

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Lab 6: Lab Tổng Hợp

GVHD: Ngô Khánh Khoa

Nhóm: 6

1. THÔNG TIN CHUNG:

Lớp: NT213.P11.ANTT.2

STT	Họ và tên	MSSV	Email
1	Lại Quan Thiên	22521385	22521385@gm.uit.edu.vn
2	Mai Nguyễn Nam Phương	22521164	22521164@gm.uit.edu.vn
3	Hồ Diệp Huy	22520541	22520541@gm.uit.edu.vn
4	Nguyễn Phúc Nhi	22521041	22521041@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình Trạng	Thực hiện
1	Bài 1	100%	Nhóm 6
2	Bài 2	0%	Nhóm 6
3	Bài 3	80%	Nhóm 6
4	Bài 4,5	50%	Nhóm 6

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Bài tập 1:(2đ): Báo cáo lỗ hổng tìm thấy của lab1: review-lab.

Tiêu đề: Directory Indexing được bật

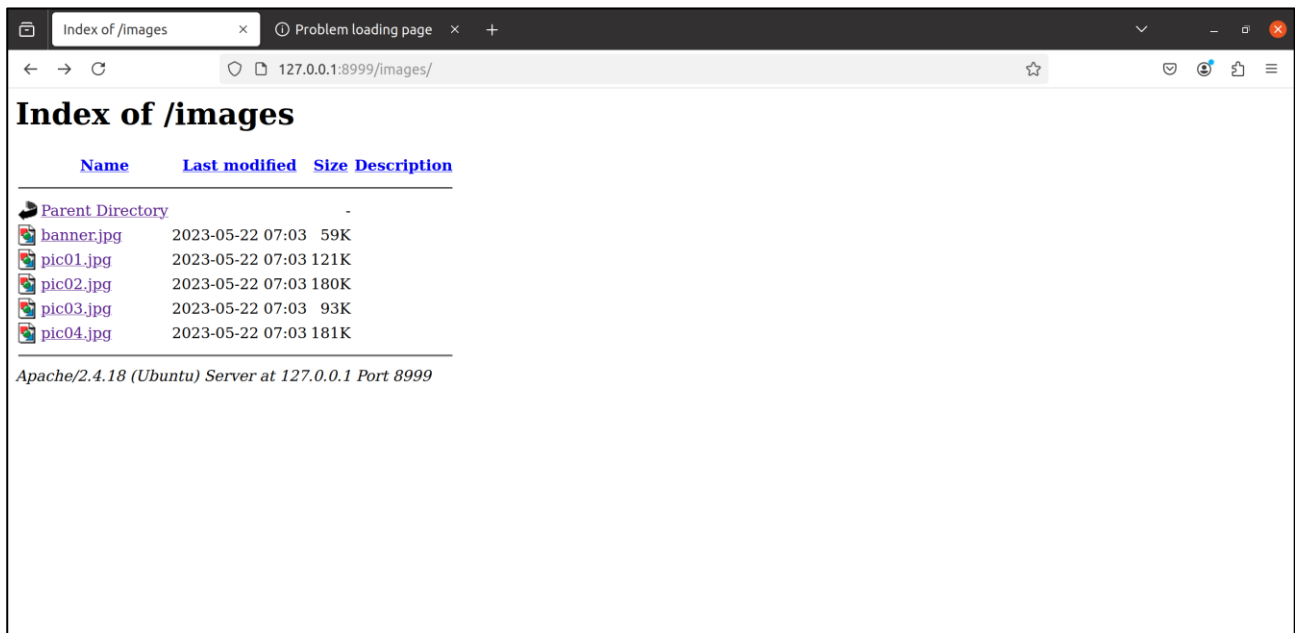
- Mô tả lỗ hổng:

+ **Tóm tắt:** Máy chủ cho phép duyệt thư mục /images/, điều này có thể làm lộ dữ liệu nhạy cảm.

+ **Các bước thực hiện và minh chứng:**

1. Truy cập URL: <http://127.0.0.1:8999/images/>.

2. Duyệt được danh sách các tệp trong thư mục, bao gồm cả các tệp có thể chứa thông tin nhạy cảm.



- **Mức độ ảnh hưởng của lỗ hổng:** Cho phép truy cập trái phép vào các tệp hoặc thư mục nhạy cảm, dẫn đến việc lộ thông tin và có thể bị khai thác bởi tin tặc.

- Khuyến cáo khắc phục:

+ Tắt Directory Indexing trong tệp cấu hình Apache:

```
<Directory /path/to/images>
```

```
Options -Indexes
```

```
</Directory>
```

+ Sau đó khởi động lại Apache:

```
sudo systemctl restart apache2
```

Tiêu đề: Tập nháy cảm được tìm thấy

- **Mô tả lỗi hỏng:**

+ **Tóm tắt:** Một số tập nháy cảm được tìm thấy trên máy chủ web, có thể tiết lộ thông tin về hệ thống:

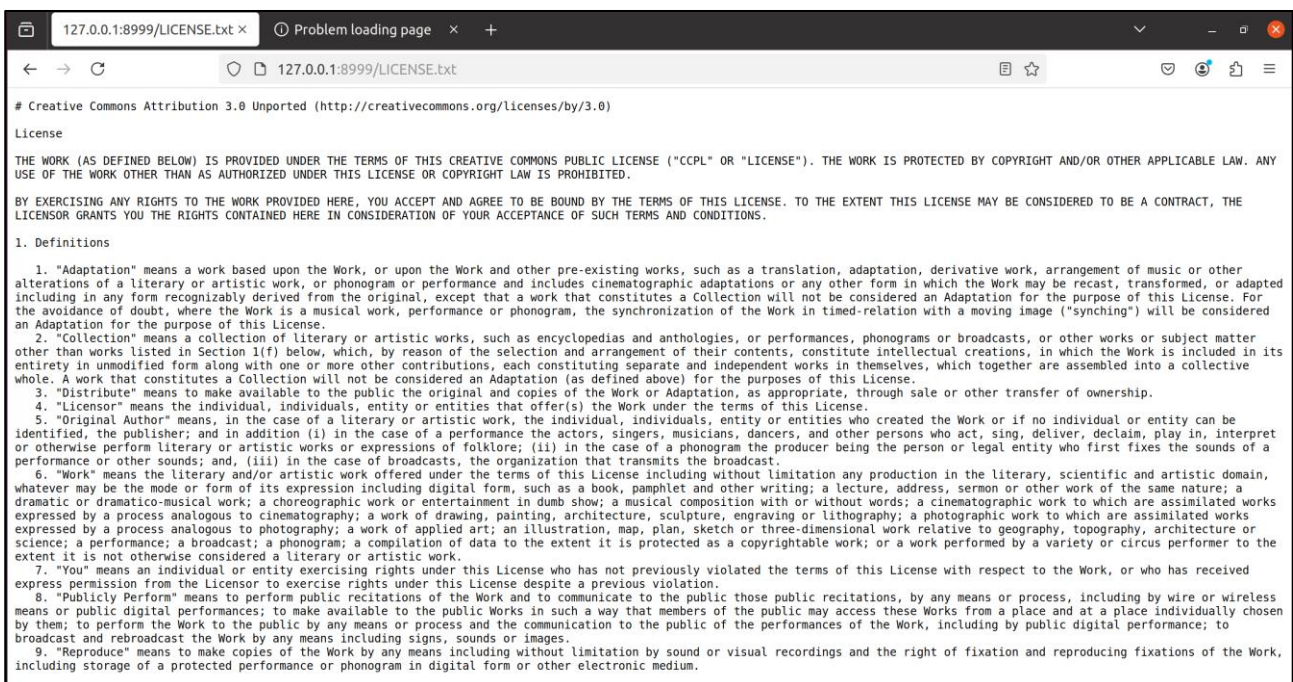
+ /LICENSE.txt: File này tiết lộ thông tin phần mềm hoặc framework đang được sử dụng.

+ /icons/README: Đây là tệp mặc định của Apache, có thể tiết lộ cấu hình máy chủ.

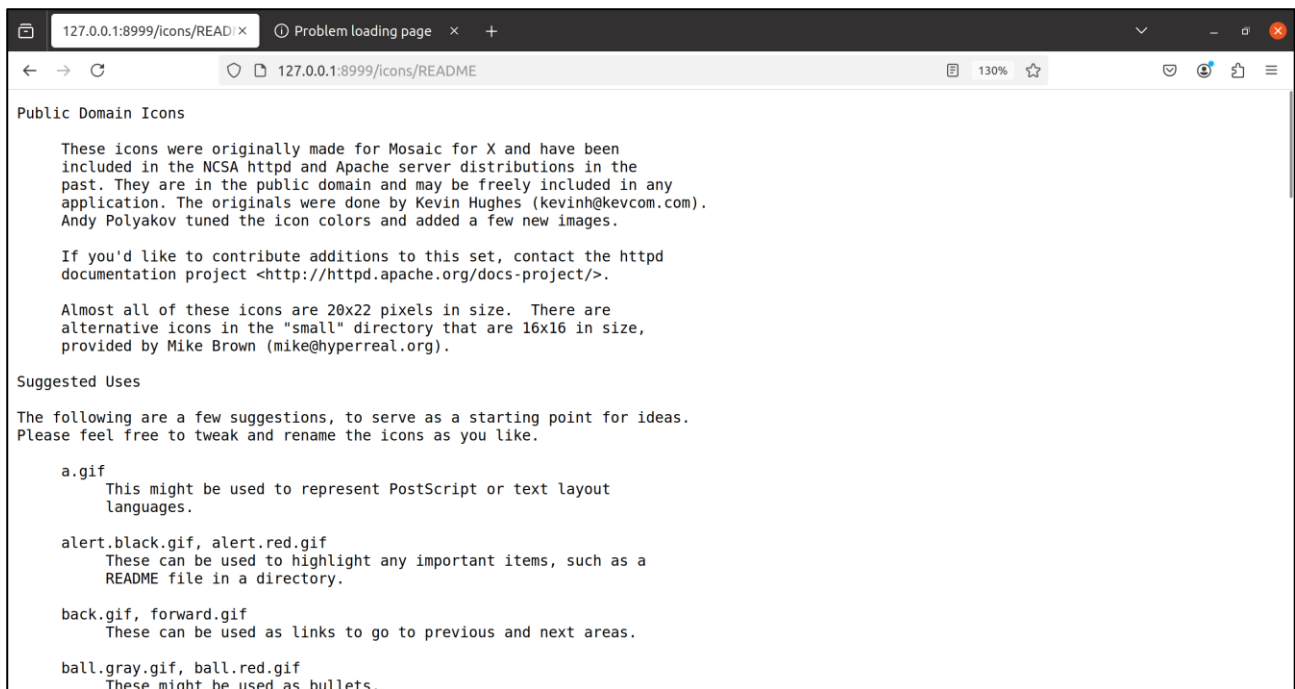
+ **Các bước thực hiện và minh chứng:**

1. Truy cập các URL trực tiếp:

+ <http://127.0.0.1:8999/LICENSE.txt>



+ <http://127.0.0.1:8999/icons/README>



2. Nội dung tệp có thể đọc được, cung cấp thông tin hệ thống nhạy cảm.

- **Mức độ ảnh hưởng của lỗ hổng:** Thông tin tiết lộ có thể hỗ trợ tin tặc xác định phiên bản phần mềm hoặc cấu hình máy chủ, từ đó tiến hành các cuộc tấn công có chủ đích.

- **Khuyến cáo khắc phục:**

+ Xóa các tệp không cần thiết:

```
sudo rm /var/www/html/LICENSE.txt
```

```
sudo rm /var/www/html/icons/README
```

+ Hạn chế quyền truy cập vào các tệp hoặc thư mục không cần thiết bằng cách sử dụng cấu hình máy chủ web.

Bài tập 2:(2đ): Báo cáo lỗi hỏng tìm thấy của lab2.

Tiêu đề:

- Mô tả lỗi hỏng:

+ Tóm tắt:

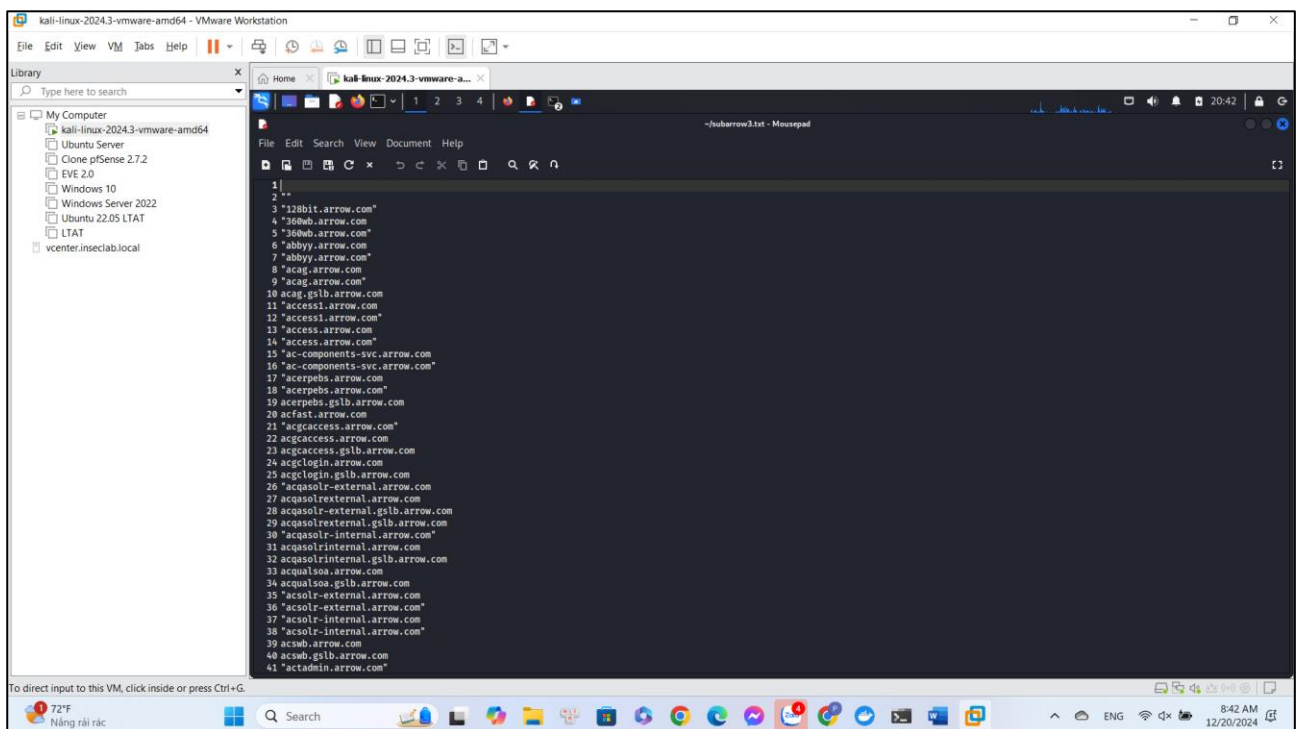
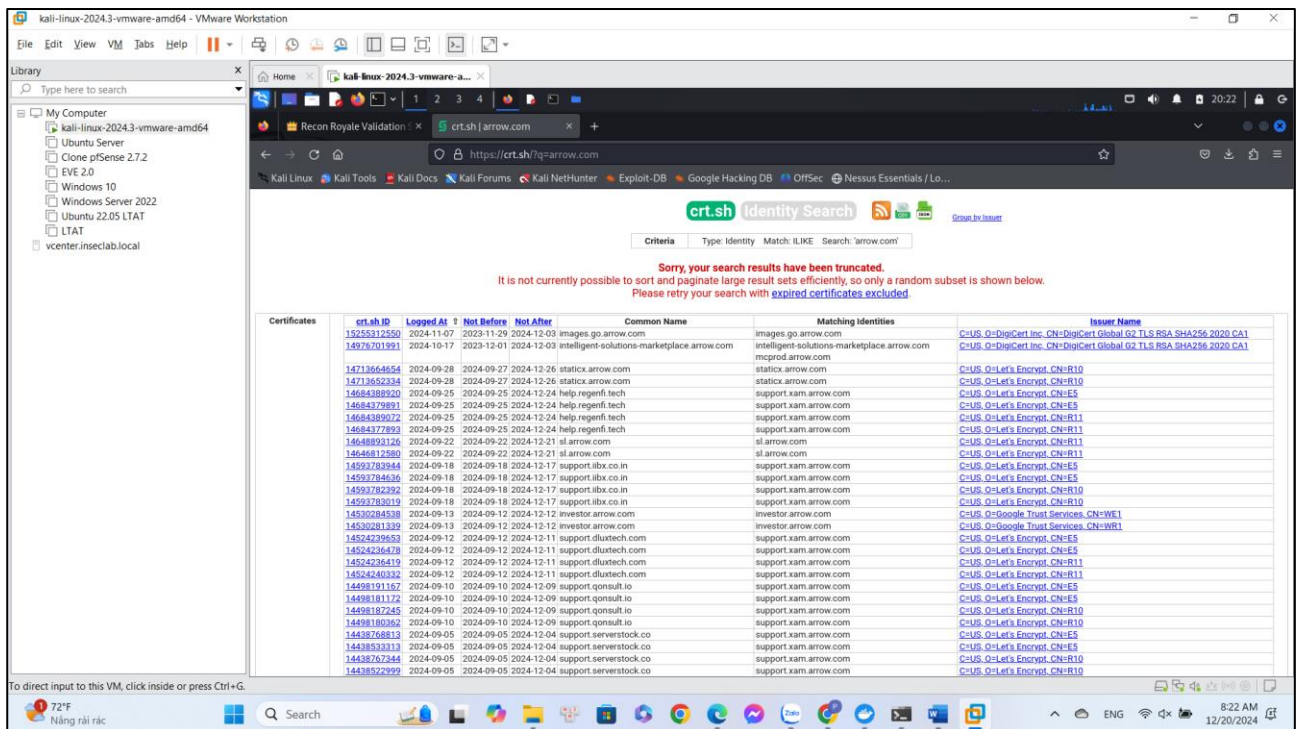
+ Các bước thực hiện và minh chứng:

- Mức độ ảnh hưởng của lỗi hỏng:

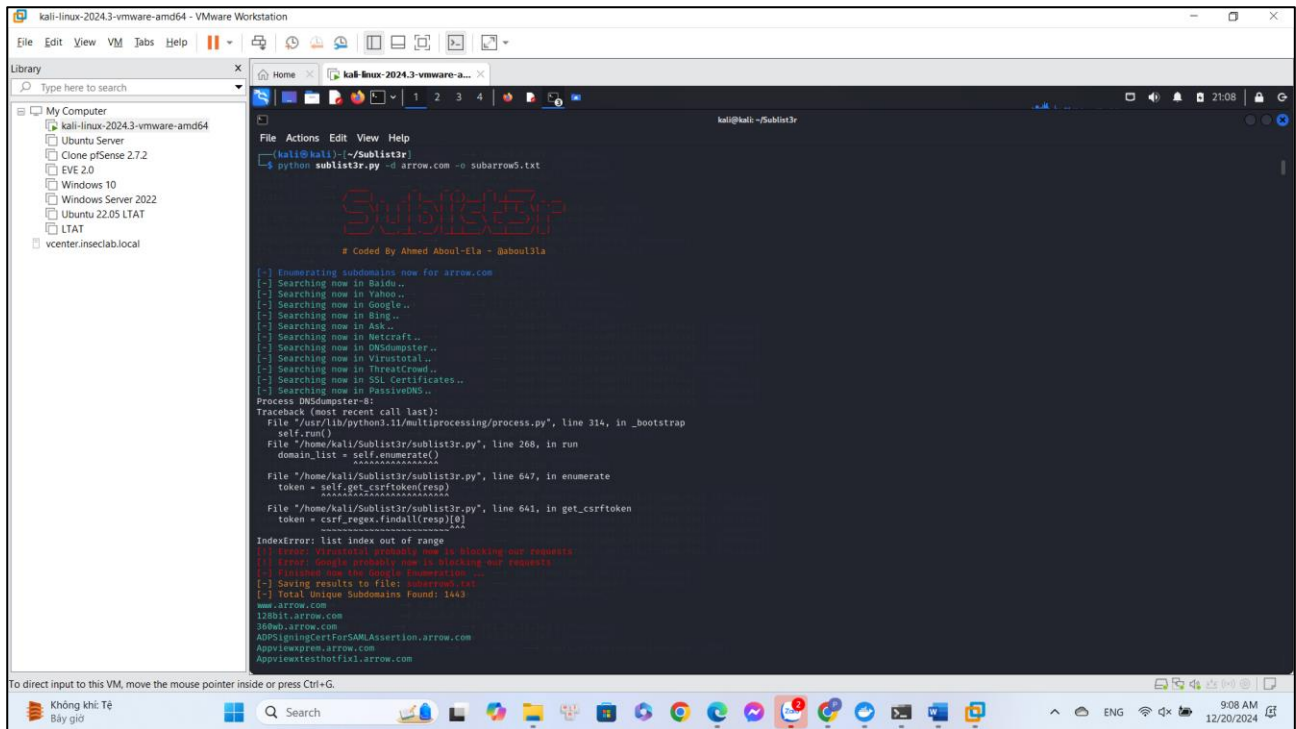
- Khuyến cáo khắc phục:

Bài tập 3:(2đ): Tìm subdomain thuộc tên miền chính ở trang web sau: arrow.com.

- Dùng <https://crt.sh/> để tìm subdomain của arrow.com và lưu vào file



Dùng Sublist3r để tìm subdomain của arrow.com và lưu vào file

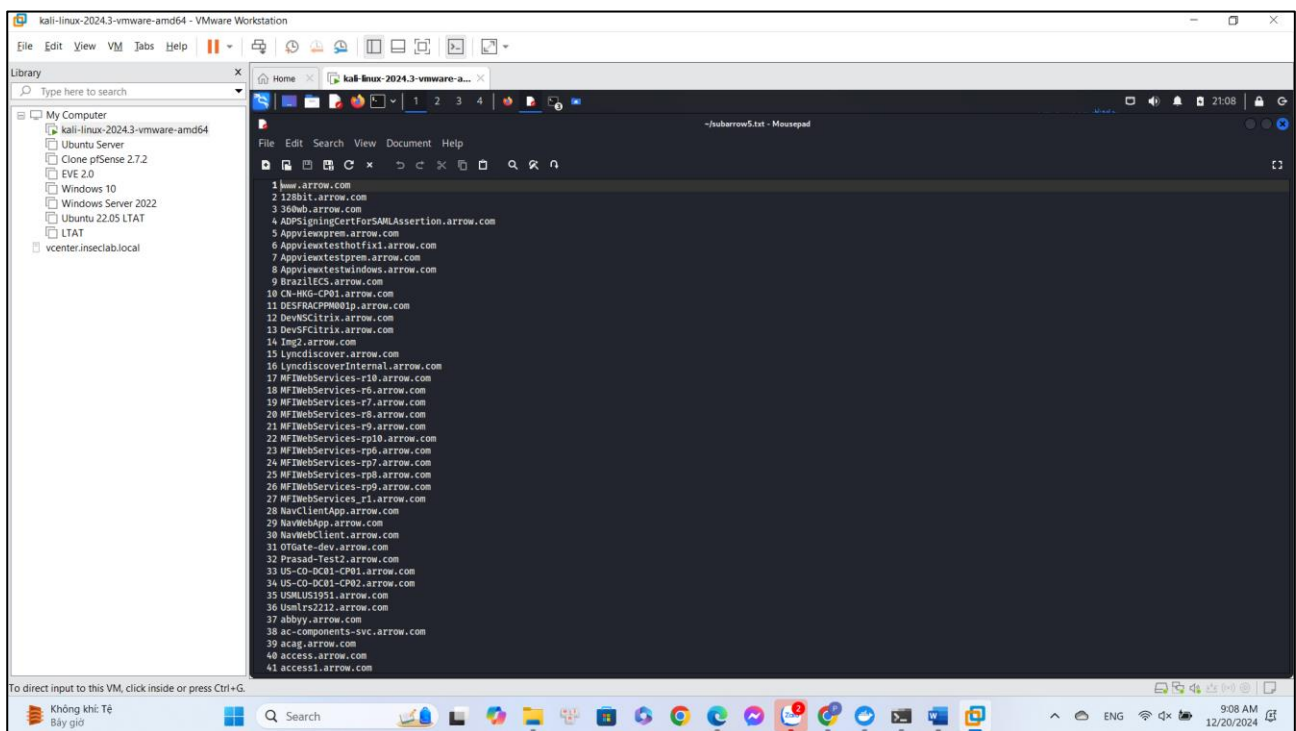


The screenshot shows a Kali Linux terminal window with the Sublist3r tool running. The tool is searching for subdomains for the domain arrow.com. The output shows a list of subdomains found, including www.arrow.com, 128bit.arrow.com, 360web.arrow.com, and others. The terminal also displays a traceback for a recent call last, indicating an IndexError: list index out of range.

```
File Actions Edit View Help
kali@kali:~/Sublist3r
$ python sublist3r.py -d arrow.com -o subarrow5.txt

Sublist3r
# Coded By Ahmed Aboul-Ela - @abool3la

[+] Enumerating subdomains now for arrow.com
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSdumpster..
[+] Searching now in Virustotal..
[+] Searching now in ThreatCrowd..
[+] Searching now in SSL certificates..
[+] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.11/multiprocessing/process.py", line 314, in _bootstrap
    self.run()
  File "/home/kali/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrf_token(resp)
  File "/home/kali/Sublist3r/sublist3r.py", line 641, in get_csrf_token
    token = csrf_regex.findall(resp)[0]
IndexError: list index out of range
[+] Error: VirusTotal probably now is blocking our requests
[+] Error: Google probably now is blocking our requests
[+] Finished now the Google Enumeration...
[+] Saving results to file: subarrow5.txt
[+] Total Unique Subdomains Found: 1443
www.arrow.com
128bit.arrow.com
360web.arrow.com
ADPSigningCertForSAMLAssertion.arrow.com
Appviewprem.arrow.com
Appviewtesthotfix1.arrow.com
```

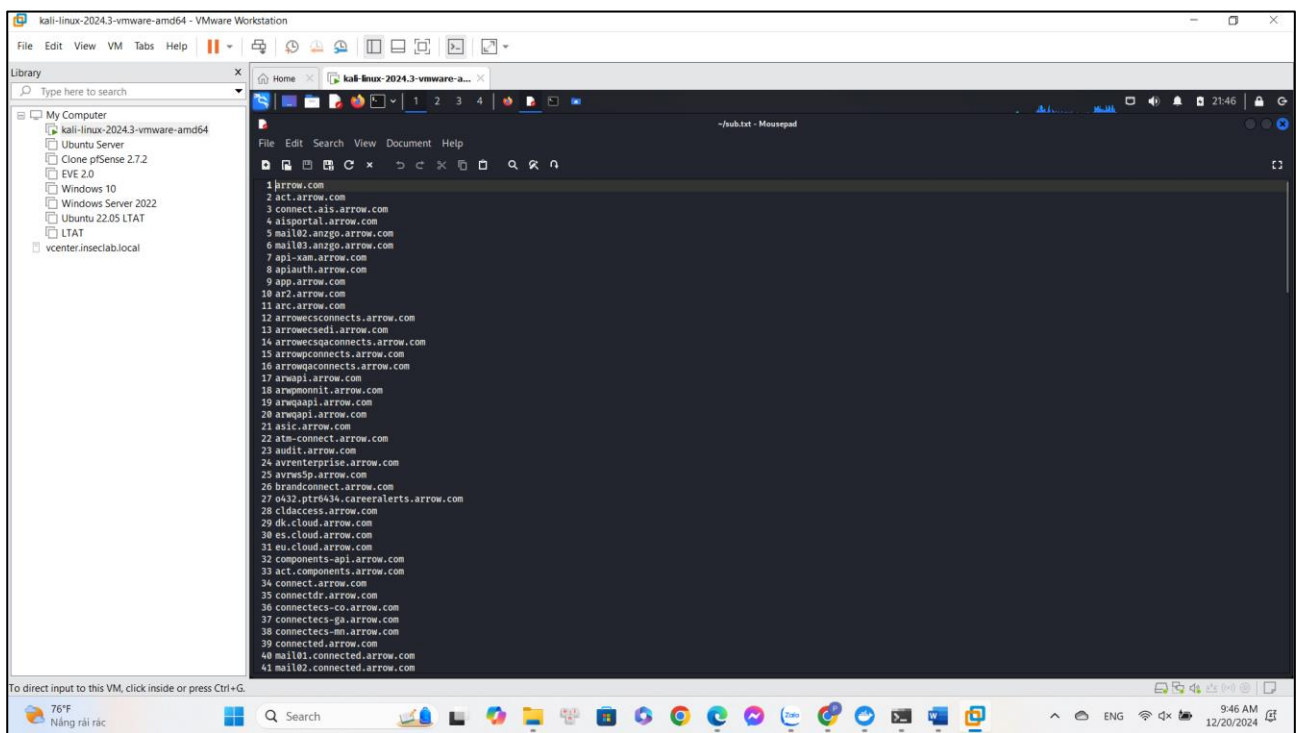
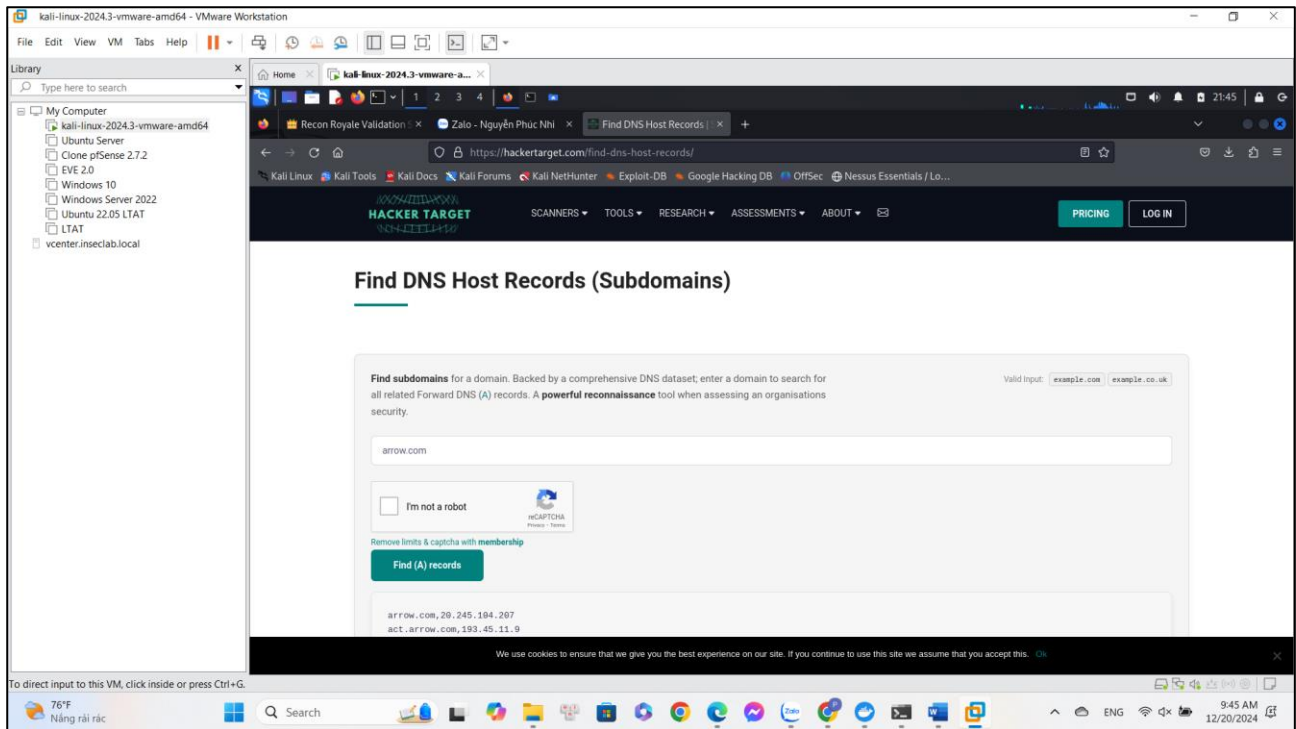


The screenshot shows the output of the Sublist3r tool, listing 41 subdomains for arrow.com. The list includes various services and internal domains, such as www.arrow.com, 128bit.arrow.com, 360web.arrow.com, and others.

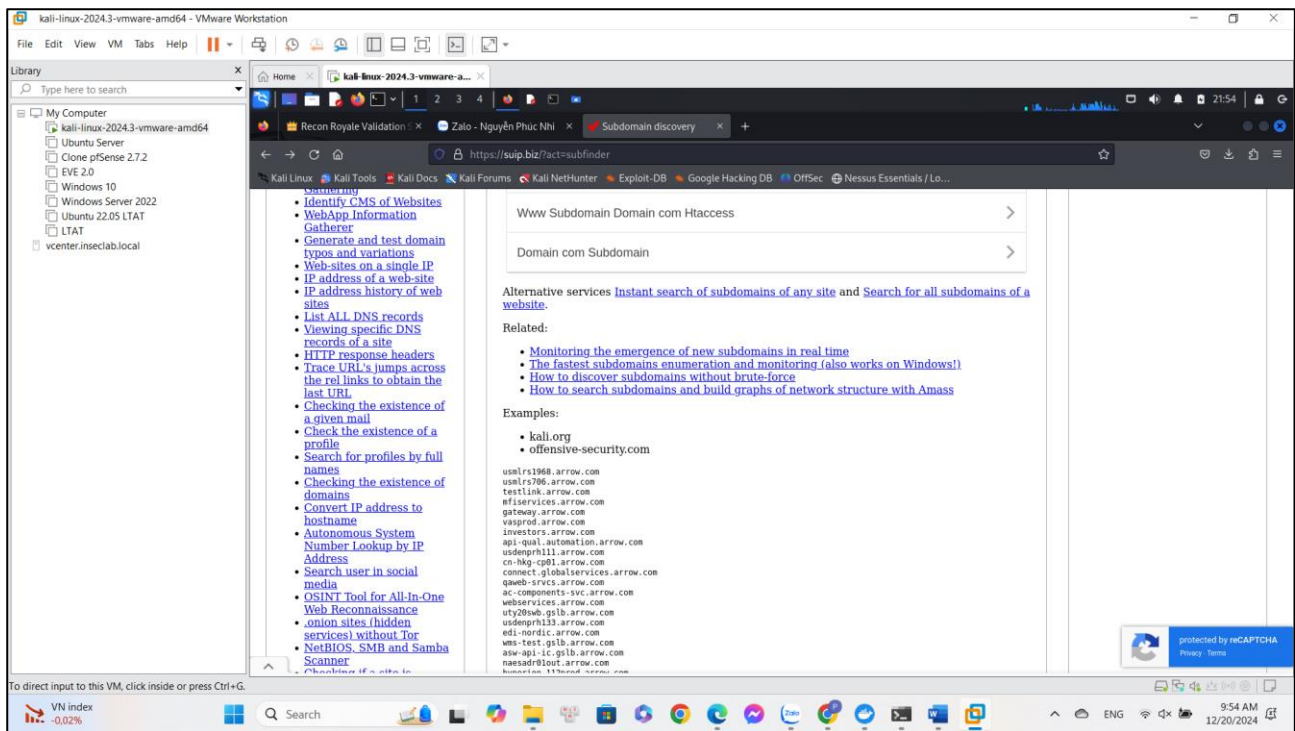
```
File Edit Search View Document Help
~/Subarrow5.txt - Mousepad

1 www.arrow.com
2 128bit.arrow.com
3 360web.arrow.com
4 ADPSigningCertForSAMLAssertion.arrow.com
5 Appviewprem.arrow.com
6 Appviewtesthotfix1.arrow.com
7 Appviewtestprem.arrow.com
8 Appviewtestwindows.arrow.com
9 BrcilICS.arrow.com
10 CH-HMG-CP01.arrow.com
11 DESFRACPPM0a1p.arrow.com
12 DevWSCitrix.arrow.com
13 DevSFCitrix.arrow.com
14 Eng2.arrow.com
15 Lyncdiscover.arrow.com
16 LyncdiscoverInternal.arrow.com
17 MFTWebServices-r18.arrow.com
18 MFTWebServices-r6.arrow.com
19 MFTWebServices-r7.arrow.com
20 MFTWebServices-r8.arrow.com
21 MFTWebServices-r9.arrow.com
22 MFTWebServices-rp10.arrow.com
23 MFTWebServices-rp6.arrow.com
24 MFTWebServices-rp7.arrow.com
25 MFTWebServices-rp8.arrow.com
26 MFTWebServices-rp9.arrow.com
27 MFTWebServices_r1.arrow.com
28 NavClientApp.arrow.com
29 NavWebApp.arrow.com
30 NavWebClient.arrow.com
31 OTGate-dev.arrow.com
32 Prasad-Test2.arrow.com
33 US-CO-DC01-CP01.arrow.com
34 US-CO-DC01-CP02.arrow.com
35 USMLUS1951.arrow.com
36 Usmlrs2212.arrow.com
37 abbyy.arrow.com
38 ac-components-svc.arrow.com
39 acag.arrow.com
40 access.arrow.com
41 access1.arrow.com
```

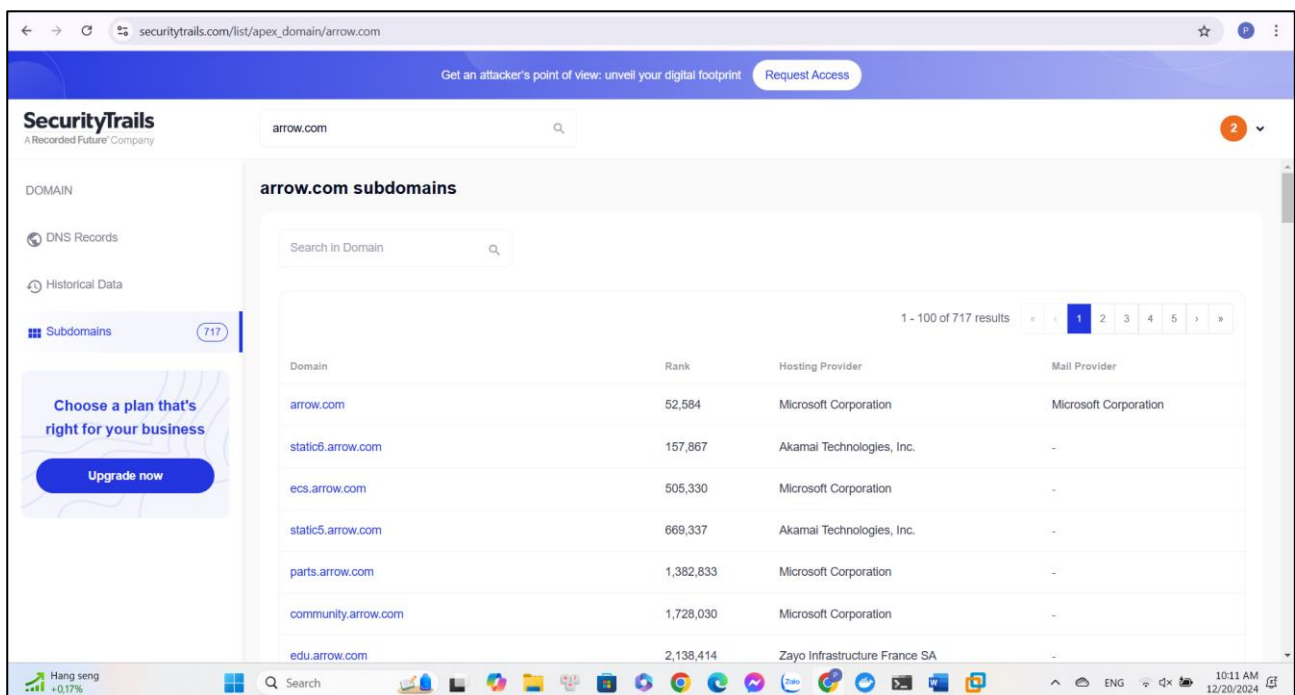
Dùng <https://hackertarget.com/> để tìm subdomain của arrow.com và lưu vào file



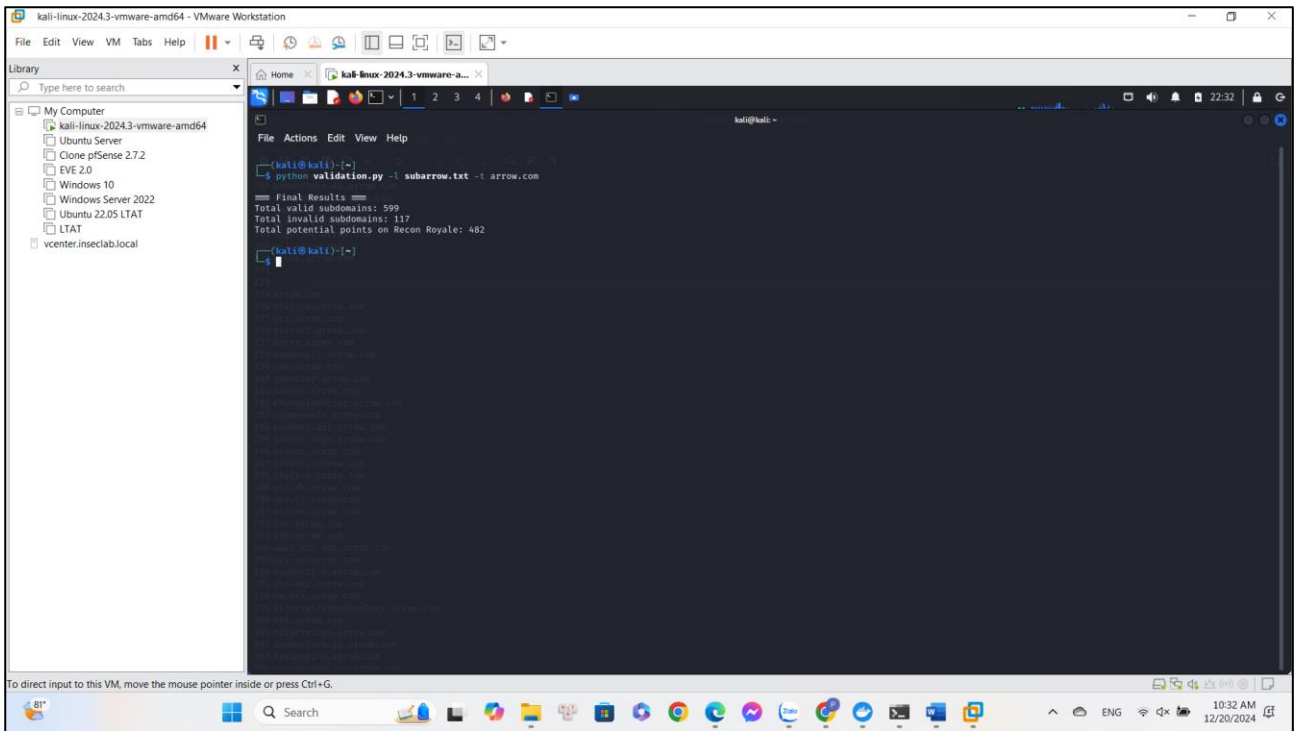
Dùng <https://suip.biz/?act=subfinder> để tìm subdomain của arrow.com và lưu vào file



Dùng <https://securitytrails.com/> để tìm subdomain của arrow.com và lưu vào file



Gộp kết quả và lưu vào file subarrow.txt và dùng tool được cung cấp để check số lượng invalid subdomain, ta thấy có 599 invalid subdomain



Bài tập 4, 5:(4đ): Báo cáo lỗi hồng tìm thấy của netsight.apk.**Lỗi hồng 1:**

- **Tiêu đề:** Lỗi hồng bảo mật ở LaunchActivity của ứng dụng video_player.apk

- **Mô tả lỗi hồng:**

+ **Tóm tắt:** Lỗi hồng cho phép ứng dụng video_player.apk khởi chạy LaunchActivity từ bên ngoài, dẫn đến việc truy cập không mong muốn và yêu cầu quyền đối với album media của người dùng.

+ **Các bước thực hiện và minh chứng:**

1. Khi khởi động ứng dụng thông thường, chỉ hiển thị một video và không cho phép người dùng tương tác.



2. Chạy lệnh như hình và quan sát thấy ứng dụng có thể được mở từ một nguồn bên ngoài.

1.

```
C:\Users\WanThinnn>adb shell dumpsys package razi.apa.ctf.videoPlayer | grep -i "Activity\|Receiver\|Provider"
Activity Resolver Table:
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
  c514047 razi.apa.ctf.videoPlayer/.ui.LaunchActivity filter a55be12
```

```
C:\Users\WanThinnn>adb shell am start -n razi.apa.ctf.videoPlayer/.ui.LaunchActivity
Starting: Intent { cmp=razi.apa.ctf.videoPlayer/.ui.LaunchActivity }
```

3. Khi chạy lệnh trên, ứng dụng tự động chuyển hướng đến giao diện media và yêu cầu quyền truy cập vào Album Media của người dùng.



- **Mức độ ảnh hưởng của lỗ hổng:** Lỗ hổng này có thể bị lợi dụng để truy cập trái phép vào giao diện media của ứng dụng, dẫn đến rủi ro về quyền riêng tư hoặc xâm phạm dữ liệu nhạy cảm của người dùng.

- **Khuyến cáo khắc phục:**

+ Cấu hình AndroidManifest.xml để hạn chế truy cập từ bên ngoài:

xml

Copy code

```
<activity  
    android:name=".ui.LaunchActivity"  
    android:exported="false">  
</activity>
```

+ Kiểm tra và bảo vệ các quyền nhạy cảm trong ứng dụng, đảm bảo rằng chỉ được yêu cầu khi cần thiết và thông qua sự đồng ý của người dùng.

Lỗ hổng 2:**- Tiêu đề: WebView Cho Phép Điều Hướng Đến URL Không An Toàn Trong WebviewActivity****- Mô tả lỗ hổng**

+ Lỗ hổng này cho phép kẻ tấn công điều hướng ứng dụng đến các URL không an toàn thông qua WebView trong WebviewActivity.

+ Do cấu hình của ứng dụng (android:exported="true") và việc không kiểm tra URL truyền vào, kẻ tấn công có thể sử dụng adb để chuyển hướng ứng dụng đến một trang web độc hại, mở ra nguy cơ đánh cắp dữ liệu hoặc thực hiện các hành động trái phép.

- Tóm tắt

+ **Lỗ hổng:** WebviewActivity được định nghĩa trong AndroidManifest.xml với thuộc tính

```
<activity android:exported="true"
android:name="com.tcpip.netsight.WebviewActivity"/>
```

=> Điều này cho phép các ứng dụng khác hoặc kẻ tấn công sử dụng Intent để khởi chạy activity này. URL được truyền vào không được kiểm tra hoặc xác minh trước khi tải trong WebView.

+ Hệ quả bảo mật:

- Kẻ tấn công có thể chuyển hướng ứng dụng đến các trang web giả mạo hoặc độc hại.
- Nguy cơ xảy ra tấn công lừa đảo (phishing), đánh cắp thông tin hoặc thực thi mã JavaScript độc hại.

- Các bước để thực hiện lại và bằng chứng:

+ **Bước 1: Kiểm tra thuộc tính android:exported:** Mở file AndroidManifest.xml và xác nhận cấu hình:

```
<activity android:exported="true"
android:name="com.tcpip.netsight.WebviewActivity"/>
```

+ Bước 2: Khởi chạy WebviewActivity bằng lệnh ADB

Sử dụng lệnh sau để điều hướng ứng dụng đến URL không an toàn:

```
adb shell am start -n com.tcpip.netsight/.WebviewActivity -e url
"http://example.com"
```

+ Bước 3: Quan sát hành vi

- Ứng dụng sẽ mở http://example.com trong WebView mà không kiểm tra hoặc cảnh báo.
- Logcat hiển thị như sau: START u0 {dat=http://example.com/... flg=0x10000000 cmp=com.tcpip.netsight/.WebviewActivity} from uid 0

- Mức độ ảnh hưởng của lỗ hổng**1. Tác động bảo mật:**

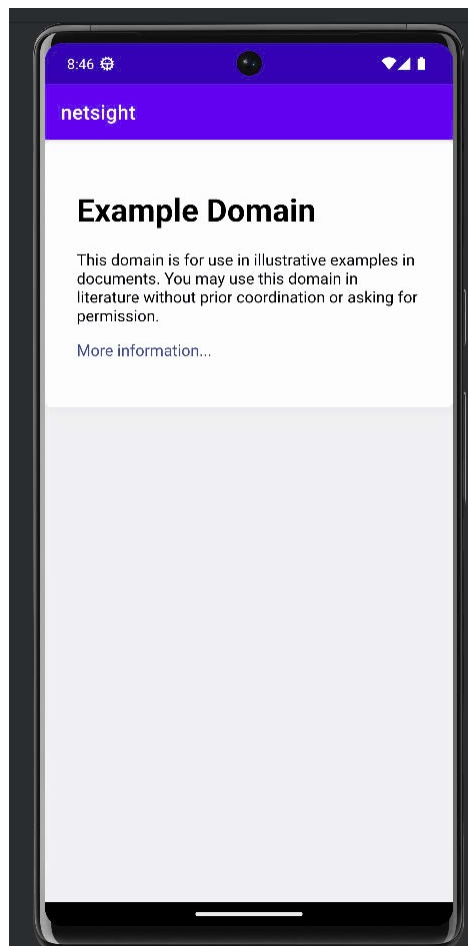
- **Tấn công phishing:** Kẻ tấn công có thể chuyển hướng ứng dụng đến trang giả mạo, lừa người dùng nhập thông tin nhạy cảm.

- **Thực thi JavaScript độc hại:** WebView với `setJavaScriptEnabled(true)` có thể chạy mã JavaScript nguy hiểm từ trang web độc hại.
 - **Nguy cơ rò rỉ thông tin:** Nếu ứng dụng tải URL không an toàn qua HTTP, dữ liệu có thể bị chặn hoặc thay đổi trong quá trình truyền.
2. **Nguy cơ xảy ra tấn công:** Cao, đặc biệt nếu ứng dụng được cài đặt trên thiết bị của nhiều người dùng mà không kiểm tra đầu vào URL.

- Khuyến cáo khắc phục

1. **Kiểm tra và xác minh URL đầu vào:**
 - Thêm kiểm tra trong mã nguồn WebViewActivity để chỉ cho phép các URL đáng tin cậy:
2. **Giới hạn quyền truy cập:** Đặt `android:exported="false"` trong `AndroidManifest.xml` nếu không cần cho phép các ứng dụng khác khởi chạy activity này.
3. **Sử dụng HTTPS:** Chỉ tải các URL bắt đầu bằng `https://` để tránh bị tấn công MITM.

- Minh chứng:




```
C:\Users\WanThinnn\Documents\UIT\Nam_3\HK1\NT213-BMWUD\Thuc_hanh\Lab_6\Lab6.2\Lab6.2\netsight\smali_classes3\com\tcpip\netsight>adb logcat | grep WebViewActivity
12-20 08:43:26.037 570 885 I ActivityTaskManager: START u0 {dat=http://example.com/... flg=0x10000000 cmp=com.tcpip.netsight/.WebViewActivity} from uid 0
12-20 08:43:26.115 570 992 D CoreBackPreview: Window{81fb603 u0 com.tcpip.netsight/com.tcpip.netsight.WebviewActivit
y}: Setting back callback OnBackInvokedCallbackInfo{mCallback=android.window.IOnBackInvokedCallback$Stub$Proxy@418bb9, m
Priority=0}
12-20 08:43:26.447 570 611 I ActivityTaskManager: Displayed com.tcpip.netsight/.WebViewActivity: +408ms
12-20 08:45:53.207 570 885 I ActivityTaskManager: START u0 {flg=0x10000000 cmp=com.tcpip.netsight/.WebViewActivity (
has extras)} from uid 0
12-20 08:45:53.292 570 885 D CoreBackPreview: Window{623c627 u0 com.tcpip.netsight/com.tcpip.netsight.WebviewActivit
y}: Setting back callback OnBackInvokedCallbackInfo{mCallback=android.window.IOnBackInvokedCallback$Stub$Proxy@4dee572,
mPriority=0}
12-20 08:45:53.482 570 611 I ActivityTaskManager: Displayed com.tcpip.netsight/.WebViewActivity: +273ms
```

```
C:\Users\WanThinnn>adb shell am start -n com.tcpip.netsight/.WebViewActivity -e url "http://example.com"
Starting: Intent { cmp=com.tcpip.netsight/.WebViewActivity (has extras) }
```

Lỗi hỏng 3:

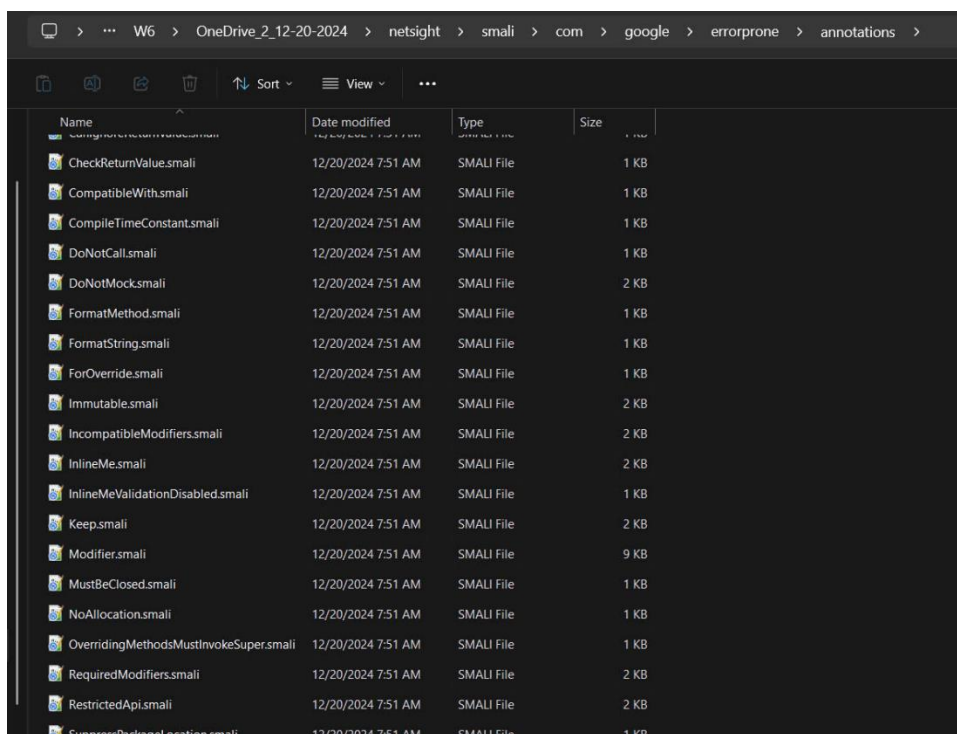
- Tiêu đề: Lỗi hỏng Reverse Engineering ở file netsight.apk

- Mô tả lỗi hỏng

+ Có lỗi hỏng Reverse Engineering ở file netsight.apk, cụ thể khi sử dụng apktool để decompile file apk này ra và thực hiện truy xuất vào các file smali, thì ta sẽ thấy được rằng file này chưa được làm rối mã, tên các hàm và class để nguyên tên thuận tiện cho việc khai thác

+ Truy cập vào vào các file MainActivity\$.x, sẽ thấy được các link đường dẫn đến các trang web trong app, từ đó có thể khai thác bằng cách dịch ngược lại nó rồi thay thế nó bằng các đường dẫn độc hại

```
C:\Code\Bảo mật web và ứng dụng - NT213.P11.ANTT\Lab\W6\OneDrive_2_12-20-2024>apktool d netsight.apk
I: Using Apktool 2.10.0 on netsight.apk with 16 thread(s).
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: C:\Users\namphuong\AppData\Local\apktool\framework\1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
```



Name	Date modified	Type	Size
CheckReturnValue.smali	12/20/2024 7:51 AM	SMALI File	1 KB
CompatibleWith.smali	12/20/2024 7:51 AM	SMALI File	1 KB
CompileTimeConstant.smali	12/20/2024 7:51 AM	SMALI File	1 KB
DoNotCall.smali	12/20/2024 7:51 AM	SMALI File	1 KB
DoNotMock.smali	12/20/2024 7:51 AM	SMALI File	2 KB
FormatMethod.smali	12/20/2024 7:51 AM	SMALI File	1 KB
FormatString.smali	12/20/2024 7:51 AM	SMALI File	1 KB
ForOverride.smali	12/20/2024 7:51 AM	SMALI File	1 KB
Immutable.smali	12/20/2024 7:51 AM	SMALI File	2 KB
IncompatibleModifiers.smali	12/20/2024 7:51 AM	SMALI File	2 KB
InlineMe.smali	12/20/2024 7:51 AM	SMALI File	2 KB
InlineMeValidationDisabled.smali	12/20/2024 7:51 AM	SMALI File	1 KB
Keep.smali	12/20/2024 7:51 AM	SMALI File	2 KB
Modifier.smali	12/20/2024 7:51 AM	SMALI File	9 KB
MustBeClosed.smali	12/20/2024 7:51 AM	SMALI File	1 KB
NoAllocation.smali	12/20/2024 7:51 AM	SMALI File	1 KB
OverridingMethodsMustInvokeSuper.smali	12/20/2024 7:51 AM	SMALI File	1 KB
RequiredModifiers.smali	12/20/2024 7:51 AM	SMALI File	2 KB
RestrictedApi.smali	12/20/2024 7:51 AM	SMALI File	2 KB
SuppressPackageLocation.smali	12/20/2024 7:51 AM	SMALI File	1 KB

+ Do cấu hình của ứng dụng (android:exported="true") và việc không kiểm tra URL truyền vào, kẻ tấn công có thể sử dụng adb để chuyển hướng ứng dụng đến một trang web độc hại, mở ra nguy cơ đánh cắp dữ liệu hoặc thực hiện các hành động trái phép.