -Indexes in Apache configuration.

8. PHP Script Info Disclosure (/usr/doc)

- **Finding:** Sensitive PHP scripts in /usr/doc may disclose system or application details.
- **Remediation:** Restrict access or remove unnecessary documentation files.

9. phpMyAdmin Exposed (Default Interface)

- **Finding:** phpMyAdmin is exposed to the internet, making it a target for brute force and exploitation attempts.
- **Remediation:** Restrict phpMyAdmin access to specific IPs, enable strong authentication, or remove it if not required.

10. phpMyAdmin Changelog Reveals Version Info

- **Finding:** The phpMyAdmin changelog is publicly available, leaking version details useful to attackers.
- **Remediation:** Restrict access to changelog files or remove them from the public web directory.

11. /test/ Directory Exposed (Potential Code/Files)

- **Finding:** The /test/ directory is exposed, which may contain test scripts or sensitive code.
- **Remediation:** Remove the /test/ directory or restrict access with authentication and IP filtering.

12. /icons/ Directory Indexing Enabled

- **Finding:** Apache's /icons/ directory indexing is enabled, exposing unnecessary files.
- **Remediation:** Disable directory listing for /icons/ and remove unused files.

13. Apache Default File /icons/README Found

- **Finding:** The default Apache /icons/README file was found, which provides information about server configuration.
- **Remediation:** Remove default files and harden the Apache installation by cleaning unnecessary content.

14. wp-config.php# Backup File Exposed (Credentials Leak)

- **Finding:** A backup file of wp-config.php was found, potentially exposing database credentials and sensitive configuration.
- **Remediation:** Remove exposed backup files immediately. Store configuration files securely and restrict file access permissions.

Escalation Email (100 words)

Subject: Security Findings from Nikto Scan on 192.168.56.104

Dear Development Team,

During a routine vulnerability assessment, I conducted a Nikto scan against the host **192.168.56.104**. The scan revealed multiple potential security risks including outdated Apache server versions, directory indexing enabled, and information disclosure through default files. These findings could allow attackers to enumerate sensitive directories or exploit unpatched vulnerabilities.

Proof of Concept (PoC):

```
L$ nikto -h http://192.168.56.104
- Nikto v2.5.0

+ Target IP: 192.168.56.104
+ Target Hostname: 192.168.56.104
+ Target Port: 80
+ Start Time: 2025-08-22 04:12:20 (GMT-4)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
```

Requesting you to review and patch these issues promptly to harden the application's security posture. Please confirm once fixes are applied.

Best regards,
Hilary H. Joachim

2.Reconnaissance Example (dvwa.co.uk (104.21.32.202)

Step 1

During this reconnaissance exercise, I conducted a comprehensive open-source intelligence (OSINT) gathering and asset mapping exercise targeting IP address 104.21.32.202. This step is critical for building an understanding of the target's digital footprint before proceeding with vulnerability scanning and penetration testing.

Step 2 – Search on Shodan “104.21.32.202”

Shodan

Maps

Images

Monitor

Developer

More...

SHODAN

Explore

Pricing

Search

104.21.32.202

Regular View

Raw Data

Timeline

// TAGS:

cdn

General Information

Country

United States

City

San Francisco

Organization

Cloudflare, Inc.

ISP

Cloudflare, Inc.

ASN

AS13335

Web Technologies

CDN

Open Ports

80

443

2052

2082

2083

2086

2087

2096

8080

8443

8888

// 80 / TCP

CloudFlare

Direct IP access not allowed | Cloudflare

HTTP/1.1 403 Forbidden

Date: Thu, 21 Aug 2025 23:28:01 GMT

Content-Type: text/html; charset=UTF-8

Content-Length: 6234

Connection: close

X-Frame-Options: SAMEORIGIN

Referrer-Policy: same-origin

Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Expires: Thu, 01 Jan 1970 00:00:01 GMT

Vary: Accept-Encoding

Server: CloudFlare

Step 3 – Results Found

Timestamp	Tool	Finding
2025-08-22 16:48:00	Shodan	Target IP: 104.21.94.204 (Cloudflare)
2025-08-22 16:49:00	Shodan	Location: San Francisco, US (ASN: AS13335)
2025-08-22 16:50:00	Shodan	Open ports: 80, 443, 8080, 8443, 8888
2025-08-22 16:51:00	WHOIS	Domain: testphp.vulnweb.com
2025-08-22 16:55:00	Sublist3r	Found: admin.testphp.vulnweb.com
2025-08-22 16:56:00	Wappalyzer	Technology: PHP, Apache, MySQL
2025-08-22 16:57:00	Maltego	Infrastructure relationship mapped

Summary:

Shodan reconnaissance revealed testphp.vulnweb.com hosted on Cloudflare infrastructure (104.21.94.204) in San Francisco. Multiple ports exposed including HTTP/HTTPS and high-numbered development ports. Direct IP access blocked by Cloudflare proxy with security headers