

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Tên chủ đề: Reconnaissance

GVHD: Ngô Đức Hoàng Sơn

Nhóm: 12

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O21.ANTT.1

| STT | Họ và tên | MSSV | Email |
|-----|------------------------|----------|------------------------|
| 1 | Nguyễn Triệu Thiên Bảo | 21520155 | 21520155@gm.uit.edu.vn |
| 2 | Trần Lê Minh Ngọc | 21521195 | 21521195@gm.uit.edu.vn |
| 3 | Huỳnh Minh Khuê | 21522240 | 21522240@gm.uit.edu.vn |

2. NỘI DUNG THỰC HIỆN:¹

| STT | Nội dung | Tình trạng | Trang |
|------------------|-----------|------------|-------|
| 1 | Yêu cầu 1 | 100% | |
| 2 | Yêu cầu 2 | 100% | |
| 3 | Yêu cầu 3 | 100% | |
| 4 | Yêu cầu 4 | 100% | |
| 5 | Yêu cầu 5 | 100% | |
| Điểm tự đánh giá | | | 10/10 |

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

1. Subdomain Enumeration

a) Liệt kê thông qua các nguồn trên internet

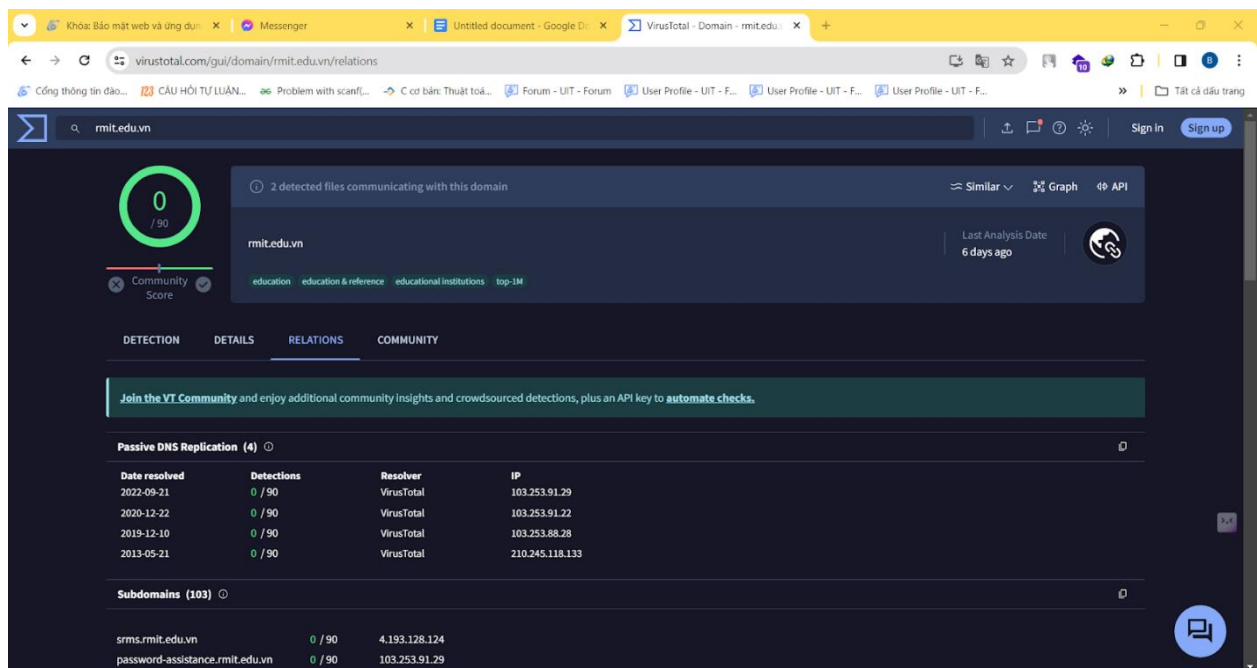
Chậm lại và suy nghĩ 1: Các nguồn có thể tìm kiếm dữ liệu công khai tên miền phụ ở đâu?

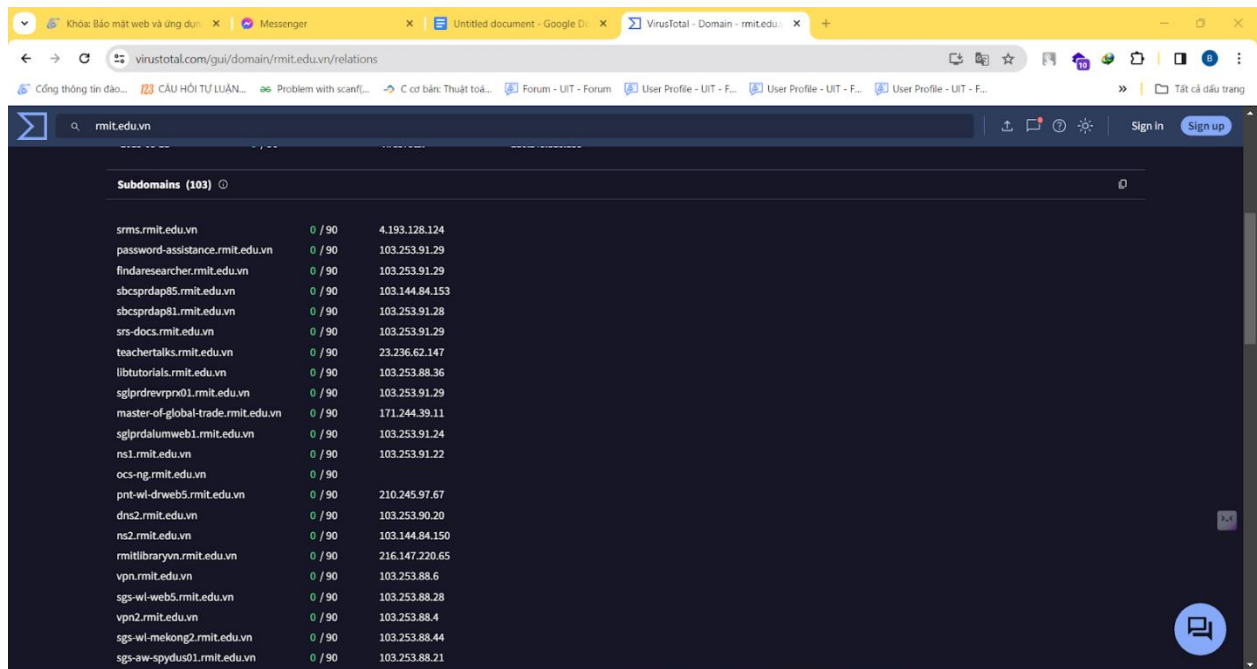
Có thể tìm kiếm tên miền phụ bằng các cách sau:

- Sử dụng các search engine (google, bing,...) và kỹ thuật google dorking
- Sử dụng các website chuyên tìm kiếm tên miền phụ như VirusTotal, Subdomain Finder,...

Bài tập 1: Liệt kê ra ít nhất 100 tên miền phụ của rmit.edu.vn, kết quả được lưu trong file csv.

- Sử dụng trang web VirusTotal để tìm kiếm, ta được kết quả như sau:





Kết quả được đính kèm trong file Lab3_ex01.csv

b) Tìm kiếm chủ động tên miền thông qua kỹ thuật brute-force

Chậm lại và suy nghĩ 2: Tập các danh sách tên miền phụ có thể tìm kiếm ở đâu và cách nào để đưa tên miền phụ vào burpsuite để tìm kiếm?

Tập danh sách các tên miền phụ có thể tìm được trong SecLists. SecLists là một bộ sưu tập các danh sách được sử dụng trong các đánh giá bảo mật, các loại danh sách bao gồm username, password, URL, DNS,...

Tập dữ liệu subdomain có thể được tìm thấy trong đường dẫn :

/usr/share/seclists/Discovery/DNS/...

Hoặc trong github:

<https://github.com/danielmiessler/SecLists/blob/master/Discovery/DNS/>

```

ngoc@ngoc: /usr/share/seclists/Discovery/DNS
File Actions Edit View Help
(ngoc@ngoc)-[~]
$ cd /usr/share/seclists/
(ngoc@ngoc)-[/usr/share/seclists]
$ ls
Discovery  IOCs  Passwords  Payloads  Usernames
Fuzzing  Miscellaneous  Pattern-Matching  README.md  Web-Shells
(ngoc@ngoc)-[/usr/share/seclists]
$ cd Discovery
(ngoc@ngoc)-[/usr/share/seclists/Discovery]
$ ls
DNS  File-System  Infrastructure  Mainframe  SNMP  Variables  Web-Content
(ngoc@ngoc)-[/usr/share/seclists/Discovery]
$ cd DNS
(ngoc@ngoc)-[/usr/share/seclists/Discovery/DNS]
$ ls
README.md
bitquark-subdomains-top100000.txt
bug-bounty-program-subdomains-trickest-inventory.txt
combined_subdomains.txt
deepmagic.com-prefixes-top500.txt
deepmagic.com-prefixes-top50000.txt
dns-3haddix.txt
fiercer-hostlist.txt
italian-subdomains.txt
n0kovo_subdomains.txt
namelist.txt
shubs-stackoverflow.txt
shubs-subdomains.txt
sortedcombined-knock-dnsrecon-fierce-reconng.txt
subdomains-spanish.txt
subdomains-top1million-110000.txt
subdomains-top1million-20000.txt
subdomains-top1million-5000.txt

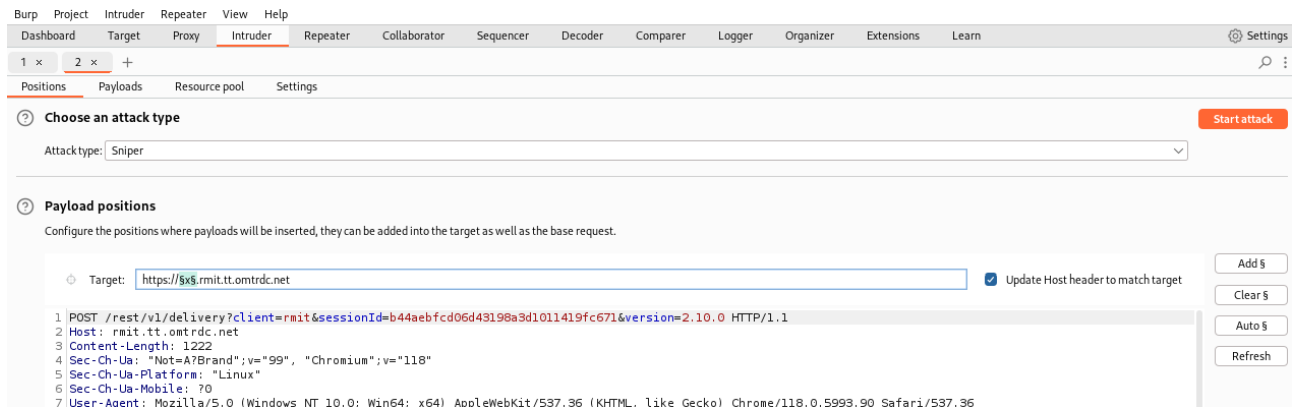
```

Bài tập 2: Dựa vào các tên miền phụ đã tìm kiếm được ở bài tập 1 và các tên miền đã bruteforce được thêm bằng burpsuite intruder. Phân loại các tên miền có kết quả trả về status code 200 và các tên miền có kết quả trả về khác.

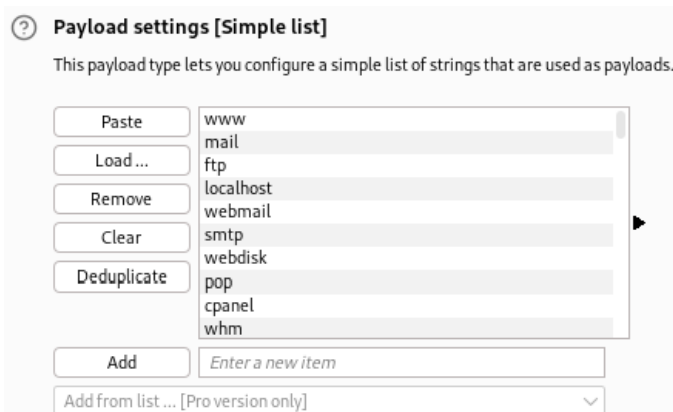
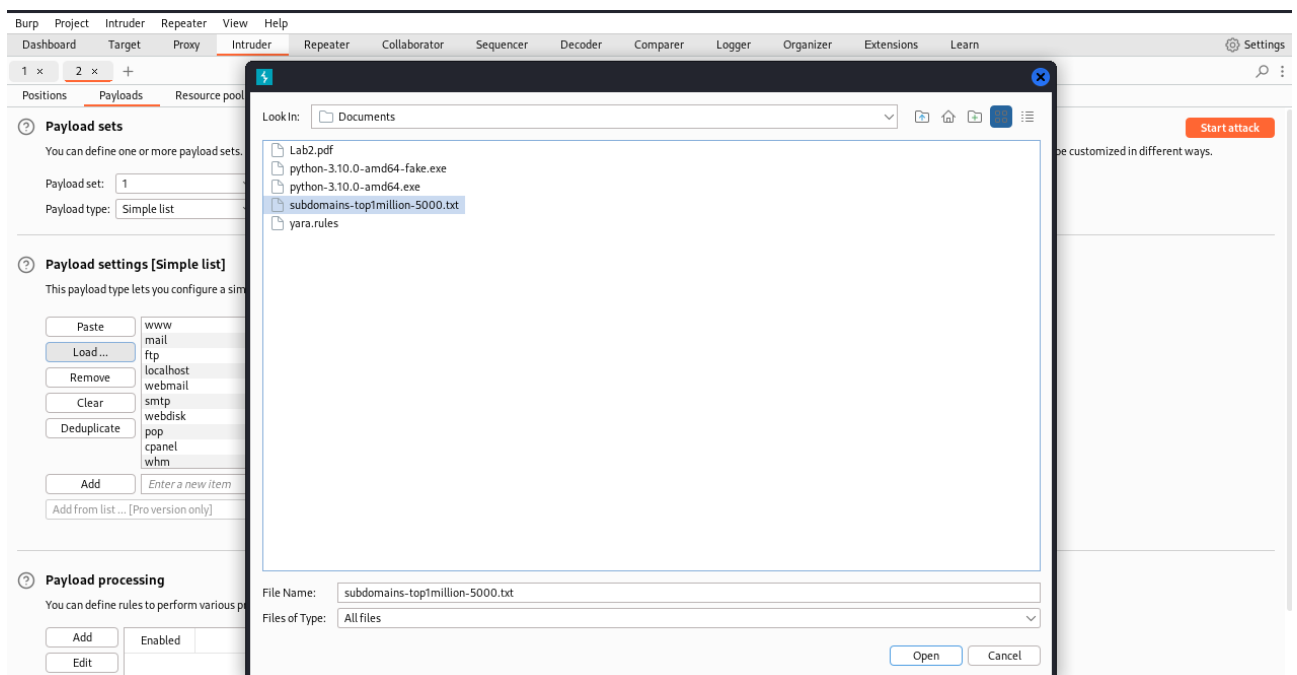
- **Bước 1:** Thực hiện truy vấn tên miền trong tab Proxy của Burpsuite. Sau đó đưa tên miền vào tab Intruder bằng cách nhấn chuột phải vào tên miền và chọn Send to Intruder.

| # | Host | Method | URL | Params | Editor |
|-----|-----------------------------------|--------|--|--------|--------|
| 177 | https://js.zohocdn.com | GET | /salesiq/js/embedpostload_AzTWQmR... | | |
| 4 | https://www.rmit.edu.vn | GET | /ruxitagentjs_ICANVfhru_10287240325... | | |
| 73 | https://dsum-sec.casalemedia.c... | GET | /rum?cm_dsp_id=88&external_user_id... | ✓ | |
| 169 | https://salesiq.zohopublic.com | GET | /rmituniversity/fetchvisitorconfiguratio... | ✓ | |
| 44 | https://rmit.tt.omtrdc.net | POST | /rest/v1/delivery?client=rmit&sessionId... | ✓ | |
| 175 | https://www.rmit.edu.vn | | https://www.rmit.edu.vn/rb_b...=3837081405&en=gdlxaxje&end=1 | | |
| 76 | https://www.rmit.edu.vn | | Add to scope | | |
| 176 | https://www.rmit.edu.vn | | Scan | | |
| 55 | https://cm.g.doubleclick.net | | | | |
| 49 | https://cm.g.doubleclick.net | | | | |
| 140 | https://sync.search.spotxchange | | Send to Intruder | | Ctrl+I |
| 96 | https://googleads.g.doubleclick | | Send to Repeater | | Ctrl+R |

- **Bước 2:** Vào tab Intruder để thực hiện bruteforce.



- **Bước 3:** Chọn tab Payloads trong Intruder và load tập dữ liệu được dùng để thực hiện bruteforce. Ở đây nhóm chọn tập dữ liệu là subdomains-top1million-5000.txt



- **Bước 4:** Nhấn nút Start attack để bắt đầu bruteforce. Quá trình tấn công sẽ diễn ra như sau:
- Kết quả được lưu trong file Lab3_ex02.csv

3. Intruder attack of https://\$x\$.rmit.tt.omtrdc.net - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request ^ | Payload | Target | Status code | Error | Timeout | Length | Comment |
|-----------|--------------|----------------------------------|-------------|--------------------------|--------------------------|--------|---------|
| 0 | | https://x.rmit.tt.omtrdc.net | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1139 | |
| 1 | www | https://www.rmit.tt.omtrdc.... | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1139 | |
| 2 | mail | https://mail.rmit.tt.omtrdc.... | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1139 | |
| 3 | ftp | https://ftp.rmit.tt.omtrdc.net | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1139 | |
| 4 | localhost | https://localhost.rmit.tt.omt... | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 1139 | |
| 5 | webmail | https://webmail.rmit.tt.omt... | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 6 | smtp | https://smtp.rmit.tt.omtrdc.... | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 7 | webdisk | https://webdisk.rmit.tt.omtr... | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 8 | pop | https://pop.rmit.tt.omtrdc.net | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 9 | cpanel | https://cpanel.rmit.tt.omtrd... | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 10 | whm | https://whm.rmit.tt.omtrdc.... | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 11 | ns1 | https://ns1.rmit.tt.omtrdc.net | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 12 | ns2 | https://ns2.rmit.tt.omtrdc.net | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 13 | autodiscover | https://autodiscover.rmit.tt.... | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 14 | autoconfig | https://autoconfig.rmit.tt.o... | | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 15 | ns | https://ns.rmit.tt.omtrdc.net | | <input type="checkbox"/> | <input type="checkbox"/> | | |

2. Host and Port Discovery

a) Tìm kiếm các host tương ứng

Chậm lại và suy nghĩ 3: Sử dụng cách nào để nhận được địa chỉ IP khi có được tên miền?

- Sử dụng lệnh nslookup để tra cứu tên miền
- Sử dụng các website chuyên tìm kiếm IP từ tên miền như Digital Ocean
- Sử dụng thư viện lập trình hoặc các API để tạo nên chương trình truy vấn IP từ tên miền

Bài tập 3: Ghi nhận lại các địa chỉ IP của tên miền phụ tìm được của *.rmit.edu.vn. Kết quả lưu trong file csv.

- Sử dụng lệnh nslookup để truy vấn IP từ tên miền

```
(kali@kali)-[~]
$ nslookup chame.rmit.edu.vn
Server:      192.168.81.2
Address:     192.168.81.2#53

Non-authoritative answer:
Name:   chame.rmit.edu.vn
Address: 192.0.78.235
Name:   chame.rmit.edu.vn
Address: 192.0.78.153

(kali@kali)-[~]
$
```

- Vì nslookup không thể nhận input đầu vào từ một file ngoài nên ta cần viết shell script vừa đọc được file vừa truy vấn bằng nslookup.

```
#!/bin/bash
for host in $(cat c1.txt);
do
    result=$(nslookup "$host" | grep "Address: " | awk '{print $2}');
    echo "$result"
done
```

- Chạy shell script trên ta được kết quả sau:

```
(kali㉿kali)-[~]
$ ./c2cp.sh
103.253.91.29
103.253.91.29
103.144.84.153
103.253.91.28
23.236.62.147
103.253.91.29
171.244.39.11
103.253.91.22
216.147.220.65
103.253.88.6
103.253.88.38
210.245.97.71
103.253.88.36
103.253.88.40
```

Chú thích: Các chỗ trống trong kết quả là do có một số subdomain không thể truy vấn được IP

Kết quả được đính kèm trong file Lab3_ex03.csv

b) Tìm kiếm port tương ứng

Chậm lại và suy nghĩ 4: Các công cụ scan port hiện nay có thể sử dụng là gì?

Các công cụ scan port thường được sử dụng hiện nay:

- *Nmap*: là một trong những công cụ scan port phổ biến nhất và mạnh mẽ. Nó cung cấp nhiều tính năng như scan port TCP và UDP, phân tích hệ thống, phát hiện phiên bản phần mềm và hệ điều hành, và nhiều tính năng khác.
- *Hping*: Hping là một công cụ mạnh mẽ cho việc tạo và gửi các gói tin mạng tùy chỉnh, có thể được sử dụng để kiểm tra các cổng mạng và phân tích các giao thức mạng.

- **Metasploit Framework:** Metasploit là một nền tảng thử nghiệm xâm nhập mạnh mẽ, cung cấp nhiều công cụ bao gồm một công cụ scan cổng mạng, ví dụ như Auxiliary Scanners. Metasploit có nhiều auxiliary modules được thiết kế để thực hiện quét cổng mạng như:

auxiliary/scanner/portscan/tcp, auxiliary/scanner/portscan/syn,...

```
msf6 > search auxiliary/scanner/portscan

Matching Modules
=====
```

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--------------------------------------|-----------------|--------|-------|---------------|
| 0 | auxiliary/scanner/portscan/ftpbounce | | normal | No | FTP Bounce Po |
| 1 | auxiliary/scanner/portscan/xmas | | normal | No | TCP "XMas" Po |
| 2 | auxiliary/scanner/portscan/ack | | normal | No | TCP ACK Firew |
| 3 | auxiliary/scanner/portscan/tcp | | normal | No | TCP Port Scan |
| 4 | auxiliary/scanner/portscan/syn | | normal | No | TCP SYN Port |

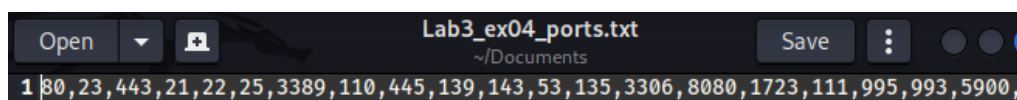
```
msf6 > search auxiliary/scanner/discovery

Matching Modules
=====
```

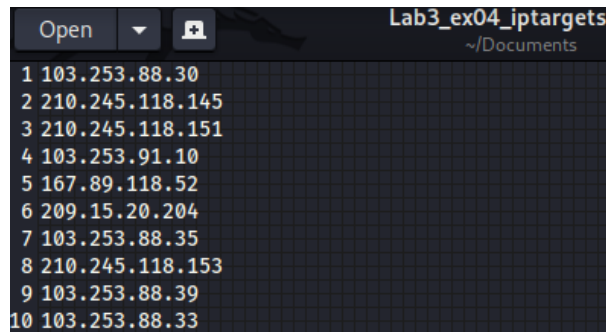
| # | Name | Disclosure Date | Rank | Check | Description |
|---|--|-----------------|--------|-------|--|
| 0 | auxiliary/scanner/discovery/arp_sweep | | normal | No | ARP Sweep Local Network Discovery |
| 1 | auxiliary/scanner/discovery/ipv6_multicast_ping | | normal | No | IPv6 Link Local/Node Local Ping Discovery |
| 2 | auxiliary/scanner/discovery/ipv6_neighbor | | normal | No | IPv6 Local Neighbor Discovery |
| 3 | auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement | | normal | No | IPv6 Local Neighbor Discovery Using Router Advertisement |
| 4 | auxiliary/scanner/discovery/empty_udp | | normal | No | UDP Empty Prober |
| 5 | auxiliary/scanner/discovery/udp_probe | | normal | No | UDP Service Prober |
| 6 | auxiliary/scanner/discovery/udp_sweep | | normal | No | UDP Service Sweeper |

Bài tập 4: Thực hiện scan 1000 port phổ biến trên các danh sách IP tìm được của *.rmit.edu.vn. Báo cáo kết quả tìm được trong file csv.

- Danh sách 1000 port phổ biến sẽ được lưu trong file Lab3_ex04_ports.txt



- Danh sách IP tìm được sẽ được lưu trong file Lab3_ex04_iptargets.txt

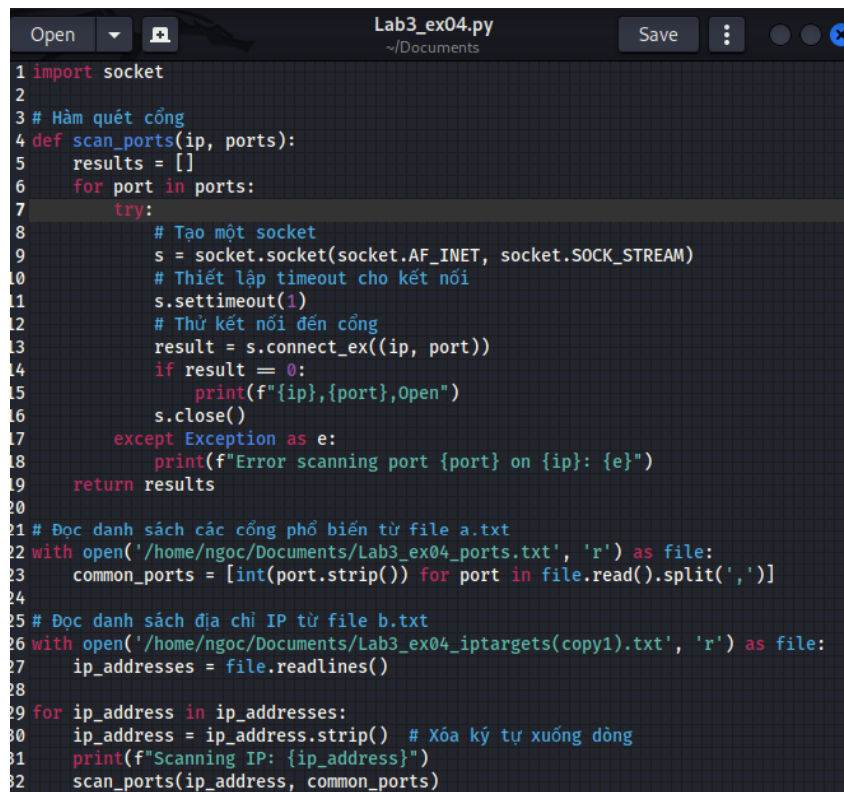


```

1 103.253.88.30
2 210.245.118.145
3 210.245.118.151
4 103.253.91.10
5 167.89.118.52
6 209.15.20.204
7 103.253.88.35
8 210.245.118.153
9 103.253.88.39
10 103.253.88.33

```

- Viết một đoạn code để duyệt tự động quá các port và danh sách IP tìm được ở câu 1, scan port và in kết quả ra màn hình

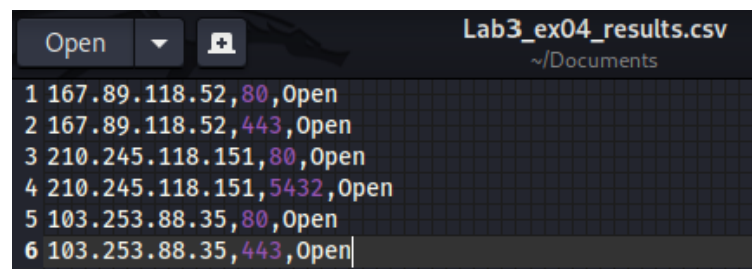


```

1 import socket
2
3 # Hàm quét cổng
4 def scan_ports(ip, ports):
5     results = []
6     for port in ports:
7         try:
8             # Tạo một socket
9             s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
10            # Thiết lập timeout cho kết nối
11            s.settimeout(1)
12            # Thử kết nối đến cổng
13            result = s.connect_ex((ip, port))
14            if result == 0:
15                print(f"{ip},{port},Open")
16            s.close()
17        except Exception as e:
18            print(f"Error scanning port {port} on {ip}: {e}")
19    return results
20
21 # Đọc danh sách các cổng phổ biến từ file a.txt
22 with open('/home/ngoc/Documents/Lab3_ex04_ports.txt', 'r') as file:
23     common_ports = [int(port.strip()) for port in file.read().split(',')]
24
25 # Đọc danh sách địa chỉ IP từ file b.txt
26 with open('/home/ngoc/Documents/Lab3_ex04_iptargets(copy1).txt', 'r') as file:
27     ip_addresses = file.readlines()
28
29 for ip_address in ip_addresses:
30     ip_address = ip_address.strip() # Xóa ký tự xuống dòng
31     print(f"Scanning IP: {ip_address}")
32     scan_ports(ip_address, common_ports)

```

- Kết quả sẽ được lưu trong file Lab3_ex04_result.csv



```

1 167.89.118.52,80,Open
2 167.89.118.52,443,Open
3 210.245.118.151,80,Open
4 210.245.118.151,5432,Open
5 103.253.88.35,80,Open
6 103.253.88.35,443,Open

```

3. Truy tìm thông tin của website

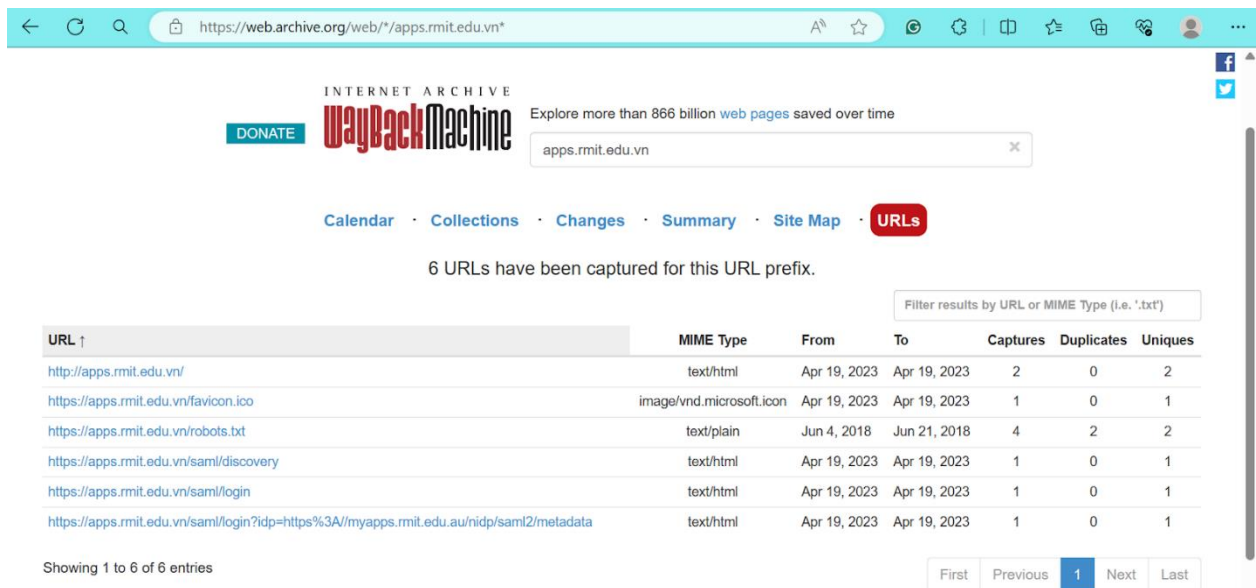
a) Tìm kiếm thông qua Internet Archive

Bài tập 5: Sử dụng <https://web.archive.org/> tìm kiếm và ghi nhận lại dữ liệu quá khứ các tên miền phụ không còn tồn tại hiện nay của *.rmit.edu.vn.

- Chọn một vài tên miền trong các tên miền phụ của rmit.edu.vn để tìm kiếm trên trang web <https://web.archive.org/>



- Kết quả tìm kiếm: ta có thể thấy các tên miền phụ trên đã không còn tồn tại từ năm 2023 trở về trước.



Báo cáo Lab3
HOC KỲ 2 – NĂM HOC 2023-2024

The screenshot shows the Exploit Database interface. The search results are displayed in a table with columns: Date Added, Dork, Category, and Author. The search term 'domain' is entered in the Quick Search box.

| Date Added | Dork | Category | Author |
|------------|--|--------------------------------|----------------------|
| 2023-10-02 | intitle:"index of" "domain.txt" | Files Containing Juicy Info | Ranjeet Jaiswal |
| 2021-09-16 | intitle:"Domain Default page" "Parallels IP Holdings GmbH" | Web Server Detection | Mugdha Peter Bansode |
| 2021-08-23 | intitle:"ManageEngine ServiceDesk Plus" "domain" intext:"ManageEngine ServiceDesk Plus" ".com" | Pages Containing Login Portals | s Thakur |
| 2021-02-01 | inurl:print.htm intext:"Domain Name:" + "Open printable report" | Sensitive Directories | Alexandros Pappas |
| 2020-01-27 | intitle:"index of" domain.key -public | Sensitive Directories | Bruno Schmid |
| 2019-09-17 | index.of "crossdomain.xml" | Files Containing Juicy Info | Mayur Parmar |
| 2018-07-10 | inurl:"root?originalDomain" | Files Containing Juicy Info | Bruno Schmid |

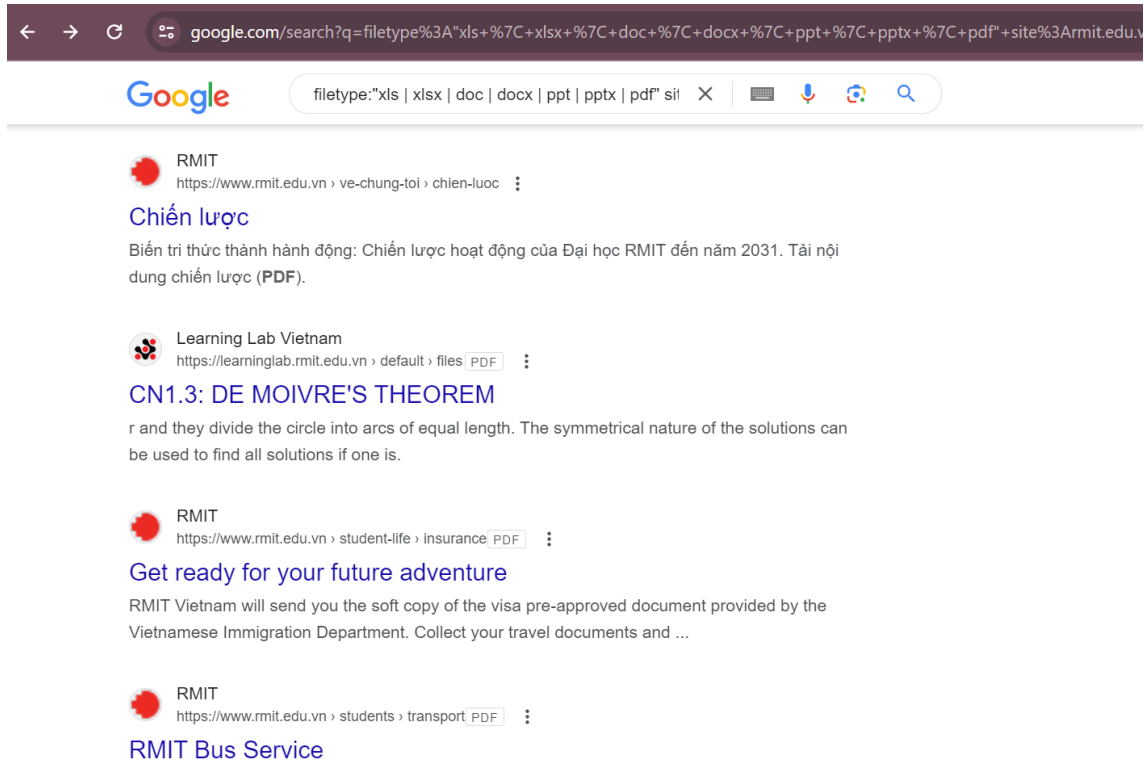
- Sử dụng lệnh để tìm kiếm file PDF:
intitle:"Index of" "rmit.edu.vn.pdf"
filetype:"pdf" site:rmit.edu.vn

The screenshot shows a Google search result for the query: `intitle:"index of" "rmit.edu.vn.pdf" filetype:"pdf" site:rmit.edu.vn`. The search results show approximately 9 results (0.49 seconds).

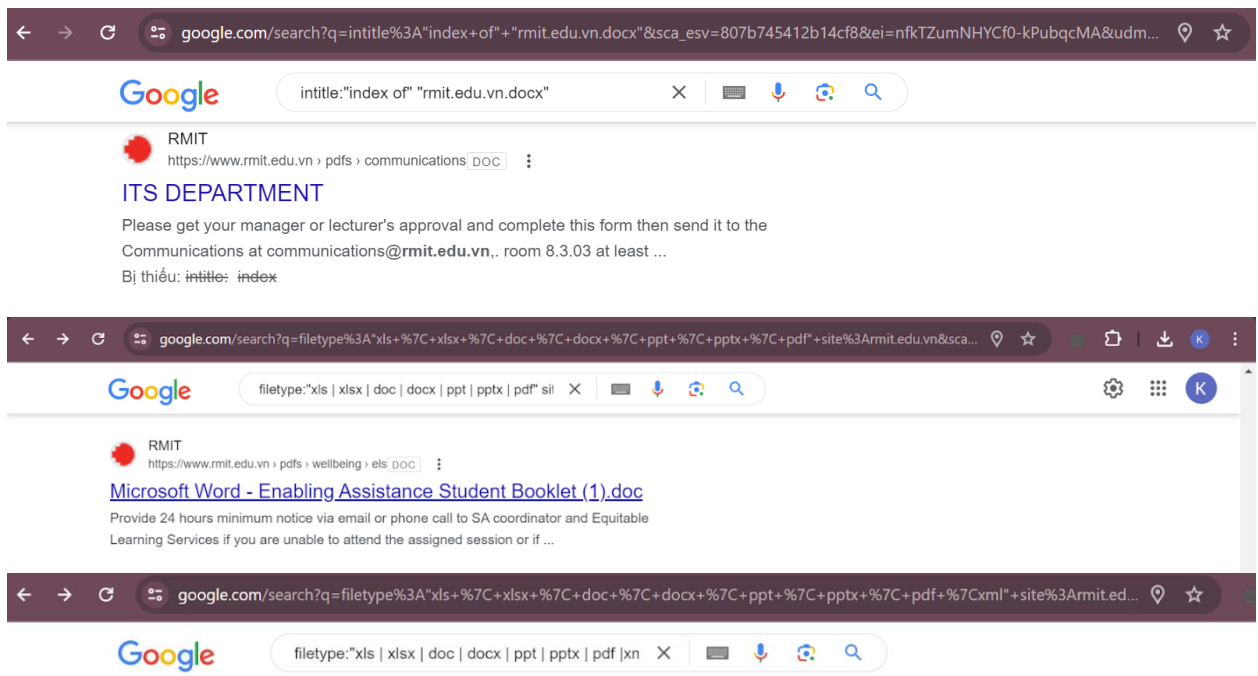
Không tìm thấy kết quả nào cho `intitle:"index of" "rmit.edu.vn.pdf"`.

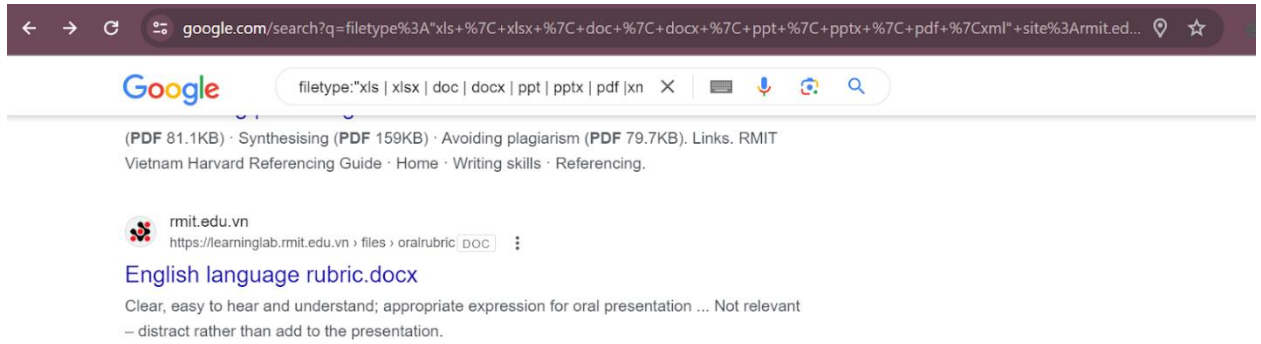
Kết quả cho `intitle: index of rmit.edu.vn.pdf` (không có dấu gạch kép):

- RMIT**
<https://www.rmit.edu.vn/pdfs/about-us> PDF
- Vietnam Country Commitment**
4 thg 6, 2023 — In over more than two decades, **RMIT Vietnam** has become a vibrant part of Vietnam's education landscape, industry ecosystems and broader ...
Bị thiếu: `intitle:` | Phải có: `intitle:`
- RMIT**
<https://www.rmit.edu.vn/pdfs/english-pdf/a...> PDF
- application form - đơn đăng ký nhập học**
I will notify **RMIT** University **Vietnam** immediately of any change to my personal details. Tôi xác nhận rằng tôi hiểu rõ tất cả các thông tin tôi đã điền trong đơn ...

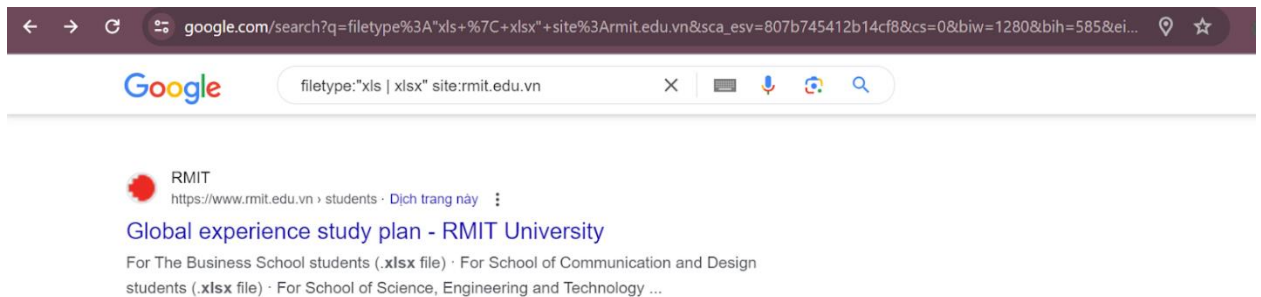
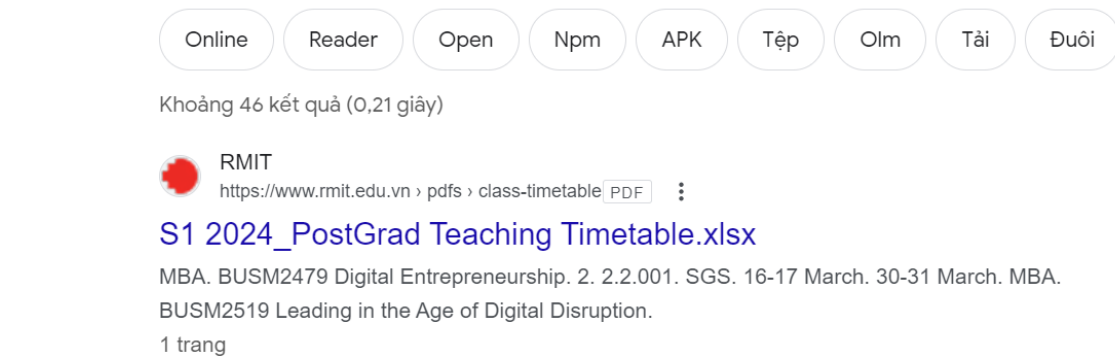
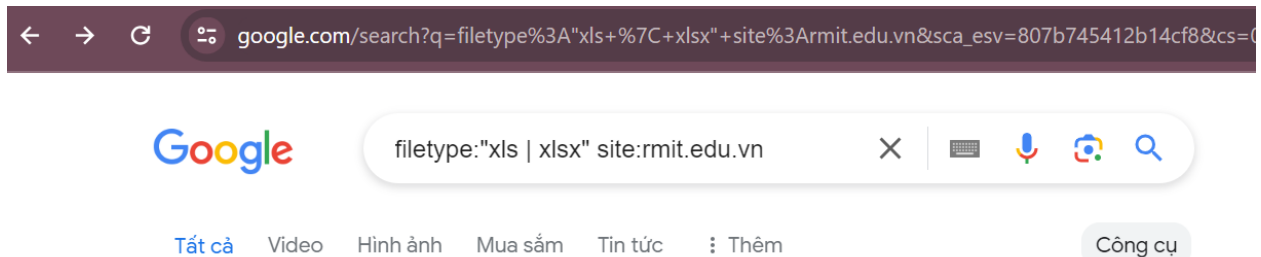


- Sử dụng lệnh để tìm kiếm file Word:
intitle:"Index of" "rmit.edu.vn.docx"
filetype:"doc | docx" site:rmit.edu.vn





- Sử dụng lệnh để tìm kiếm file Excel: **filetype:"xls | xlsx" site:rmit.edu.vn**



Google search results for "filetype:xls | xlsx" site:rmit.edu.vn

rmit.edu.vn
https://rmitlibraryvn.rmit.edu.vn › action › Dịch trang này

Prediction and analysis of three gene families related to leaf ...
viết bởi FY Peng · 2017 · Trích dẫn 23 bài viết — (XLSX 141 kb). Additional file 2: Annotation of the putative ABC, NLR and START genes in wheat using the sequences of plant resistance...

rmit.edu.vn
https://rmitlibraryvn.rmit.edu.vn › action › Dịch trang này

Mapping quantitative trait loci associated with leaf rust ...
viết bởi FE Bokore · 2020 · Trích dẫn 29 bài viết — (XLSX). S1 Table. Pedigree description and expected leaf rust resistance genes of wheat cultivars used in to generate five mapping ...

rmit.edu.vn
https://rmitlibraryvn.rmit.edu.vn › action › Dịch trang này

Edible solid lipid nanoparticles (SLN) as carrier system for ...
viết bởi K Oehlke · 2017 · Trích dẫn 75 bài viết — (XLSX). S2 Dataset. Proportions of peak, peak 2 and peak 3 in melting curves of SLN containing different amounts of FA or Toc....

c) Tìm kiếm thông tin qua github

Bài tập 7: Ghi nhận một vài thông tin tìm được trên github với domain *.rmit.edu.vn. (lưu ý: không sử dụng thông tin này để khai thác thông tin cá nhân có thể có, mọi hành vi sử dụng không được phép sẽ chịu trách nhiệm trước pháp luật)

- Thực hiện tìm kiếm trên rmit.edu.vn

GitHub search results for "apps.rmit.edu.vn"

Filter by

- <> Code 15
- Repositories 0
- Issues 0
- Pull requests 0
- Discussions 0
- Users 0
- More

Languages

- Text
- CSV
- More languages...

15 files (389 ms)

trickest/inventory - RMIT University Vulnerability Disclosure Program/hostnames.txt

```
125 apps.itsdev.rmit.edu.vn
126 apps.rmit.edu.vn
127 apps.staging.rmit.edu.vn
```

Show 11 more matches

0xrh0d4m1n/inventory - RMIT University Vulnerability Disclosure Program/servers.txt

```
15 https://policies-dev.its.rmit.edu.au:443
16 https://omeka.rmit.edu.vn:443
17 https://podcasts.online.rmit.edu.au:443
18 http://apps.rmit.edu.vn:80
19 http://artcollection.rmit.edu.au:80
20 https://redcap.rmit.edu.au:443
21 http://nas.rmit.edu.au:80
```

- Danh sách các lỗ hổng server của trường đại học RMIT đã được phát hiện và báo cáo cho Vulnerability Disclosure Program.

Files

38bc04a

Go to file

RMIT University Vulnerability Dis...

dns-report.csv

hostnames.txt

server-report.csv

servers.txt

Rabobank

Railto LLC

Rakuten VDP

Range

Rarible

Razer

Razorpay

inventory / RMIT University Vulnerability Disclosure Program / server-report.csv

Preview Code Blame 54 lines (54 loc) · 31.8 KB Code 55% faster with GitHub Copilot

Raw

| | | | | |
|----|---|---|-----|-----|
| 20 | next.rmit.edu.au | RMIT NEXT | 200 | 366 |
| 21 | nrtgps.smgs.rmit.edu.au | 403 Forbidden | 403 | 202 |
| 22 | omeka.rmit.edu.vn | INTRODUCTION TO THIS ARCHIVE · An Urban Archive of District 4, Ho Chi Minh City | 200 | 265 |
| 23 | orsee.bf.rmit.edu.au | ORSEE3: | 200 | 735 |
| 24 | podcasts.online.rmit.edu.au | | 403 | 243 |
| 25 | policies-dev.its.rmit.edu.au | 403 Forbidden | 403 | 294 |
| 26 | postgrad.rmit.edu.au | Postgraduate study - RMIT University | 200 | 406 |
| 27 | pss.sagepub.com.ezproxy.lib.rmit.edu.au | Shibboleth Authentication Request | 200 | 137 |
| 28 | redcap.rmit.edu.au | REDCap | 200 | 362 |
| 29 | results-stg.seup.rmit.edu.vn | Sign in to your account | 200 | 200 |
| 30 | rusu.rmit.edu.au | RUSU - RUSU Homepage | 200 | 345 |
| 31 | sgs-wl-omeka.rmit.edu.vn | 403 Forbidden | 403 | 202 |
| 32 | shortcourses.rmit.edu.au | Short courses - RMIT University | 200 | 378 |