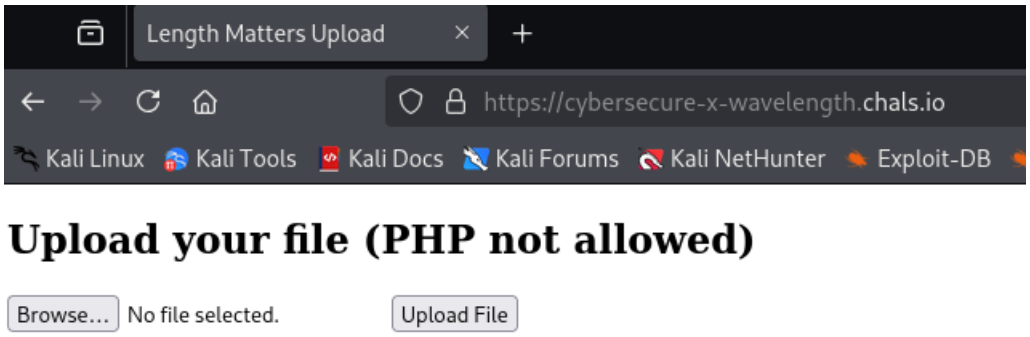
🌐 Challenge Name: Wavelength – (350) (Web)

I opened the challenge URL and saw a basic HTML upload form that says:



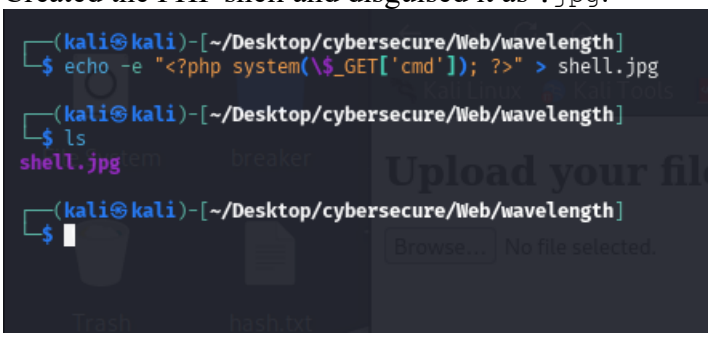
⚙️ Bypass Strategy

The filter says “PHP not allowed,” but doesn't check actual content — only the filename/extension. So, we:

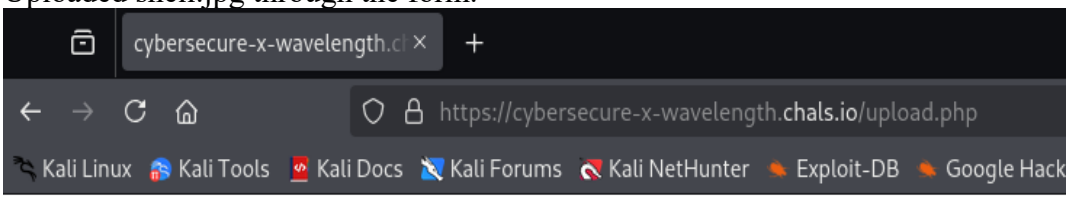
1. Write a simple PHP shell into a file **named like an image**.
2. Upload it.
3. Access it via URL and use the cmd parameter to run commands.

💣 Payload

- Created the PHP shell and disguised it as `.jpg`:



- Uploaded shell.jpg through the form.



File uploaded to: uploads/shell.jpg

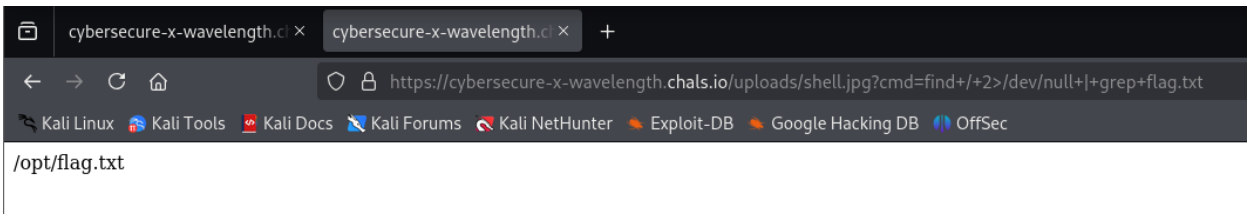
- Then accessed it:

uid=33(www-data) gid=33(www-data) groups=33(www-data)

- This confirmed RCE (Remote Command Execution) works.

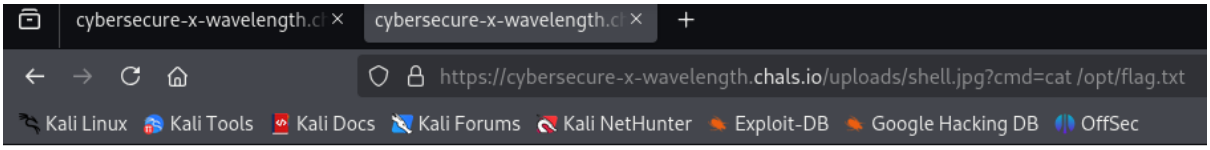
🔍 Locating the Flag

Used find to search the whole server:



Found path: **/opt/flag.txt**

Then dumped the flag:



FLAG{rce_filename_bypass_1337}

🏁 Flag Captured

Success. Upload filter was weak — blocked .php extension but not PHP code inside other filetypes.

FLAG: FLAG{rce_filename_bypass_1337}

~By Team justahacker