

Challenge 2

Target: 10.5.5.12

Vulnerability: Information Disclosure (Directory Indexing)

1. Executive Summary

During the reconnaissance phase, the web server at 10.5.5.12 was found to be misconfigured. Specifically, directory indexing was enabled on sensitive folders. This allowed for the manual traversal of the file system via a web browser, leading to the discovery of sensitive files and the "Challenge 2" flag.

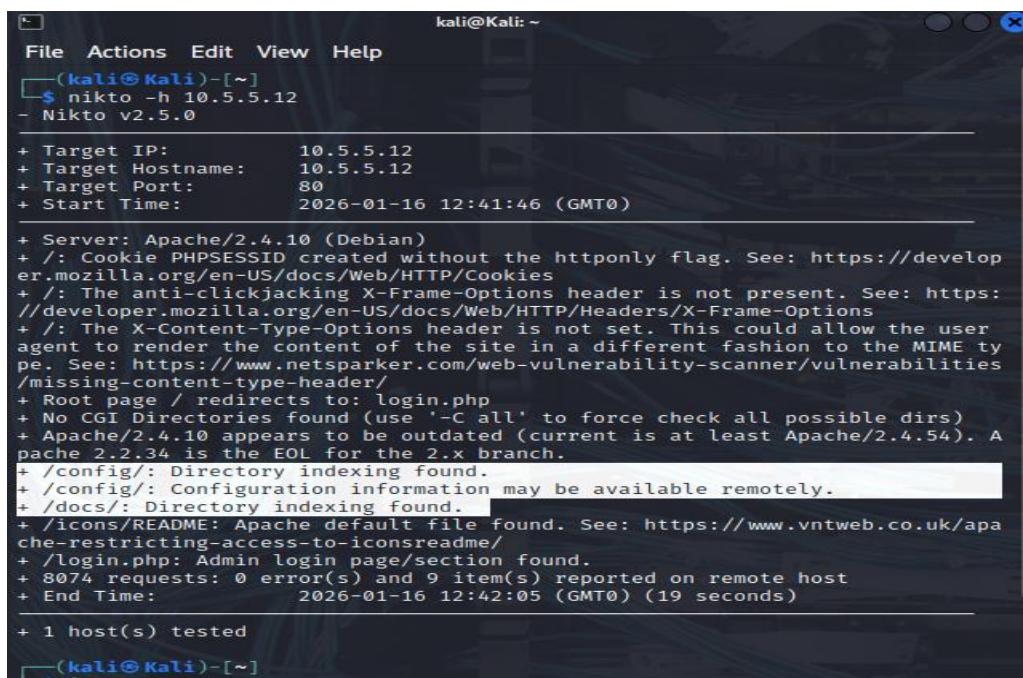
2. Reconnaissance & Discovery

Using the vulnerability scanner **Nikto**, the following directories were identified as having "Directory Indexing" enabled:

- /config/
- /docs/

Tools Used:

- **Nikto:** nikto -h 10.5.5.12



The screenshot shows a terminal window titled 'kali@Kali: ~'. The user runs the command '\$ nikto -h 10.5.5.12' followed by the Nikto version 'Nikto v2.5.0'. The output details the target configuration and various findings:

```
kali@Kali: ~
File Actions Edit View Help
[(kali㉿Kali)-[~]]$ nikto -h 10.5.5.12
- Nikto v2.5.0

+ Target IP:          10.5.5.12
+ Target Hostname:   10.5.5.12
+ Target Port:        80
+ Start Time:        2026-01-16 12:41:46 (GMT0)

+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: 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)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). A apache 2.2.34 is the EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2026-01-16 12:42:05 (GMT0) (19 seconds)

+ 1 host(s) tested

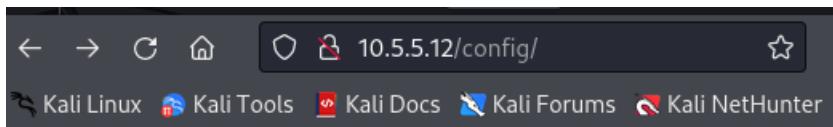
[(kali㉿Kali)-[~]]$
```

3. Exploitation (Directory Traversal)

By navigating to these directories directly in a web browser, the file structure was visible without authentication.

- **Subdirectories accessed:** /config/ and /docs/
- **Filename found:** db_form.html
- **Location:** /config/

Proof of Concept:

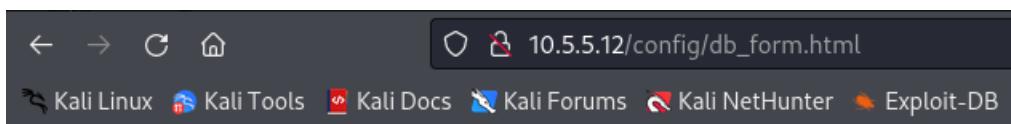


Index of /config

Name	Last modified	Size	Description
Parent Directory		-	
config.inc.php	2017-10-31 17:28	1.9K	
db_form.html	2012-12-07 00:00	1.3K	

Apache/2.4.10 (Debian) Server at 10.5.5.12 Port 80

The flag file was opened, revealing the following message/code: **Flag Code:** aWe-4975



Great work!

You found the flag file for *Challenge 2*!

The code for this flag is: **aWe-4975**

4. Remediation Recommendations

To mitigate the risk of information disclosure through directory listing, the following steps are recommended:

1: Server Configuration

Disable the `Indexes` option in the web server configuration file.

2: Index Placeholder Files

Place a default index file (e.g., `index.html` or `index.php`) in every directory. This prevents the server from displaying the file list even if directory indexing is technically enabled.