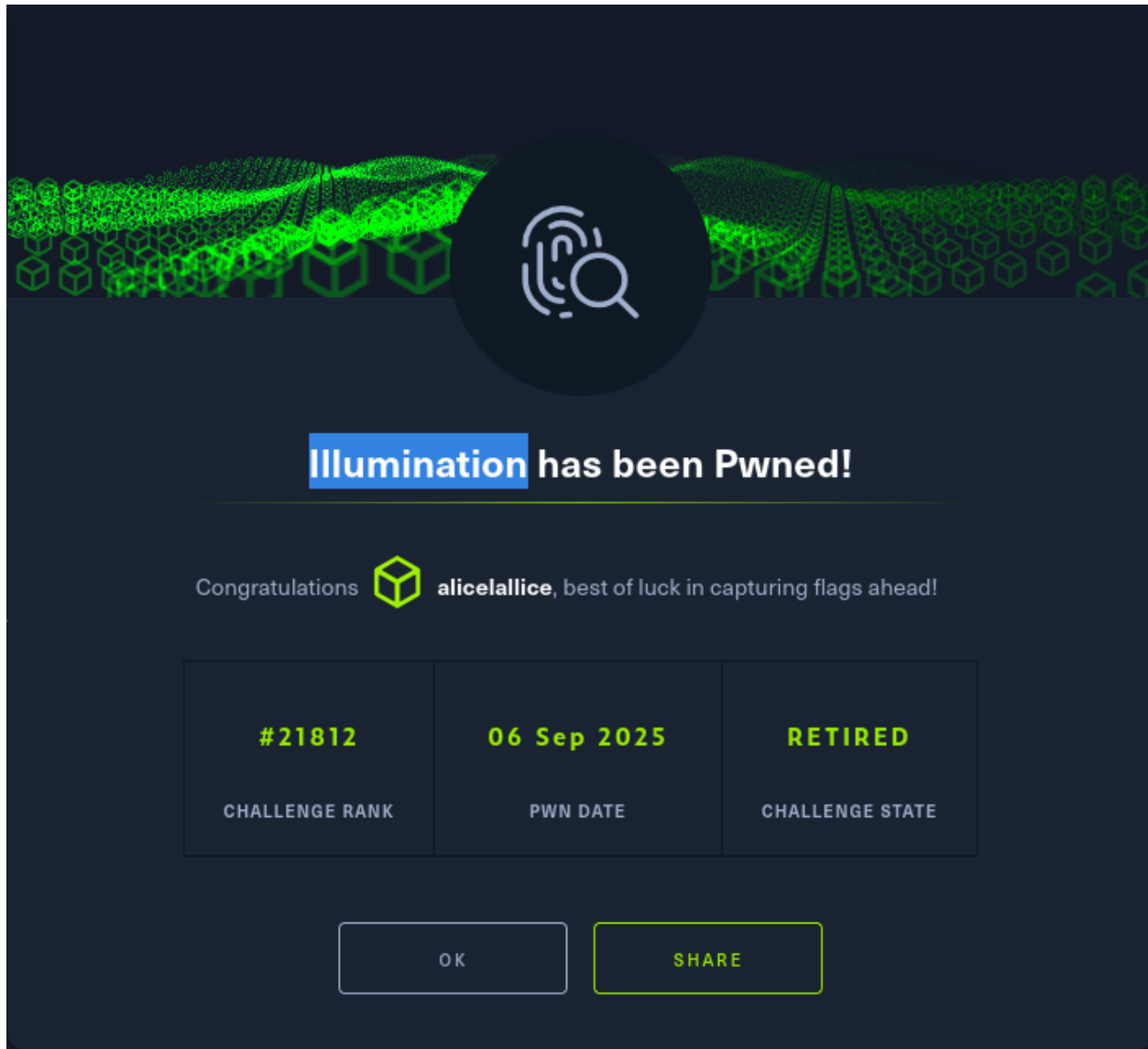


Illumination

Types	forensic
CTF	HTB



Challenge Description

We are given a small Node.js project containing a Discord bot (`bot.js`) and a `config.json` . The challenge hints that sensitive information might be hidden in the

repository.

Initial Enumeration

Start by listing the files:

```
ls -la
```

```
(kali@kali)-[~/Desktop/htb/Illumination.JS]
$ ls -la
total 20
drwxrwxr-x 3 kali kali 4096 Sep  6 09:49 .
drwxrwxr-x 9 kali kali 4096 Sep  6 09:27 ..
-rw-rw-r-- 1 kali kali 2635 May 30 2019 bot.js
-rw-rw-r-- 1 kali kali 199 May 30 2019 config.json
drwxrwxr-x 7 kali kali 4096 May 30 2019 .git
```

The `.git/` folder immediately stands out. This means we can inspect the repository history for secrets.

Inspecting `config.json`

The current `config.json` contains:

```
(kali@kali)-[~/Desktop/htb/Illumination.JS]
$ cat config.json
{
  "token": "Replace me with token when in use! Security Risk!",
  "prefix": "-",
  "lightNum": "1337",
  "username": "UmVkiEhlcnJpbmcsIHJlYWQdGhIEpTIGNhcmVmdWxseQ==",
  "host": "127.0.0.1"
}
```

Decoding the base64 in `username`:

```
(kali@kali)-[~/Desktop/htb/Illumination.JS]
$ echo 'UmVkiEhlcnJpbmcsIHJlYWQdGhIEpTIGNhcmVmdWxseQ==' | base64 -d
Red Herring, read the JS carefully
```

⚠ This tells us the username field is a **decoy**. We need to dig deeper.

Exploring Git History

Check commits that touched `config.json` :

```
git log --oneline config.json
```

```
(kali@kali)~/Desktop/htb/Illumination.JS
$ git log --oneline config.json
47241a4 Thanks to contributors, I removed the unique token as it was a security risk. Thanks for reporting responsibly!
335d6cf Moving to Git, first time using it. First Commit!
```

The first commit (`335d6cf`) is suspicious because it likely contains the original token.

Recovering the Old Token

Show `config.json` at commit `335d6cf` :

```
git show 335d6cf:config.json
```

```
(kali@kali)~/Desktop/htb/Illumination.JS
$ git show 335d6cf:config.json
{
  "token": "SFRCe3YzcnNpMG5fYzBudHIwbF9hbV9JX3JpZ2h0P30=",
  "prefix": "-",
  "lightNum": "1337",
  "username": "UmVkiEhlcncjpbmcsIHJlYWQgdGh1EptIGNhcndmdWxseQ==",
  "host": "127.0.0.1"
}
```

Illumination has been Pwned!

anantkumar

Foren

Decoding the Token

Decode with base64:

```
echo 'SFRCe3YzcnNpMG5fYzBudHIwbF9hbV9JX3JpZ2h0P30=' | base64 -d
```

```
(kali@kali)~/Desktop/htb/Illumination.JS
$ echo 'SFRCe3YzcnNpMG5fYzBudHIwbF9hbV9JX3JpZ2h0P30=' | base64 -d
HTB{v3rsi0n_c0ntr0l_am_I_right?}
```

`HTB{v3rsi0n_c0ntr0l_am_I_right?}`

That's the flag.

Root Cause / Lessons Learned

- **Version control leaks:** Developers often commit secrets to Git before realizing the mistake and overwriting them. But git keeps history, so the secrets remain.
- **Base64 encoding:** The bot stored its token in base64, but that provides no security, only obfuscation.
- **Forensic tip:** Always check `.git/` or backup files in forensic challenges. Secrets love to hide in history.