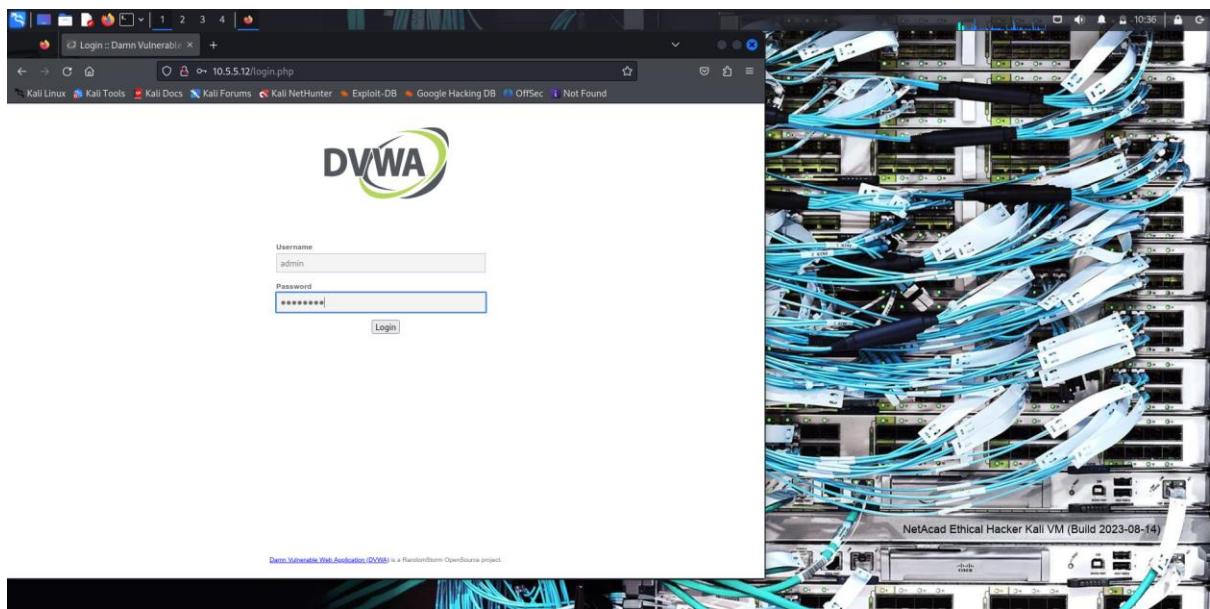


Challenge 2: Web Server Vulnerabilities

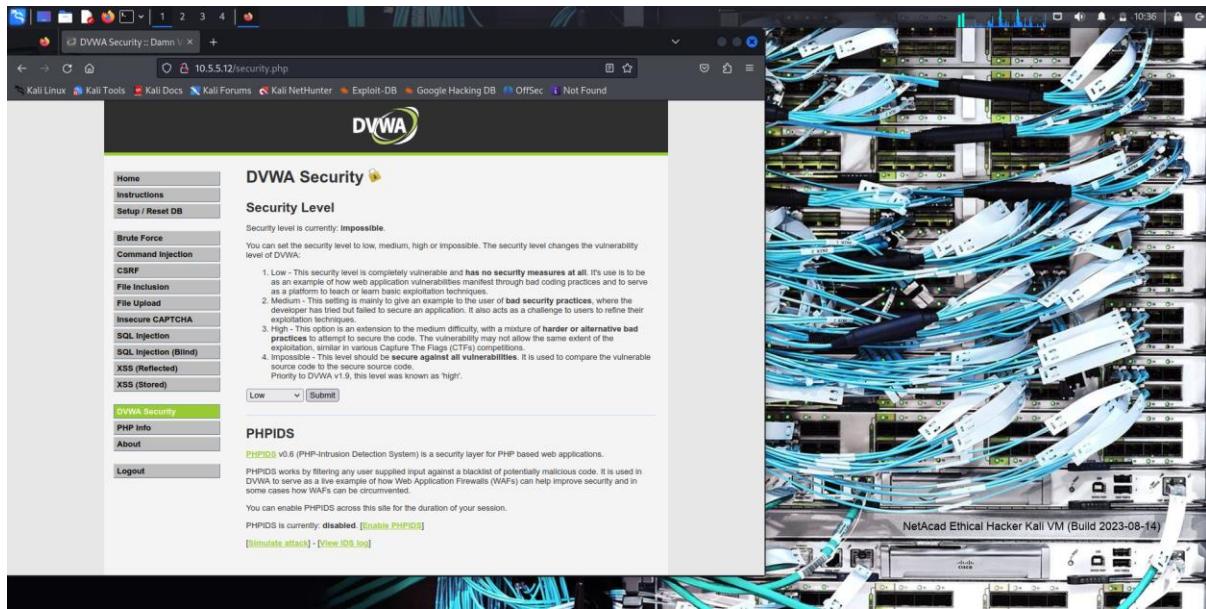
In this challenge, I found vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in the directories on the server. You can use any tool for reconnaissance to find vulnerabilities in the directories and locate the file in a vulnerable directory on a web server.

Step 1: Preliminary setup

Log into the server at 10.5.5.12 with the username: admin and password: password

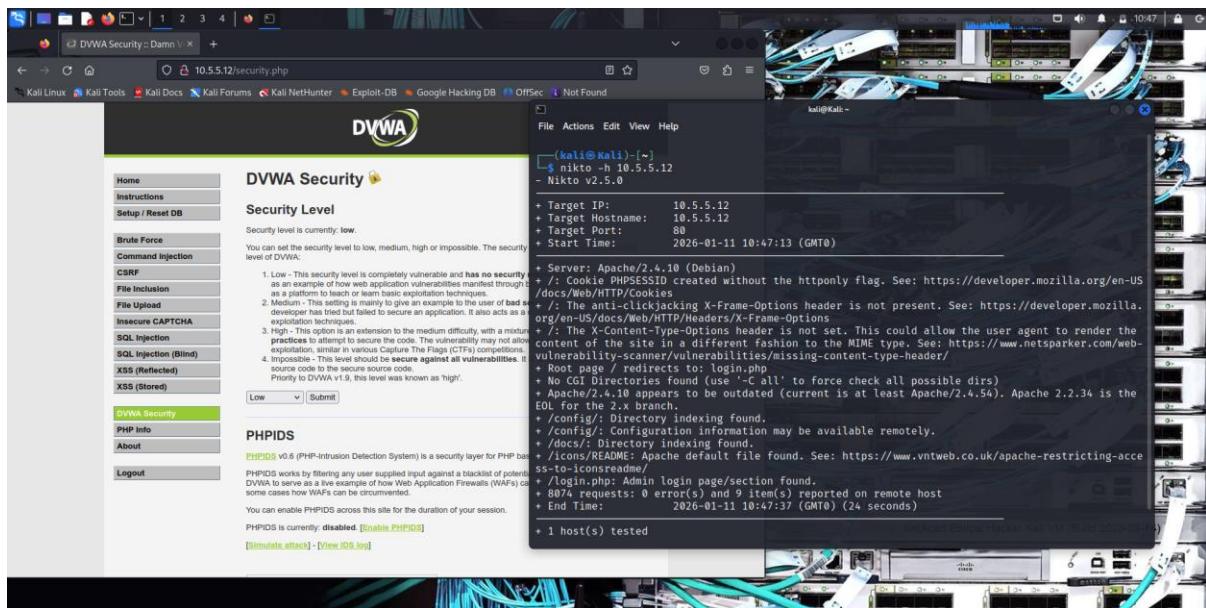


Set the application security to low and then click submit

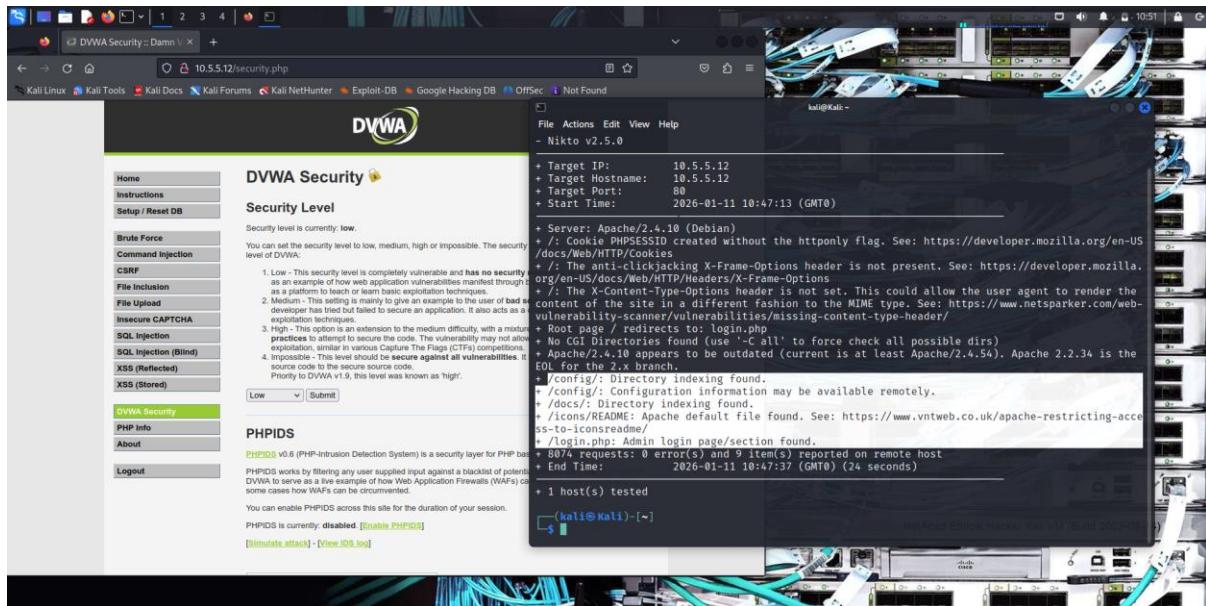


Step 2: From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation

Perform reconnaissance on the server to find directories where indexing was found using nikto command: nikto –h 10.5.5.12

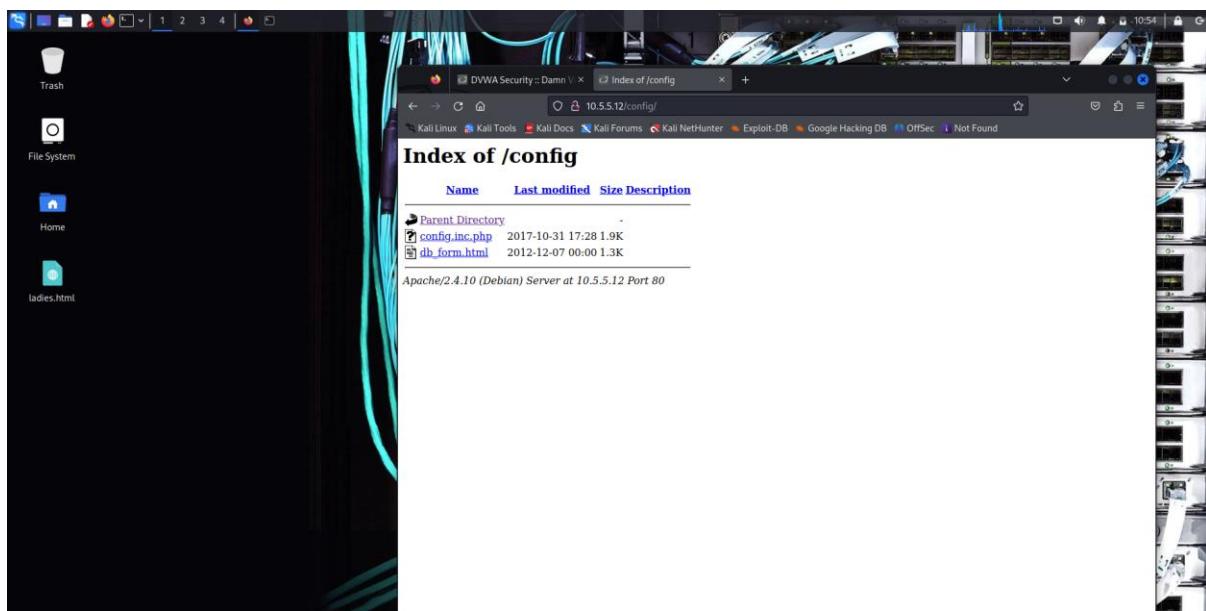


Some directories can be accessed through a web browser to list the files and subdirectories that they contain



Step 3: View the files contained in each directory to find the db_form.html file.

Create a URL in the web browser to access the viewable subdirectories and find the file with the code for challenge 2 located in one of the subdirectories



In which two subdirectories can the file be located

DVWA Security

Security Level

Security level is currently: **low**.

1. Low - This security level is completely vulnerable and has no security as an example of how web application vulnerabilities manifest through the user interface.

2. Medium - This setting is mainly to give an example to the user of bad developer has tried but failed to secure an application. It also acts as a medium difficulty for the user to learn how to fix them.

3. High - The High option is an extension to the medium difficulty, with a minor practices to attempt to secure the code. The vulnerability may not allow for a full exploit but will still be a challenge for the user to fix.

4. Impossible - This level should be secure against all vulnerabilities. Prior to DVWA v1.9, this level was known as 'high'.

Low Submit

PHPIDIS

PHPIDS v0.8 (PHP-Intrusion Detection System) is a security layer for PHP based applications. PHPIDS works by filtering any user supplied input against a blacklist of potential DVWA to serve as a live example of how Web Application Firewalls (WAFs) can some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Bimote attack] - [View ID9 flag]

Nikto v2.5.0

- + Target IP: 10.5.5.12
- + Target Hostname: 10.5.5.12
- + Target Port: 80
- + Start Time: 2026-01-11 10:47:13 (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
- + /: 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). Apache 2.2.34 is the EOL for the 2.x branch.
- + /config/: Directory indexing found.
- + /docs/: Configuration information may be available remotely.
- + /icons/README: Apache default file found. See: https://www.vmtweb.co.uk/apache-restricting-access-to-iconreadme/
- + /login.php: Admin login page/section found.
- + 8074 requests: 0 error(s) and 9 item(s) reported on remote host
- + End Time: 2026-01-11 10:47:37 (GMT0) (24 seconds)
- + 1 host(s) tested

What is the file name with the challenge 2 code

DVWA Security - Damn Vulnerable Web Application

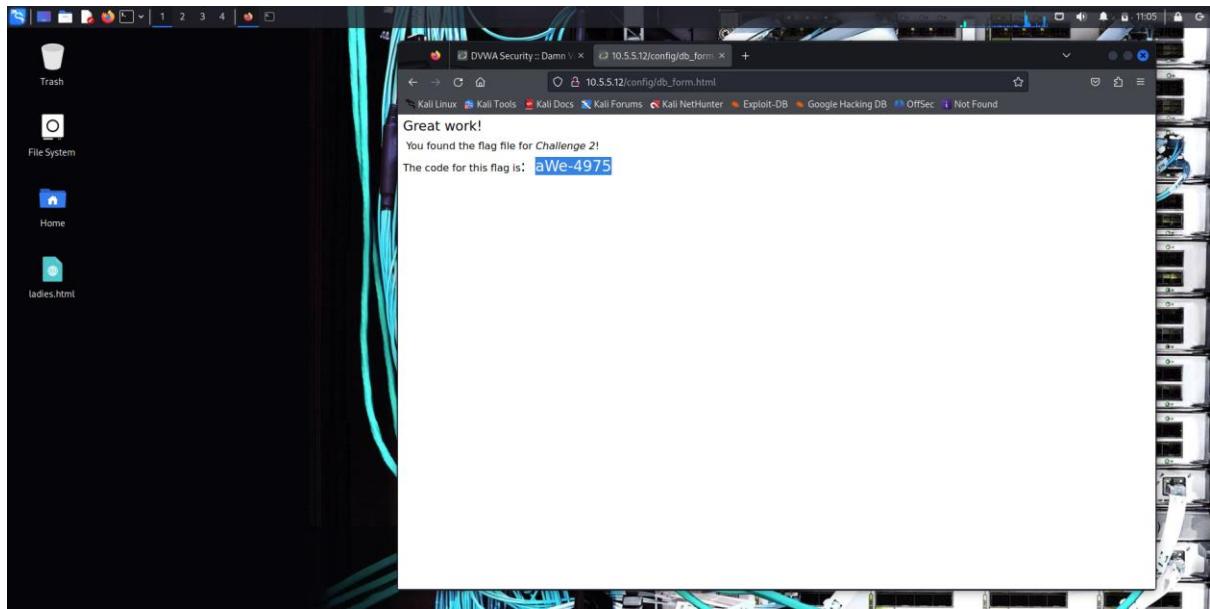
Index of /config

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

What is the message contained in the flag file

"Great Work"



Step 4: Research and propose directory listing exploit remediation

- Disabling directory listing in your web server
- Placing a default index file e.g. index.html