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 Vỉ Khánh | 22520633 | 22520633@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| 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.**

BÁO CÁO CHI TIẾT

# 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

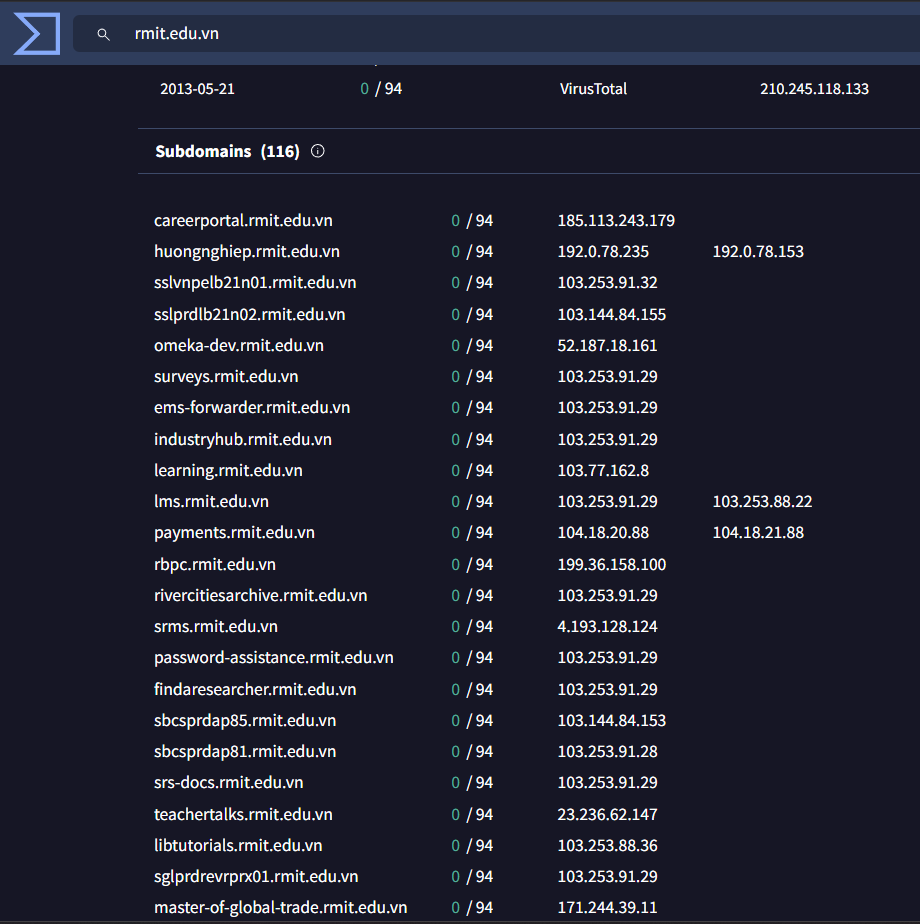
- Duckduck go

- Virustotal

- Netcraft

## 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.



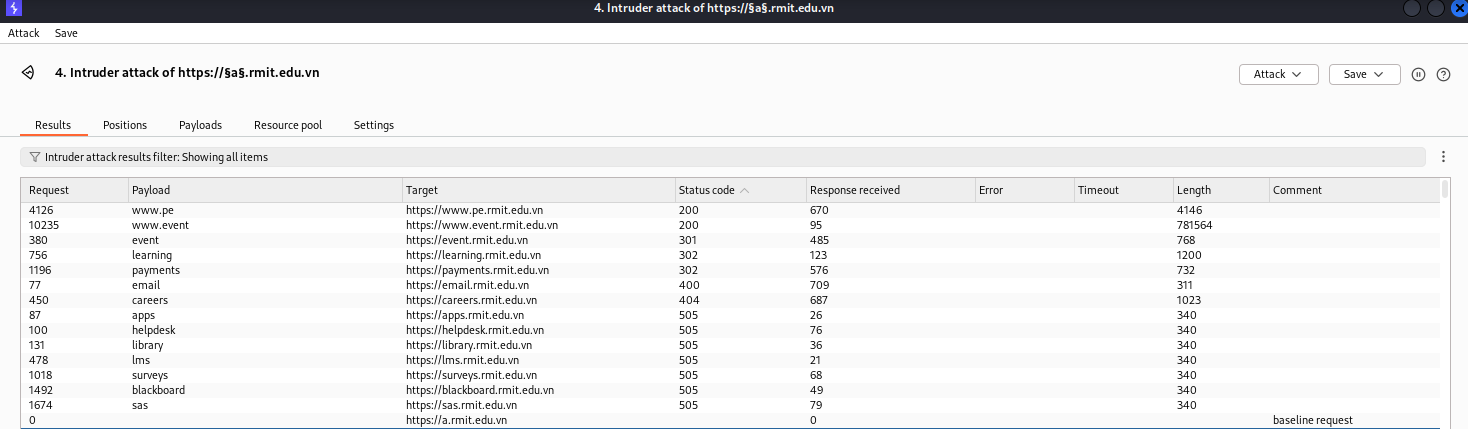
**Chậm lại và suy nghĩ 2: Tập các danh sách tên miền phụ có thể tìm kiếm ở đâu và cách nào để đưa tên miền phụ và burpsuite để tìm kiếm?**

**- Có thể kiếm 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.**

## 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



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



**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]*

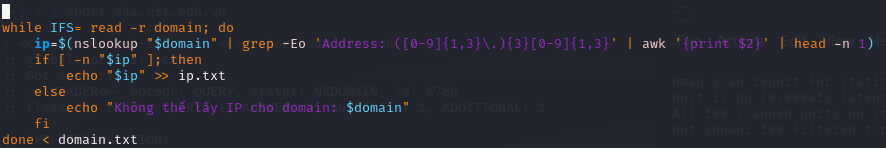
+ resolveip + *[tên miền]*

+ dig +short + *[tên miền]*

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

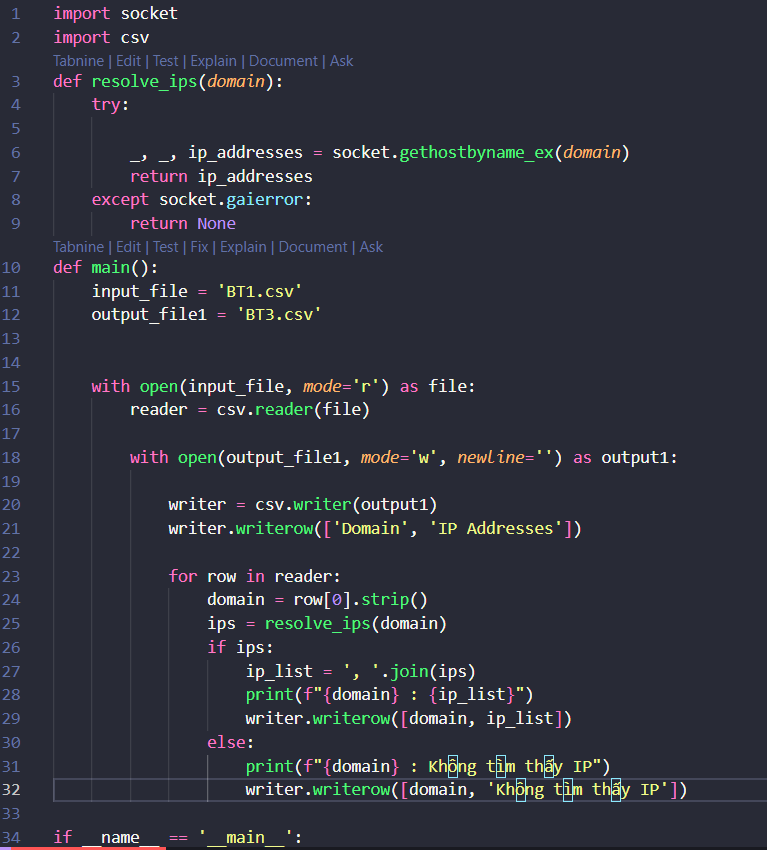
## Ghi nhận lại các địa chỉ IP của tên miền phụ tìm được của \*.rmit.edu.vn. Kết quả lưu trong file csv.

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

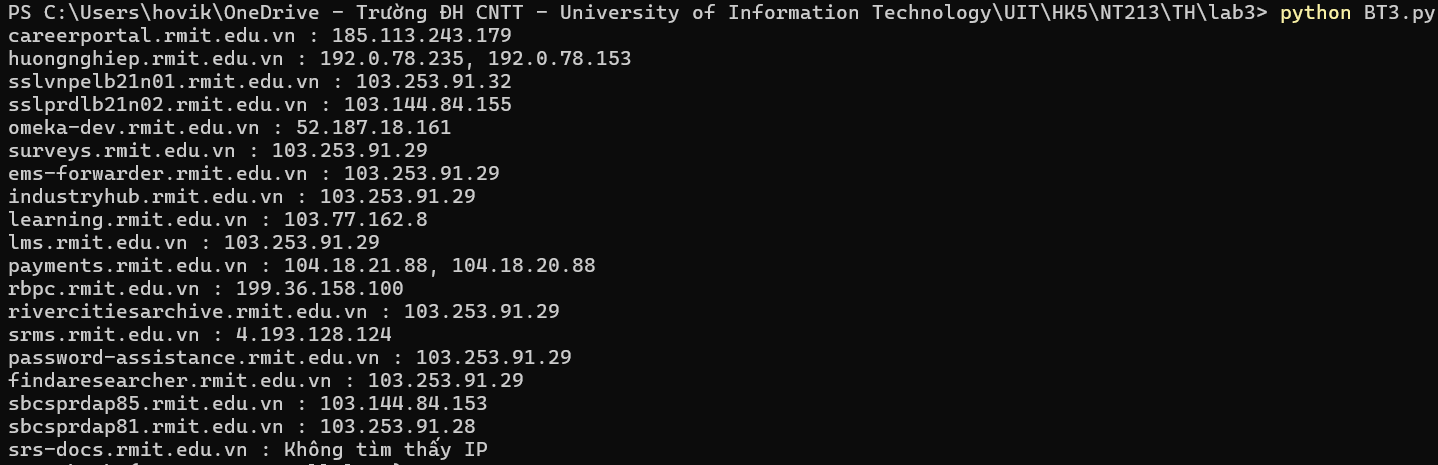


- Cách 2:

Viết chương trình python dung 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



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

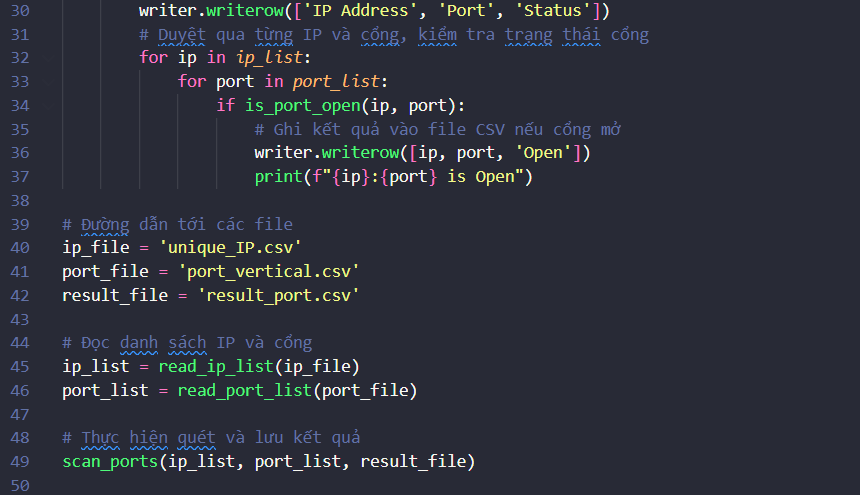


## Thực hiện scan 1000 port phổ biến trên các danh sách IP tìm được của \*.rmit.edu.vn. Báo cáo kết quả tìm được trong file csv.

**- 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.





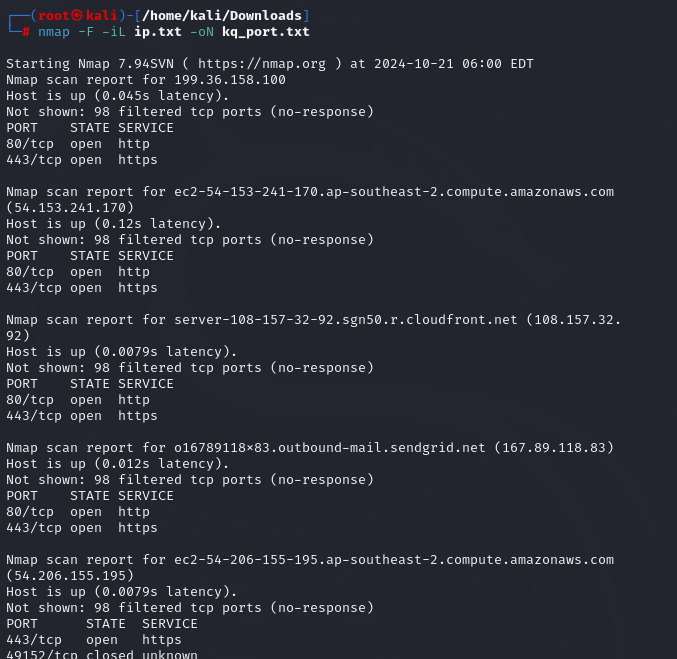
Chạy chương trình và ghi kết quả vào file result\_port.csv (Nhưng cách này khá lâu :>)



**- 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

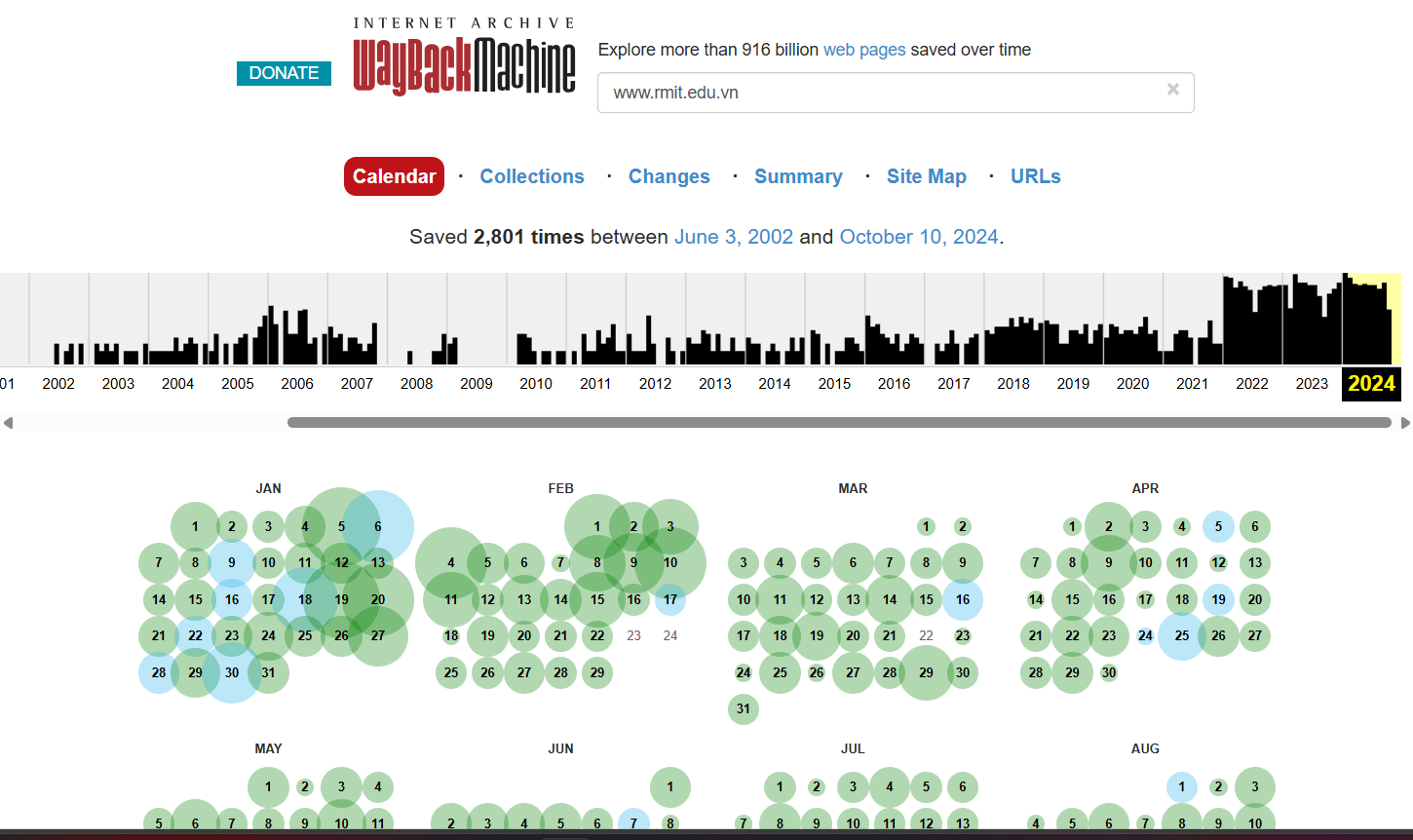
-F: scan 1000 port phổ biến.

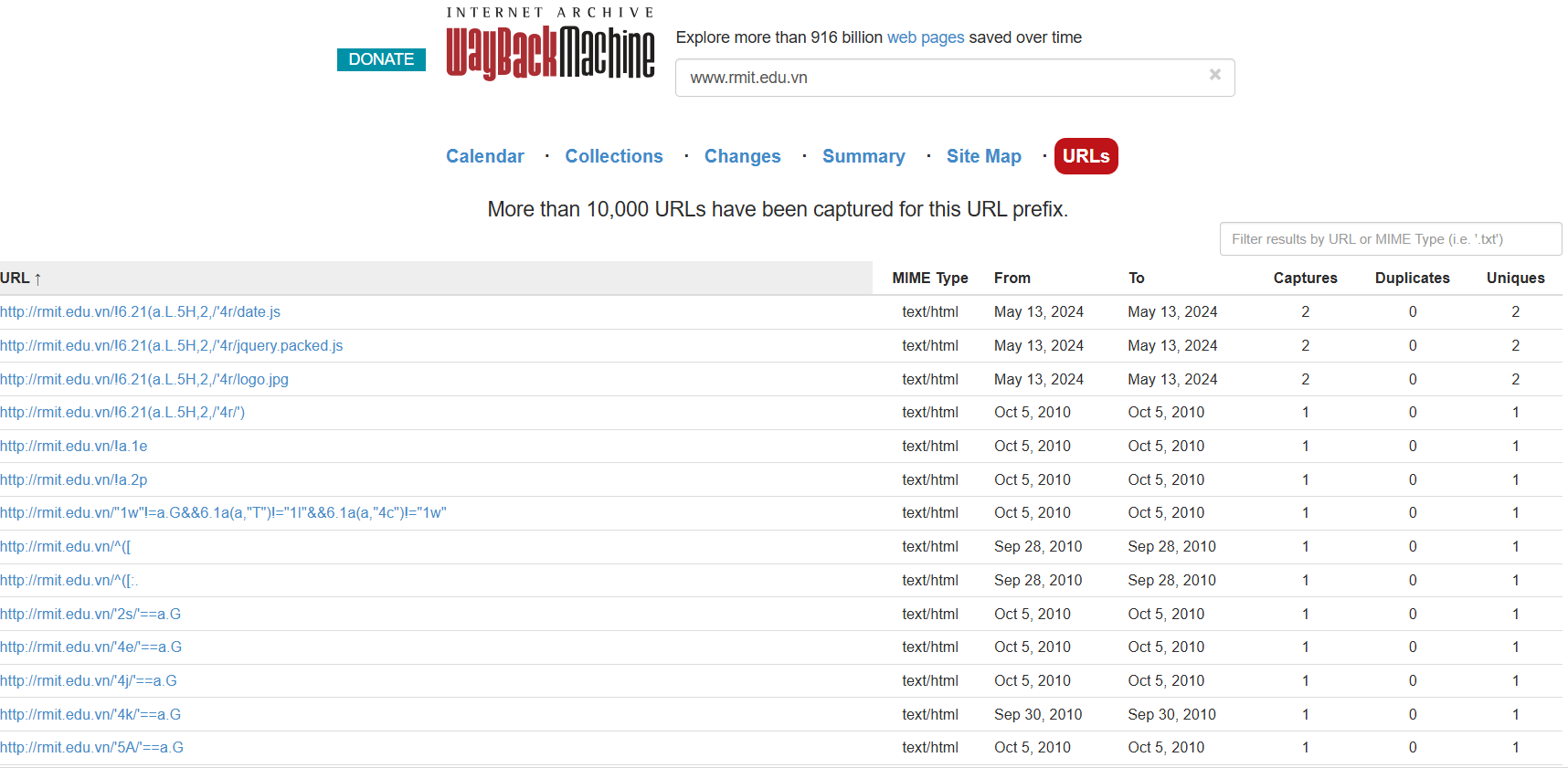


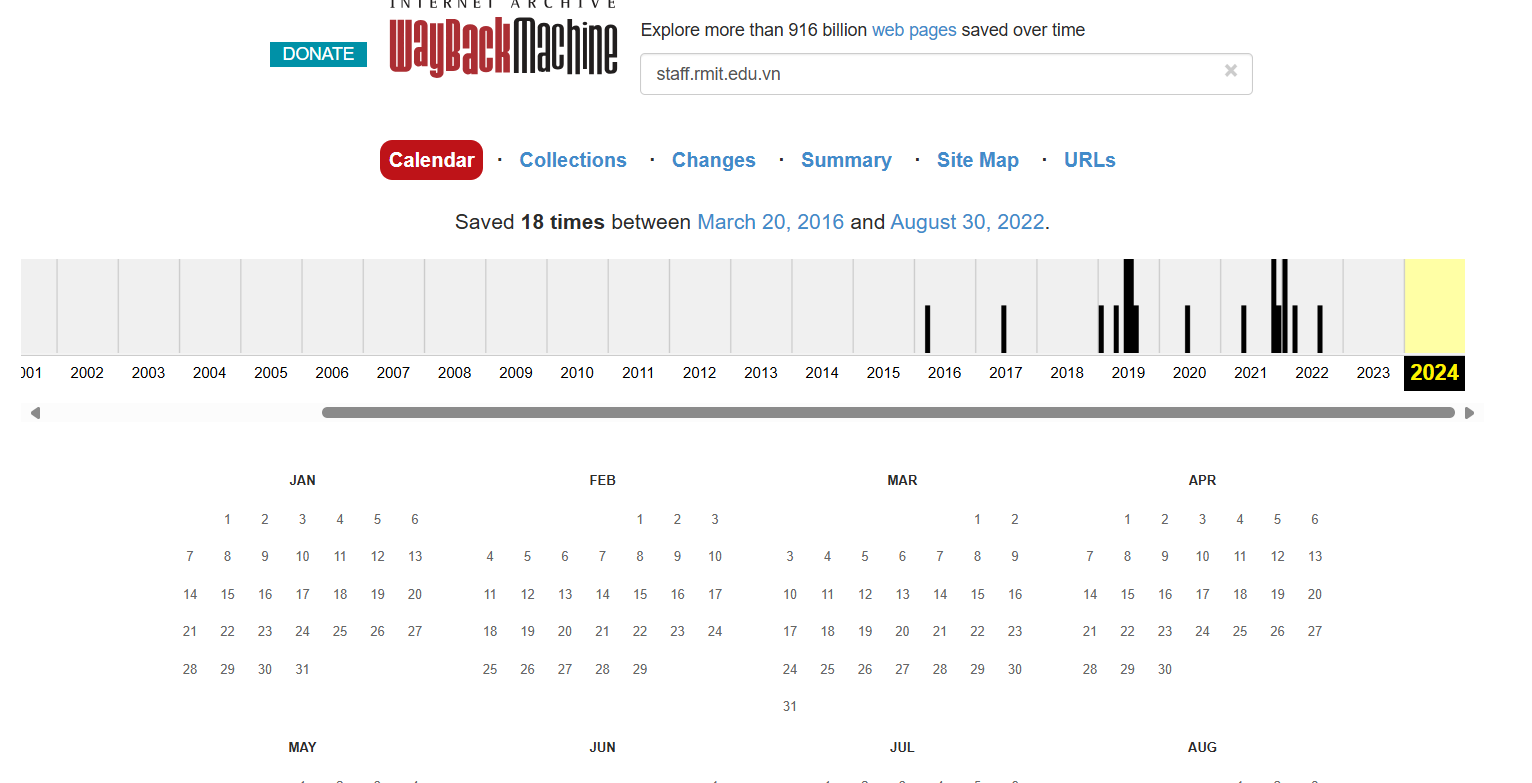
## Sử dụng https://web.archive.org/ tìm kiếm và ghi nhận lại dữ liệu quá khứ các tên miền phụ không còn tồn tại hiện nay của \*.rmit.edu.vn.

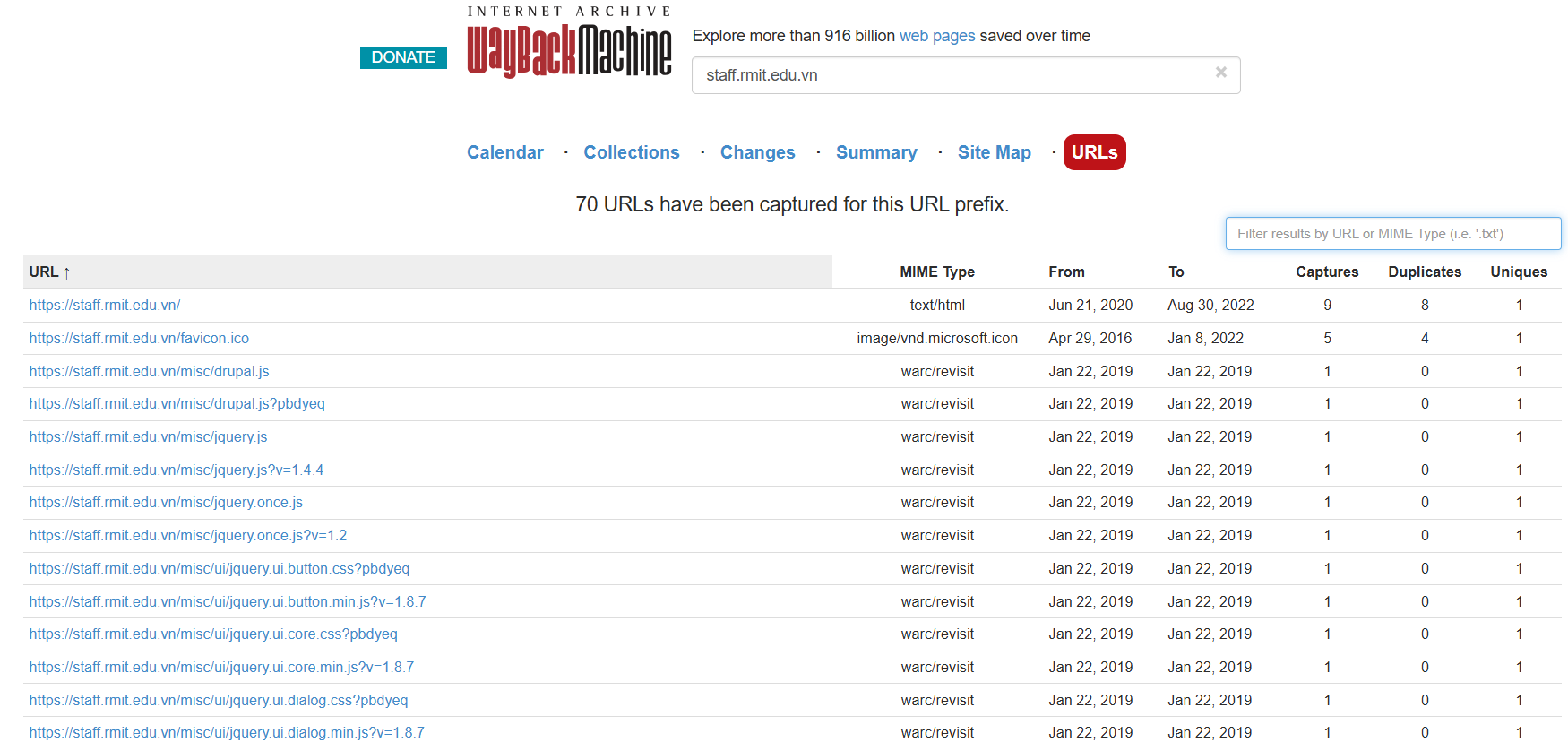
- Sử dụng trang web wayback machine để tìm kím dữ liệu trong quá khứ của các tiên miền staff.rmit.edu.vn, [www.rmit.edu.vn](http://www.rmit.edu.vn) và sso.rmit.edu.vn

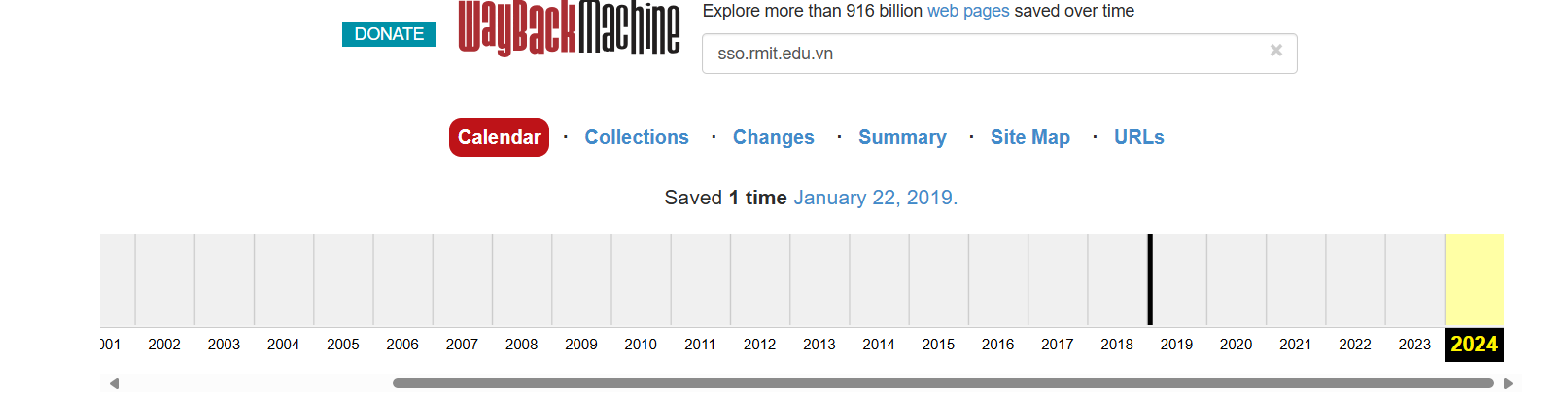
Ta thấy: Dữ liệu tên miền [www.rmit.edu.vn](http://www.rmit.edu.vn) được truy cập, sửa đổi và cập nhật thường xuyên cho đến ngày này. Còn tên miền staff.rmit.edu.vn và sso.rmit.edu.vn có vẻ ít được cập nhật sửa đổi hơn nhìu so với [www.rmit.edu.vn](http://www.rmit.edu.vn). Và cho tới ngày nay thì theo web wayback machine cập nhật được sso.rmit.edu.vn chỉ được được lưu 1 lần vào 22 tháng 1 năm 2019. 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.

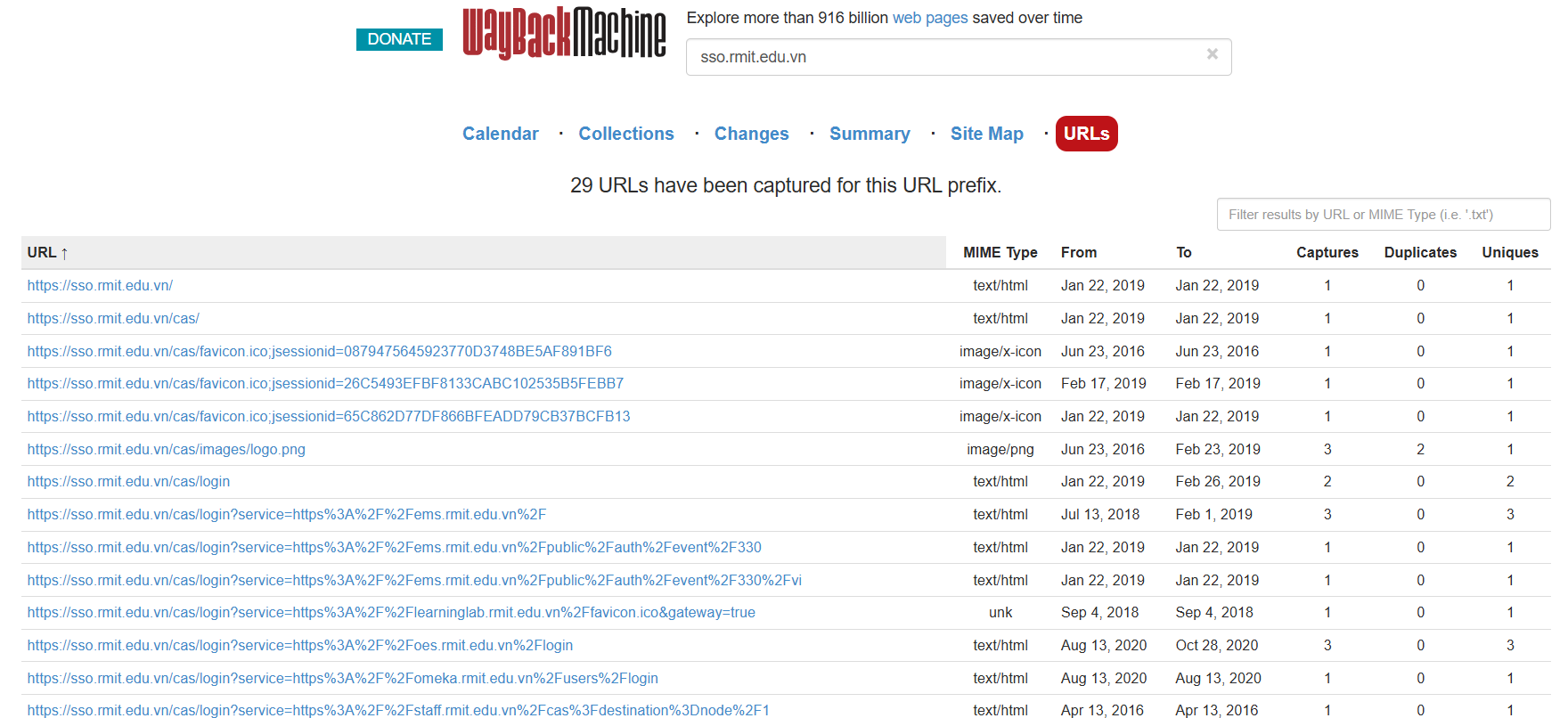








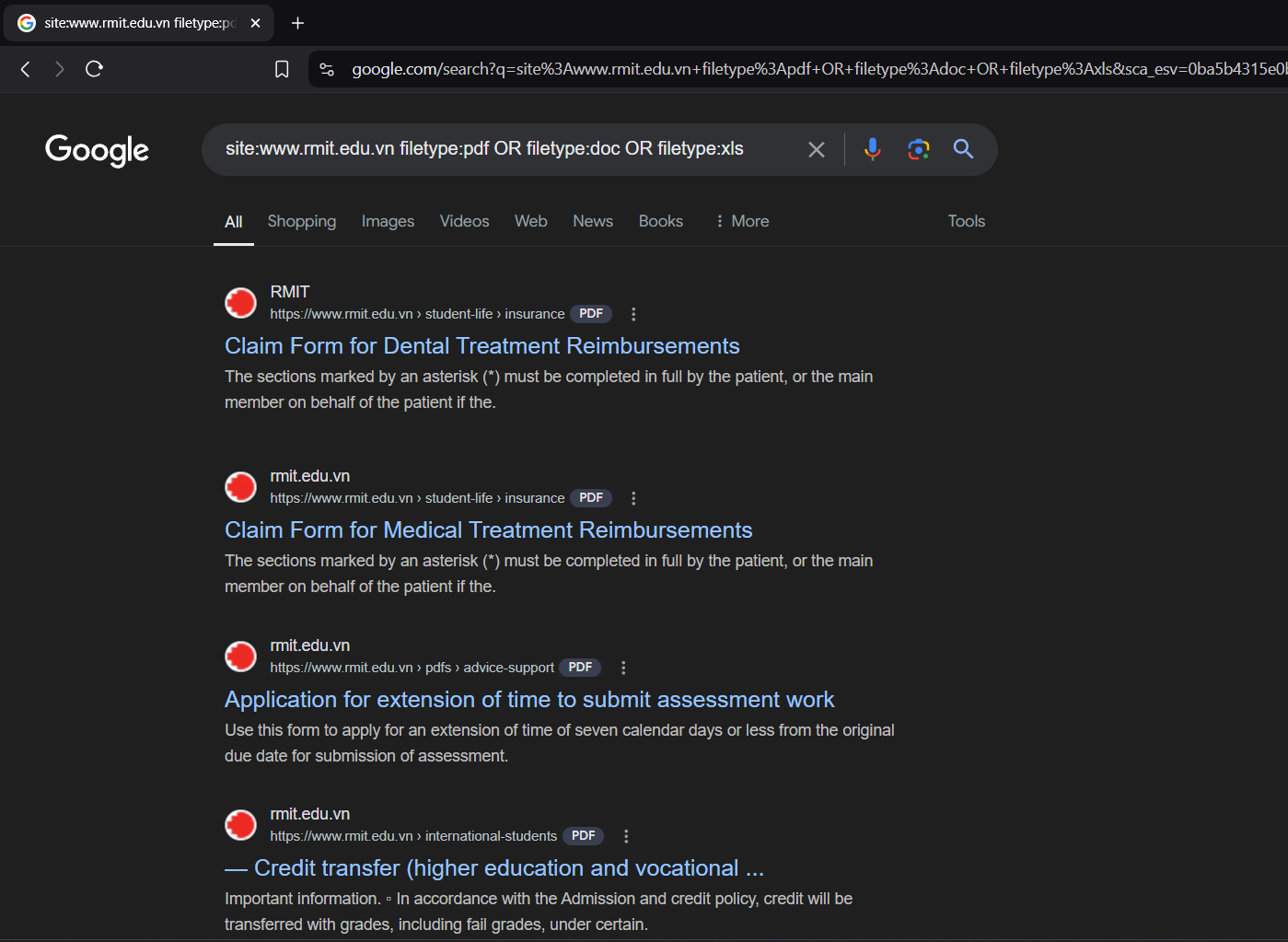




## Tìm kiếm các tập tin pdf, excel, word, trên \*.rmit.edu.vn.

- 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



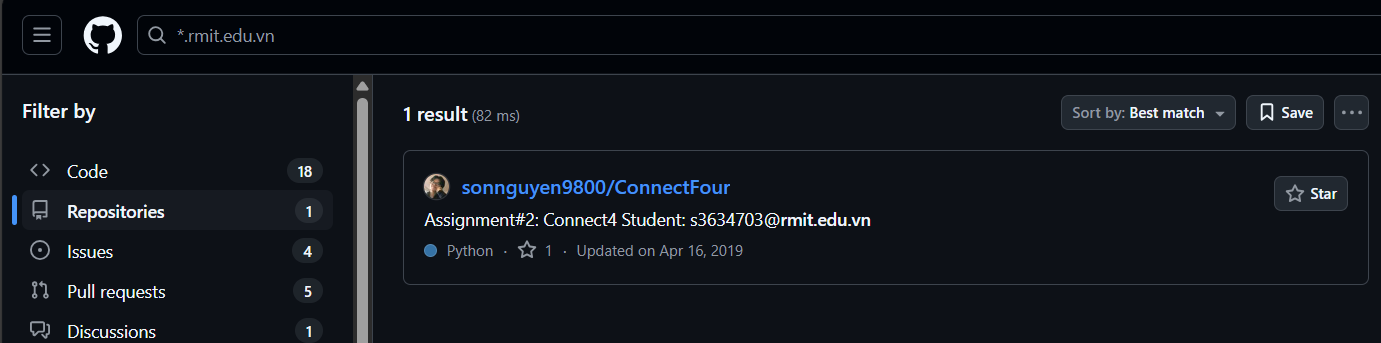
## Ghi nhận một vài thông tin tìm được trên github với domain \*.rmit.edu.vn. (lưu ý: không sử dụng thông tin này để khai thác thông tin cá nhân có thể có, mọi hành vi sử dụng không được phép sẽ chịu trách nhiệm trước pháp luật).

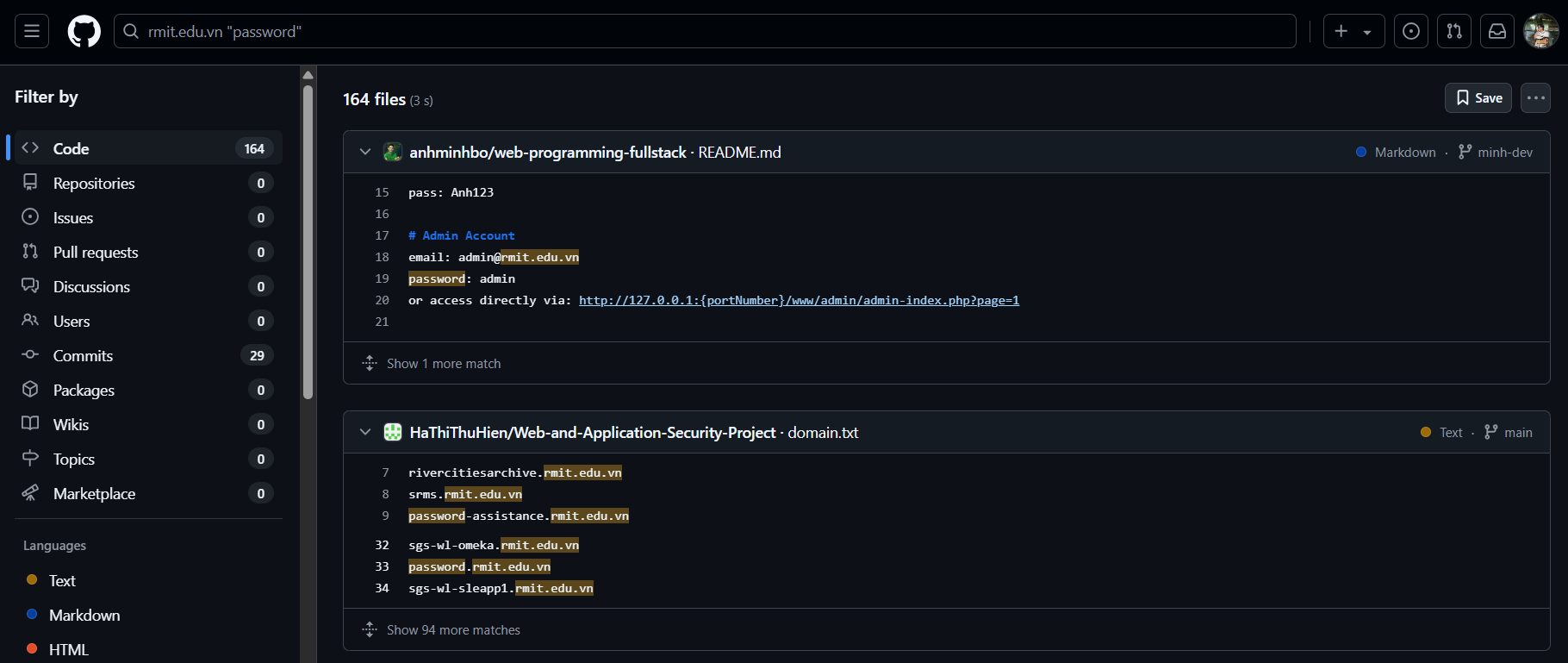
- Dùng github search thu được bởi các keyword

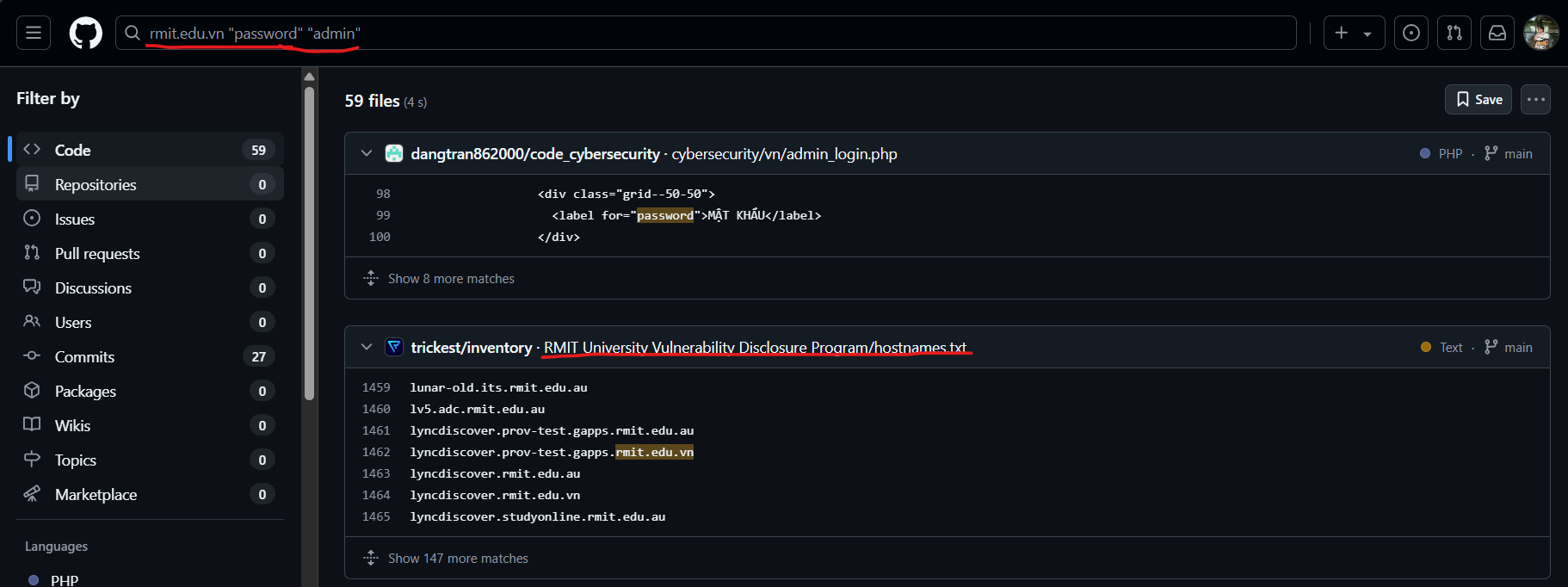
\*.rmit.edu.vn

rmit.edu.vn “password”

rmit.edu.vn “password” “admin”



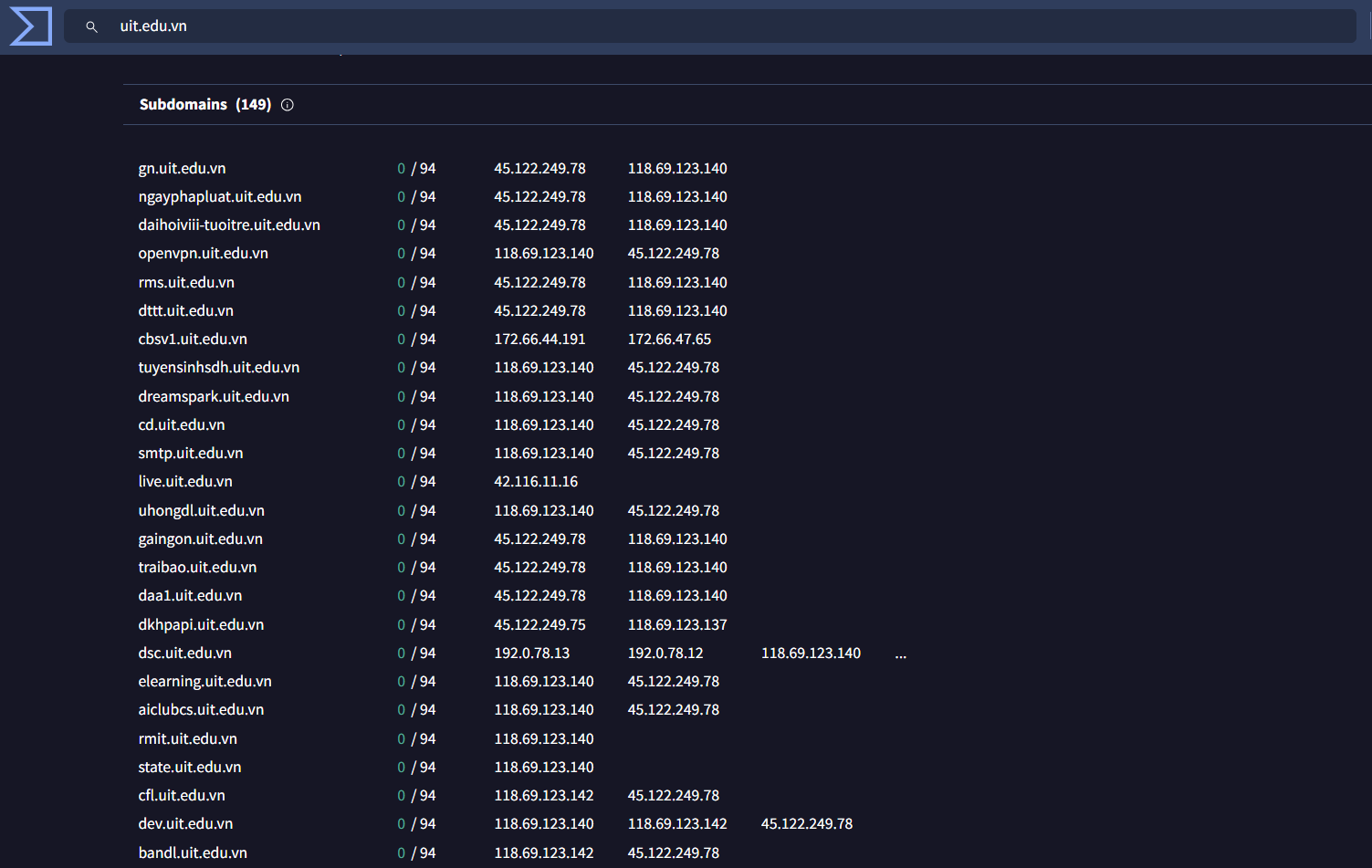


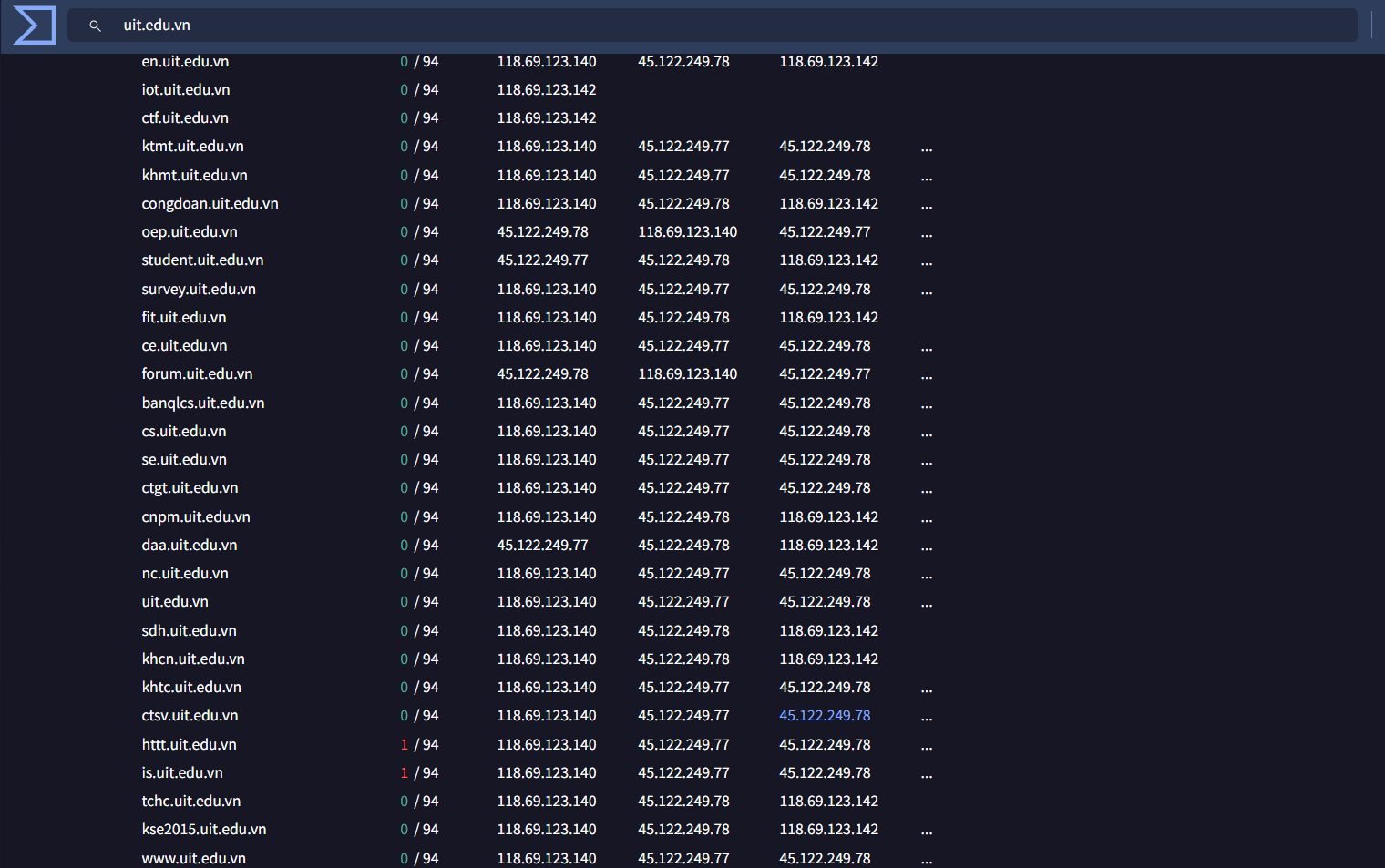


# Bài tập thực hành

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

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

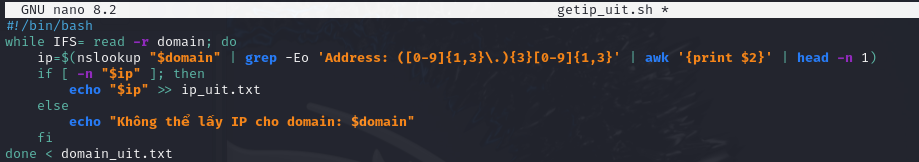




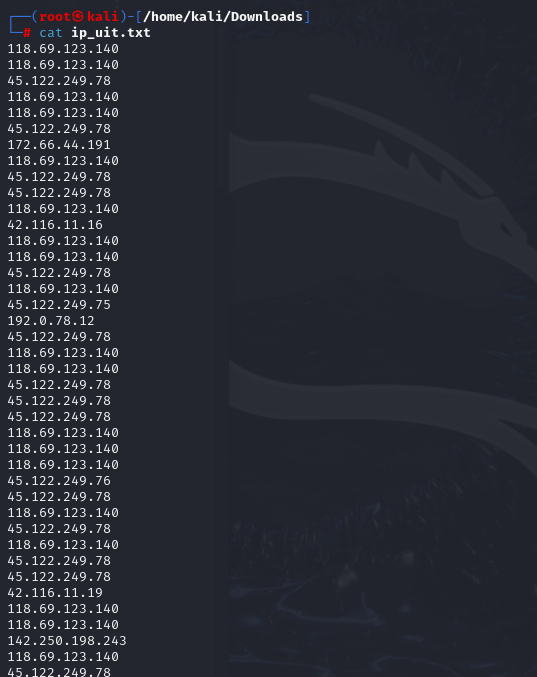
1. Tìm kiếm các địa chỉ IP thuộc \*.uit.edu.vn và các cổng đang mở tương ứng

- Lấy IP:

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

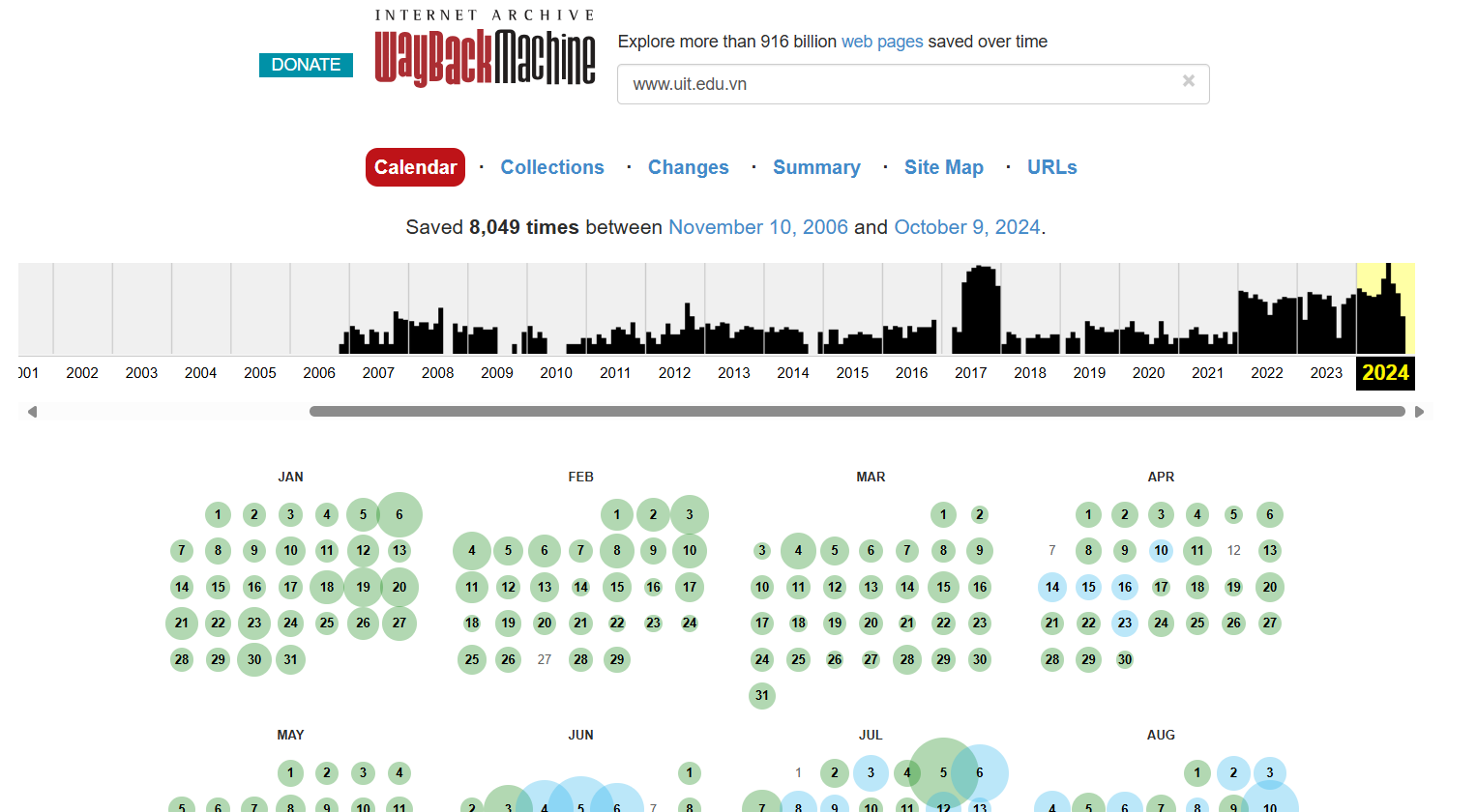


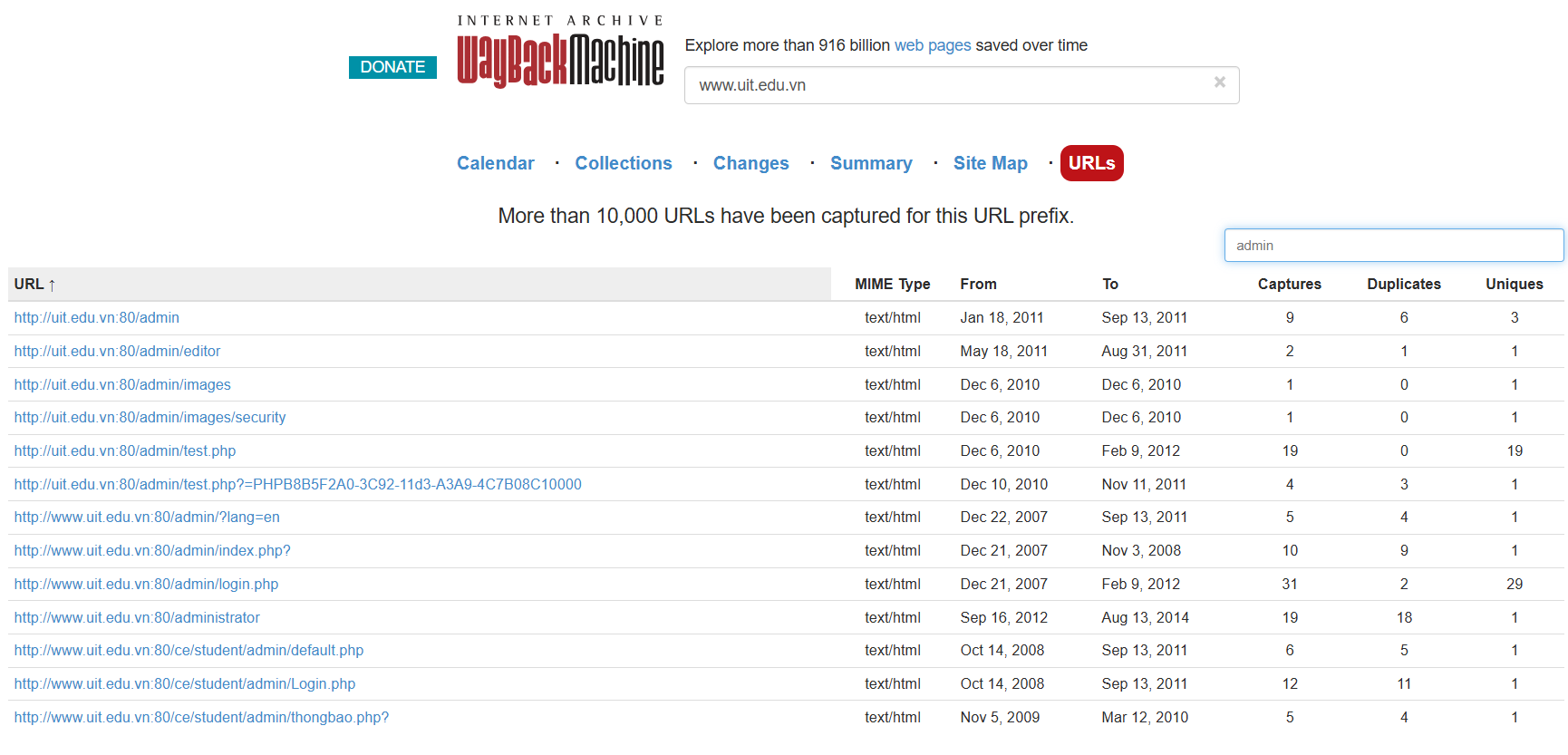
Kết quả



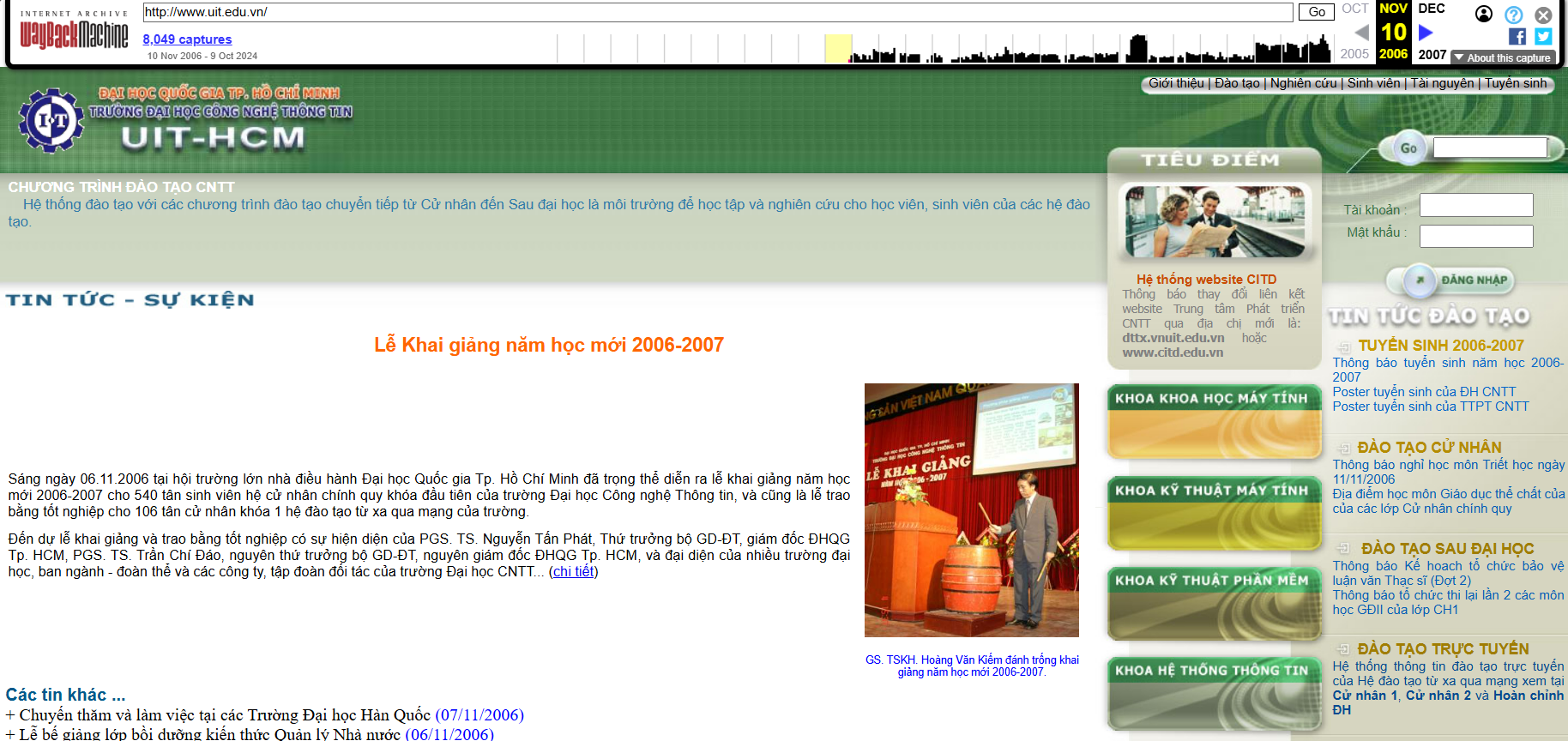
- Các cổng đang mở dùng lệnh

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

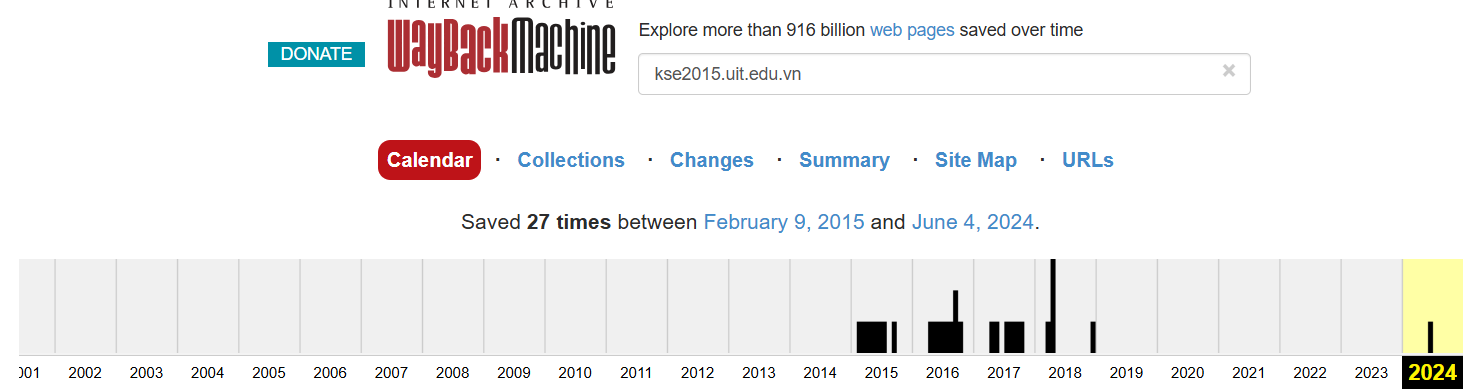




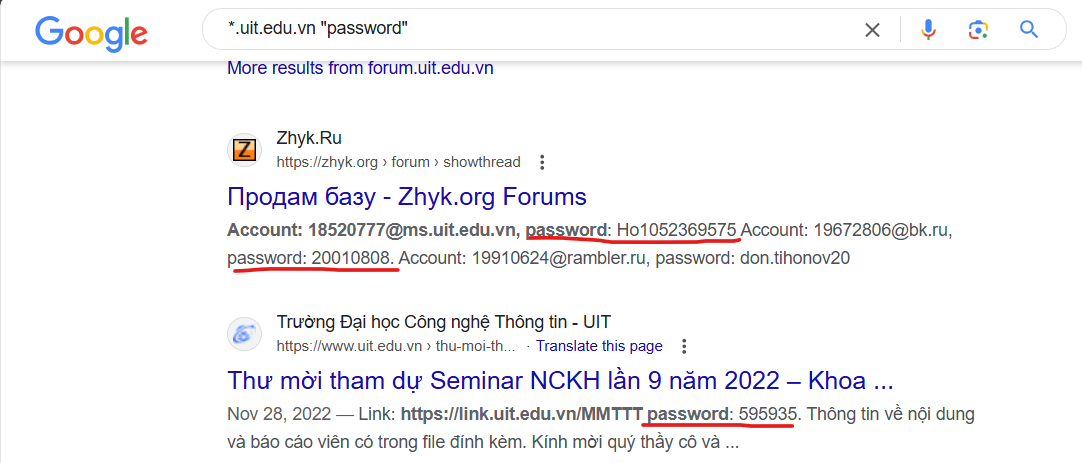
- Web trường mình vào ngày 10 tháng 11 năm 2006



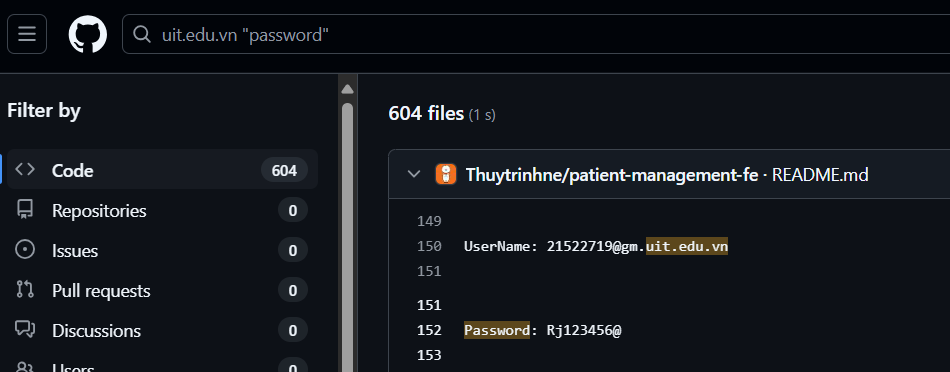
- Hiện tại không thấy subdomain này còn dùng nữa mà link qua www.uit.edu.vn

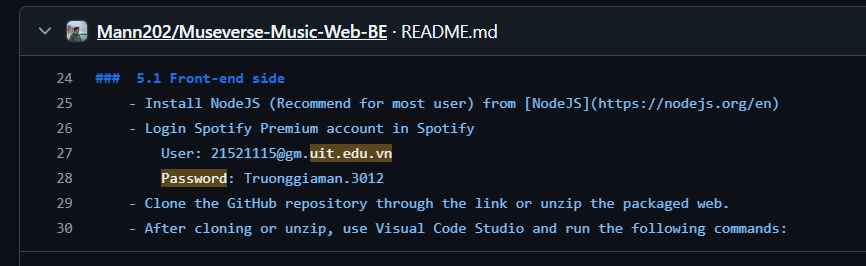


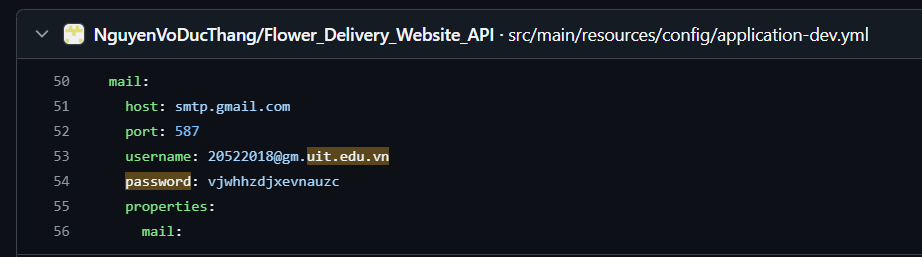
1. Tìm kiếm các dữ liệu nhạy cảm của \*.uit.edu.vn thông qua google dork và github



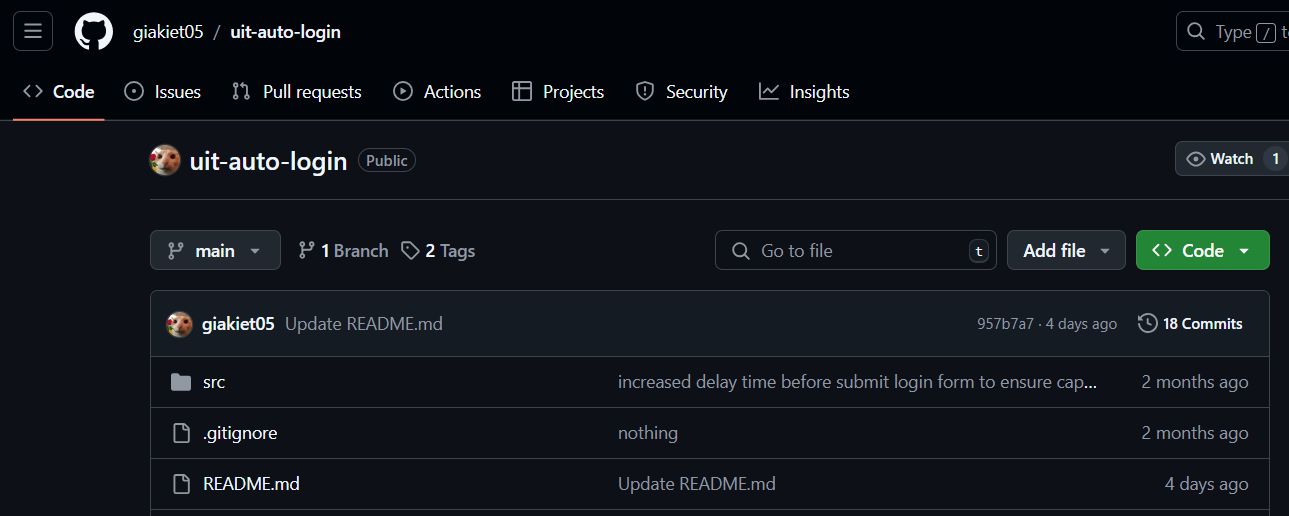
- Lộ password tài khoản mail







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



-- HẾT --

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)