Hosted Toasted

Challenge

Hoasted Toasted 🍞

150

We have discovered what we believe is a North Torbian public website and have suspicions there is a secret internal-only site hidden there as well. Figure out how to connect to the hidden site and find the flag!

The sites is at https://not-torbian.ethtrader-ai.com/

Unlock Hint for 25 points

Unlock Hint for 25 points

Flag   Submit

Workflow

Recon

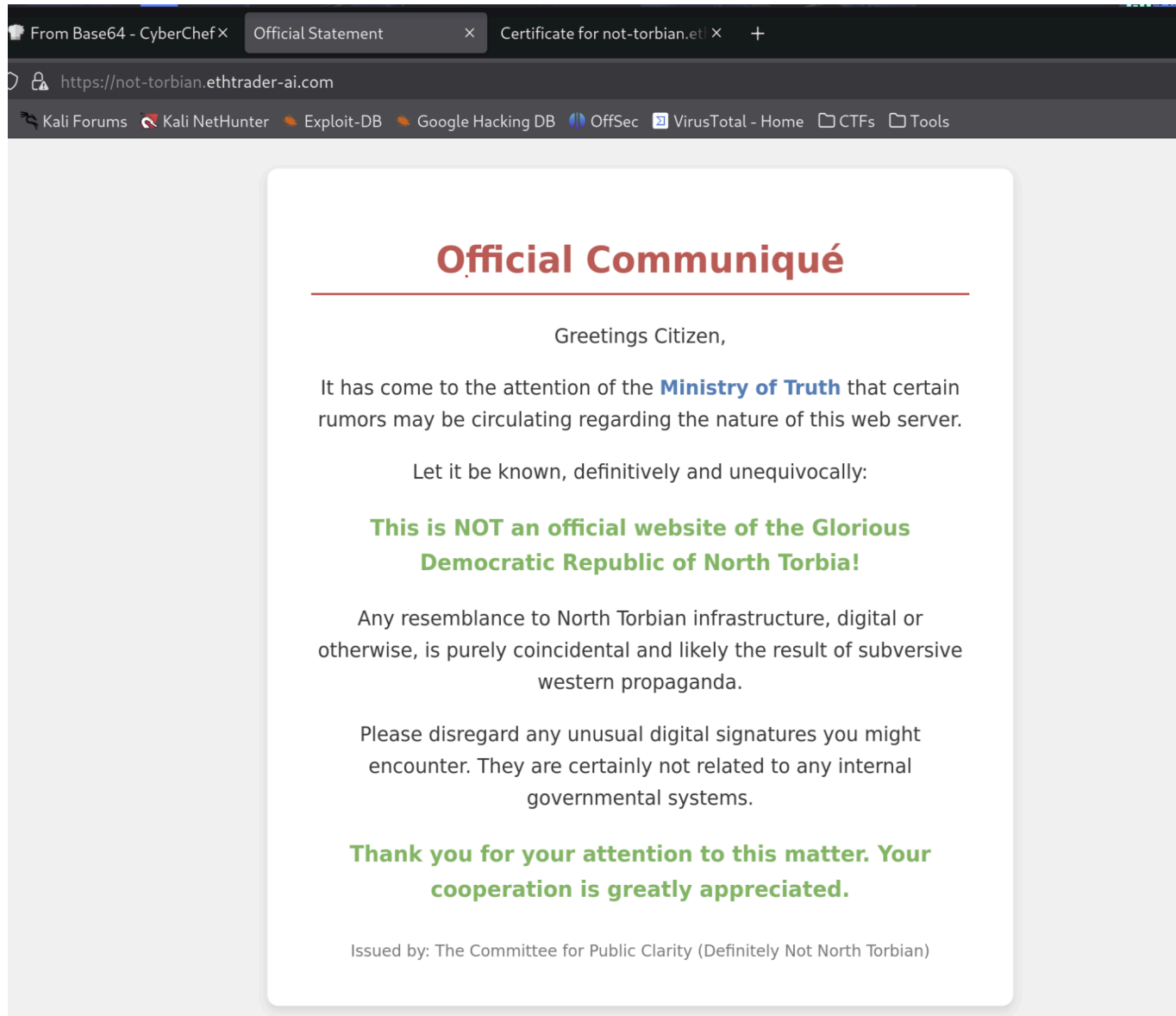Visiting https://not-torbian.ethtrader-ai.com/ triggered a browser warning due to a self-signed TLS certificate. This hinted that the certificate might contain useful metadata.

Inspecting the TLS certificate revealed a Subject Alternative Name (SAN) entry for an internal-only domain: definitelynotaflag.north.torbia. This domain wasn't accessible via public DNS.

not-torbian.ethtrader-ai.com

Subject Name

Country	NT
State/Province	GloriousState
Locality	CapitalCity
Organization	Ministry of Truth
Organizational Unit	Web Operations
Common Name	not-torbian.ethtrader-ai.com

Issuer Name

Country	NT
State/Province	GloriousState
Locality	CapitalCity
Organization	Ministry of Truth
Organizational Unit	Web Operations
Common Name	not-torbian.ethtrader-ai.com

Validity

|	
Not Before	Wed, 14 May 2025 11:25:12 GMT
Not After	Thu, 14 May 2026 11:25:12 GMT

Subject Alt Names

DNS Name	not-torbian.ethtrader-ai.com
DNS Name	definitelynotaflag.north.torbia

To access the internal site, I resolved not-torbian.ethtrader-ai.com to its IP address using the dig command, then mapped that IP to `definitelynotaflag.north.torbia` in my /etc/hosts file. (sorry forgot to screenshot)

After editing the hosts file, I navigated to https://definitelynotaflag.north.torbia and was greeted by a secret portal filled with humorous "classified" content. Clicking around led me to the Secret

Access page.
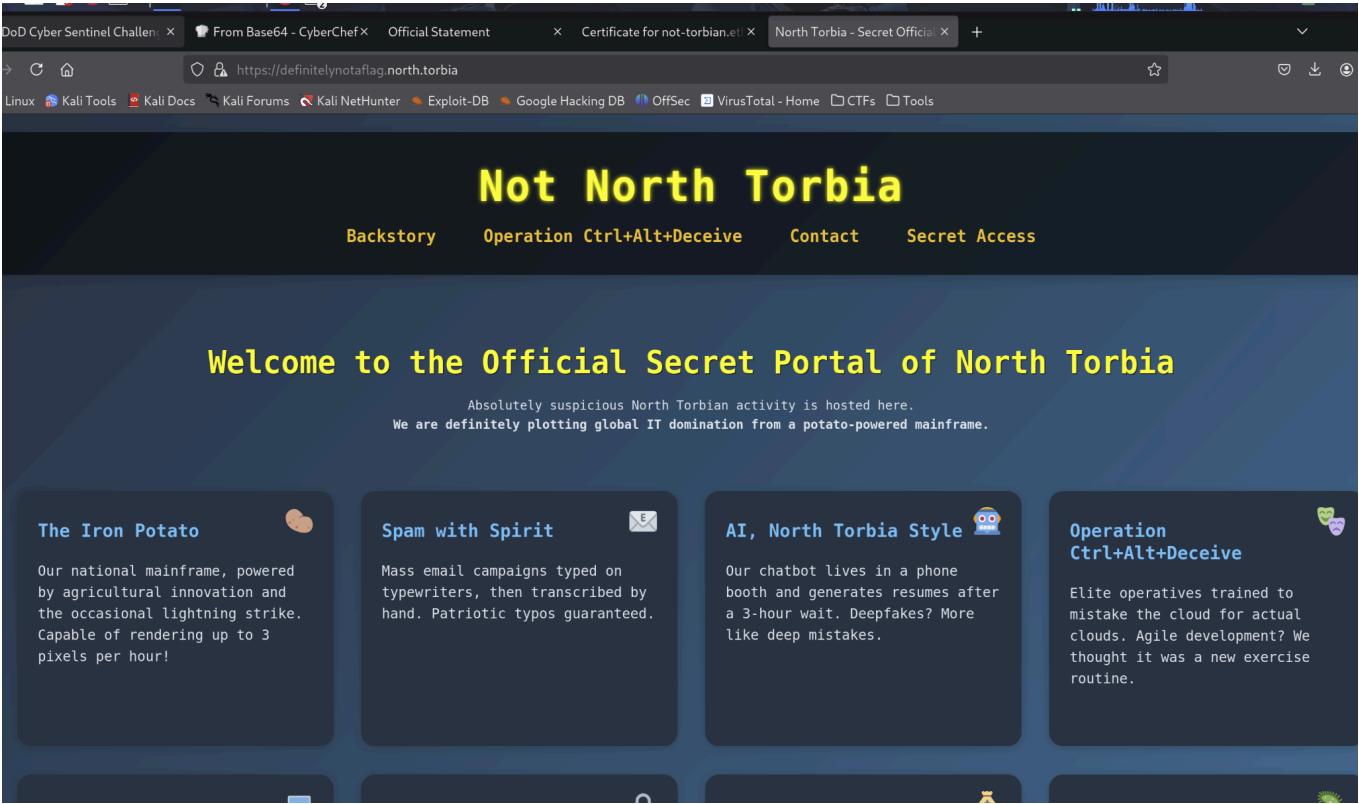
The internal access page confirmed successful hostname spoofing and revealed the flag when i scrolled down

*** TOP SECRET - INTERNAL ACCESS ***

Authentication successful via internal hostname resolution.

Welcome, Agent! You have bypassed standard access protocols.

Your flag is:

C1{vH0st_S4n_M4g1c_R3ve4l3d}

```
    .-'-.
   |o o |
   |:_/ |
  //   \ \
 ((     ) )
  /'\_   _/`\
  \___)=(___/
```

Remember: Glorious Leader is always watching... and so is the potato.