

3

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Reconnaissance

Thực hành môn Bảo mật web và ứng dụng

Tháng 3/2023

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

- Giúp sinh viên có cái nhìn tổng quan hơn về cách thông tin của ứng dụng bị lộ lọt trên internet như thế nào.
- Ở bài thực hành 3, sẽ tìm hiểu cách thức để do thám trang web. Sinh viên cần hiểu rõ cách thức thông tin bị tiết lộ ra bên ngoài internet như thế nào, đồng thời có giải pháp để khắc phục các lỗ hổng.

2. Thời gian thực hành

- Thực hành tại lớp: **5** tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa **13** ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

1. Phần mềm yêu cầu

- Phần mềm Burp Suite được cung cấp hoặc bất kỳ một phần mềm proxy nào mà sinh viên sử dụng quen thuộc.

C. THỰC HÀNH

1. Subdomain Enumeration

Liệt kê ra các tên miền phụ là kỹ thuật nhằm phát hiện ra có bao nhiêu tên miền phụ thuộc về domain chính, từ đó sử dụng vào các mục đích khác nhau, ví dụ đối với người quản trị web, có thể biết được website mình đang quản lý có bao nhiêu tên miền được public ra internet và có những điểm yếu nào cần bảo vệ.

a) Liệt kê thông qua các nguồn trên internet

i. Mô tả

- Liệt kê tên miền phụ thông qua các dữ liệu được công khai trên internet. Các công cụ hỗ trợ tìm kiếm như google dork, duckduckgo,

ii. Kịch bản thực hành

- Thực hành tìm kiếm các tên miền phụ của **rmit.edu.vn**

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

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

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

i. Mô tả

- Một số các tên miền sẽ không được liệt kê công khai trên internet, do đó các công cụ tìm kiếm, các công cụ ghi log thụ động không thể tìm thấy, do đó chúng ta có thể sử dụng các danh sách tên miền phụ đã biết được tổng hợp để tìm kiếm tập các tên miền phụ.

ii. Kịch bản thực hành

- Sử dụng burpsuite intruder để tìm kiếm các tên miền phụ.

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?

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.

4. Intruder attack of https://\$subdomain.rmit.edu.vn\$ - Temporary attack - Not saved to project file

Results

Positions

Payloads

Resource pool

Settings

Filter: Showing all items

Request	Payload	Target	Status ^	Error	Timeout	Length	Comment
1	alumninetwork.rmit.edu.vn	https://alumninetwork.rmit.ed...	200	<input type="checkbox"/>	<input type="checkbox"/>	164339	baseline request
16	findaresearcher.rmit.edu.vn	https://findaresearcher.rmit.e...	200	<input type="checkbox"/>	<input type="checkbox"/>	1101	
17	helpdesk.rmit.edu.vn	https://helpdesk.rmit.edu.vn	200	<input type="checkbox"/>	<input type="checkbox"/>	5138	
2	apps.rmit.edu.vn	https://apps.rmit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	821	
15	experienceday.rmit.edu.vn	https://experienceday.rmit.e...	302	<input type="checkbox"/>	<input type="checkbox"/>	359	
5	careers.rmit.edu.vn	https://careers.rmit.edu.vn	404	<input type="checkbox"/>	<input type="checkbox"/>	32452	
0		https://subdomain.rmit.edu.vn		<input type="checkbox"/>	<input type="checkbox"/>		
3	appsdr.rmit.edu.vn	https://appsdr.rmit.edu.vn		<input type="checkbox"/>	<input type="checkbox"/>		
4	blackboard.rmit.edu.vn	https://blackboard.rmit.edu.vn		<input type="checkbox"/>	<input type="checkbox"/>		
6	chame.rmit.edu.vn	https://chame.rmit.edu.vn		<input type="checkbox"/>	<input type="checkbox"/>		
7	crmdr.rmit.edu.vn	https://crmdr.rmit.edu.vn		<input type="checkbox"/>	<input type="checkbox"/>		
8	democlass.rmit.edu.vn	https://democlass.rmit.edu.vn		<input type="checkbox"/>	<input type="checkbox"/>		

2. Host and Port Discovery

Với các tên miền phụ đã biết, để hiểu sâu hơn về các trang web đã tìm được, có thể tìm kiếm các IP tương ứng với các tên miền đó và port tương ứng

a) Tìm kiếm các host tương ứng

i. Mô tả:

- Mỗi tên miền sẽ được tương ứng với 1 địa chỉ IP tương ứng do DNS trả về. Tùy theo mục đích sử dụng thì 1 IP có thể có nhiều tên miền được trả về và được quản lý bởi bộ phân giải tên miền của người quản trị. Việc biết được IP giúp cho người quản trị dễ dàng hơn trong việc nhận định xem địa chỉ IP đó có đang được host quá nhiều dịch vụ hay không, hoặc các thông tin mặc định được tiết lộ thông qua cấu hình DNS sai hay không.

ii. Kịch bản thực hành

- Tìm kiếm các địa chỉ IP tương ứng với các tên miền phụ đã tìm được ở bài tập 1 và 2.

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

```
> nslookup helpdesk.rmit.edu.vn
Server:          1.1.1.1
Address:         1.1.1.1#53

Non-authoritative answer:
helpdesk.rmit.edu.vn canonical name = sglprdrevrprx01.rmit.edu.vn.
Name:   sglprdrevrprx01.rmit.edu.vn
Address: 103.253.91.29
```

b) Tìm kiếm port tương ứng*i. Mô tả:*

- Mỗi địa chỉ IP có thể được public nhiều port khác nhau lên internet, mỗi port chạy 1 dịch vụ. Có thể dịch vụ trên port 80 không gây ra lỗi, tuy nhiên port 1337, 8080 chạy các dịch vụ không xác thực, dẫn đến gây nên một điểm yếu của hệ thống, hiểu được kỹ thuật tìm kiếm các port có thể giúp người quản trị biết được các port nào đang được public ra internet và hạn chế các thông tin quan trọng bị khai thác.

ii. Kịch bản thực hành

- Thực hiện scan các port phổ biến trên các địa chỉ IP tìm được.

Chậm lại và suy nghĩ 4: Các công cụ scan port hiện nay có thể sử dụng là gì nmap, naabu, nessus, netcat ...?

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 tại <https://raw.githubusercontent.com/HeckerBirb/top-nmap-ports-csv/master/top-1000-most-popular-tcp-ports-nmap-sorted.csv>

3. Truy tìm thông tin của website

Đôi lúc website được hosting trong quá khứ tồn tại những thông tin nhạy cảm và được lưu giữ lại. Việc phát hiện và xóa, hoặc thay đổi là cần thiết để không ảnh hưởng đến các website hiện tại

a) Tìm kiếm thông qua Internet Archive

iii. Mô tả:

- Đây là một địa chỉ lưu trữ nhưng thông tin website trong quá khứ, tuy không phải toàn bộ, nhưng phần lớn các thông tin có thể có của website, nếu đã public trên internet có thể được lưu giữ.

iv. Kịch bản thực hành

- Tìm kiếm các thông tin quá khứ của các tên miền phụ không còn tồn tại hiện nay của *.rmit.edu.vn

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.

The screenshot shows the search results on web.archive.org for the query `https://staff.rmit.edu.vn/*`. The table lists various URLs, their MIME types, and the dates they were captured.

URL ↑	MIME Type	From	To	Captures	D
https://staff.rmit.edu.vn/	text/html	Jun 21, 2020	Aug 30, 2022	10	
https://staff.rmit.edu.vn/favicon.ico	image/vnd.microsoft.icon	Apr 29, 2016	Jan 8, 2022	5	
https://staff.rmit.edu.vn/misc/drupal.js	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	
https://staff.rmit.edu.vn/misc/drupal.js?pbdyeq	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	
https://staff.rmit.edu.vn/misc/jquery.js	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	
https://staff.rmit.edu.vn/misc/jquery.js?v=1.4.4	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	
https://staff.rmit.edu.vn/misc/jquery.once.js	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	
https://staff.rmit.edu.vn/misc/jquery.once.js?v=1.2	warc/revisit	Jan 22, 2019	Jan 22, 2019	1	

b) Tìm kiếm thông qua google dork

iii. Mô tả:

- Google dork cung cấp các câu lệnh để tìm kiếm chính xác hơn các thông tin trên website, dựa vào đó có thể tìm được các nguồn thông tin có giá trị, ví dụ như username, password hoặc các key nhạy cảm trên website.

iv. Kịch bản thực hành

- Sử dụng google dork để tìm kiếm các thông tin trên các tên miền phụ tìm được. Tham khảo các câu lệnh tại <https://www.exploit-db.com/google-hacking-database>

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

c) Tìm kiếm thông qua github

v. Mô tả:

- Ngày nay, các mã nguồn được chia sẻ lên github ngày càng nhiều, cùng với đó là các thông tin nhạy cảm cũng được chia sẻ theo. Cho nên việc tìm kiếm các thông tin của trang web mục tiêu cũng có thể được sử dụng thông qua chức năng tìm kiếm của github

vi. Kịch bản thực hành

- Sử dụng github để tìm kiếm các thông tin trên các tên miền phụ tìm được. Tham phương pháp tại <https://infosecwriteups.com/github-dork-553b7b84bcf4>

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)

4. Bài tập thực hành

- Tìm kiếm các tên miền phụ của *.uit.edu.vn
- Tìm kiếm các địa chỉ IP thuộc *.uit.edu.vn và các cổng đang mở tương ứng.
- Tìm kiếm các dữ liệu quá khứ của *.uit.edu.vn
- Tìm kiếm các dữ liệu nhạy cảm của *.uit.edu.vn thông qua google dork và github
- (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)

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm đã đăng ký**.
- Nộp báo cáo kết quả gồm **Code, CSDL được export** và chi tiết những việc (**Report**) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-LabX_MSSV1-MSSV2-MSSV3**.
Ví dụ: [NT213.K11.ANTN.1]-Lab1_1852xxxx-1852yyyy-1852zzzz.
- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trộm, ... sẽ được xử lý tùy mức độ vi phạm.

E. GIẢI ĐÁP MẪU CÁC CÂU HỎI CHẬM LẠI VÀ SUY NGHĨ

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

- Có thể tìm kiếm tên miền phụ ở google dork.

Sử dụng **site:"state.gov"**. Các tên miền phụ của state.gov được liệt kê, ghi nhận các tên miền này lại để sử dụng sau này, trong các domain được ghi nhận, có thể sẽ có các domain không còn được liên kết với máy chủ trả về các thông báo như **This site can't be reached**. Tuy nhiên ở bước liệt kê này, chúng ta cũng sẽ ghi nhận lại và ghi chú.



This site can't be reached

Check if there is a typo in fepp.state.gov.

DNS_PROBE_FINISHED_NXDOMAIN

domain	note
1997-2001.state.gov	ok
2001-2009.state.gov	ok
2009-2017.state.gov	ok
2009-2017-fpc.state.gov	ok
2009-2017-usun.state.gov	ok
2012-keystonepipeline-xl.state.gov	ok
access.pmddtc.state.gov	ok
access.staging.pmddtc.state.gov	ok
adgcore.state.gov	ok
adgcore-staging.state.gov	ok
adggap.state.gov	ok
adggap-staging.state.gov	ok
adgstandards.state.gov	ok
adgsupport.state.gov	ok

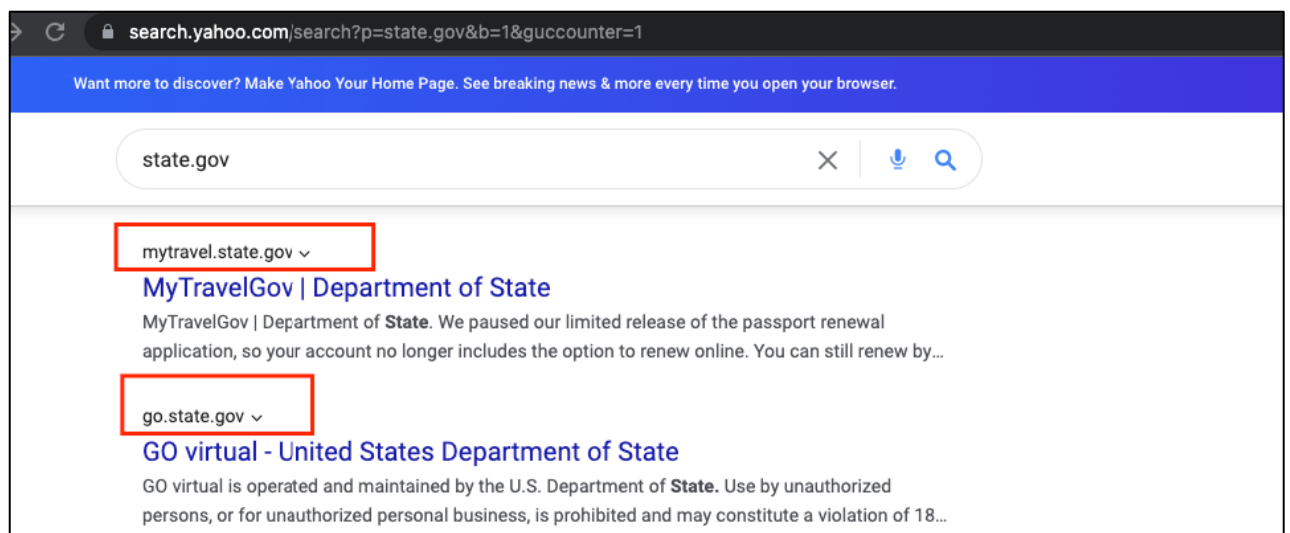
- Tìm kiếm tên miền phụ sử dụng baidu.com

<https://www.baidu.com/s?pn=1&wd=state.gov&oq=state.gov>



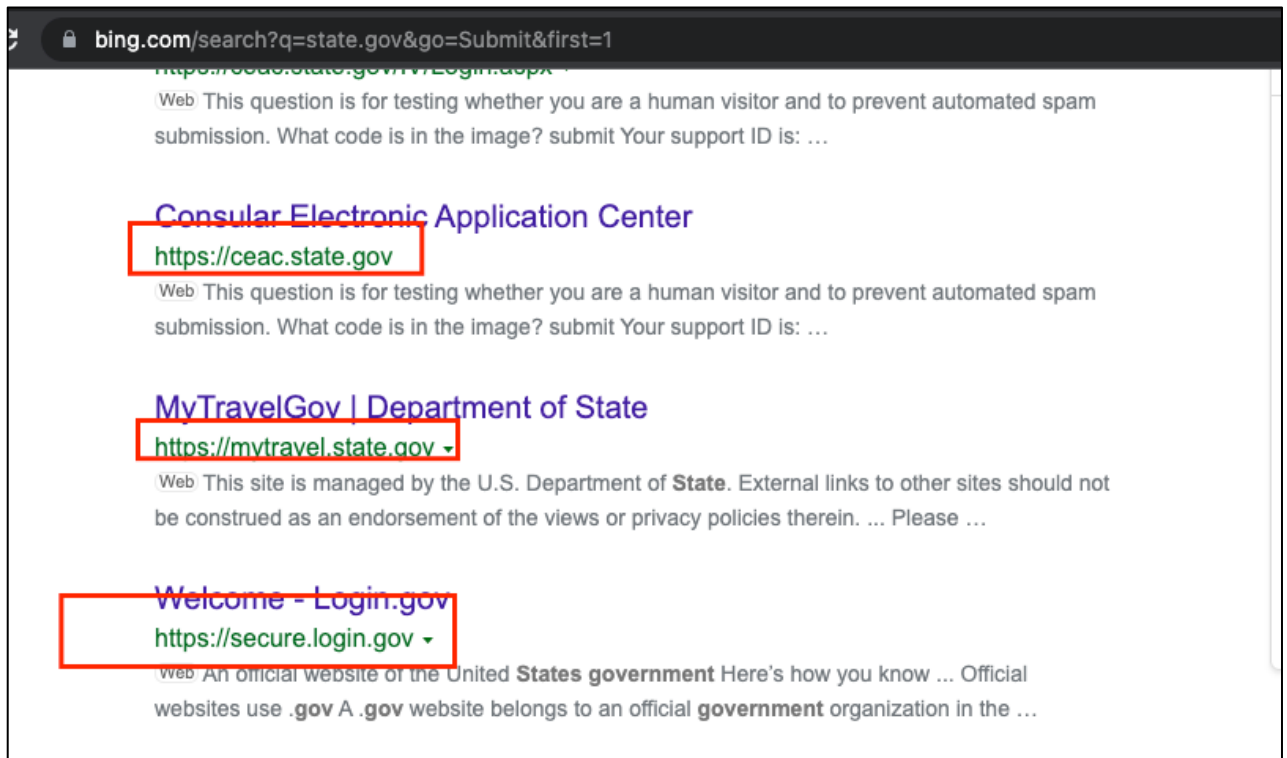
- Tìm kiếm tên miền phụ sử dụng yahoo:

<https://search.yahoo.com/search?p=state.gov&b=1>

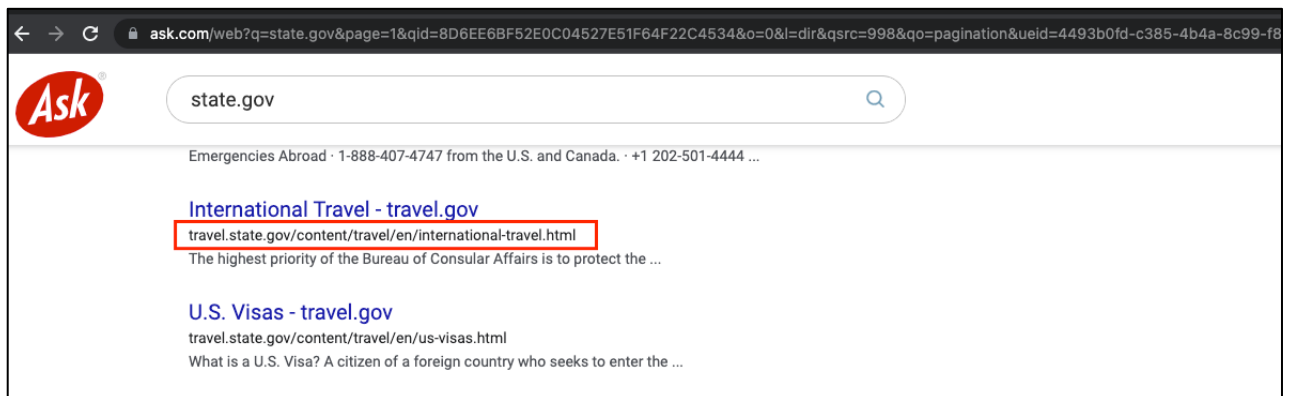


- Tìm kiếm tên miền phụ sử dụng Bing:

<https://www.bing.com/search?q=state.gov&go=Submit&first=1>



- Tìm kiếm tên miền phụ sử dụng Ask:
<http://www.ask.com/web?q=state.gov&page=1&qid=8D6EE6BF52E0C04527E51F64F22C4534&o=0&l=dir&qsrc=998&qo=pagination>



- Sử dụng netcraft:
<https://searchdns.netcraft.com/?restriction=site+ends+with&host=state.gov>

ID	Domain	First Seen	Organization	IP
3987	dvprogram.state.gov	March 2020	U.S. Department of State	FS BIG-IP
15224	www.state.gov	February 2002	Akamai Technologies	Linux
19595	tsg.phototool.state.gov	May 2021	PAUL HELLER	unknown
21770	pptform.state.gov	August 2005	U.S. Department of State	FS BIG-IP
27735	caprovservice.state.gov	May 2019	U.S. Department of State	unknown
29137	caaauthservice.state.gov	May 2019	U.S. Department of State	unknown
30567	passportstatus.state.gov	October 2005	U.S. Department of State	FS BIG-IP

- Sử dụng DNSDumpster: <https://dnsdumpster.com/> nhập domain cần tìm state.gov

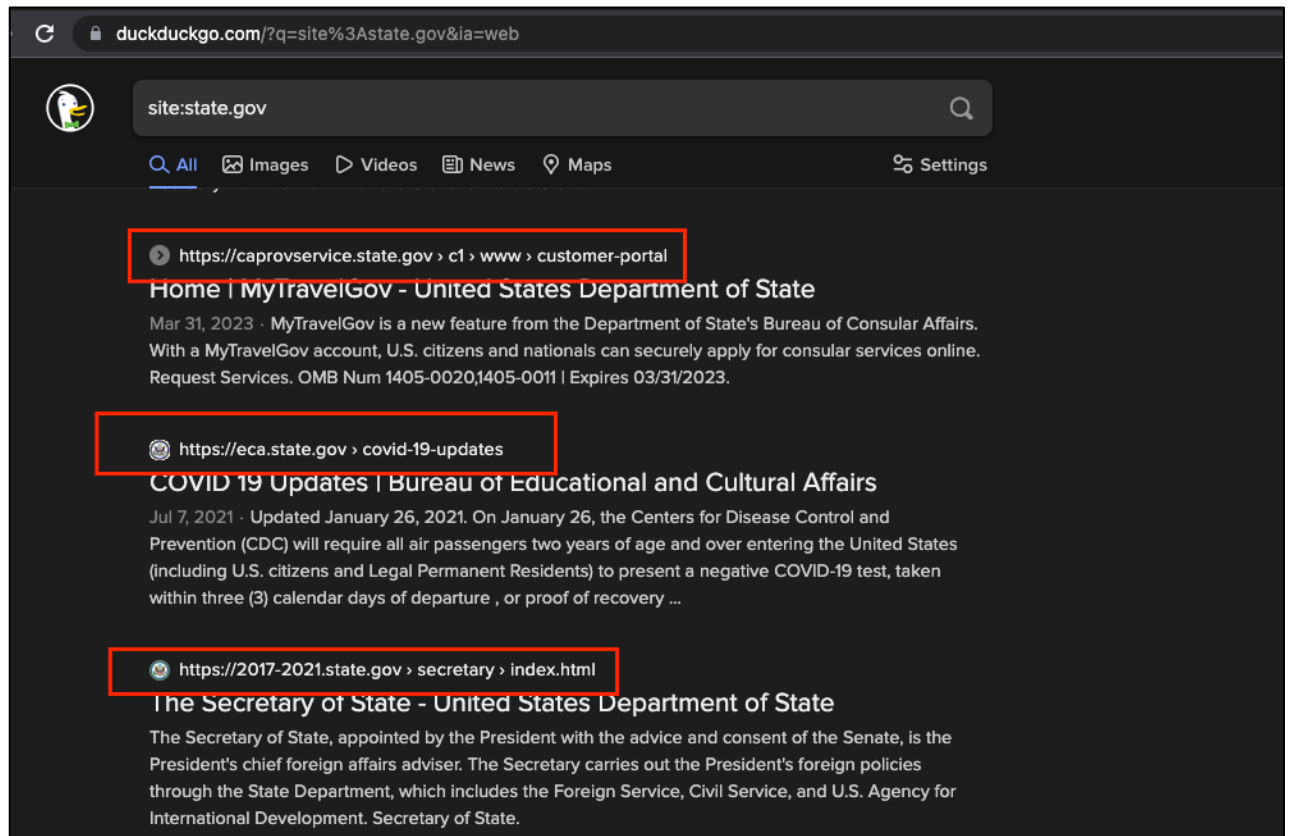
Domain	IP	Organization
dtas-online.pmdtcc.state.gov	12.190.99.27	ATT-INTERNET4 United States
data.geonode.state.gov	108.138.64.48 server-108-138-64-48.iad12.r.cloudfront.net	AMAZON-02 United States
hrex.state.gov	169.253.172.158 hrex.state.gov	USDOS United States
coins.state.gov	169.253.172.112	USDOS United States
Sidious.sierra.state.gov	169.253.172.91 sidious.sierra.state.gov	USDOS United States
caprovservice-npe-dev-shared.state.gov	169.253.40.15	USDOS United States

- Sử dụng Virustotal: <https://www.virustotal.com/gui/domain/state.gov/relations>

Date	Score	Engine	IP
2019-10-08	0 / 85	VirusTotal	72.166.186.169
2013-10-03	0 / 85	VirusTotal	72.166.186.151

Subdomain	Score	IP
casdev.state.gov	0 / 85	52.245.210.224
videodirect.state.gov	0 / 85	169.253.193.5
library.state.gov	0 / 85	169.253.2.209
results.state.gov	0 / 85	169.253.2.26
irmweb.state.gov	0 / 85	169.253.2.1
haig3.state.gov	0 / 85	169.253.194.10
haig2.state.gov	0 / 85	169.253.194.10
dnsmaster.state.gov	0 / 85	169.253.53.53
managingforresults.state.gov	0 / 85	169.253.219.131
paremote.state.gov	0 / 85	204.14.133.171

- Sử dụng duckduckgo: <https://duckduckgo.com/?q=site%3Astate.gov&ia=web>

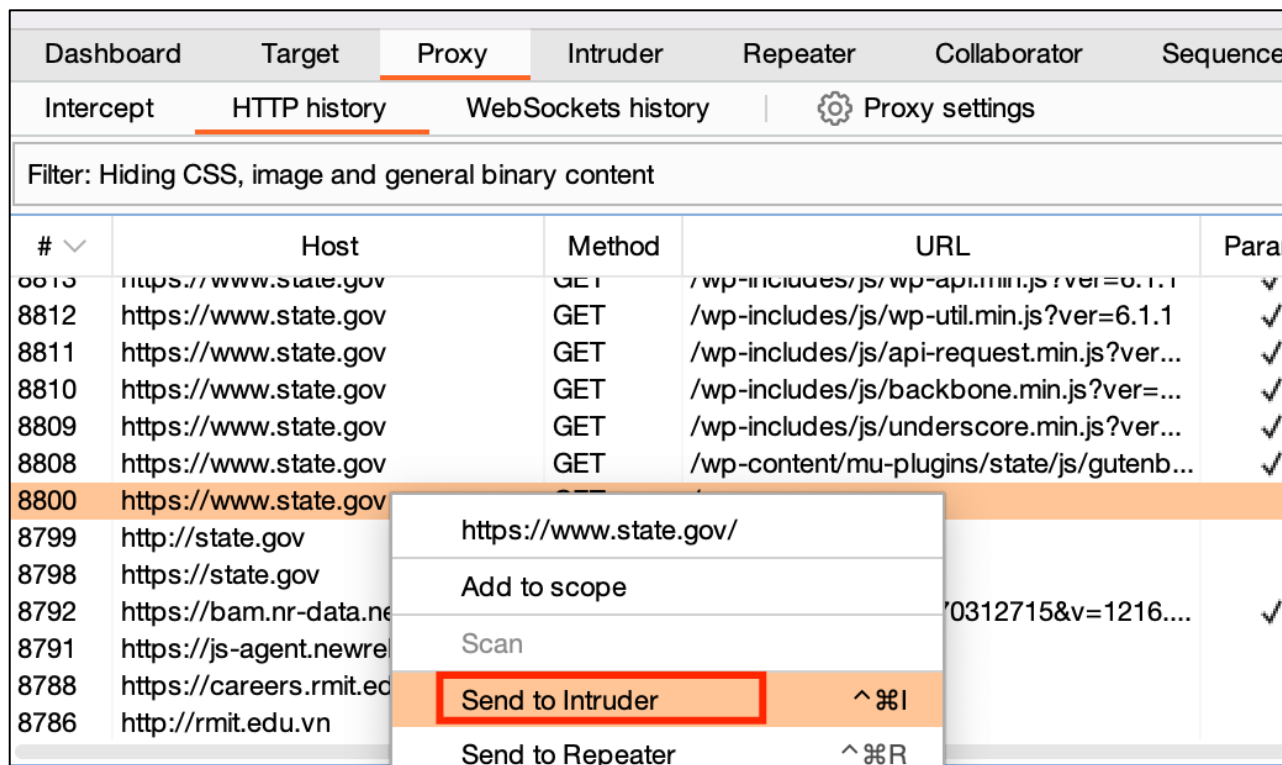


- Sử dụng c99.nl: <https://subdomainfinder.c99.nl>

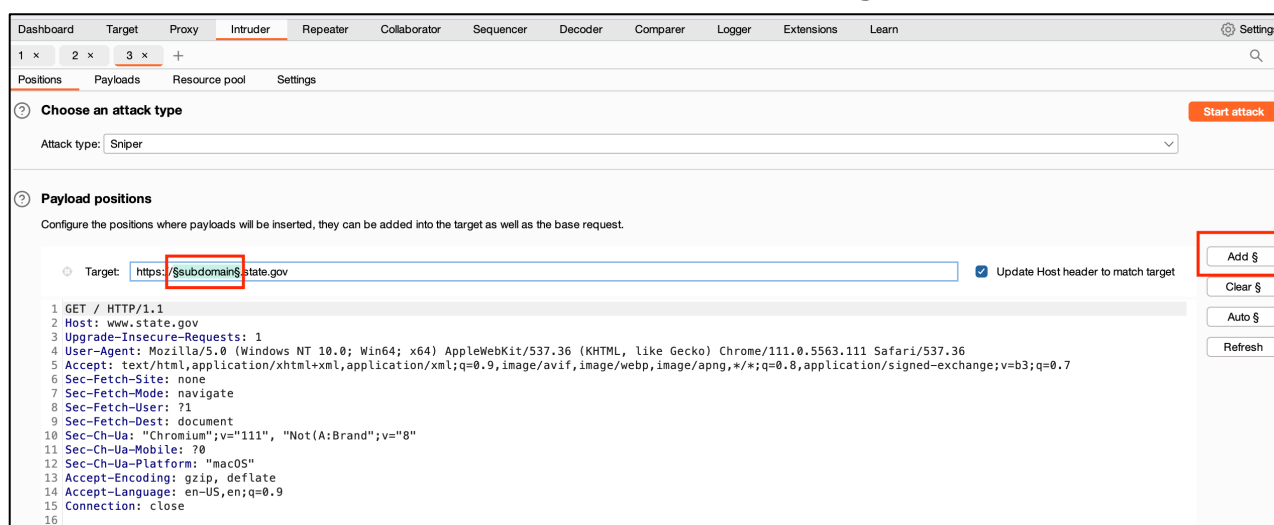
Subdomain	IP	Cloudflare
1997-2001.state.gov	23.36.162.210	Yes
2001-2009.state.gov	23.36.162.210	Yes
2009-2017.state.gov	23.36.162.210	Yes
2009-2017-fpc.state.gov	23.36.162.200	Yes
2009-2017-usun.state.gov	2.16.187.89	Yes
2012-keystonepipeline-xl.state.gov	23.36.162.200	Yes
access.pmddtc.state.gov	52.247.170.98	Yes
access.staging.pmddtc.state.gov	52.227.177.52	Yes
adgcore.state.gov	13.107.238.45	Yes
adgcore-staging.state.gov	13.107.237.45	Yes
adggap.state.gov	13.107.237.45	Yes
adggap-staging.state.gov	13.107.237.45	Yes
adgstandards.state.gov	104.45.129.178	Yes
adgsupport.state.gov	104.16.51.111	No

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 tìm được danh sách này ở trên github. Ví dụ: <https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/DNS/subdomains-top1million-5000.txt>
- Thực hiện đưa danh sách vào burpsuite intruder. Tham khảo thêm tại: <https://portswigger.net/burp/documentation/desktop/testing-workflow/mapping/hidden-content/enumerating-subdomains>
- **Bước 1:** Truy cập vào trang web muốn tìm tên miền phụ thông qua browser của burpsuite để ghi nhận HTTP history, sau đó send request này vào intruder.



- **Bước 2:** Thêm subdomain vào url để tìm kiếm, sử dụng nút Add\$



- **Bước 3:** Qua tab payload, tiến hành load list subdomain vào

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be used.

Payload set: 1 Payload count: 4,989

Payload type: Simple list Request count: 4,989

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste: www
Load ...: mail
Remove: ftp
Clear: localhost
Deduplicate: webmail
Add: smtp
webdisk
pop
cpanel
whm

Add from list ... [Pro version only]

- Bước 4:** Start attack và kiểm tra kết quả trả về, có thể tùy chỉnh thời gian giữa 2 câu request tại Resource pool để phù hợp với tốc độ trả về của trang web cần tìm kiếm, tránh việc trang web bị ddos.

2. Intruder attack of https://\$subdomain\$.state.gov - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Target	Status ^	Error	Timeout	Length	Comment
1	www	https://www.state.gov	200			189387	
63	video	https://video.state.gov	200			122277	
19	dev	https://dev.state.gov	302			1692	
74	ads	https://ads.state.gov	302			1131	
69	sip	https://sip.state.gov	404			294	
0		https://subdomain.state.gov					baseline request
2	mail	https://mail.state.gov					
3	ftp	https://ftp.state.gov					
4	localhost	https://localhost.state.gov					
5	webmail	https://webmail.state.gov					
6	smtp	https://smtp.state.gov					
7	webdisk	https://webdisk.state.gov					

Request Response

Pretty Raw Hex

```

1 GET / HTTP/2
2 Host: www.state.gov
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.111 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
  
```

0 matches

88 of 4989

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

- Sử dụng công cụ **nslookup** [tên miền]

```
> nslookup ads.state.gov
Server:      1.1.1.1
Address:     1.1.1.1#53

Non-authoritative answer:
ads.state.gov canonical name = arrivals-departures.azurewebsites.net.
arrivals-departures.azurewebsites.net canonical name = waws-prod-blu-039.vip.
azurewebsites.windows.net.
waws-prod-blu-039.vip.azurewebsites.windows.net canonical name = waws-prod-blu-
39.cloudapp.net.
Name:   waws-prod-blu-039.cloudapp.net
Address: 23.96.103.159
```

Chậm lại và suy nghĩ 4: Các công cụ scan port hiện nay có thể sử dụng là gì nmap, naabu, nessus, netcat ...?

Tham khảo các công cụ scan port tại <https://linuxhint.com/port-scan-netcat/>

- Sử dụng nmap để scan list port: **nmap -p 80,8080 ip**

```
> nmap -p 80,8080,443 23.96.103.159
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-09 12:54 +07
Nmap scan report for 23.96.103.159
Host is up (0.022s latency).

PORT      STATE      SERVICE
80/tcp    open      http
443/tcp   filtered  https
8080/tcp   filtered  http-proxy
```

HẾT

Chúc các bạn hoàn thành tốt!