Web Server Enumeration & Misconfiguration Lab

Lab Environment: Docker Debian Web Server (Apache 2.4.66)

Author: Shimon Talukder Raj

Date: 2026-02-13 06:08 Pm

1. Executive Summary

Purpose: Demonstrate web server security assessment in a controlled lab.
Scope: Local Docker container lab.
Key Findings:

- Directory listing enabled
- Missing security headers
- Server version disclosure
  Risk Level: Low (Lab Environment)
  Recommendation: Apply Apache hardening and security headers.

---

2. Target Information

- **Target IP:** 192.168.0.111
- **Open Ports:** 8080/tcp
- **Service:** Apache 2.4.66 (Debian)
- **Environment:** Docker Container on local WiFi network
- **Tools Used:** Nmap, Gobuster, Nikto, Curl

---

3. Methodology

1. **Port Scanning & Service Detection:** Identify active ports and services using Nmap.
2. **Directory Enumeration:** Find accessible files/directories using Gobuster.
3. **Vulnerability Scanning:** Identify misconfigurations and missing security headers using Nikto.
4. **Verification:** Accessed services via browser/curl to confirm findings.

---

4. Findings

Finding	Description	Risk	Screenshot
Directory Listing	Apache exposed directory structure	Medium	Gobuster + Browser Index Page
Server Version Disclosure	Apache 2.4.66 revealed	Low	Nmap Output
Missing Security Headers	X-Frame-Options & X-Content-Type-Options missing	Medium	Nikto Output

5. Recommendations

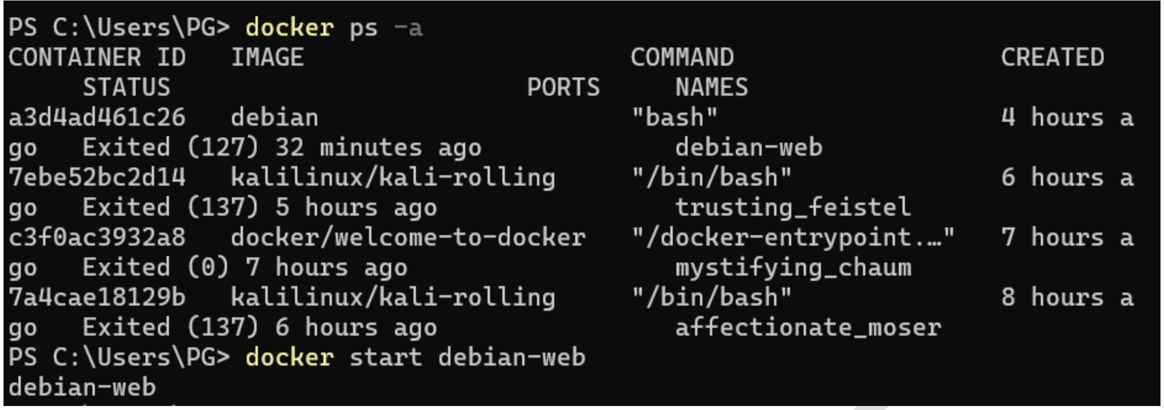
- Disable directory listing (`Options -Indexes`)
- Hide Apache version (`ServerTokens Prod`)
- Add security headers:
  - `X-Frame-Options: SAMEORIGIN`
  - `X-Content-Type-Options: nosniff`

6. Conclusion

- Lab successfully demonstrates web server enumeration and misconfiguration exploitation.
- Provides a baseline for future Red Team exercises and controlled penetration testing scenarios.

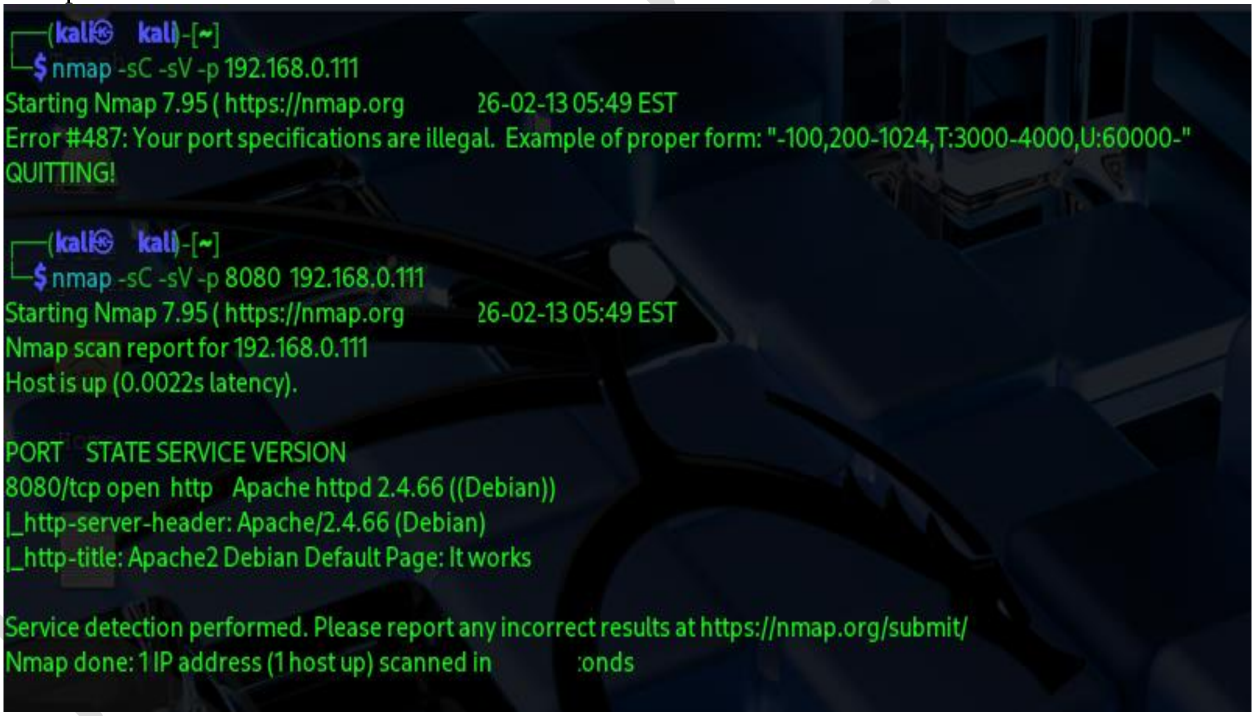
7. Appendix / Screenshots

- Docker running container (`docker ps`)



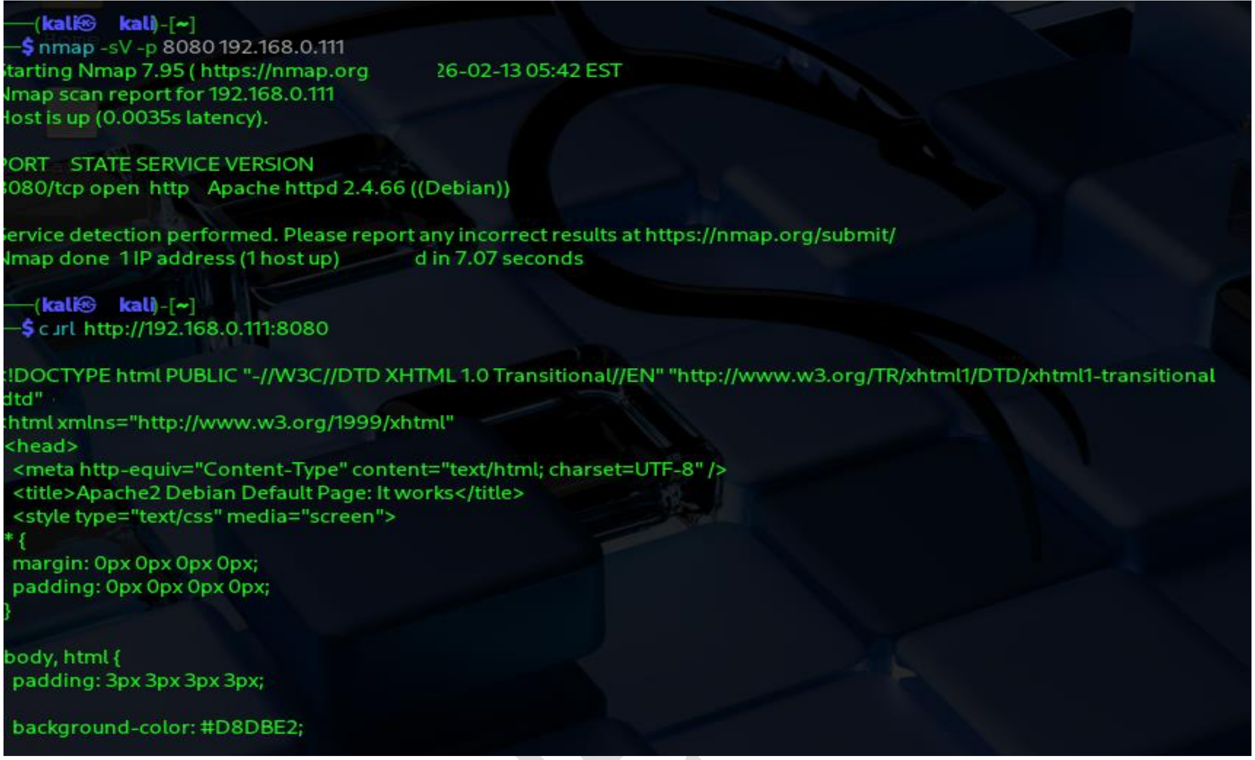
```
PS C:\Users\PG> docker ps -a
CONTAINER ID   IMAGE                            COMMAND                  CREATED
     STATUS                          PORTS     NAMES
a3d4ad461c26   debian                           "bash"                   4 hours a
go   Exited (127) 32 minutes ago                  debian-web
7ebe52bc2d14   kalilinux/kali-rolling           "/bin/bash"              6 hours a
go   Exited (137) 5 hours ago                     trusting_feistel
c3f0ac3932a8   docker/welcome-to-docker         "/docker-entrypoint.…"   7 hours a
go   Exited (0) 7 hours ago                       mystifying_chaum
7a4cae18129b   kalilinux/kali-rolling           "/bin/bash"              8 hours a
go   Exited (137) 6 hours ago                     affectionate_moser
PS C:\Users\PG> docker start debian-web
debian-web
```

- Nmap scan result



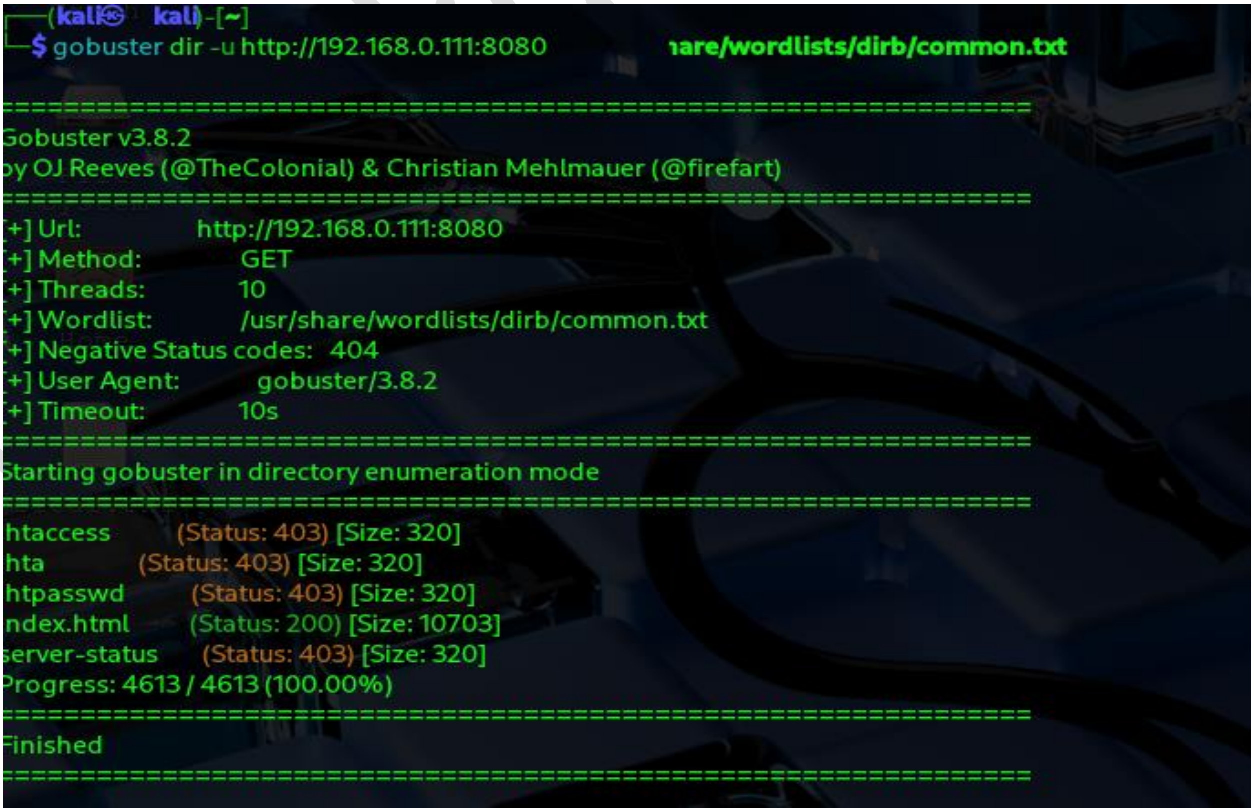
```
┌──(kali㉿ kali)-[~]
└─$ nmap -sC -sV -p 192.168.0.111
Starting Nmap 7.95 ( https://nmap.org          26-02-13 05:49 EST
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(kali㉿ kali)-[~]
└─$ nmap -sC -sV -p 8080  192.168.0.111
Starting Nmap 7.95 ( https://nmap.org          26-02-13 05:49 EST
Nmap scan report for 192.168.0.111
Host is up (0.0022s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache httpd 2.4.66 ((Debian))
|_http-server-header: Apache/2.4.66 (Debian)
|_http-title: Apache2 Debian Default Page: It works

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

- Nmap and curl scan result



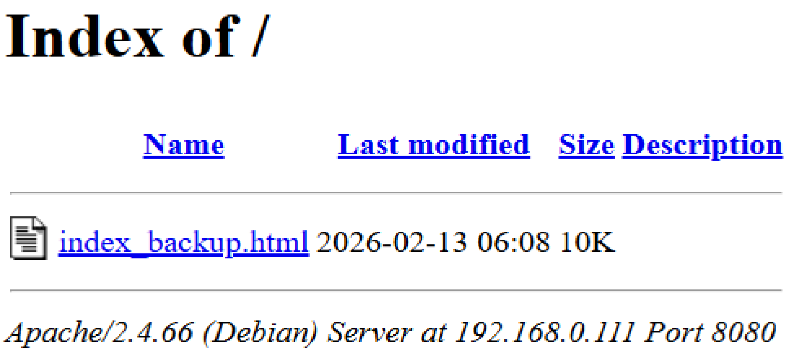
```
──(kali㉿ kali)-[~]
─$ nmap -sV -p 8080 192.168.0.111
tarting Nmap 7.95 ( https://nmap.org          26-02-13 05:42 EST
Imap scan report for 192.168.0.111
Host is up (0.0035s latency).

PORT    STATE SERVICE VERSION
8080/tcp open  http    Apache httpd 2.4.66 ((Debian))

ervice detection performed. Please report any incorrect results at https://nmap.org/submit/
Imap done  1 IP address (1 host up)            d in 7.07 seconds

──(kali㉿ kali)-[~]
─$ c ɹrl  http://192.168.0.111:8080

:!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional
dtd"
:html xmlns="http://www.w3.org/1999/xhtml"
<head>
 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
 <title>Apache2 Debian Default Page: It works</title>
 <style type="text/css" media="screen">
* {
 margin: 0px 0px 0px 0px;
 padding: 0px 0px 0px 0px;
}

body, html {
 padding: 3px 3px 3px 3px;

 background-color: #D8DBE2;
```

- Gobuster scan result



```
┌──(kali㉿ kali)-[~]
└─$ gobuster dir -u http://192.168.0.111:8080              ıare/wordlists/dirb/common.txt

===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                   http://192.168.0.111:8080
[+] Method:                GET
[+] Threads:               10
[+] Wordlist:              /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:            gobuster/3.8.2
[+] Timeout:               10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
htaccess          (Status: 403) [Size: 320]
hta               (Status: 403) [Size: 320]
htpasswd          (Status: 403) [Size: 320]
ndex.html         (Status: 200) [Size: 10703]
erver-status      (Status: 403) [Size: 320]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

- Browser showing directory listing (`Index of /`)

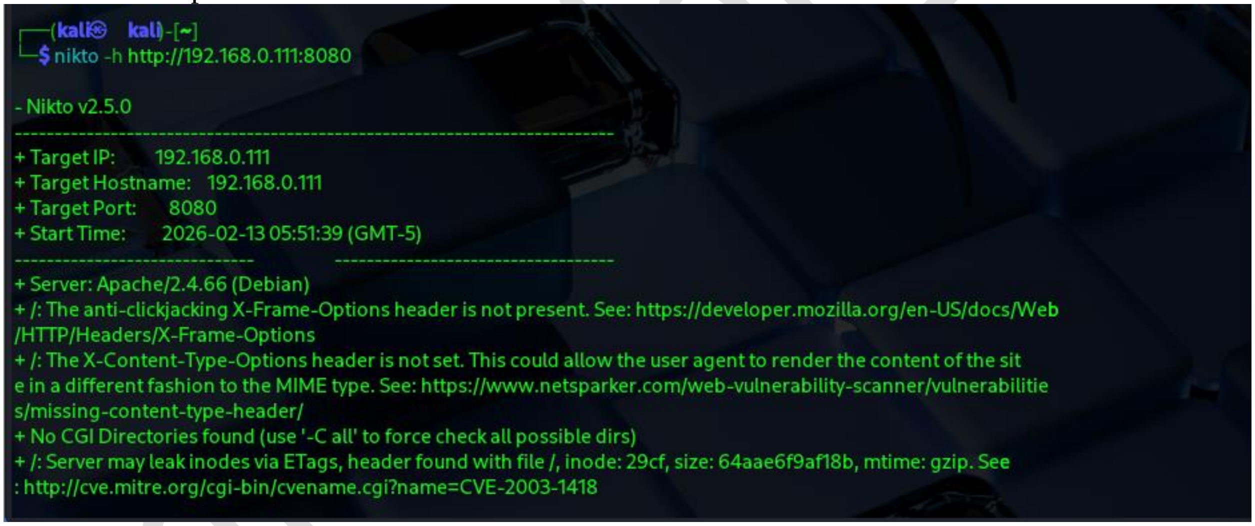


Index of /

Name	Last modified	Size	Description
🗎 index_backup.html	2026-02-13 06:08	10K	

Apache/2.4.66 (Debian) Server at 192.168.0.111 Port 8080

Nikto scan output



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.0.111:8080

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.0.111
+ Target Hostname:    192.168.0.111
+ Target Port:        8080
+ Start Time:         2026-02-13 05:51:39 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.66 (Debian)
+ /: 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 sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 64aae6f9af18b, mtime: gzip. See
: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
```