Phòng thí nghiệm An toàn Thông tin InsecLab
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Tên chủ đề: Lab 3 - Reconnaissance

GVHD: Ngô Đức Hoàng Sơn

Nhóm: 14

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	Vũ Tuấn Sơn	21521389	21521389@gm.uit.edu.vn
2	Bùi Đức Anh Tú	21522735	21522735@gm.uit.edu.vn
3	Lê Huy Hiệp	21522067	21522067@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	90%	1 - 3
2	Yêu cầu 2	50%	3 - 5
3	…	…	…
Điểm tự đánh giá			**?/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

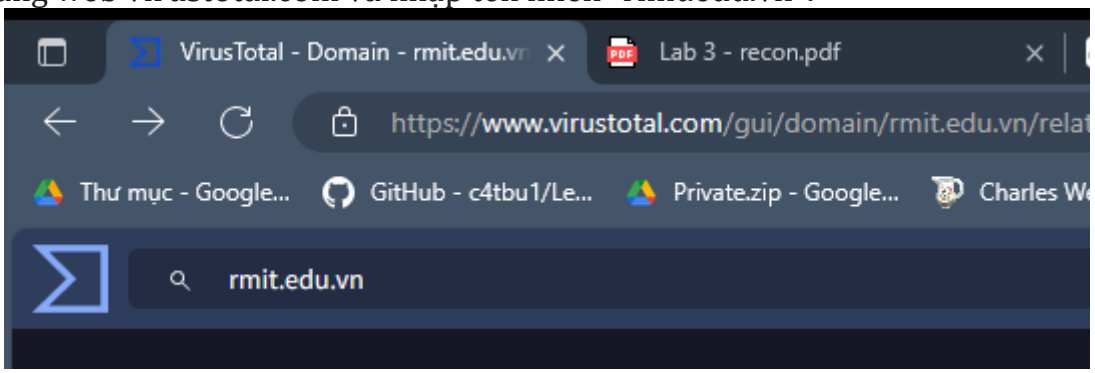
BÁO CÁO CHI TIẾT

1. Subdomain Enumeration

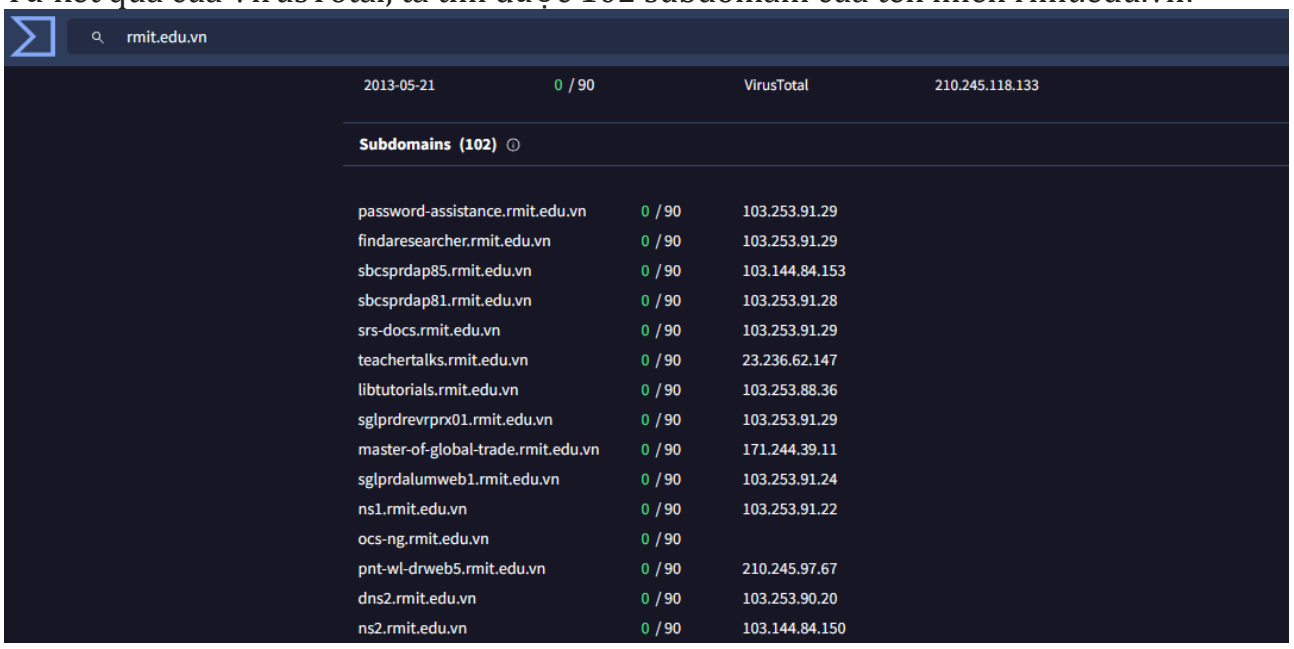
a) Liệt kê thông qua các nguồn trên Internet:

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

Vào trang web virustotal.com và nhập tên miền "rmit.edu.vn":



Từ kết quả của VirusTotal, ta tìm được 102 subdomain của tên miền rmit.edu.vn:



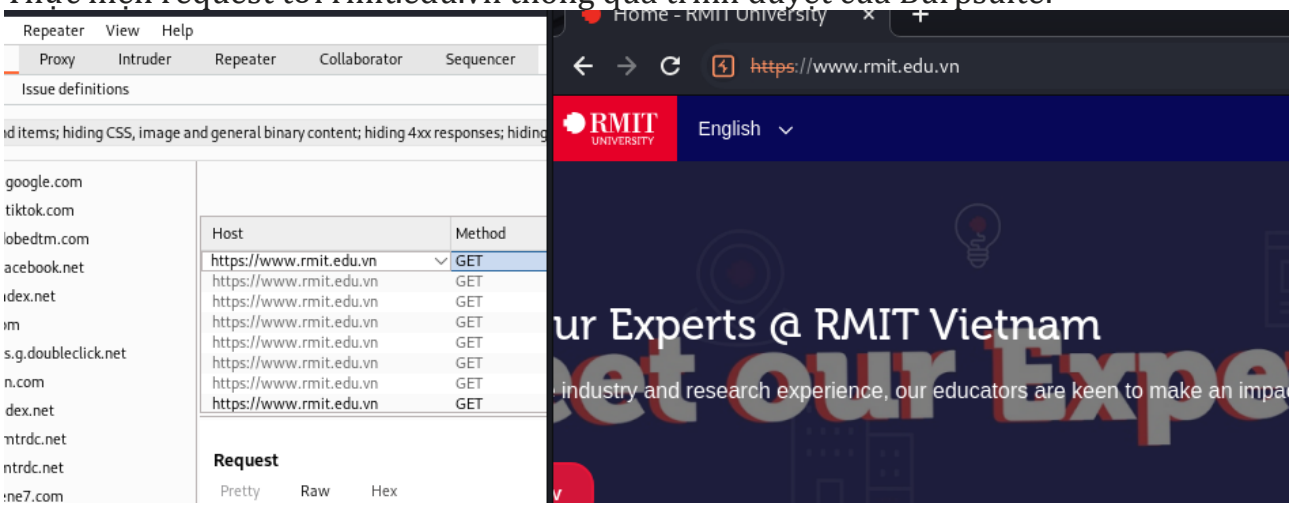
Ta copy các tên miền vừa tìm được vào 1 file .csv để chuẩn bị cho các bước tiếp theo:

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ cat 100rmitDomain.csv
password-assistance.rmit.edu.vn
findaresearcher.rmit.edu.vn
sbcsprdap85.rmit.edu.vn
sbcsprdap81.rmit.edu.vn
srs-docs.rmit.edu.vn
teachertalks.rmit.edu.vn
libtutorials.rmit.edu.vn
sglprdrevrprx01.rmit.edu.vn
master-of-global-trade.rmit.edu.vn
sglprdalumweb1.rmit.edu.vn
ns1.rmit.edu.vn
ocs-ng.rmit.edu.vn
pnt-wl-drweb5.rmit.edu.vn
dns2.rmit.edu.vn
ns2.rmit.edu.vn
rmitlibraryvn.rmit.edu.vn
vpn.rmit.edu.vn
sgs-wl-web5.rmit.edu.vn
vpn2.rmit.edu.vn
sgs-wl-mekong2.rmit.edu.vn
sgs-aw-spydus01.rmit.edu.vn
sgs-aw-hrapp1.rmit.edu.vn
drwprdhrapp01.rmit.edu.vn
sgs-wl-omeka.rmit.edu.vn
```

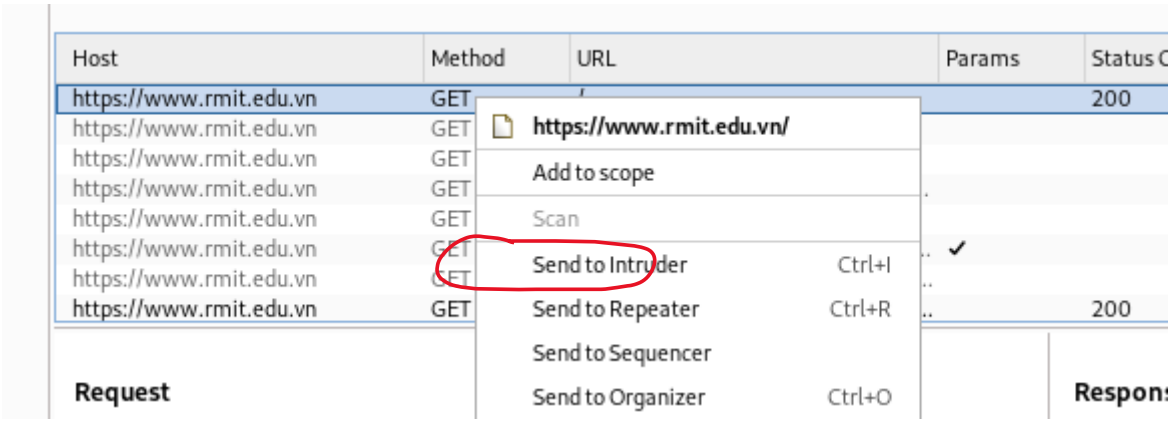
b) Tìm kiếm chủ động tên miền thông qua kĩ thuật brute-force

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.

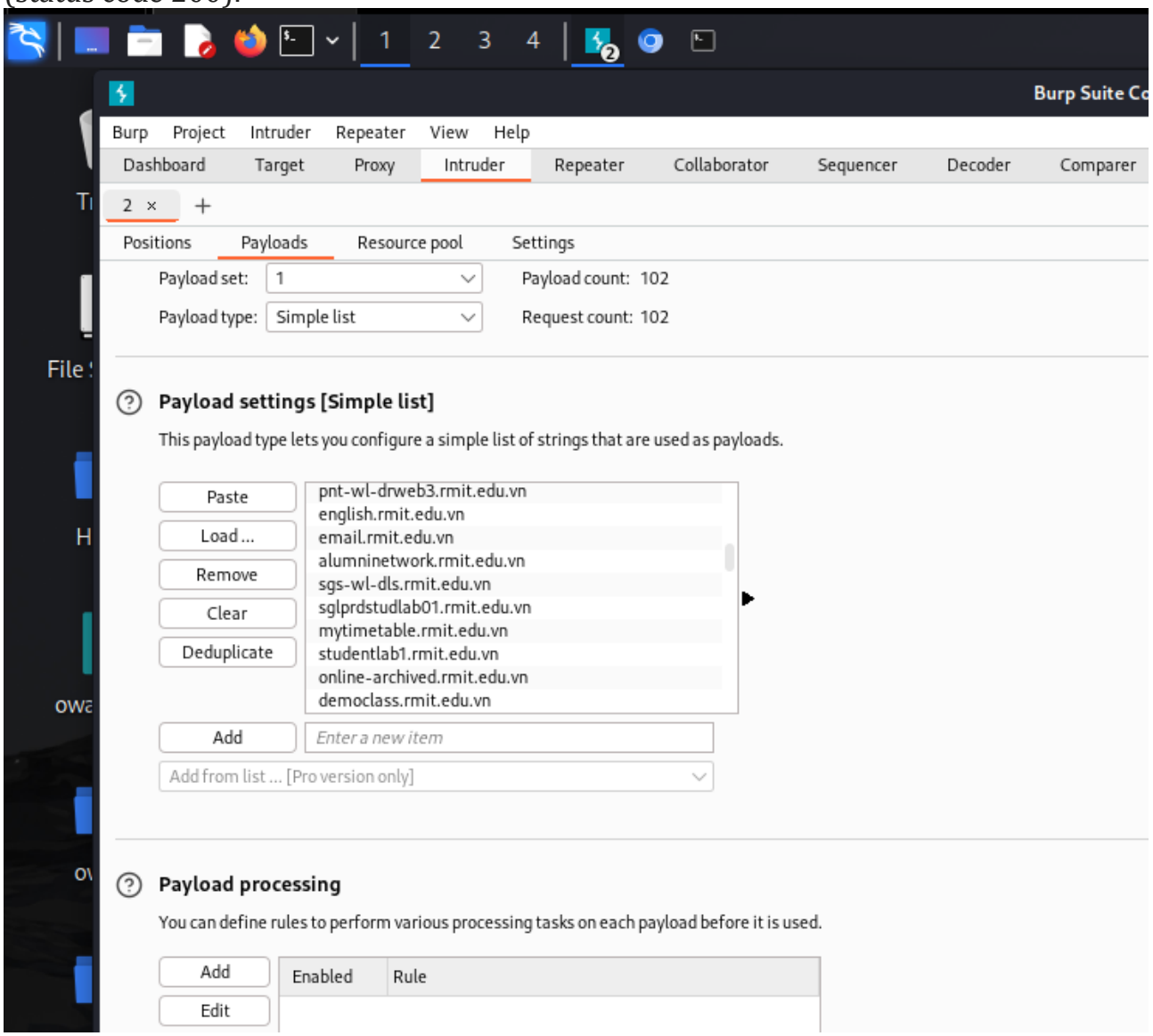
Thực hiện request tới rmit.edu.vn thông qua trình duyệt của Burpsuite:



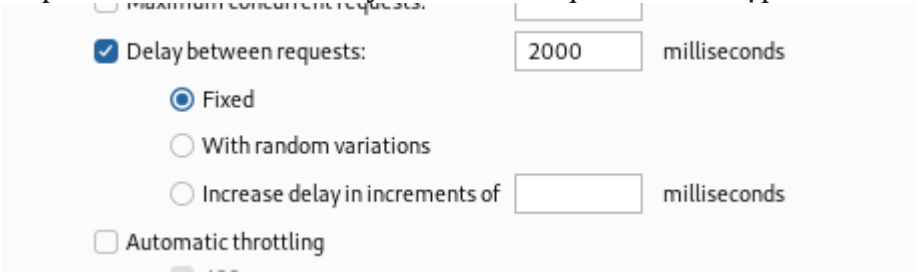
Chuột phải chọn 1 request và chọn Send to Intruder:



Làm theo hướng dẫn các bước trong link tại [đây] với payload là file .csv được tạo ra từ các subdomain đã tìm thấy bên trên để tiến hành tìm các tên miền có thể truy cập được (status code 200):



Để tránh bị coi là bruteforce vào tên miền này, ta sẽ cho delay các request bằng cách chọn Resource pool → tick vào ô delay between requests và nhập số ms mình muốn:



Sau khi chạy xong, ta lọc được request tới các subdomain sau đây có status code 200:

Request	Payload	Target	Status code	Response received
0		https://www.rmit.edu.vn	200	92
2	findaresearcher.rmit.edu.vn	https://findaresearcher.rmit.edu.vn	200	144
7	libtutorials.rmit.edu.vn	https://libtutorials.rmit.edu.vn	200	101
10	sglprdalumweb1.rmit.edu.vn	https://sglprdalumweb1.rmit.edu.vn	200	190
29	english.rmit.edu.vn	https://english.rmit.edu.vn	200	316
31	alumninetwork.rmit.edu.vn	https://alumninetwork.rmit.edu.vn	200	1012
33	sglprdstudlab01.rmit.edu.vn	https://sglprdstudlab01.rmit.edu.vn	200	144
35	studentlab1.rmit.edu.vn	https://studentlab1.rmit.edu.vn	200	155
37	democlass.rmit.edu.vn	https://democlass.rmit.edu.vn	200	171
38	experienceday.rmit.edu.vn	https://experienceday.rmit.edu.vn	200	201
48	helpdesk.rmit.edu.vn	https://helpdesk.rmit.edu.vn	200	204
72	sas.rmit.edu.vn	https://sas.rmit.edu.vn	200	313
75	pe.rmit.edu.vn	https://pe.rmit.edu.vn	200	787
76	omeka.rmit.edu.vn	https://omeka.rmit.edu.vn	200	366
90	design.rmit.edu.vn	https://design.rmit.edu.vn	200	558
92	chame.rmit.edu.vn	https://chame.rmit.edu.vn	200	107
95	etal.rmit.edu.vn	https://etal.rmit.edu.vn	200	600
99	learninglab.rmit.edu.vn	https://learninglab.rmit.edu.vn	200	1022
102	www.rmit.edu.vn	https://www.rmit.edu.vn	200	372
6	teachertalks.rmit.edu.vn	https://teachertalks.rmit.edu.vn	301	541

Như vậy, ta tìm được 18 subdomain trả về status code 200. Còn lại sẽ là các status code khác.

2. Host and Port Discovery

a) Tìm kiếm các host tương ứng

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

Do ta đã tìm hơn 100 subdomain khác nhau của *.rmit.edu.vn nên để dễ dàng hơn cho việc tìm kiếm IP, ta sẽ sử dụng Shellscript.

Nội dung của Shellscript như sau:

```
┌──(kali㉿kali)-[~]
└─$ cat rmit_ip.sh
#!/bin/bash

for i in $(cat 100rmitDomain.csv); do
        printf "%s\\n" $(resolveip -s "$i") >> rmit_ip.csv
done
```

Shellscript này sẽ thực hiện việc lấy từng dòng của file 100rmitDomain.csv (file chứa các subdomain đã tìm được) và sử dụng công cụ resolveip để tìm IP của subdomain đó. Tất cả các kết quả sẽ được ghi thành từng dòng trong file "rmit_ip.csv".

Tiến hành chạy thử đoạn script trên và kiểm tra:

```
┌──(kali㉿kali)-[~]
└─$ ./rmit_ip.sh
resolveip: Unable to find hostid for 'srs-docs.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'ocs-ng.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'pnt-wl-drweb5.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'dns2.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-web5.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-mekong2.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-aw-spydus01.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'password.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'pnt-wl-drweb3.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-dls.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'online-archived.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'ave.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'careerhub.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'crm.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'dialin.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'election.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'ems.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'itop.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'lyncdiscover.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'mekong.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'mekong1.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'orsee.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-web3.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-ww-livesrv.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sip.rmit.edu.vn': host not found
```

```
┌──(kali㉿kali)-[~]
└─$ cat rmit_ip.csv
103.253.91.29
103.253.91.29
103.144.84.153
103.253.91.28

23.236.62.147
103.253.88.36
103.253.91.29
171.244.39.11
103.253.91.24
103.253.91.22



103.144.84.150
216.147.220.65
103.253.88.6

103.253.88.4


103.253.88.38
210.245.97.71
```

Sau đó dùng lệnh "paste" để nối 2 file này với nhau theo từng dòng.
Ta có kết quả cuối cùng:

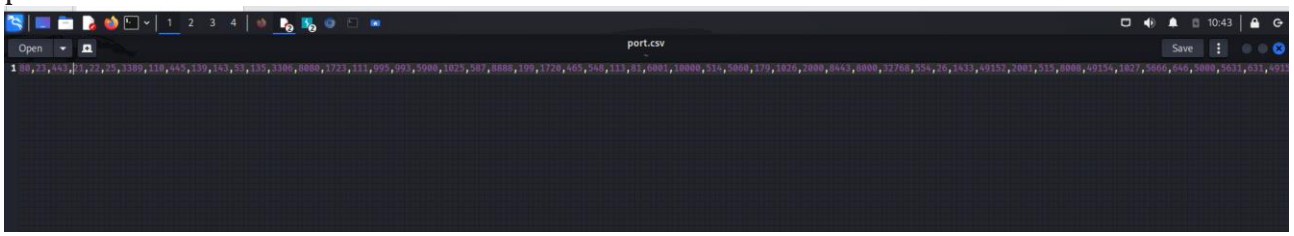
```
┌──(kali㉿kali)-[~]
└─$ paste 100rmitDomain.csv rmit_ip.csv > rmit_subdomain_ip.csv

┌──(kali㉿kali)-[~]
└─$ cat rmit_subdomain_ip.csv
password-assistance.rmit.edu.vn 103.253.91.29
findaresearcher.rmit.edu.vn     103.253.91.29
sbcsprdap85.rmit.edu.vn 103.144.84.153
sbcsprdap81.rmit.edu.vn 103.253.91.28
srs-docs.rmit.edu.vn
teachertalks.rmit.edu.vn        23.236.62.147
libtutorials.rmit.edu.vn        103.253.88.36
sglprdrevrprx01.rmit.edu.vn     103.253.91.29
master-of-global-trade.rmit.edu.vn      171.244.39.11
sglprdalumweb1.rmit.edu.vn      103.253.91.24
ns1.rmit.edu.vn 103.253.91.22
ocs-ng.rmit.edu.vn
pnt-wl-drweb5.rmit.edu.vn
dns2.rmit.edu.vn
ns2.rmit.edu.vn 103.144.84.150
rmitlibraryvn.rmit.edu.vn       216.147.220.65
vpn.rmit.edu.vn 103.253.88.6
sgs-wl-web5.rmit.edu.vn
vpn2.rmit.edu.vn        103.253.88.4
sgs-wl-mekong2.rmit.edu.vn
sgs-aw-spydus01.rmit.edu.vn
```

b) Tìm kiếm port tương ứng

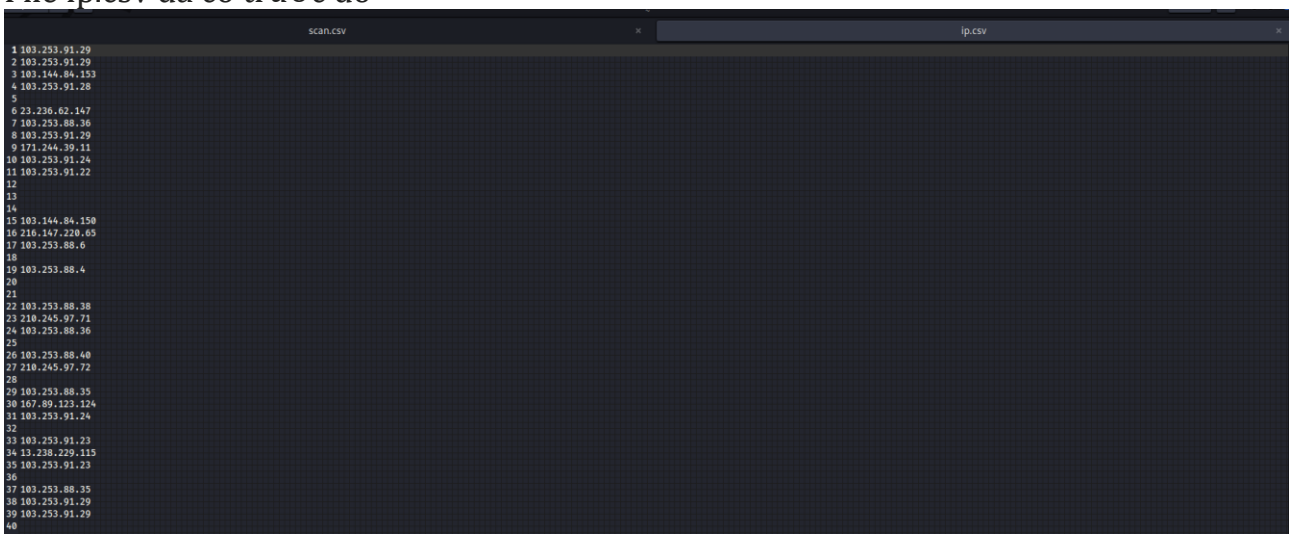
Bài tập 4: Thực hiện scan 1000 port phổ biến trên các danh sách IP tìm được của *.rmit.edu.vn. Báo cáo kết quả tìm được trong file csv

Dựa vào danh sách port đã được cung cấp
https://raw.githubusercontent.com/HeckerBirb/top-nmap-ports-csv/master/top-1000-most-popular-tcp-ports-nmap-sorted.csv

Trong danh sách có 2 port 1 và 1999 bị trùng lặp. Loại bỏ port trùng lặp và đưa vào file port.csv



File ip.csv đã có trước đó



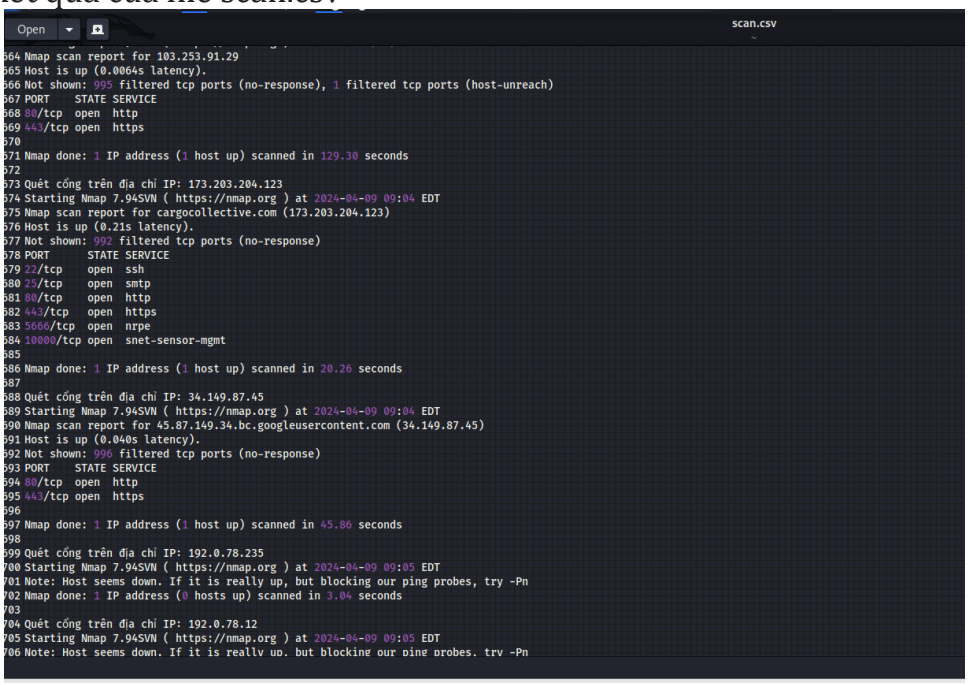
Thực hiện tự động hóa quét port bằng đoạn mã bash script

```bash
#!/bin/bash

# Kiểm tra xem tệp port.csv có tồn tại không
if [ ! -f "port.csv" ]; then
    echo "Tệp port.csv không tồn tại."
    exit 1
fi

# Kiểm tra xem tệp ip.csv có tồn tại không
if [ ! -f "ip.csv" ]; then
    echo "Tệp ip.csv không tồn tại."
    exit 1
fi

# Kiểm tra xem tệp scan.csv đã tồn tại, nếu không thì tạo mới và ghi tiêu đề
if [ ! -f "scan.csv" ]; then
    > scan.csv
fi

# Đọc từng địa chỉ IP từ tệp ip.csv và thực hiện quét
while IFS= read -r target_ip; do

    # Loại bỏ khoảng trắng đầu và cuối của địa chỉ IP
    target_ip=$(echo "$target_ip" | tr -d '[:space:]')
    # Kiểm tra nếu địa chỉ IP không trống
    if [ -n "$target_ip" ]; then
        echo
        echo "Quét cổng trên địa chỉ IP: $target_ip"
        echo >> scan.csv
        echo "Quét cổng trên địa chỉ IP: $target_ip">> scan.csv
        # Thực hiện quét với Nmap
        nmap -p $(cat port.csv | tr '\n' ',') $target_ip >> scan.csv
    fi
done < "ip.csv"
```

Mục đích là đưa 2 file ip.csv và port.csv vào và sử dụng nmap để tự động quét file port cho mỗi địa chỉ IP
Cuối cùng là đưa output vào file scan.csv
Thực hiện đoạn bash script

```
┌──(kali㉿kali)-[~]
└─$ ./doccsv.sh ip.csv port.csv

Quét cổng trên địa chỉ IP: 103.253.91.29

Quét cổng trên địa chỉ IP: 103.253.91.29

Quét cổng trên địa chỉ IP: 103.144.84.153

Quét cổng trên địa chỉ IP: 103.253.91.28

Quét cổng trên địa chỉ IP: 23.236.62.147

Quét cổng trên địa chỉ IP: 103.253.88.36

Quét cổng trên địa chỉ IP: 103.253.91.29

Quét cổng trên địa chỉ IP: 171.244.39.11

Quét cổng trên địa chỉ IP: 103.253.91.24

Quét cổng trên địa chỉ IP: 103.253.91.22

Quét cổng trên địa chỉ IP: 103.144.84.150

Quét cổng trên địa chỉ IP: 216.147.220.65

Quét cổng trên địa chỉ IP: 103.253.88.6

Quét cổng trên địa chỉ IP: 103.253.88.4

Quét cổng trên địa chỉ IP: 103.253.88.38

Quét cổng trên địa chỉ IP: 210.245.97.71

Quét cổng trên địa chỉ IP: 103.253.88.36

Quét cổng trên địa chỉ IP: 103.253.88.40

Quét cổng trên địa chỉ IP: 210.245.97.72

Quét cổng trên địa chỉ IP: 103.253.88.35

Quét cổng trên địa chỉ IP: 167.89.123.124

Quét cổng trên địa chỉ IP: 103.253.91.24

Quét cổng trên địa chỉ IP: 103.253.91.23
```

Sau khi chạy xong vào xem file scan.csv
Một phần kết quả của file scan.csv



3. Truy tìm thông tin của website

a) Tìm kiếm thông qua Internet Archive

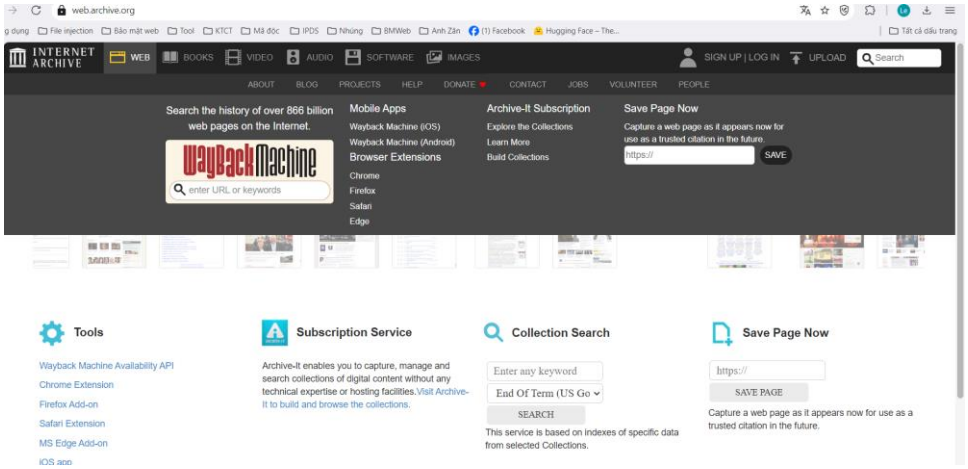
Internet Archive là một thư viện số phi lợi nhuận có trụ sở tại San Francisco, với sứ mệnh lưu trữ nội dung trên Internet. Một trong những dự án nổi tiếng của họ là Wayback Machine, một công cụ cho phép xem lại các phiên bản trang web từ quá khứ

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.

Khi tên miền phụ không còn hoạt động nó sẽ trả về status code 4xx

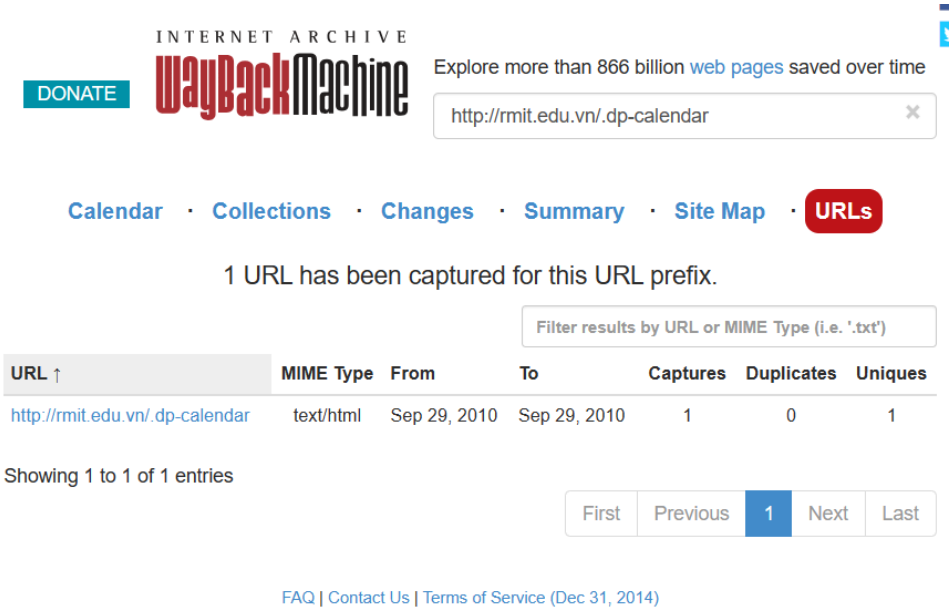
Thực hiện tìm kiếm thông qua Internet Archive

Giao diện:

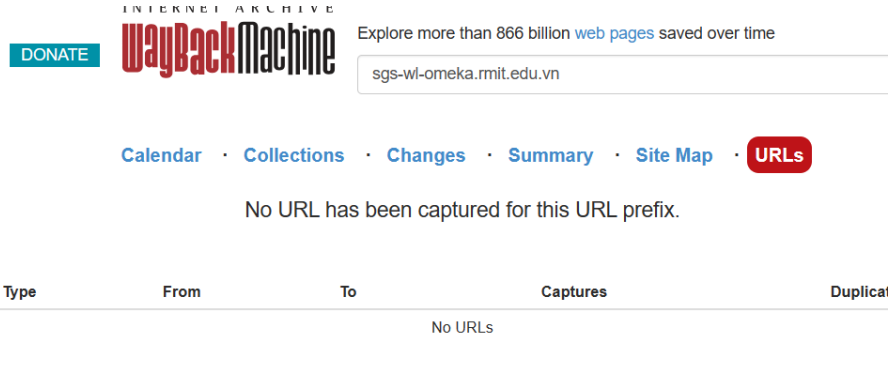


Thực hiện tìm kiếm với các trang web

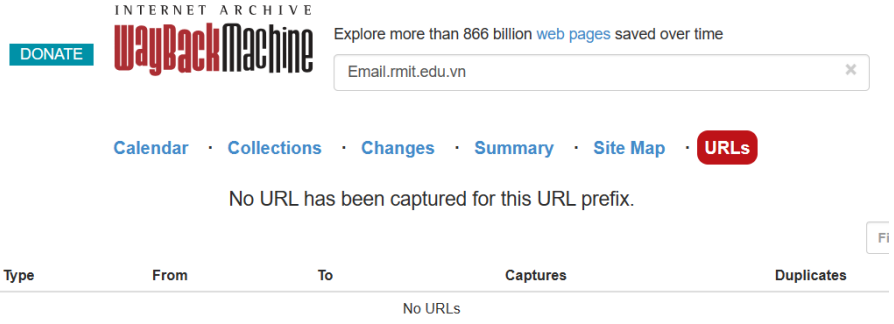
Srms.rmit.edu.vn 403



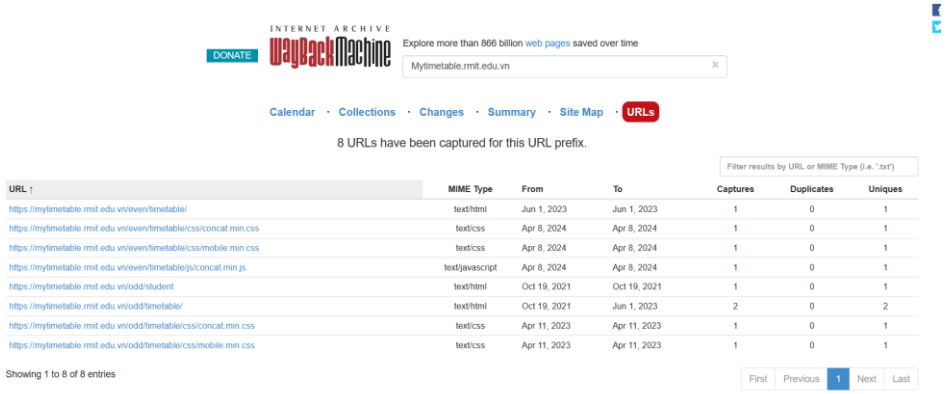
sgs-wl-omeka.rmit.edu.vn 403



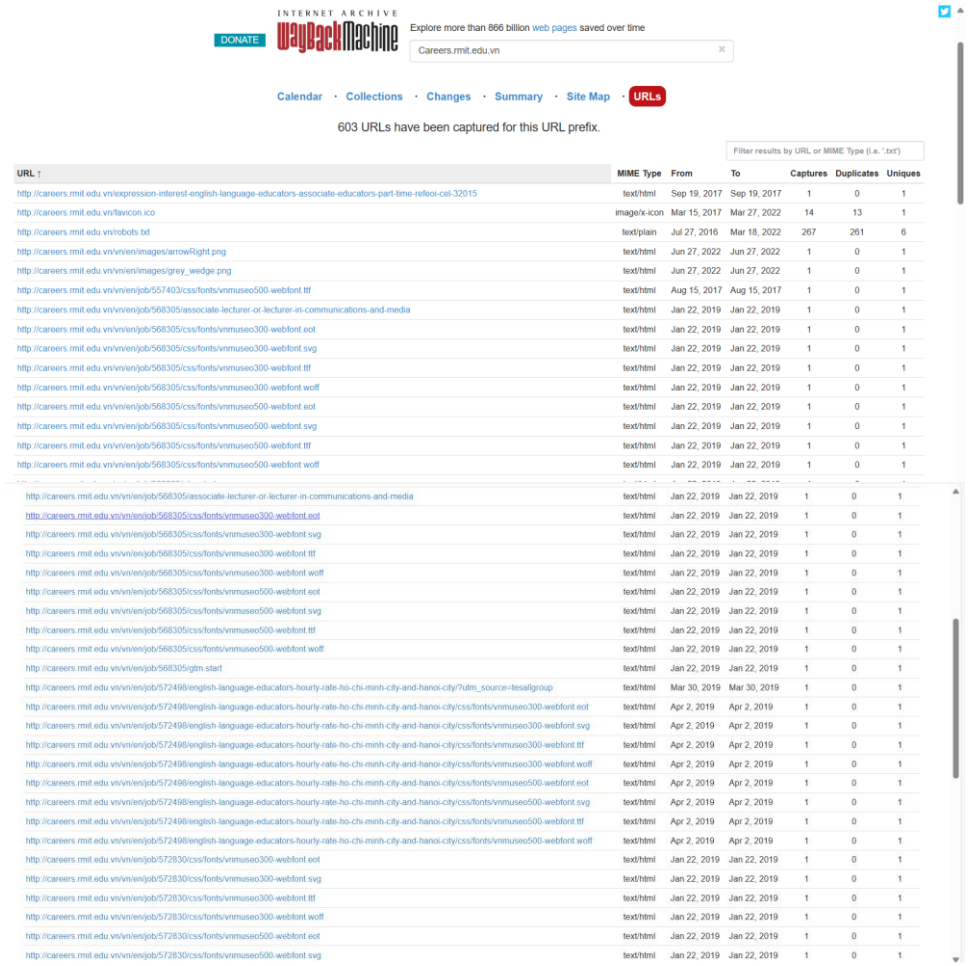
Email.rmit.edu.vn 404



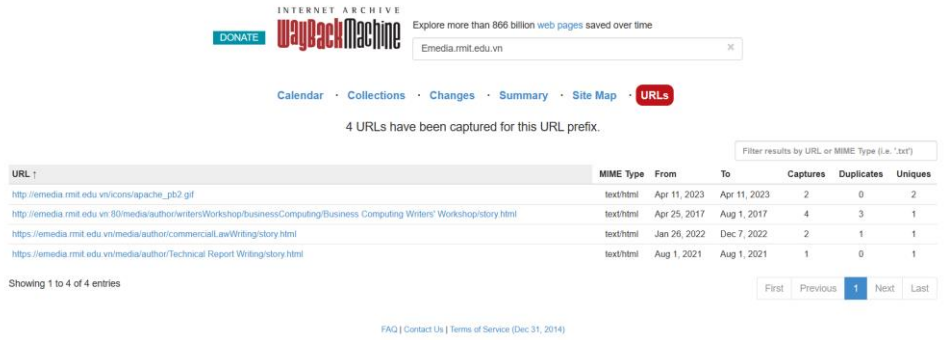
Mytimetable.rmit.edu.vn 410



Careers.rmit.edu.vn 404



Emedia.rmit.edu.vn 403

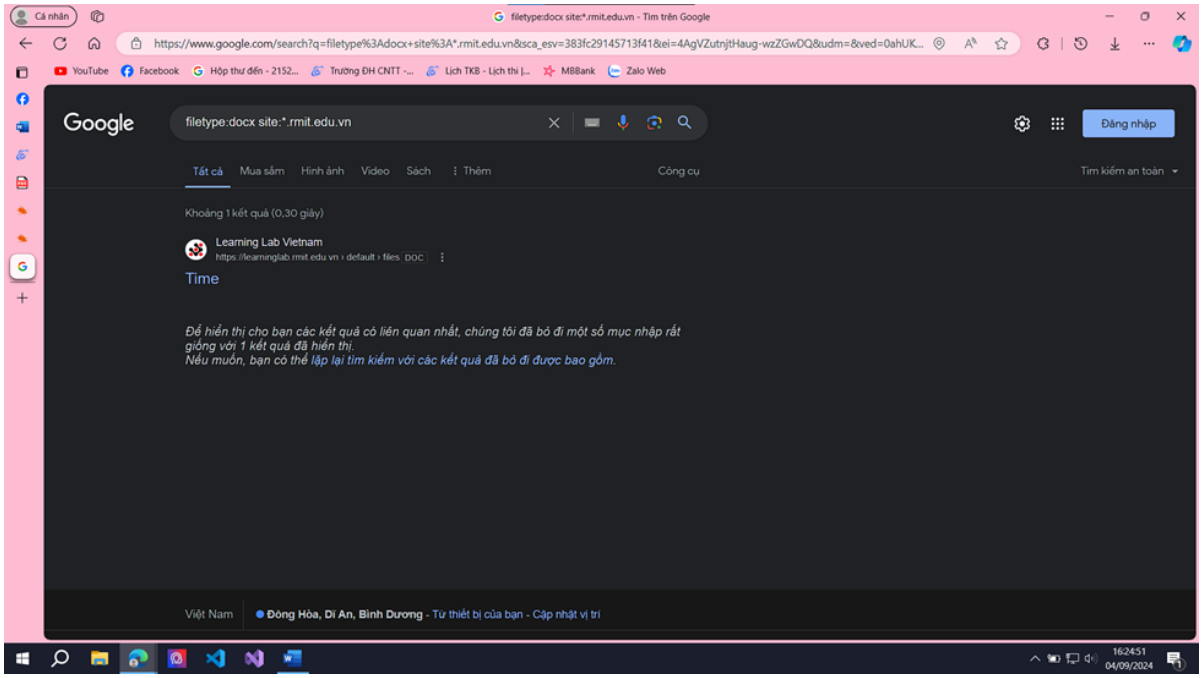


b) Tìm kiếm thông qua google dork

Bài tập 6: Tìm kiếm các tập tin pdf, excel, word, trên *.rmit.edu.vn.

Ta có thể tìm kiếm các tập tin docx được tìm kiếm trên domain *.rmit.edu.vn. bằng cách search trên google: **filetype:docx site:*.rmit.edu.vn**

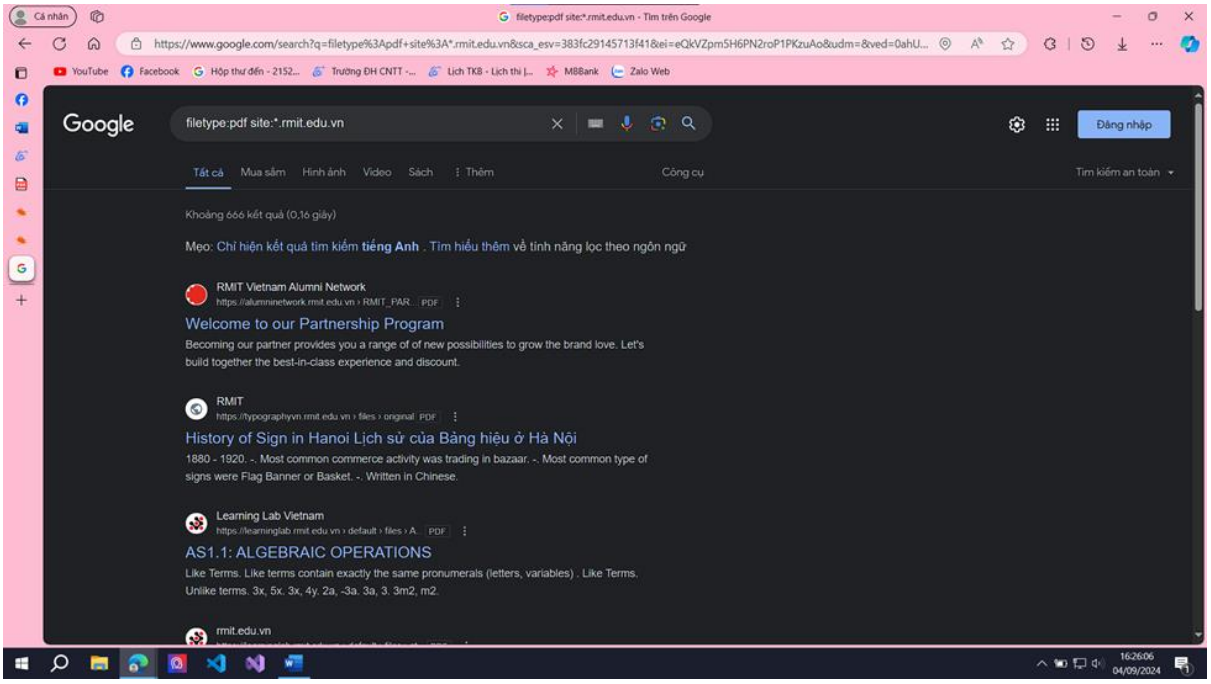
Kết quả



Tương tự cho các tập tin khác

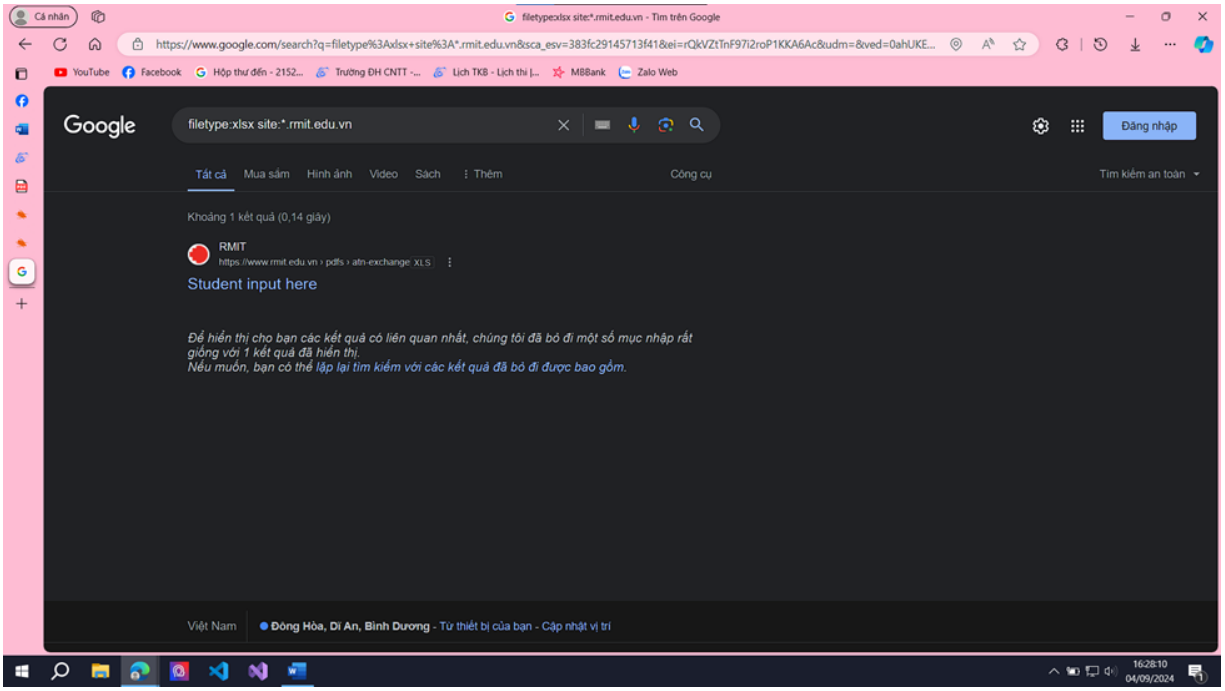
- Tập tin pdf: filetype:pdf site:*.rmit.edu.vn

Kết quả:



- Tập tin xlsx: filetype:xlsx site:*.rmit.edu.vn

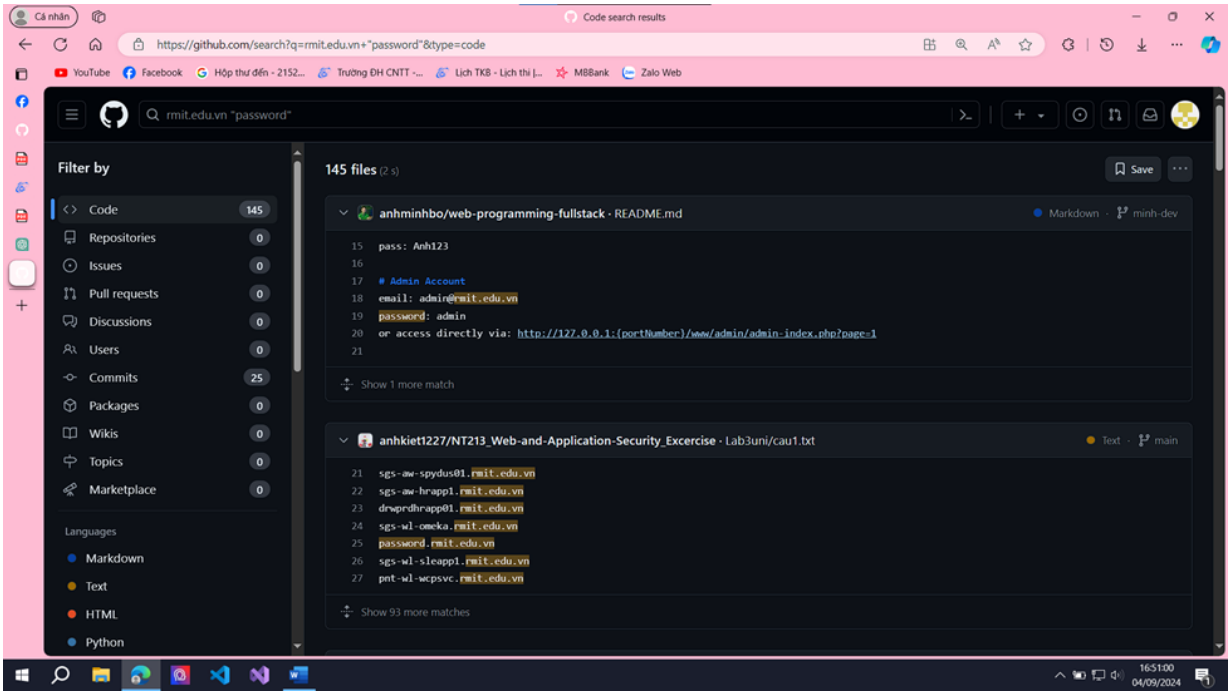
Kết quả:



c) Tìm kiếm thông qua github

Bài tập 7: Ghi nhận một vài thông tin tìm được trên github với domain *.rmit.edu.vn.

Thực hiện tìm kiếm trên github bằng phương pháp thủ công thì ta sẽ thực hiện bằng lệnh: rmit.edu.vn “password” chúng ta sẽ có được 1 số thông tin password có trong các phần code của 1 số cá nhân



Thực hiện tìm kiếm tự động:

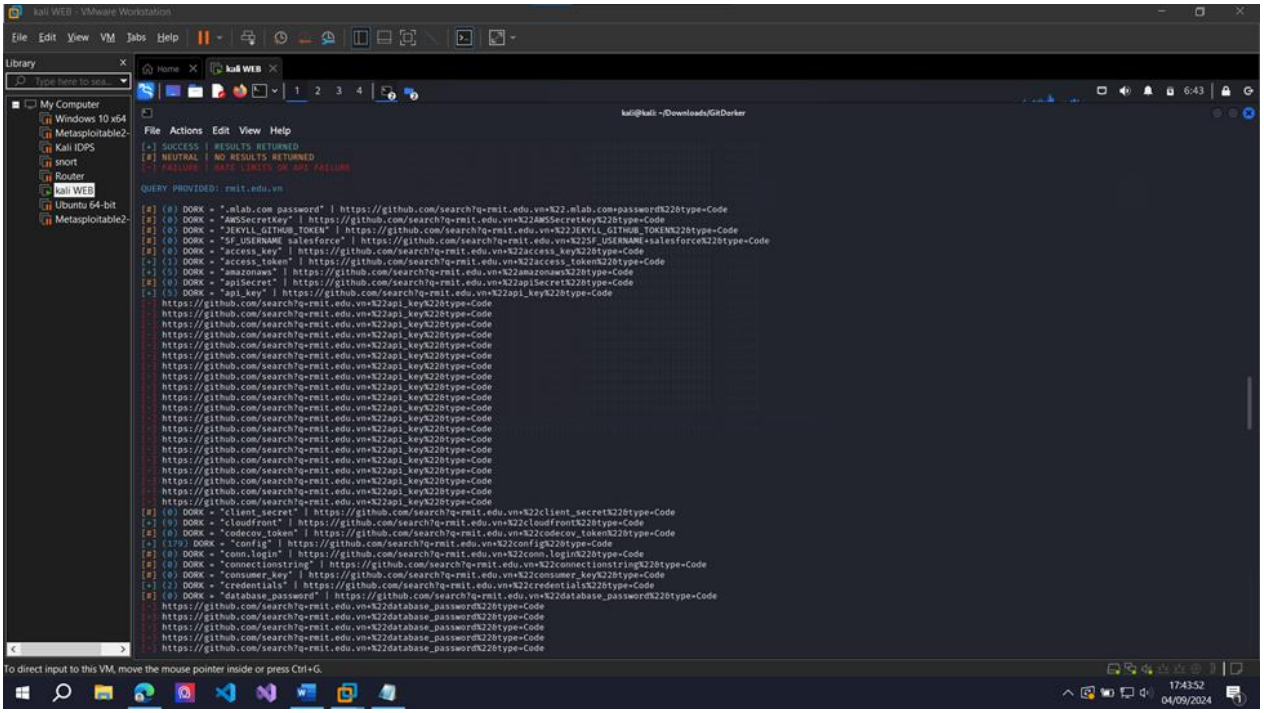
Chúng ta sử dụng công cụ gitdorker để thực hiện tìm kiếm tự động

Giao điện của công cụ

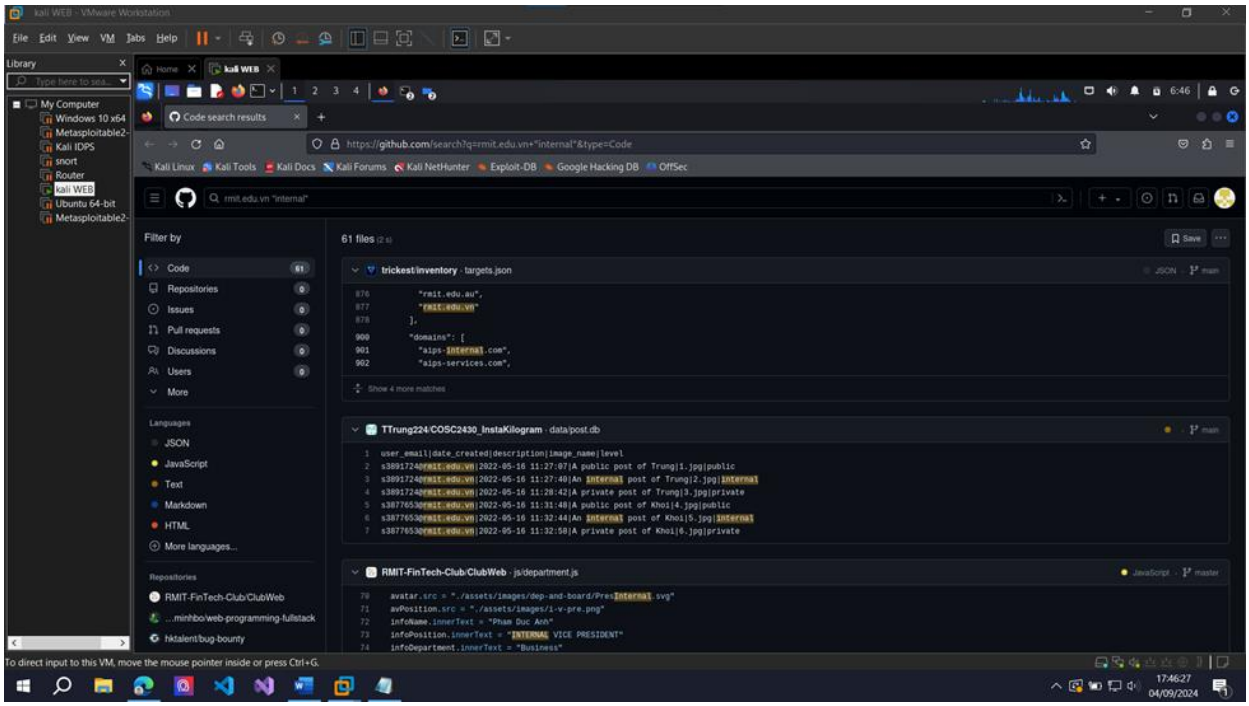
Thực hiện tìm kiếm với lệnh:

python3 GitDorker.py -tf tf/TOKENSFILE -q rmit.edu.vn -d Dorks/medium_dorks.txt -o rmit

Kết quả:



Kiểm tra 1 số link tìm thấy:



4. Bài tập thực hành