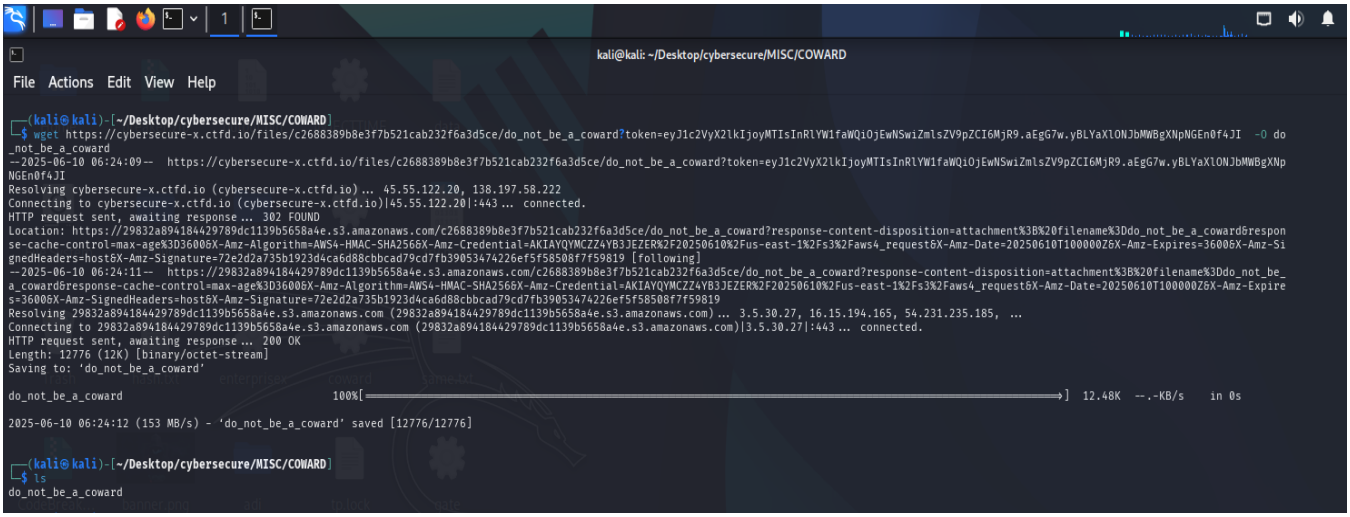
🧩 Challenge: COWARD!! (200 points) (MISC)

The challenge provided a downloadable file named **do_not_be_a_coward**.
I used **wget** to grab it:



I ran the file command to identify it:

```
(kali㉿kali)-[~/Desktop/cybersecure/MISC/COWARD]
$ file do_not_be_a_coward
do_not_be_a_coward: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), BuildID[sha1]=0c512f0cf21010bff3a6258d135cdeca80ea04d9, for GNU/Linux 3.2.0, statically linked, no section header
```

I made it executable with:

```
(kali㉿kali)-[~/Desktop/cybersecure/MISC/COWARD]
$ chmod +x do_not_be_a_coward
```

Then I executed the file:

The program simulated a **fake hacking environment**, with messages about system compromise and payload deployment.

Waited for the Fake Payload Countdown

After a dramatic countdown, the program displayed a **message revealing the flag**.

FLAG: flag{h4ck3r_m0d3_4ct1v4t3d_5ucc355fully!}

~By Team justahacker