

# BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Tên chủ đề: Reconnaissance

GVHD: Ngô Đức Hoàng Sơn

**Nhóm: 08**

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P12.ANTT

STT	Họ và tên	MSSV	Email
1	Hồ Vĩ Khánh	22520633	22520633@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng
1	Bài tập 1	100%
2	Bài tập 2	100%
3	Bài tập 3	100%
4	Bài tập 4	100%
5	Bài tập 5	100%
6	Bài tập 6	100%
7	Bài tập 7	100%
8	Bài tập Thực hành	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.

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

## BÁO CÁO CHI TIẾT

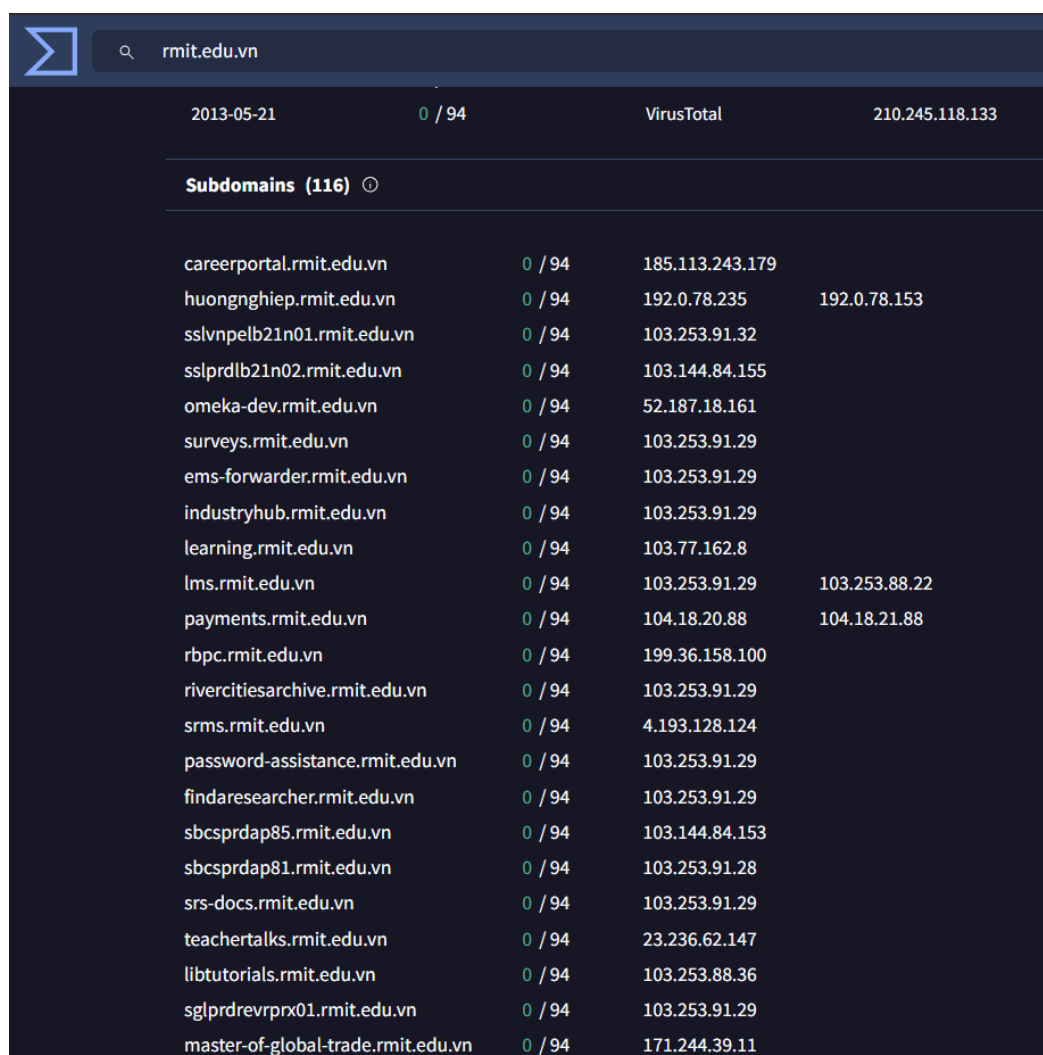
### A. Thực hành

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

- Google dork
- Duckduck go
- Virustotal
- Netcraft

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

- Sử dụng virustotal.com để thực hiện kiểm các subdomains của rmit.edu.vn ta thấy được có 116 subdomains.



The screenshot shows the VirusTotal interface for the domain rmit.edu.vn. It displays a list of 116 subdomains, each with its corresponding IP address. The interface includes a search bar at the top, a date filter (2013-05-21), and a progress indicator (0 / 94). The subdomains are listed in a table format with columns for the subdomain name, the number of engines that have scanned it (0 / 94), and the IP address. Some subdomains have additional IP addresses listed to their right.

Subdomains (116)	0 / 94	VirusTotal	210.245.118.133
careerportal.rmit.edu.vn	0 / 94	185.113.243.179	
huongnghiep.rmit.edu.vn	0 / 94	192.0.78.235	192.0.78.153
sslvnpelb21n01.rmit.edu.vn	0 / 94	103.253.91.32	
sslvprdlb21n02.rmit.edu.vn	0 / 94	103.144.84.155	
omeka-dev.rmit.edu.vn	0 / 94	52.187.18.161	
surveys.rmit.edu.vn	0 / 94	103.253.91.29	
ems-forwarder.rmit.edu.vn	0 / 94	103.253.91.29	
industryhub.rmit.edu.vn	0 / 94	103.253.91.29	
learning.rmit.edu.vn	0 / 94	103.77.162.8	
lms.rmit.edu.vn	0 / 94	103.253.91.29	103.253.88.22
payments.rmit.edu.vn	0 / 94	104.18.20.88	104.18.21.88
rbpc.rmit.edu.vn	0 / 94	199.36.158.100	
rivercitiesarchive.rmit.edu.vn	0 / 94	103.253.91.29	
srms.rmit.edu.vn	0 / 94	4.193.128.124	
password-assistance.rmit.edu.vn	0 / 94	103.253.91.29	
findaresearcher.rmit.edu.vn	0 / 94	103.253.91.29	
sbcspdp85.rmit.edu.vn	0 / 94	103.144.84.153	
sbcspdp81.rmit.edu.vn	0 / 94	103.253.91.28	
srs-docs.rmit.edu.vn	0 / 94	103.253.91.29	
teachertalks.rmit.edu.vn	0 / 94	23.236.62.147	
libtutorials.rmit.edu.vn	0 / 94	103.253.88.36	
sglprdvprpx01.rmit.edu.vn	0 / 94	103.253.91.29	
master-of-global-trade.rmit.edu.vn	0 / 94	171.244.39.11	

## 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 và burpsuite để tìm kiếm?

- Có thể kiểm tra danh sách tên miền phụ thuộc ở: virustotal ở bài tập 1, google, github,...
- Cách nào để đưa tên miền phụ và burpsuite là vào burpsuite chặn và chuyển sang tab intruder, load các tên miền đã tìm được vào payload và attack.

## 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 tấn công bruteforce bằng intruder với 20000 payload các subdomain phổ biến

The screenshot shows the Burp Suite Intruder interface with the title '4. Intruder attack of https://sa.s.rmit.edu.vn'. The 'Results' tab is active, displaying a table of attack results. The table has columns: Request, Payload, Target, Status code, Response received, Error, Timeout, Length, and Comment. The results show various subdomain payloads like 'www.pe', 'event', 'learning', etc., and their corresponding status codes (200, 301, 302, 400, 404, 505) and response lengths.

Request	Payload	Target	Status code	Response received	Error	Timeout	Length	Comment
4126	www.pe	https://www.pe.rmit.edu.vn	200	670			4146	
10235	www.event	https://www.event.rmit.edu.vn	200	95			781564	
380	event	https://event.rmit.edu.vn	301	485			768	
756	learning	https://learning.rmit.edu.vn	302	123			1200	
1196	payments	https://payments.rmit.edu.vn	302	576			732	
77	email	https://email.rmit.edu.vn	400	709			311	
450	careers	https://careers.rmit.edu.vn	404	687			1023	
87	apps	https://apps.rmit.edu.vn	505	26			340	
100	helpdesk	https://helpdesk.rmit.edu.vn	505	76			340	
131	library	https://library.rmit.edu.vn	505	36			340	
478	lms	https://lms.rmit.edu.vn	505	21			340	
1018	surveys	https://surveys.rmit.edu.vn	505	68			340	
1492	blackboard	https://blackboard.rmit.edu.vn	505	49			340	
1674	sas	https://sas.rmit.edu.vn	505	79			340	
0		https://a.rmit.edu.vn		0				baseline request

Cùng với đó có thể thực hiện tấn công dựa trên 116 payload đã tìm được ở câu 1 và sắp xếp chúng theo status

Target	Status code ^
https://sglprdalumweb1.rmit.edu.vn	200
https://sgs-wl-omeka.rmit.edu.vn	200
https://english.rmit.edu.vn	200
https://alumninetwork.rmit.edu.vn	200
https://sglprdstudlab01.rmit.edu.vn	200
https://studentlab1.rmit.edu.vn	200
https://democlass.rmit.edu.vn	200
https://experienceday.rmit.edu.vn	200
https://helpdesk.rmit.edu.vn	200
https://oes.rmit.edu.vn	200
https://sas.rmit.edu.vn	200
https://pe.rmit.edu.vn	200
https://omeka.rmit.edu.vn	200
https://design.rmit.edu.vn	200
https://etal.rmit.edu.vn	200
https://www.rmit.edu.vn	200
https://lms.rmit.edu.vn	301
https://teachertalks.rmit.edu.vn	301
https://blackboard.rmit.edu.vn	301
https://event.rmit.edu.vn	301
https://infosession.rmit.edu.vn	301
https://chame.rmit.edu.vn	301
https://rmitenglishevent.rmit.edu.vn	301
https://learninglab.rmit.edu.vn	301
https://library.rmit.edu.vn	301
https://surveys.rmit.edu.vn	302
https://industryhub.rmit.edu.vn	302
https://learning.rmit.edu.vn	302
https://payments.rmit.edu.vn	302
https://rivercitiesarchive.rmit.edu.vn	302
https://password-assistance.rmit.edu.vn	302
https://sglprdevrpx01.rmit.edu.vn	302
https://rmitlibraryvn.rmit.edu.vn	302
https://apps.rmit.edu.vn	302
https://typographyvn.rmit.edu.vn	302
https://rivf2020.rmit.edu.vn	302
https://srms.rmit.edu.vn	403
https://careerportal.rmit.edu.vn	404
https://master-of-global-trade.rmit.edu.vn	404

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

- Ta có thể dùng các lệnh sau để có thể tìm được IP khi có tên miền
  - + nslookup + [tên miền]
  - + resolveip + [tên miền]
  - + dig +short + [tên miền]

*\*\*Thay tên miền bằng các tên miền phụ của \*.rmit.edu.vn*

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

- Cách 1: Viết chương trình shell dùng nslookup để tìm và filter ra IP

```
while IFS= read -r domain; do
  ip=$(nslookup "$domain" | grep -Eo 'Address: ([0-9]{1,3}\.){3}[0-9]{1,3}' | awk '{print $2}' | head -n 1)
  if [ -n "$ip" ]; then
    echo "$ip" >> ip.txt
  else
    echo "Không thể lấy IP cho domain: $domain" >> domain.txt
  fi
done < domain.txt
```

- Cách 2:

Viết chương trình python dùng lệnh resolveip [domain] để tìm ip cho các tên miền trên được lưu ở file BT1.csv. Tìm IP và lưu vào file BT3.csv

```
1  import socket
2  import csv
   Tabnine | Edit | Test | Explain | Document | Ask
3  def resolve_ips(domain):
4      try:
5
6          _, _, ip_addresses = socket.gethostbyname_ex(domain)
7          return ip_addresses
8      except socket.gaierror:
9          return None
   Tabnine | Edit | Test | Fix | Explain | Document | Ask
10 def main():
11     input_file = 'BT1.csv'
12     output_file1 = 'BT3.csv'
13
14
15     with open(input_file, mode='r') as file:
16         reader = csv.reader(file)
17
18         with open(output_file1, mode='w', newline='') as output1:
19
20             writer = csv.writer(output1)
21             writer.writerow(['Domain', 'IP Addresses'])
22
23             for row in reader:
24                 domain = row[0].strip()
25                 ips = resolve_ips(domain)
26                 if ips:
27                     ip_list = ', '.join(ips)
28                     print(f"{domain} : {ip_list}")
29                     writer.writerow([domain, ip_list])
30                 else:
31                     print(f"{domain} : Không tìm thấy IP")
32                     writer.writerow([domain, 'Không tìm thấy IP'])
33
34 if __name__ == '__main__':
```

Kết quả cho thấy IP của tên miền và một vài tên miền không tìm thấy IP

```
PS C:\Users\hovik\OneDrive - Trường ĐH CNTT - University of Information Technology\UIT\HK5\NT213\TH\lab3> python BT3.py
careerportal.rmit.edu.vn : 185.113.243.179
huongnghiep.rmit.edu.vn : 192.0.78.235, 192.0.78.153
sslvnpelb21n01.rmit.edu.vn : 103.253.91.32
sslvprdlb21n02.rmit.edu.vn : 103.144.84.155
omeka-dev.rmit.edu.vn : 52.187.18.161
surveys.rmit.edu.vn : 103.253.91.29
ems-forwarder.rmit.edu.vn : 103.253.91.29
industryhub.rmit.edu.vn : 103.253.91.29
learning.rmit.edu.vn : 103.77.162.8
lms.rmit.edu.vn : 103.253.91.29
payments.rmit.edu.vn : 104.18.21.88, 104.18.20.88
rbpc.rmit.edu.vn : 199.36.158.100
rivercitiesarchive.rmit.edu.vn : 103.253.91.29
srms.rmit.edu.vn : 4.193.128.124
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 : Không tìm thấy IP
```

#### 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.

##### - Cách 1:

Viết chương trình để scan 1000 port phổ biến trên danh sách IP. Đầu tiên ta cần loại bỏ các IP trùng lặp trong file BT3.csv và lưu thành file unique\_IP.csv.

```
1  import socket
2  import csv
3
4  # Hàm kiểm tra xem một cổng có mở trên địa chỉ IP hay không
5  def is_port_open(ip, port):
6      try:
7          # Tạo socket và kết nối với địa chỉ IP và cổng
8          with socket.create_connection((ip, port), timeout=1):
9              return True
10     except (socket.timeout, ConnectionRefusedError, OSError):
11         return False
12
13     # Đọc danh sách IP từ file IP.csv
14     def read_ip_list(filename):
15         with open(filename, 'r') as file:
16             reader = csv.reader(file)
17             return [row[0] for row in reader]
18
19     # Đọc danh sách cổng từ file port.csv
20     def read_port_list(filename):
21         with open(filename, 'r') as file:
22             reader = csv.reader(file)
23             return [row[0] for row in reader]
24
25     # Quét các cổng trên danh sách IP và lưu kết quả vào file result_port.csv
26     def scan_ports(ip_list, port_list, result_file):
27         with open(result_file, 'w', newline='') as file:
28             writer = csv.writer(file)
29             # Ghi tiêu đề cột
30             writer.writerow(['IP Address', 'Port', 'Status'])
```

```
30 writer.writerow(['IP Address', 'Port', 'Status'])
31 # Duyệt qua từng IP và cổng, kiểm tra trạng thái cổng
32 for ip in ip_list:
33     for port in port_list:
34         if is_port_open(ip, port):
35             # Ghi kết quả vào file CSV nếu cổng mở
36             writer.writerow([ip, port, 'Open'])
37             print(f"{ip}:{port} is Open")
38
39 # Đường dẫn tới các file
40 ip_file = 'unique_IP.csv'
41 port_file = 'port_vertical.csv'
42 result_file = 'result_port.csv'
43
44 # Đọc danh sách IP và cổng
45 ip_list = read_ip_list(ip_file)
46 port_list = read_port_list(port_file)
47
48 # Thực hiện quét và lưu kết quả
49 scan_ports(ip_list, port_list, result_file)
50
```

Chạy chương trình và ghi kết quả vào file result\_port.csv (Nhưng cách này khá lâu :>)

```
PS C:\Users\hovik\OneDrive - Trường ĐH CNTT - University of Information Technology\UIT\HK5\NT213\TH\lab3> & C:/Users/hovik/AppData/Local/Programs/Python/Python313/python.exe "c:/Users/hovik/OneDrive - Trường ĐH CNTT - University of Information Technology/UIT/HK5/NT213/TH/lab3/scanport.py"
199.36.158.100:80 is Open
199.36.158.100:443 is Open
54.153.241.170:80 is Open
54.153.241.170:443 is Open
108.157.32.92:80 is Open
108.157.32.92:443 is Open
167.89.118.83:80 is Open
167.89.118.83:443 is Open
54.206.155.195:80 is Open
54.206.155.195:443 is Open
167.89.118.120:80 is Open
167.89.118.120:443 is Open
167.89.123.58:80 is Open
167.89.123.58:443 is Open
192.0.78.153:80 is Open
192.0.78.153:443 is Open
108.157.32.105:80 is Open
108.157.32.105:443 is Open
103.253.91.23:80 is Open
103.253.91.23:443 is Open
167.89.118.109:80 is Open
167.89.118.109:443 is Open
103.253.91.29:80 is Open
103.253.91.29:443 is Open
52.187.18.161:443 is Open
4.193.128.124:443 is Open
103.221.222.11:80 is Open
103.221.222.11:443 is Open
103.221.222.11:21 is Open
103.221.222.11:110 is Open
```

## - Cách 2:

Dùng lệnh **nmap -F -iL ip.txt -oN kq\_port.txt** để scan nhanh 1000 port phổ biến của IP có trong file ip.txt và ghi vào kq\_port.txt

-F: scan 1000 port phổ biến.



```
(root@kali)-[/home/kali/Downloads]
# nmap -F -iL ip.txt -oN kq_port.txt

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 06:00 EDT
Nmap scan report for 199.36.158.100
Host is up (0.045s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for ec2-54-153-241-170.ap-southeast-2.compute.amazonaws.com
(54.153.241.170)
Host is up (0.12s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for server-108-157-32-92.sgn50.r.cloudfront.net (108.157.32.
92)
Host is up (0.0079s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for o16789118x83.outbound-mail.sendgrid.net (167.89.118.83)
Host is up (0.012s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

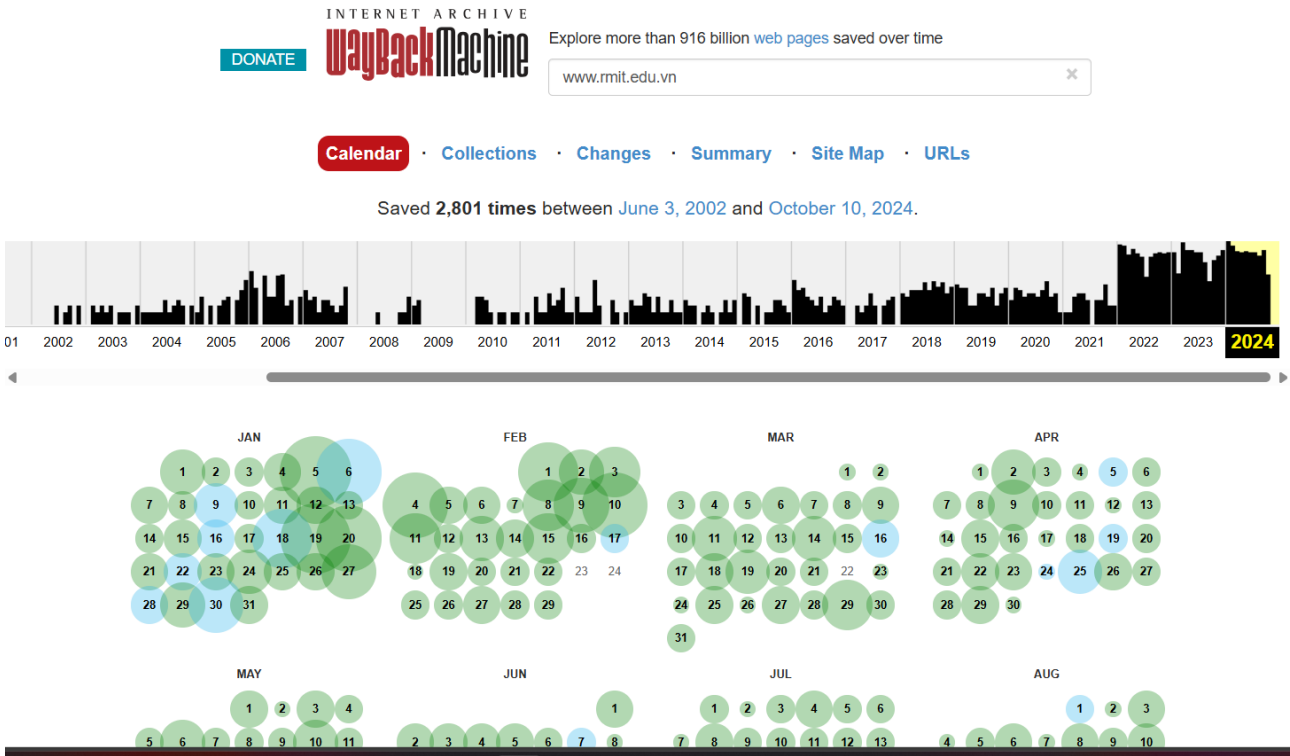
Nmap scan report for ec2-54-206-155-195.ap-southeast-2.compute.amazonaws.com
(54.206.155.195)
Host is up (0.0079s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
443/tcp   open  https
49152/tcp closed unknown
```

##### 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.

- Sử dụng trang web wayback machine để tìm kiếm dữ liệu trong quá khứ của các tên miền [staff.rmit.edu.vn](http://staff.rmit.edu.vn), [www.rmit.edu.vn](http://www.rmit.edu.vn) và [sso.rmit.edu.vn](http://sso.rmit.edu.vn)

Ta thấy: Dữ liệu tên miền [www.rmit.edu.vn](http://www.rmit.edu.vn) được truy cập, sửa đổi và cập nhật thường xuyên cho đến ngày này. Còn tên miền [staff.rmit.edu.vn](http://staff.rmit.edu.vn) và [sso.rmit.edu.vn](http://sso.rmit.edu.vn) có vẻ ít được cập nhật sửa đổi hơn nhiều so với [www.rmit.edu.vn](http://www.rmit.edu.vn). Và cho tới ngày nay thì theo web wayback machine cập nhật được [sso.rmit.edu.vn](http://sso.rmit.edu.vn) chỉ được được lưu 1 lần vào 22 tháng 1 năm 2019. [staff.rmit.edu.vn](http://staff.rmit.edu.vn) lần gần nhất là vào ngày 30 tháng 8 năm 2022. Hai tên miền phụ thuộc này không còn tồn tại hiện nay.





INTERNET ARCHIVE  
WayBackMachine

DONATE

Explore more than 916 billion web pages saved over time

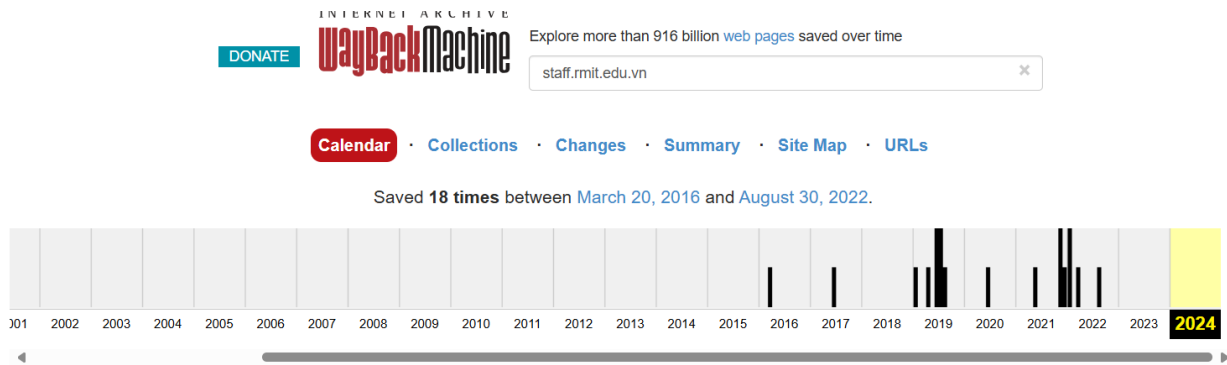
www.rmit.edu.vn

Calendar · Collections · Changes · Summary · Site Map · URLs

More than 10,000 URLs have been captured for this URL prefix.


Filter results by URL or MIME Type (i.e. '.txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://rmit.edu.vn/l6.21(a.L.5H,2,/4r/date.js	text/html	May 13, 2024	May 13, 2024	2	0	2
http://rmit.edu.vn/l6.21(a.L.5H,2,/4r/query.packed.js	text/html	May 13, 2024	May 13, 2024	2	0	2
http://rmit.edu.vn/l6.21(a.L.5H,2,/4r/logo.jpg	text/html	May 13, 2024	May 13, 2024	2	0	2
http://rmit.edu.vn/l6.21(a.L.5H,2,/4r/)	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1
http://rmit.edu.vn/l6.1e	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1
http://rmit.edu.vn/l6.2p	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1
http://rmit.edu.vn/"1w"l=a.G&&6.1a(a,"T")l="1l"&&6.1a(a,"4c")l="1w"	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1
http://rmit.edu.vn/"l	text/html	Sep 28, 2010	Sep 28, 2010	1	0	1
http://rmit.edu.vn/"l	text/html	Sep 28, 2010	Sep 28, 2010	1	0	1
http://rmit.edu.vn/"2s"/=a.G	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1
http://rmit.edu.vn/"4e"/=a.G	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1
http://rmit.edu.vn/"4j"/=a.G	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1
http://rmit.edu.vn/"4k"/=a.G	text/html	Sep 30, 2010	Sep 30, 2010	1	0	1
http://rmit.edu.vn/"5A"/=a.G	text/html	Oct 5, 2010	Oct 5, 2010	1	0	1




JAN							FEB							MAR							APR								
1	2	3	4	5	6					1	2	3					1	2					1	2	3	4	5	6	
7	8	9	10	11	12	13				4	5	6	7	8	9	10							7	8	9	10	11	12	13
14	15	16	17	18	19	20				11	12	13	14	15	16	17							14	15	16	17	18	19	20
21	22	23	24	25	26	27				18	19	20	21	22	23	24							17	18	19	20	21	22	23
28	29	30	31							25	26	27	28	29									24	25	26	27	28	29	30
																							31						
MAY							JUN							JUL							AUG								

INTERNET ARCHIVE

DONATE


Explore more than 916 billion [web pages](#) saved over time




Calendar
·
Collections
·
Changes
·
Summary
·
Site Map
·
URLs

70 URLs have been captured for this URL prefix.

Filter results by URL or MIME Type (i.e. 'txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
<a href="https://staff.rmit.edu.vn/">https://staff.rmit.edu.vn/</a>	text/html	Jun 21, 2020	Aug 30, 2022	9	8	1
<a href="https://staff.rmit.edu.vn/favicon.ico">https://staff.rmit.edu.vn/favicon.ico</a>	image/vnd.microsoft.icon	Apr 29, 2016	Jan 8, 2022	5	4	1
<a href="https://staff.rmit.edu.vn/misc/drupal.js">https://staff.rmit.edu.vn/misc/drupal.js</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/drupal.js?pbdyeq">https://staff.rmit.edu.vn/misc/drupal.js?pbdyeq</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/jquery.js">https://staff.rmit.edu.vn/misc/jquery.js</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/jquery.js?v=1.4.4">https://staff.rmit.edu.vn/misc/jquery.js?v=1.4.4</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/jquery.once.js">https://staff.rmit.edu.vn/misc/jquery.once.js</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/jquery.once.js?v=1.2">https://staff.rmit.edu.vn/misc/jquery.once.js?v=1.2</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.css?pbdyeq">https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.css?pbdyeq</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.min.js?v=1.8.7">https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.min.js?v=1.8.7</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/ui/jquery.ui.core.css?pbdyeq">https://staff.rmit.edu.vn/misc/ui/jquery.ui.core.css?pbdyeq</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/ui/jquery.ui.core.min.js?v=1.8.7">https://staff.rmit.edu.vn/misc/ui/jquery.ui.core.min.js?v=1.8.7</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.css?pbdyeq">https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.css?pbdyeq</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1
<a href="https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.min.js?v=1.8.7">https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.min.js?v=1.8.7</a>	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	0	1

[DONATE](#)

 Explore more than 916 billion [web pages](#) saved over time

[Calendar](#) · 
 [Collections](#) · 
 [Changes](#) · 
 [Summary](#) · 
 [Site Map](#) · 
 [URLs](#)



DONATE

WayBackMachine

Explore more than 916 billion web pages saved over time

sso.rmit.edu.vn

Calendar

Collections

Changes

Summary

Site Map

URLs

29 URLs have been captured for this URL prefix.

Filter results by URL or MIME Type (i.e. '.txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
https://sso.rmit.edu.vn/	text/html	Jan 22, 2019	Jan 22, 2019	1	0	1
https://sso.rmit.edu.vn/cas/	text/html	Jan 22, 2019	Jan 22, 2019	1	0	1
https://sso.rmit.edu.vn/cas/favicon.ico?sessionid=0879475645923770D3748BE5AF891BF6	image/x-icon	Jun 23, 2016	Jun 23, 2016	1	0	1
https://sso.rmit.edu.vn/cas/favicon.ico?sessionid=26C5493EFBF8133CABC102535B5FEBB7	image/x-icon	Feb 17, 2019	Feb 17, 2019	1	0	1
https://sso.rmit.edu.vn/cas/favicon.ico?sessionid=65C862D77DF866BFEADD79CB37BCFB13	image/x-icon	Jan 22, 2019	Jan 22, 2019	1	0	1
https://sso.rmit.edu.vn/cas/images/logo.png	image/png	Jun 23, 2016	Feb 23, 2019	3	2	1
https://sso.rmit.edu.vn/cas/login	text/html	Jan 22, 2019	Feb 26, 2019	2	0	2
https://sso.rmit.edu.vn/cas/login?service=https%3A%2F%2Fems.rmit.edu.vn%2F	text/html	Jul 13, 2018	Feb 1, 2019	3	0	3
https://sso.rmit.edu.vn/cas/login?service=https%3A%2F%2Fems.rmit.edu.vn%2Fpublic%2Fauth%2Fevent%2F330	text/html	Jan 22, 2019	Jan 22, 2019	1	0	1
https://sso.rmit.edu.vn/cas/login?service=https%3A%2F%2Fems.rmit.edu.vn%2Fpublic%2Fauth%2Fevent%2F330%2Fvi	text/html	Jan 22, 2019	Jan 22, 2019	1	0	1
https://sso.rmit.edu.vn/cas/login?service=https%3A%2F%2Flearninglab.rmit.edu.vn%2Ffavicon.ico&gateway=true	unk	Sep 4, 2018	Sep 4, 2018	1	0	1
https://sso.rmit.edu.vn/cas/login?service=https%3A%2F%2Foes.rmit.edu.vn%2Flogin	text/html	Aug 13, 2020	Oct 28, 2020	3	0	3
https://sso.rmit.edu.vn/cas/login?service=https%3A%2F%2Fomeka.rmit.edu.vn%2Fusers%2Flogin	text/html	Aug 13, 2020	Aug 13, 2020	1	0	1
https://sso.rmit.edu.vn/cas/login?service=https%3A%2F%2Fstaff.rmit.edu.vn%2Fcas%3Fdestination%3Dnode%2F1	text/html	Apr 13, 2016	Apr 13, 2016	1	0	1

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

- Sử dụng google để tìm kiếm các tập tin pdf, excel, word, trên [www.rmit.edu.vn](http://www.rmit.edu.vn) bằng cách dùng lệnh:

site:www.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls


site:www.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls

google.com/search?q=site%3Awww.rmit.edu.vn+filetype%3Apdf+OR+filetype%3Adoc+OR+filetype%3Axls&scas\_esv=0ba5b4315e0f


Google

site:www.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls


All Shopping Images Videos Web News Books More Tools

 RMIT  
https://www.rmit.edu.vn > student-life > insurance PDF


Claim Form for Dental Treatment Reimbursements  
The sections marked by an asterisk (\*) must be completed in full by the patient, or the main member on behalf of the patient if the.

 rmit.edu.vn  
https://www.rmit.edu.vn > student-life > insurance PDF

Claim Form for Medical Treatment Reimbursements  
The sections marked by an asterisk (\*) must be completed in full by the patient, or the main member on behalf of the patient if the.

 rmit.edu.vn  
https://www.rmit.edu.vn > pdfs > advice-support PDF

Application for extension of time to submit assessment work  
Use this form to apply for an extension of time of seven calendar days or less from the original due date for submission of assessment.

 rmit.edu.vn  
https://www.rmit.edu.vn > international-students PDF

— Credit transfer (higher education and vocational ...  
Important information. - In accordance with the Admission and credit policy, credit will be transferred with grades, including fail grades, under certain.

PHÒNG THÍ NGHIỆM  
AN TOÀN THÔNG TIN

Báo cáo Thực hành Bảo mật web và ứng dụng  
HỌC KỲ 1 – NĂM HỌC 2024-2025

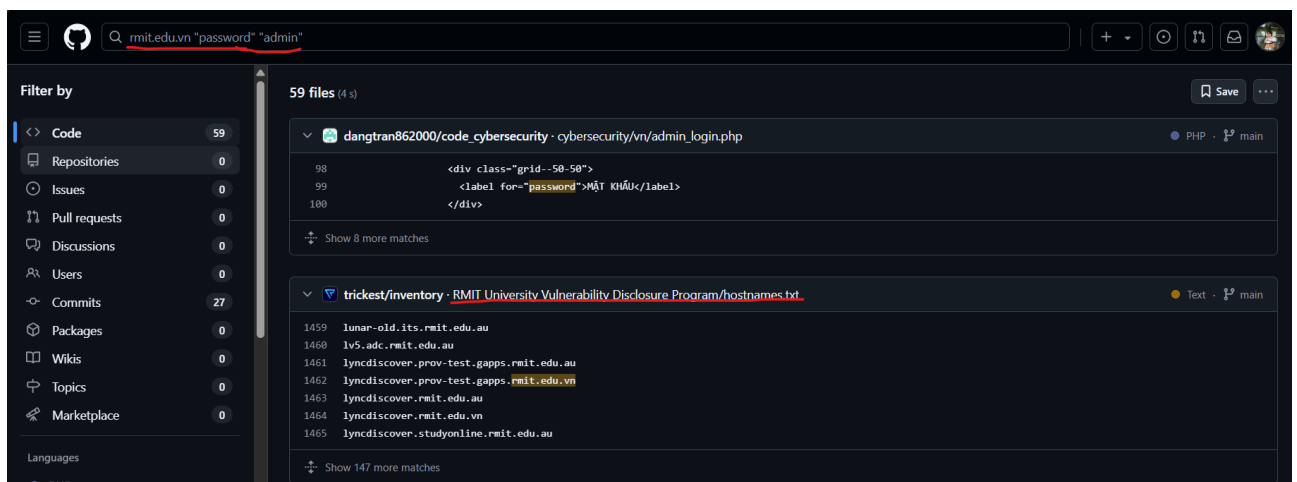
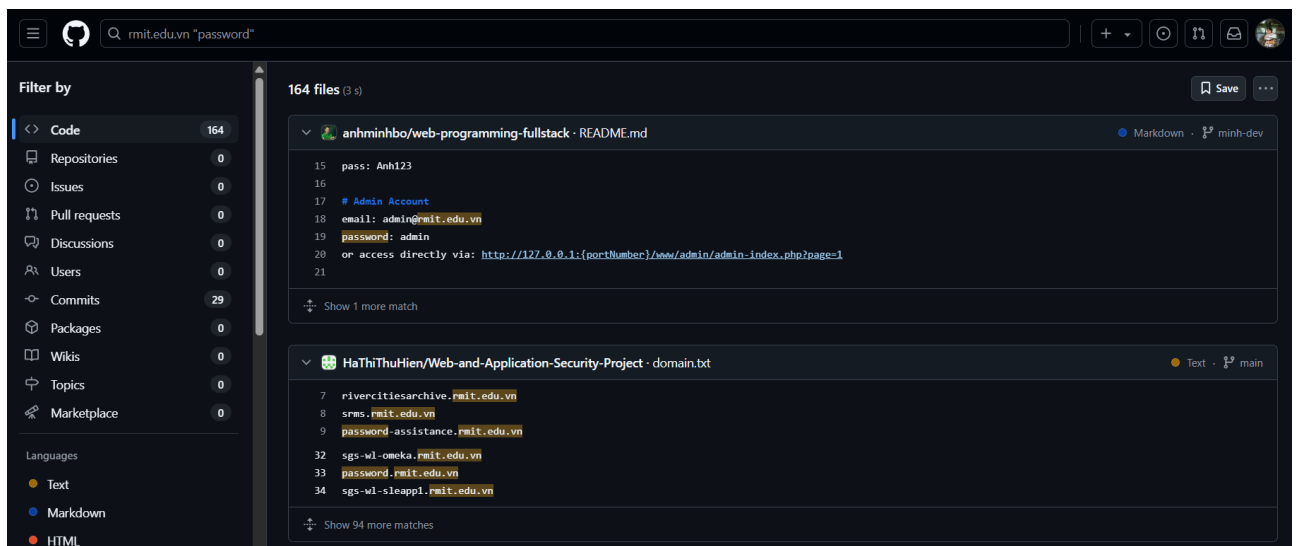
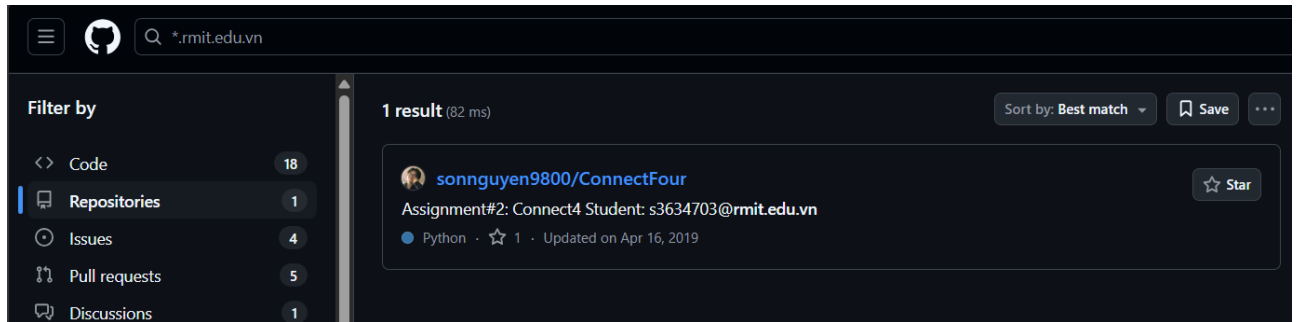
7. Ghi nhận một vài thông tin tìm được trên github với domain \*.rmit.edu.vn.  
(lưu ý: không sử dụng thông tin này để khai thác thông tin cá nhân có thể có, mọi hành vi sử dụng không được phép sẽ chịu trách nhiệm trước pháp luật).

- Dùng github search thu được bởi các keyword

\*.rmit.edu.vn

rmit.edu.vn "password"

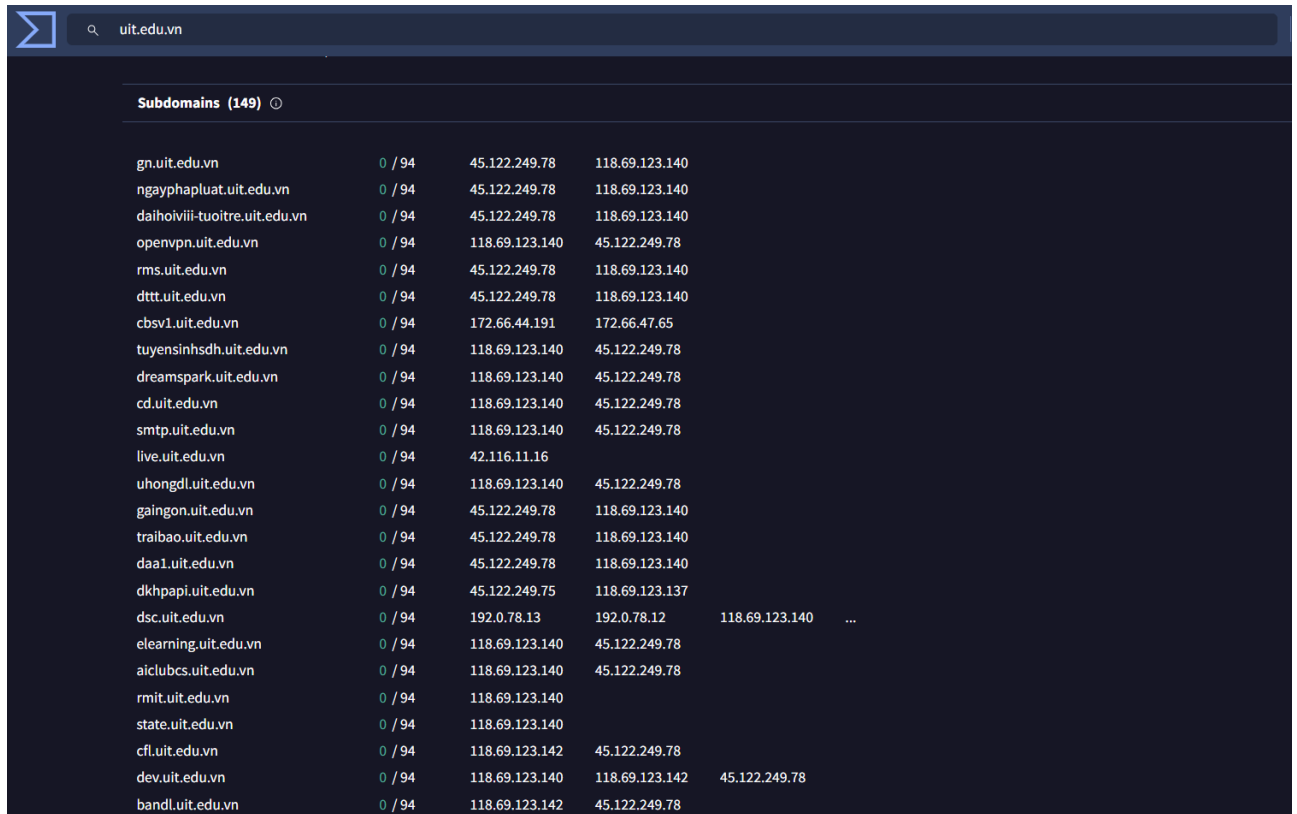
rmit.edu.vn "password" "admin"



## B. Bài tập thực hành

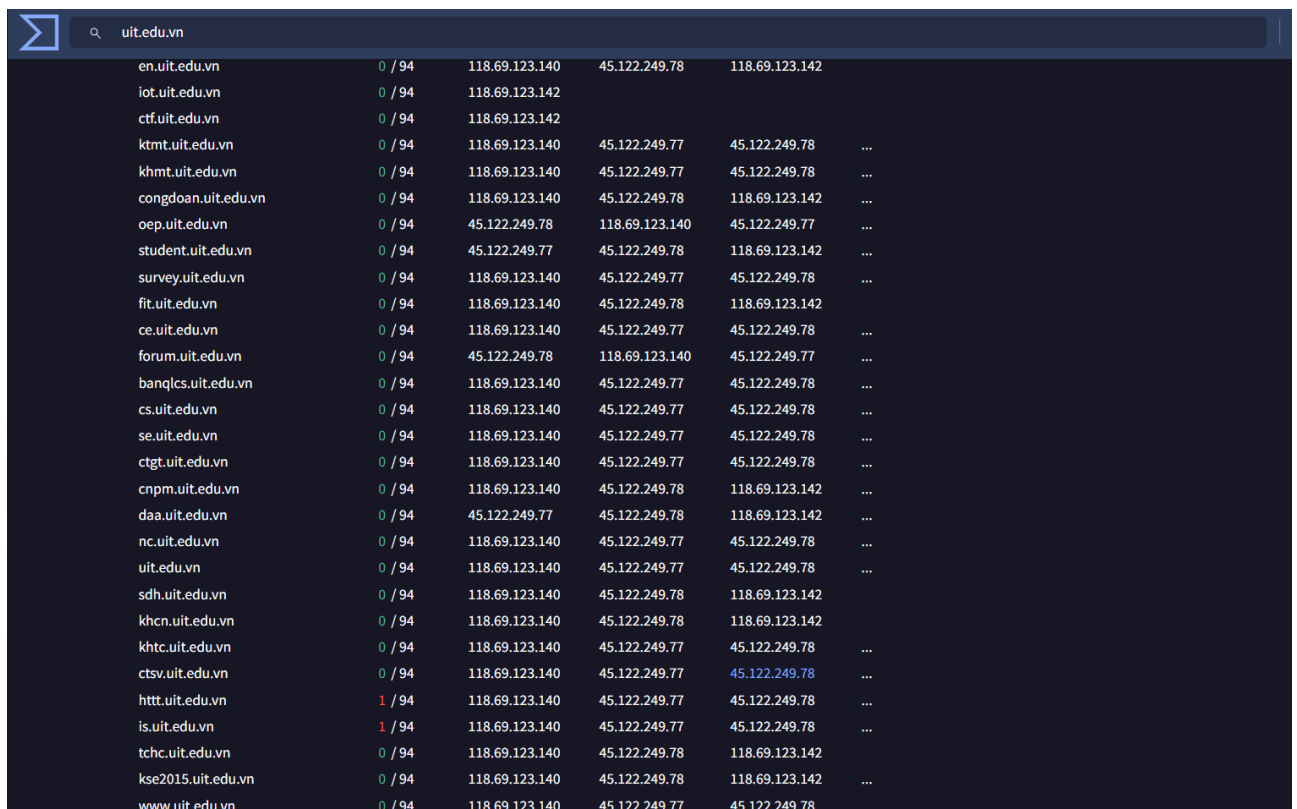
1. Tìm kiếm các tên miền phụ của \*.uit.edu.vn

- Dùng virustotal tìm ra 149 subdomain của \*.uit.edu.vn



Subdomains (149)

gn.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
ngayphapluat.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
daihoiviii-tuoiitre.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
openvpn.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
rms.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
dttt.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
cbsv1.uit.edu.vn	0 / 94	172.66.44.191	172.66.47.65	
tuyensinhshdh.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
dreamspark.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
cd.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
smtp.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
live.uit.edu.vn	0 / 94	42.116.11.16		
uhongdl.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
gaingon.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
traibao.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
daa1.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	
dkhpapi.uit.edu.vn	0 / 94	45.122.249.75	118.69.123.137	
dsc.uit.edu.vn	0 / 94	192.0.78.13	192.0.78.12	118.69.123.140 ...
elearning.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
aiclubs.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	
rmit.uit.edu.vn	0 / 94	118.69.123.140		
state.uit.edu.vn	0 / 94	118.69.123.140		
cfl.uit.edu.vn	0 / 94	118.69.123.142	45.122.249.78	
dev.uit.edu.vn	0 / 94	118.69.123.140	118.69.123.142	45.122.249.78
bandl.uit.edu.vn	0 / 94	118.69.123.142	45.122.249.78	



en.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	
iot.uit.edu.vn	0 / 94	118.69.123.142			
ctf.uit.edu.vn	0 / 94	118.69.123.142			
ktmt.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
khmt.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
congdoan.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	...
oep.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	45.122.249.77	...
student.uit.edu.vn	0 / 94	45.122.249.77	45.122.249.78	118.69.123.142	...
survey.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
fit.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	
ce.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
forum.uit.edu.vn	0 / 94	45.122.249.78	118.69.123.140	45.122.249.77	...
banqlcs.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
cs.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
se.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
ctgt.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
cnpm.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	...
daa.uit.edu.vn	0 / 94	45.122.249.77	45.122.249.78	118.69.123.142	...
nc.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
sdh.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	
khcn.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	
khct.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
ctsv.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
http.uit.edu.vn	1 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
is.uit.edu.vn	1 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...
tchc.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	
kse2015.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.78	118.69.123.142	...
www.uit.edu.vn	0 / 94	118.69.123.140	45.122.249.77	45.122.249.78	...

2. Tìm kiếm các địa chỉ IP thuộc \*.uit.edu.vn và các cổng đang mở tương ứng

- Lấy IP:

Tạo shell lấy ip từ file lưu các domain tìm kiếm được từ câu 1

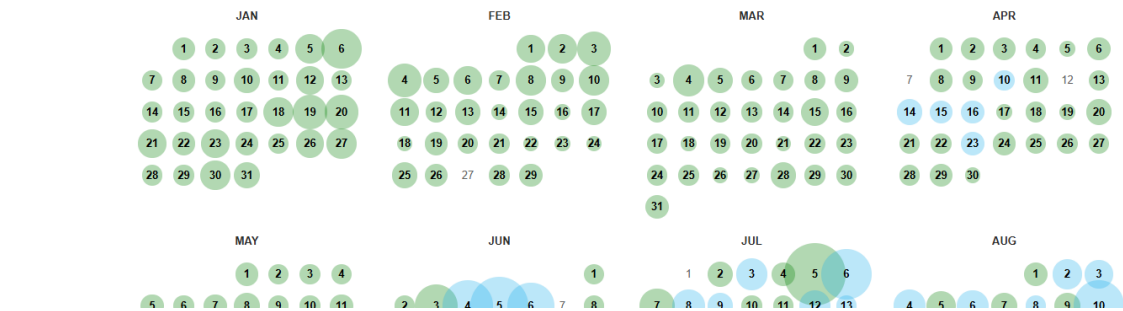
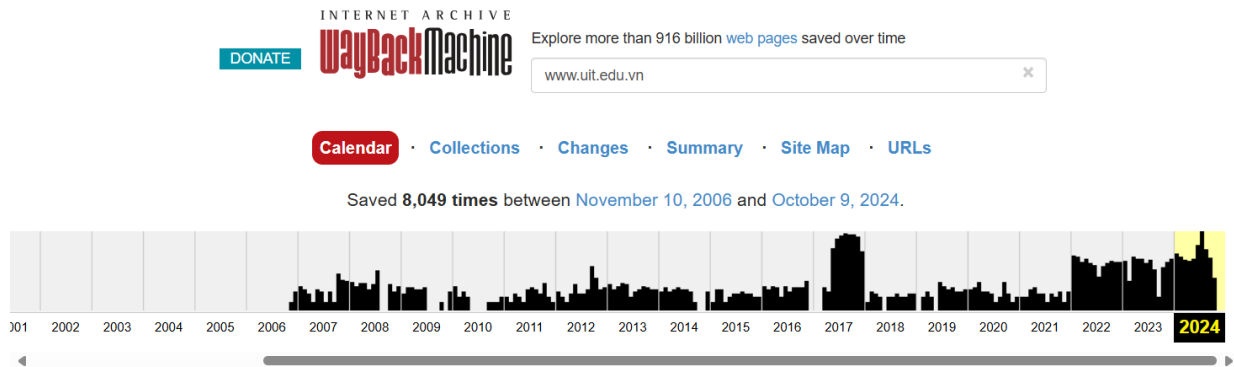
```
GNU nano 8.2 getip_uit.sh *
#!/bin/bash
while IFS= read -r domain; do
  ip=$(nslookup "$domain" | grep -Eo 'Address: ([0-9]{1,3}\.){3}[0-9]{1,3}' | awk '{print $2}' | head -n 1)
  if [ -n "$ip" ]; then
    echo "$ip" >> ip_uit.txt
  else
    echo "Không thể lấy IP cho domain: $domain"
  fi
done < domain_uit.txt
```

Kết quả

```
(root@kali)-[/home/kali/Downloads]
# cat ip_uit.txt
118.69.123.140
118.69.123.140
45.122.249.78
118.69.123.140
118.69.123.140
45.122.249.78
172.66.44.191
118.69.123.140
45.122.249.78
45.122.249.78
118.69.123.140
42.116.11.16
118.69.123.140
118.69.123.140
45.122.249.78
118.69.123.140
45.122.249.75
192.0.78.12
45.122.249.78
118.69.123.140
118.69.123.140
45.122.249.78
45.122.249.78
45.122.249.78
118.69.123.140
118.69.123.140
118.69.123.140
45.122.249.76
45.122.249.78
118.69.123.140
45.122.249.78
118.69.123.140
45.122.249.78
45.122.249.78
42.116.11.19
118.69.123.140
118.69.123.140
142.250.198.243
118.69.123.140
45.122.249.78
```

- Các cổng đang mở dùng lệnh

### 3. Tìm kiếm các dữ liệu quá khứ của \*.uit.edu.vn



INTERNET ARCHIVE  
WayBackMachine

DONATE

Explore more than 916 billion web pages saved over time

www.uit.edu.vn

Calendar · Collections · Changes · Summary · Site Map · URLs

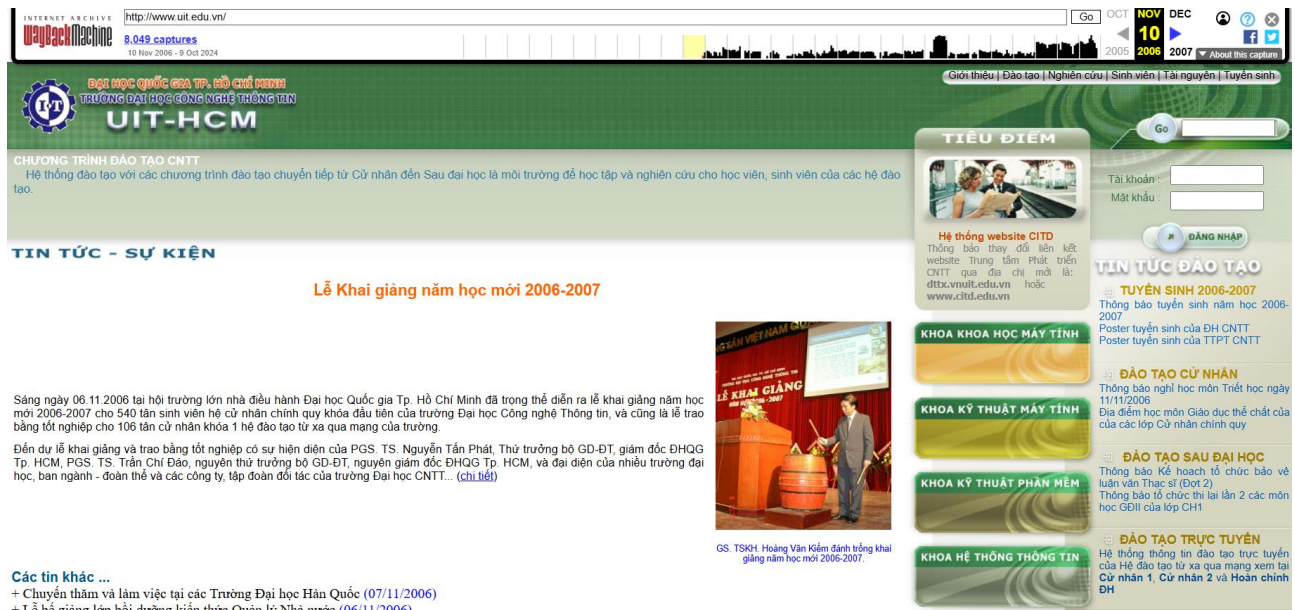
More than 10,000 URLs have been captured for this URL prefix.

admin

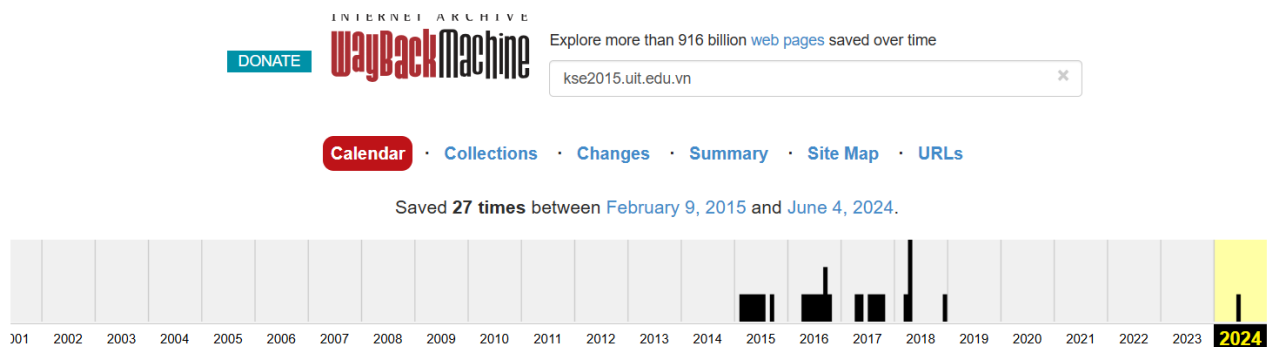
URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://uit.edu.vn:80/admin	text/html	Jan 18, 2011	Sep 13, 2011	9	6	3
http://uit.edu.vn:80/admin/editor	text/html	May 18, 2011	Aug 31, 2011	2	1	1
http://uit.edu.vn:80/admin/images	text/html	Dec 6, 2010	Dec 6, 2010	1	0	1
http://uit.edu.vn:80/admin/images/security	text/html	Dec 6, 2010	Dec 6, 2010	1	0	1
http://uit.edu.vn:80/admin/test.php	text/html	Dec 6, 2010	Feb 9, 2012	19	0	19
http://uit.edu.vn:80/admin/test.php?PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	text/html	Dec 10, 2010	Nov 11, 2011	4	3	1
http://www.uit.edu.vn:80/admin/?lang=en	text/html	Dec 22, 2007	Sep 13, 2011	5	4	1
http://www.uit.edu.vn:80/admin/index.php?	text/html	Dec 21, 2007	Nov 3, 2008	10	9	1
http://www.uit.edu.vn:80/admin/login.php	text/html	Dec 21, 2007	Feb 9, 2012	31	2	29
http://www.uit.edu.vn:80/administrator	text/html	Sep 16, 2012	Aug 13, 2014	19	18	1
http://www.uit.edu.vn:80/ce/student/admin/default.php	text/html	Oct 14, 2008	Sep 13, 2011	6	5	1
http://www.uit.edu.vn:80/ce/student/admin/Login.php	text/html	Oct 14, 2008	Sep 13, 2011	12	11	1
http://www.uit.edu.vn:80/ce/student/admin/thongbao.php?	text/html	Nov 5, 2009	Mar 12, 2010	5	4	1



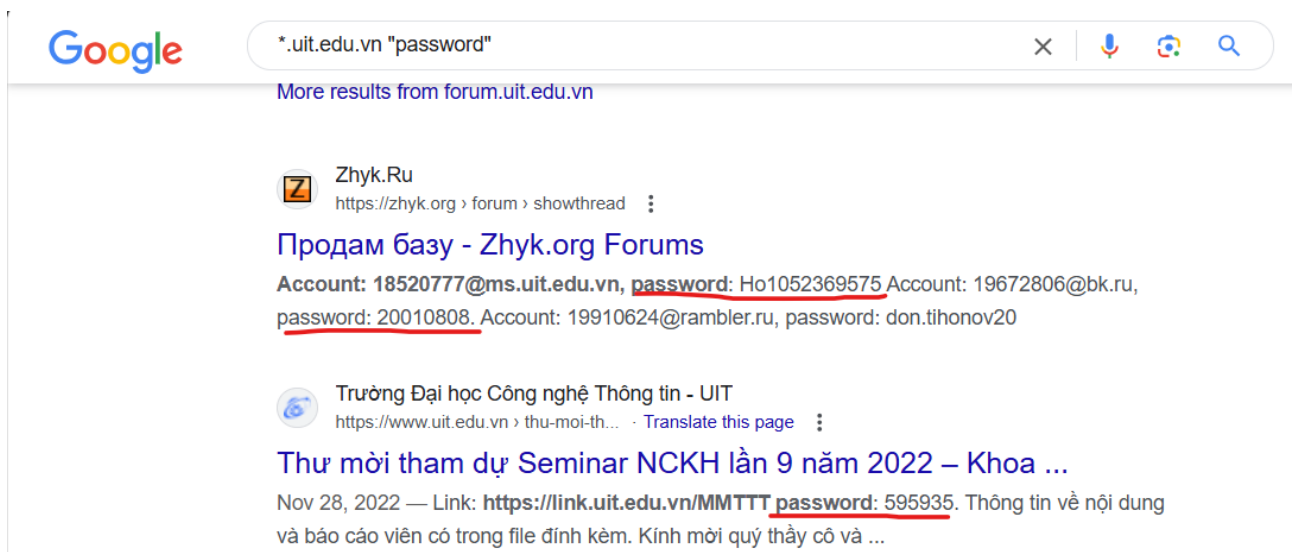
- Web trường mình vào ngày 10 tháng 11 năm 2006



- Hiện tại không thấy subdomain này còn dùng nữa mà link qua www.uit.edu.vn



4. Tìm kiếm các dữ liệu nhạy cảm của \*.uit.edu.vn thông qua google dork và github



- Lộ password tài khoản mail

A screenshot of a GitHub search interface. The search bar contains the text "uit.edu.vn password". On the left, a "Filter by" sidebar shows "Code" with 604 results, while other categories like "Repositories", "Issues", "Pull requests", "Discussions", and "Users" all show 0 results. The main area displays "604 files (1 s)". One file is expanded: "Thuytrinhne/patient-management-fe · README.md". The content of this file shows lines 149 to 153, with the following text: "UserName: 21522719@gm.uit.edu.vn", "Password: Rj123456@".

A screenshot of a GitHub README file for the repository "Mann202/Museverse-Music-Web-BE". The file content includes instructions for the front-end side, such as installing NodeJS, logging into a Spotify Premium account, and cloning the repository. It also lists credentials: "User: 21521115@gm.uit.edu.vn" and "Password: Truonggiaman.3012".

A screenshot of a GitHub configuration file for the repository "NguyenVoDucThang/Flower\_Delivery\_Website\_API". The file is located at "src/main/resources/config/application-dev.yml". It contains configuration for an SMTP email service, including the host "smtp.gmail.com", port "587", username "20522018@gm.uit.edu.vn", and password "vjwhhhdjxevnauzc".

- Bạn này làm extention auto login các trang \*.uit.edu.vn

A screenshot of a GitHub repository page for "giakiet05 / uit-auto-login". The repository is public and has 18 commits. The file list shows "src", ".gitignore", and "README.md". The "src" folder is expanded, showing a commit message "increased delay time before submit login form to ensure cap...".

-- HẾT --