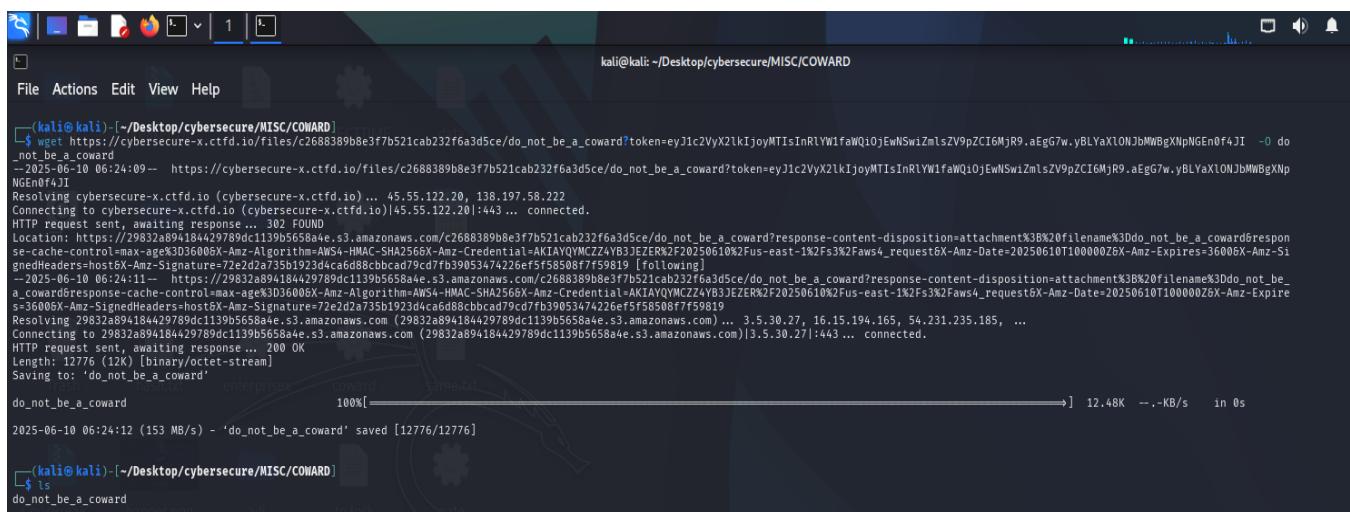


Challenge: COWARD!! (200 points) (MISC)



The challenge provided a downloadable file named **do_not_be_a_coward**.

I used **wget** to grab it:

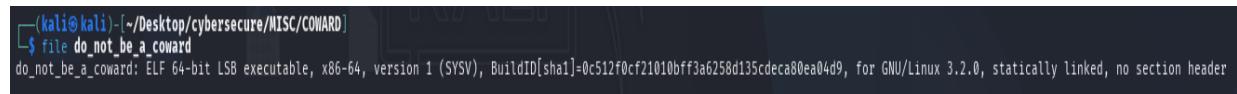


```
(kali㉿kali)-[~/Desktop/cybersecure/MISC/COWARD]
$ wget https://cybersecure-x.ctfd.io/files/c2688389b8e3f7b521cab232f6a3d5ce/do_not_be_a_coward?token=eyJ1c2VyX2lkIjoyMTIsInRlYw1faWQjOjEwNSw1ZmlsZV9pZCI6MjR9.aEgG7w.yBLyaXlONjbMWBgXNpNGEn0f4JI -O do_not_be_a_coward
--2025-06-10 06:24:09-- https://cybersecure-x.ctfd.io/files/c2688389b8e3f7b521cab232f6a3d5ce/do_not_be_a_coward?token=eyJ1c2VyX2lkIjoyMTIsInRlYw1faWQjOjEwNSw1ZmlsZV9pZCI6MjR9.aEgG7w.yBLyaXlONjbMWBgXNpNGEn0f4JI
Resolving cybersecure-x.ctfd.io (cybersecure-x.ctfd.io) ... 45.55.122.20, 138.197.58.222
Connecting to cybersecure-x.ctfd.io (cybersecure-x.ctfd.io)|45.55.122.20|:443 ... connected.
HTTP request sent, awaiting response ... 302 FOUND
Location: https://9832a89418429789dc1139b5658a4e.s3.amazonaws.com/c2688389b8e3f7b521cab232f6a3d5ce/do_not_be_a_coward?response-content-disposition=attachment%3B%20filename%3Ddo_not_be_a_coward&response-cache-control=max-age=303600&X-Amz-Credential=AKIAVQMCZ24Y83JEZER2F20250610%2Fus-east-1%2F53%2Faws4,_requestX-Amz-Expires=3000X-SignedHeaders=host&X-Amz-Signature=7ed2a735b1923dc4ad088cbcad79cd7fb3905347426ef5f58508f7f59819 ... Following
--2025-06-10 06:24:10-- https://9832a89418429789dc1139b5658a4e.s3.amazonaws.com/c2688389b8e3f7b521cab232f6a3d5ce/do_not_be_a_coward?response-content-disposition=attachment%3B%20filename%3Ddo_not_be_a_coward&response-cache-control=max-age=303600&X-Amz-Credential=AKIAVQMCZ24Y83JEZER2F20250610%2Fus-east-1%2F53%2Faws4,_requestX-Amz-Expires=3000X-SignedHeaders=host&X-Amz-Signature=7ed2a735b1923dc4ad088cbcad79cd7fb3905347426ef5f58508f7f59819
Resolving 9832a89418429789dc1139b5658a4e.s3.amazonaws.com (9832a89418429789dc1139b5658a4e.s3.amazonaws.com) ... 3.5.30.27, 16.15.194.165, 54.231.235.185, ...
Connecting to 9832a89418429789dc1139b5658a4e.s3.amazonaws.com (9832a89418429789dc1139b5658a4e.s3.amazonaws.com)|3.5.30.27|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 12776 (12K) [binary/octet-stream]
Saving to: 'do_not_be_a_coward'

do_not_be_a_coward          [  0.0%]  12.48K --.-KB/s   in 0s
2025-06-10 06:24:12 (153 MB/s) - 'do_not_be_a_coward' saved [12776/12776]

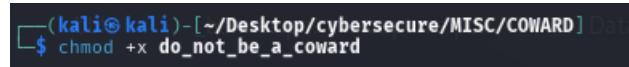
(kali㉿kali)-[~/Desktop/cybersecure/MISC/COWARD]
$ ls
do_not_be_a_coward
```

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:

```
(kali㉿kali)-[~/Desktop/cybersecure/MISC/COWARD]
$ ./do_not_be_a_coward
[sudo] password for kali:
[CRITICAL ALERT] SYSTEM COMPROMISE DETECTED!
[WARNING] s{zxvjhvijzfjeyDfef`ifedDfe`v`fyftehqDrfyjzhvqlll
[ALERT] skhfID izfr idDpf10rfyjzhvqlll
[STATUS] czhfedDtirhzDrfyjzhvqD`iDrzlll
[SYSTEM SECURITY] Do not attempt to exit this program repeatedly or you may cause an irreversible system crash!

[SYSTEM] Spawning infiltration processes ...
[SYSTEM] Enumerating target files ...
[SYSTEM] Injecting advanced persistent threat ...
[SYSTEM] Installing kernel-level rootkit ...
[SYSTEM] Establishing command and control channel ...
[SYSTEM] Deploying payload to /boot/vmlinuz ...
[SYSTEM] Modifying system call table...
[SYSTEM] Hooking network stack ...
[SYSTEM] Persistence mechanisms activated
[SYSTEM] Covering tracks ...
[SYSTEM] Initiating final phase ...
[TIMER] 50 seconds until final payload activation ...
[TIMER] 40 seconds until final payload activation ...
[TIMER] 30 seconds until final payload activation ...
[TIMER] 20 seconds until final payload activation ...
[TIMER] 10 seconds until final payload activation ...

[SYSTEM] All systems compromised successfully!
[SYSTEM] Total control achieved over target machine
[SYSTEM] Decrypting hidden payload ...
[SYSTEM] Access granted to secret vault

CONGRATULATIONS! YOU FOUND THE FLAG!

FLAG: flag{h4ck3r_m0d3_4ct1v4t3d_5ucc355fully!}
[SYSTEM] Challenge completed! Well done, hacker!
(kali㉿kali)-[~/Desktop/cybersecure/MISC/COWARD]
$
```

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