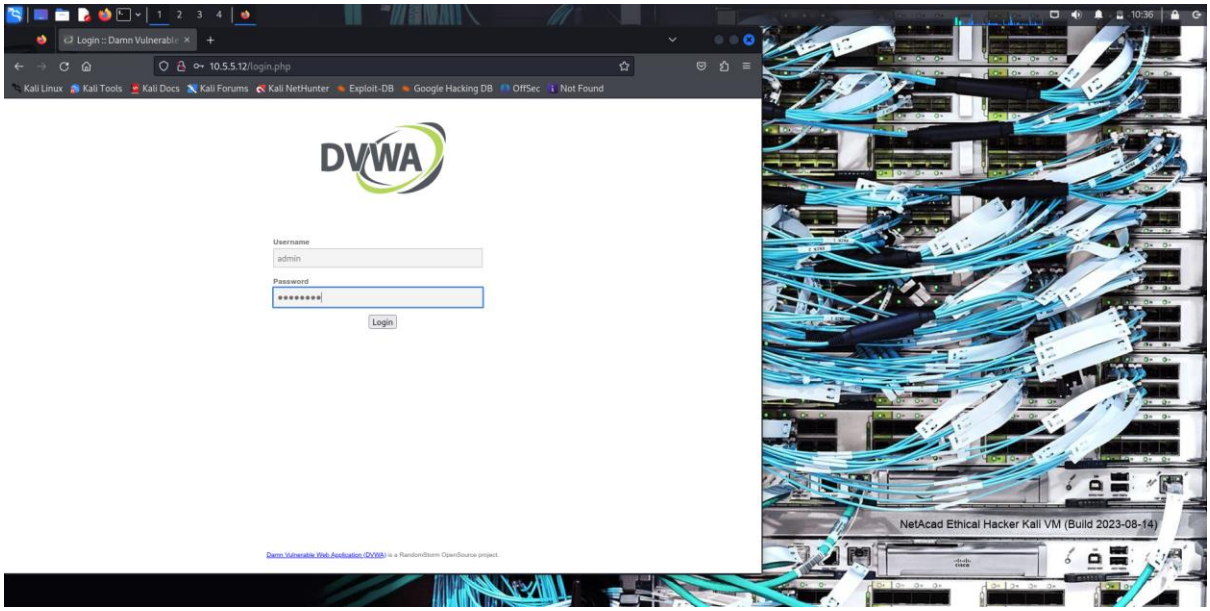
Challenge 2: Web Server Vulnerabilities

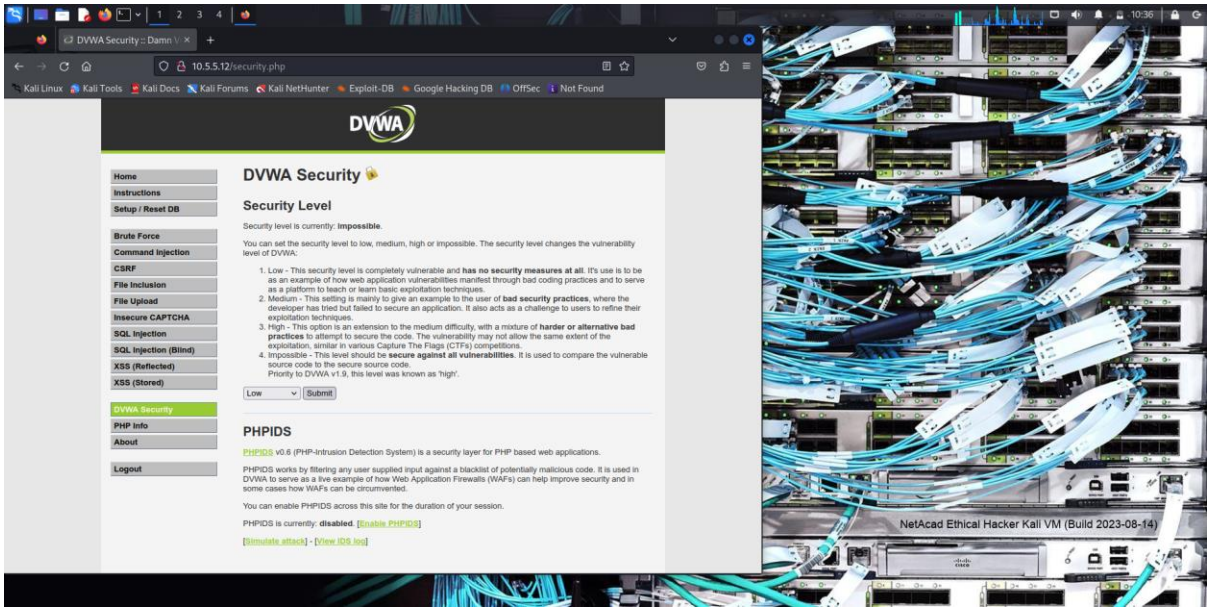
In this challenge, I found vulnerabilities on an HTTP server. Misconfiguration of a web server can allow for the listing of files contained in the directories on the server. You can use any tool for reconnaissance to find vulnerabilities in the directories and locate the file in a vulnerable directory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

Step 1: Preliminary setup

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

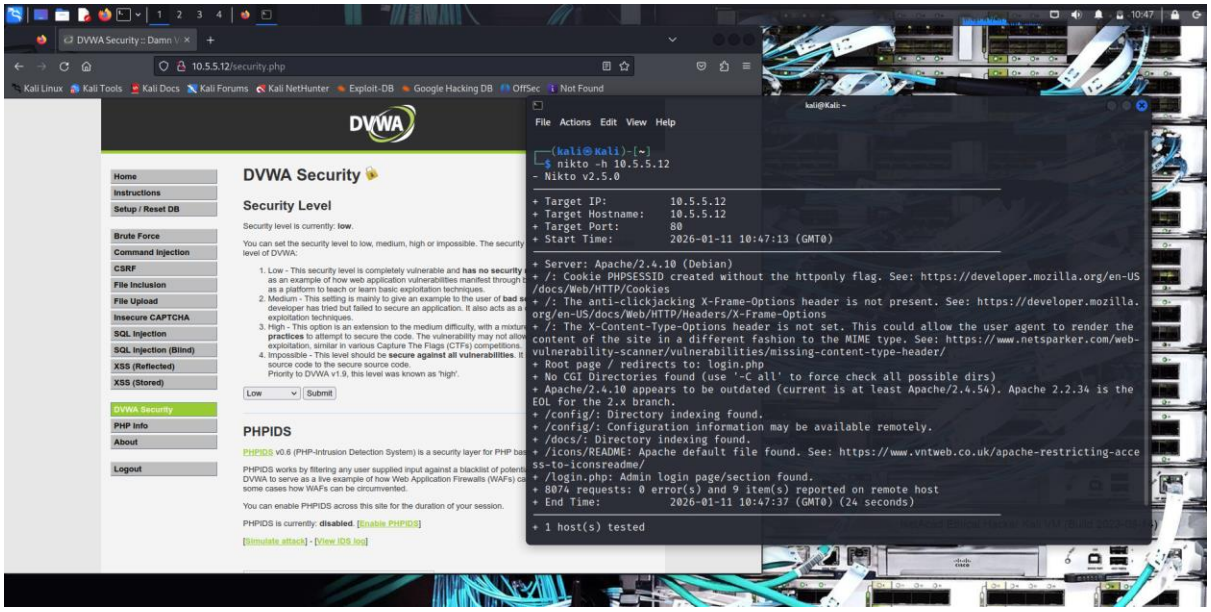


Set the application security to low and then click submit

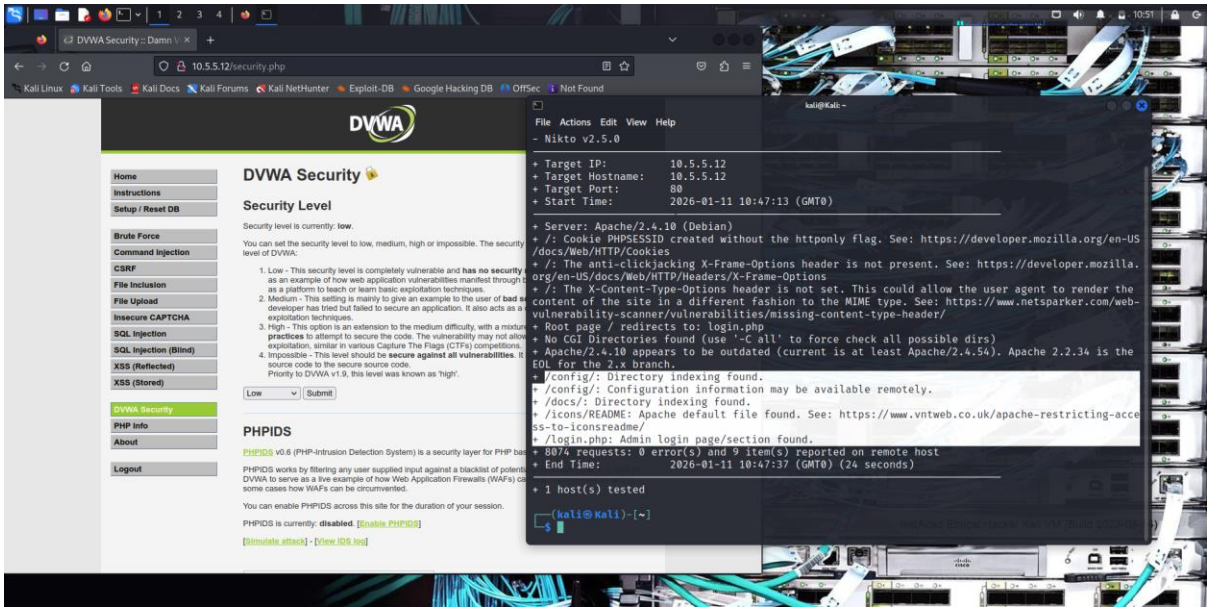


Step 2: From the results of your reconnaissance, determine which directories are viewable using a web browser and URL manipulation

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

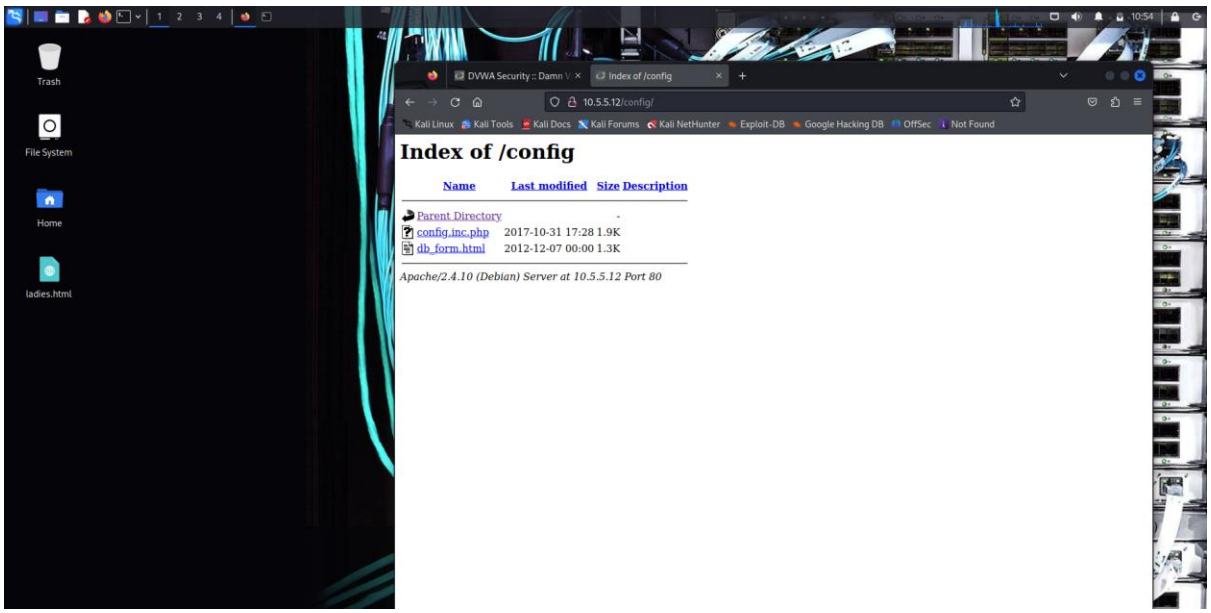


Some directories can be accessed through a web browser to list the files and subdirectories that they contain

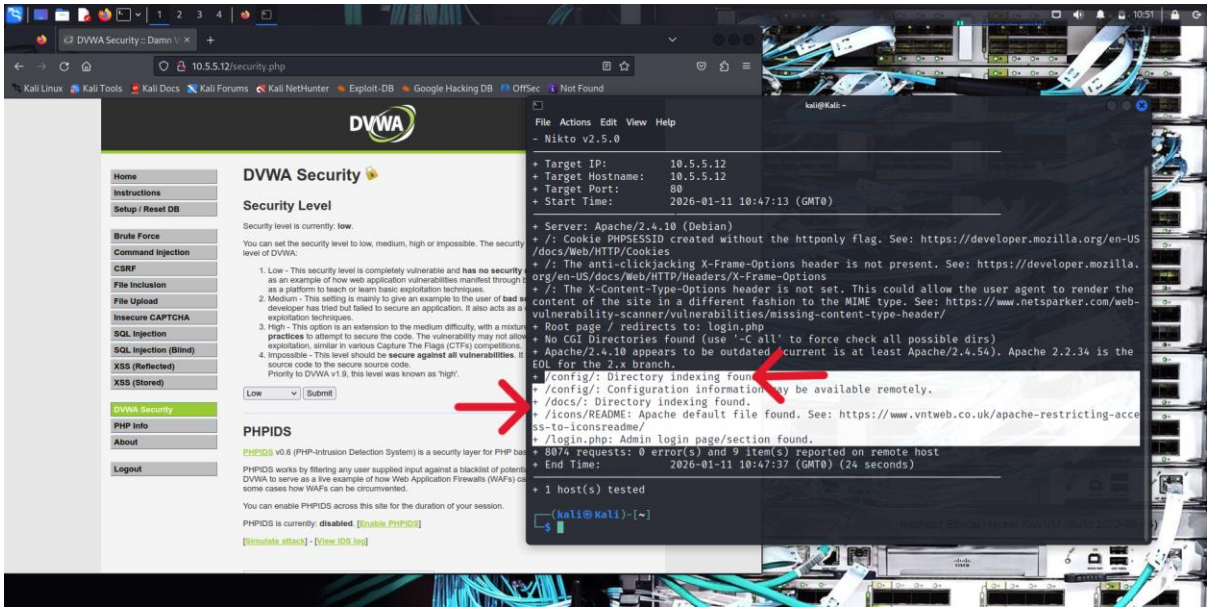


Step 3: View the files contained in each directory to find the db_form.html file.

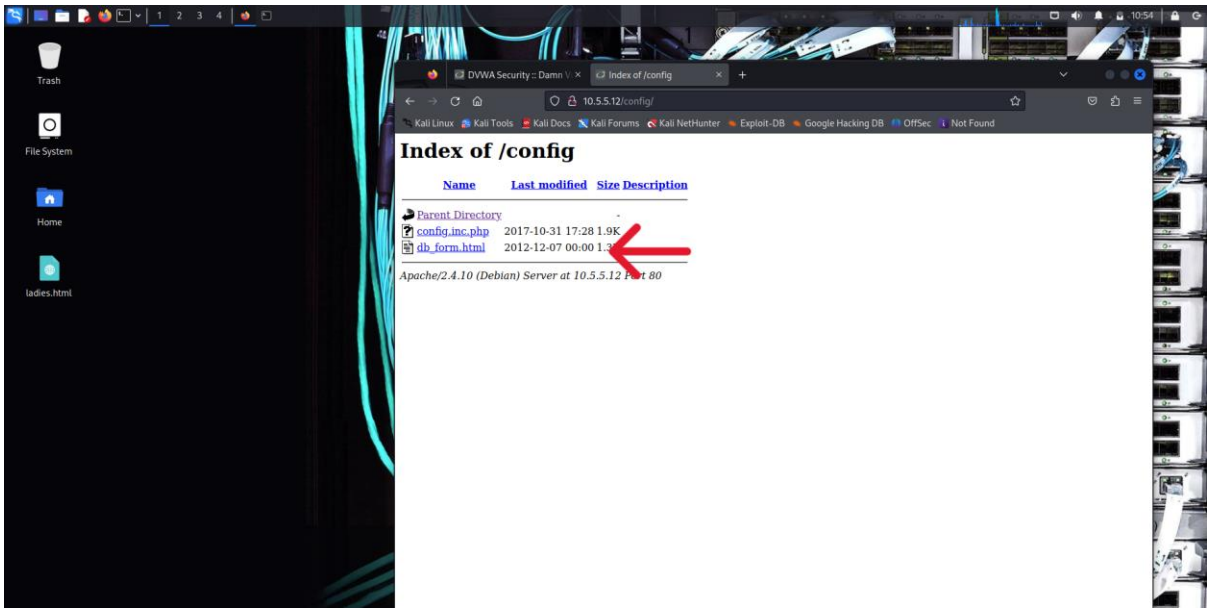
Create a URL in the web browser to access the viewable subdirectories and find the file with the code for challenge 2 located in one of the subdirectories



In which two subdirectories can the file be located

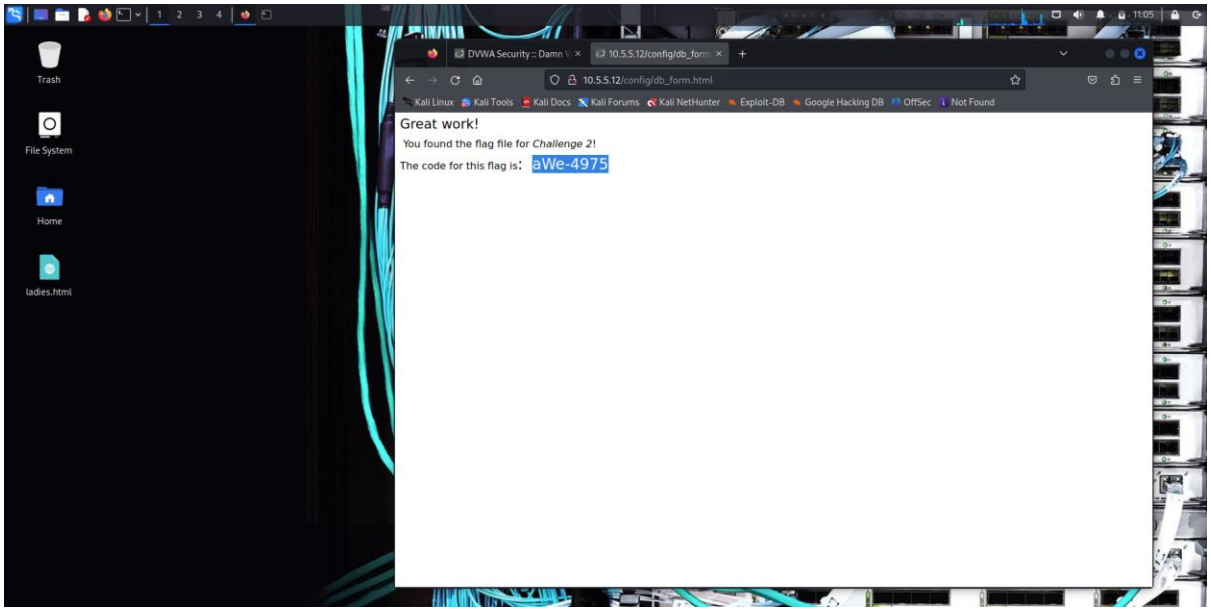


What is the file name with the challenge 2 code



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