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:

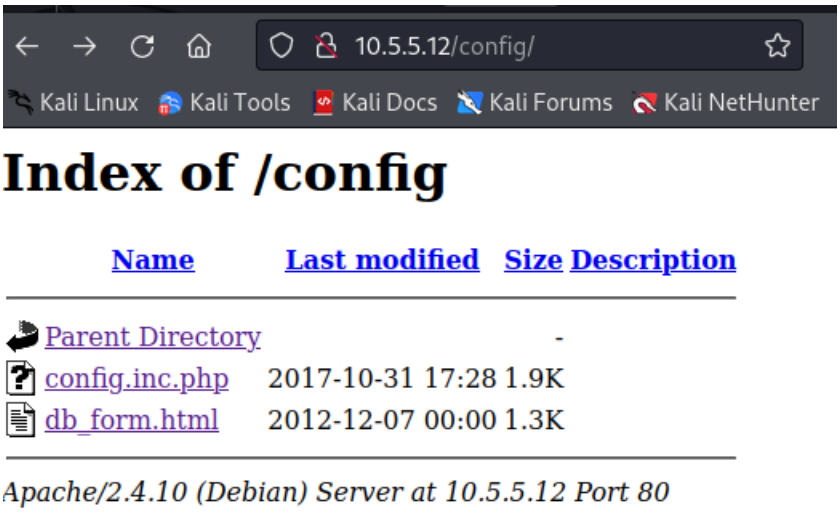
- **Nikto:** `nikto -h 10.5.5.12`

3. Exploitation (Directory Traversal)

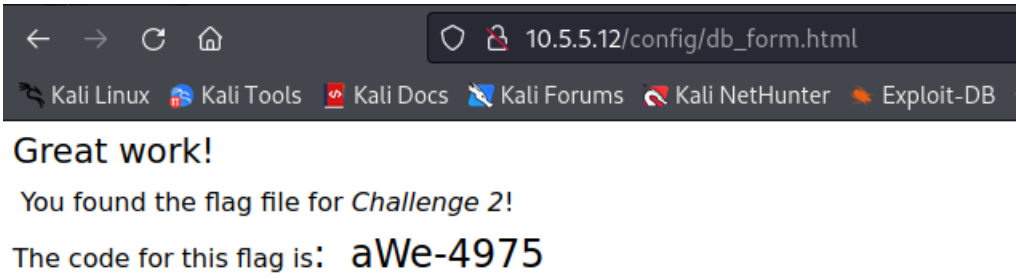
By navigating to these directories directly in a web browser, the file structure was visible without authentication.

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

Proof of Concept:



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