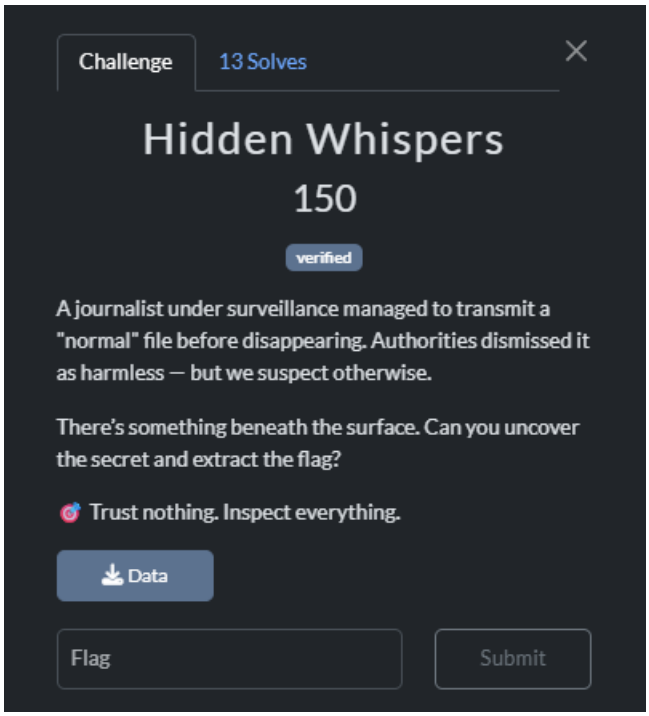
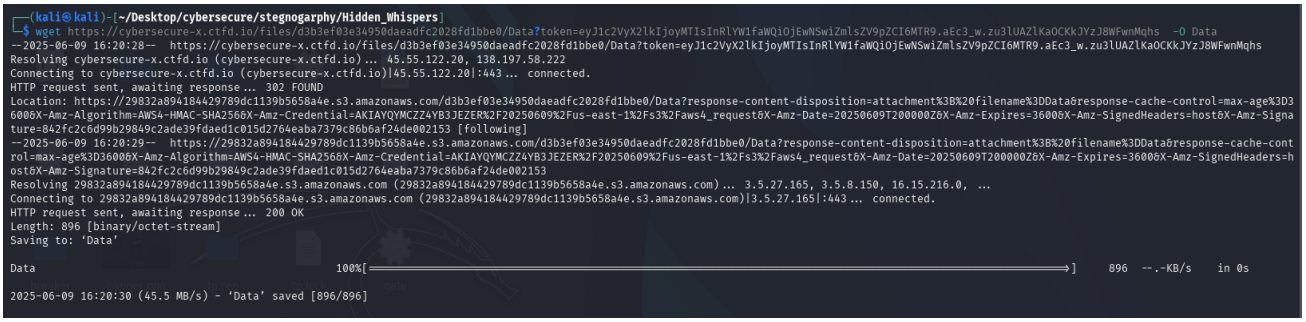
🧩 Challenge Name: Hidden Whispers — 150pts (Steganography)

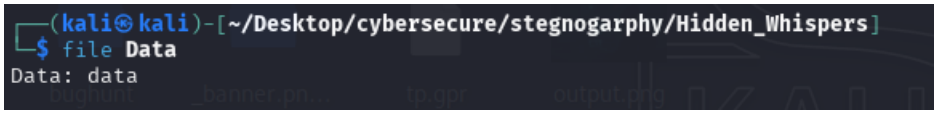


🕵️ Recon & Initial Inspection:

I downloaded the challenge file named Data using the following **wget** command:



Next, I checked the file type using the **file** command:



So, it wasn't recognized as any known file type.

Checked for strings inside:

```
┌──(kali㉿kali)-[~/Desktop/cybersecure/stegnogarphy/Hidden_Whispers]
└─$ strings Data
W%KW
XXXX
GIDATx
ZW4! L
!gLsP
Y{uRk
qu      8
}ru5
>;?Hy
IEND
```

Found PNG chunks (GIDAT, IEND), but the header started with XXXX, which is wrong.

Used hex dump to confirm:

```
┌──(kali㉿kali)-[~/Desktop/cybersecure/stegnogarphy/Hidden_Whispers]
└─$ xxd Data | head -5
00000000: 5725 4b57 0d0a 1a0a 0000 000d 5858 5858  W%KW........XXXX
00000010: 0000 0258 0000 0064 0802 0000 00d5 23d9  ...X...d......#.
00000020: 7400 0003 4749 4441 5478 9ced dadd 729b  t...GIDATx....r.
00000030: 3014 4651 d3e9 fbbf 32bd f00c 4311 3afc  0.FQ....2...C.:.
00000040: 1863 27df 5a57 3421 204c a31d 610f e338  .c'.ZW4! L..a..8
```

The PNG signature bytes should be: **89 50 4E 47 0D 0A 1A 0A** — but here it's something else.

💣 Fixing the Corrupted PNG Header:

Replaced the first 8 bytes with the correct PNG signature:

```
┌──(kali㉿kali)-[~/Desktop/cybersecure/stegnogarphy/Hidden_Whispers]
└─$ printf '\x89\x50\x4E\x47\x0D\x0A\x1A\x0A' | dd of=Data bs=1 seek=0 count=8 conv=notrunc
8+0 records in
8+0 records out
8 bytes copied, 0.000205646 s, 38.9 kB/s
```

Repaired the **IHDR** chunk name at offset 12:

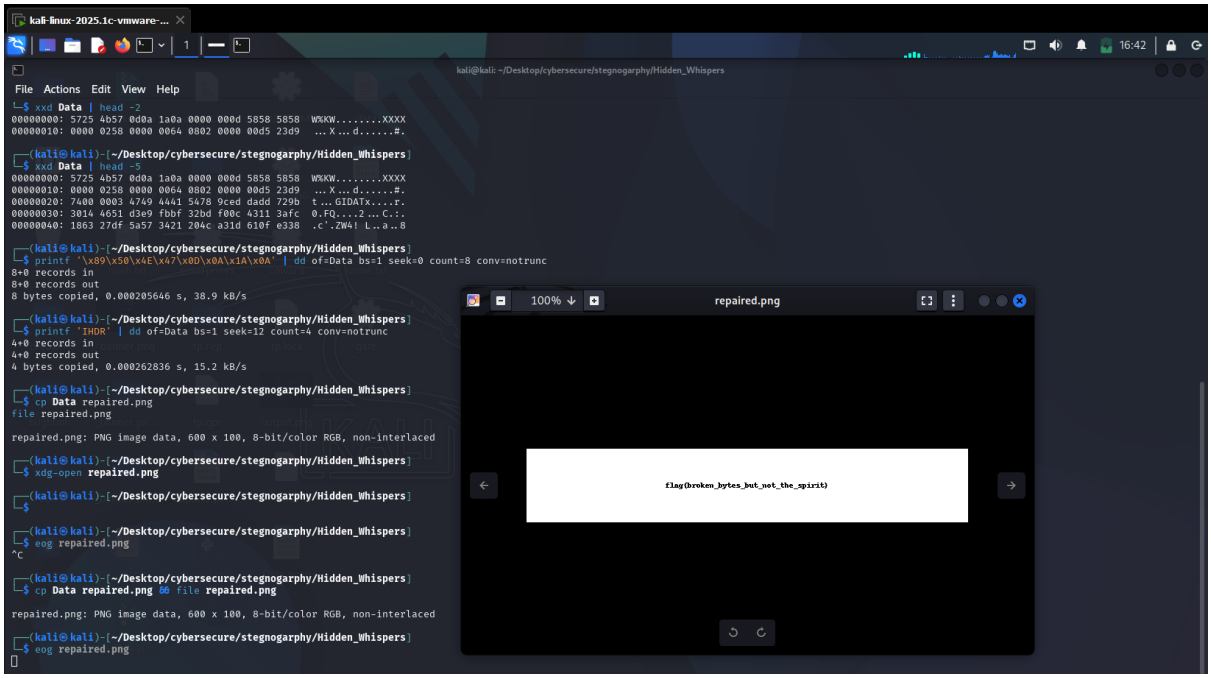
```
┌──(kali㉿kali)-[~/Desktop/cybersecure/stegnogarphy/Hidden_Whispers]
└─$ printf 'IHDR' | dd of=Data bs=1 seek=12 count=4 conv=notrunc
4+0 records in
4+0 records out
4 bytes copied, 0.000262836 s, 15.2 kB/s
```

Copied the repaired file to a new name and checked the file type again:

```
┌──(kali㉿kali)-[~/Desktop/cybersecure/stegnogarphy/Hidden_Whispers]
└─$ cp Data repaired.png && file repaired.png

repaired.png: PNG image data, 600 x 100, 8-bit/color RGB, non-interlaced
```

Opened the repaired PNG to confirm it displays normally:



So, we got our flag.
FLAG: flag{broken_bytes_but_not_the_spirit}

✅ Why We Used These Commands

- **printf '\x89\x50\x4E\x47\x0D\x0A\x1A\x0A'** → This adds the **PNG file signature** at the beginning. Without it, the system doesn't even know it's an image.
- **printf 'IHDR'** → This adds the **IHDR chunk** at the right spot. It's like telling the image viewer, "Hey, this is how to read me!"

Both commands fix the broken parts of the image so we can open it and check if anything is hidden inside.

~By Team justahacker