

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Reconnaissance

GVHD: Ngô Đức Hoàng Sơn

Ngày báo cáo: 10/04/2024

Nhóm: 07 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.022.ATCL.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Thị Kiều Trang	21520489	21520489@gm.uit.edu.vn
2	Trần Đình Huy	21522167	21522167@gm.uit.edu.vn
3	Dương Phú Cường	21521900	21521900@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
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	80%

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

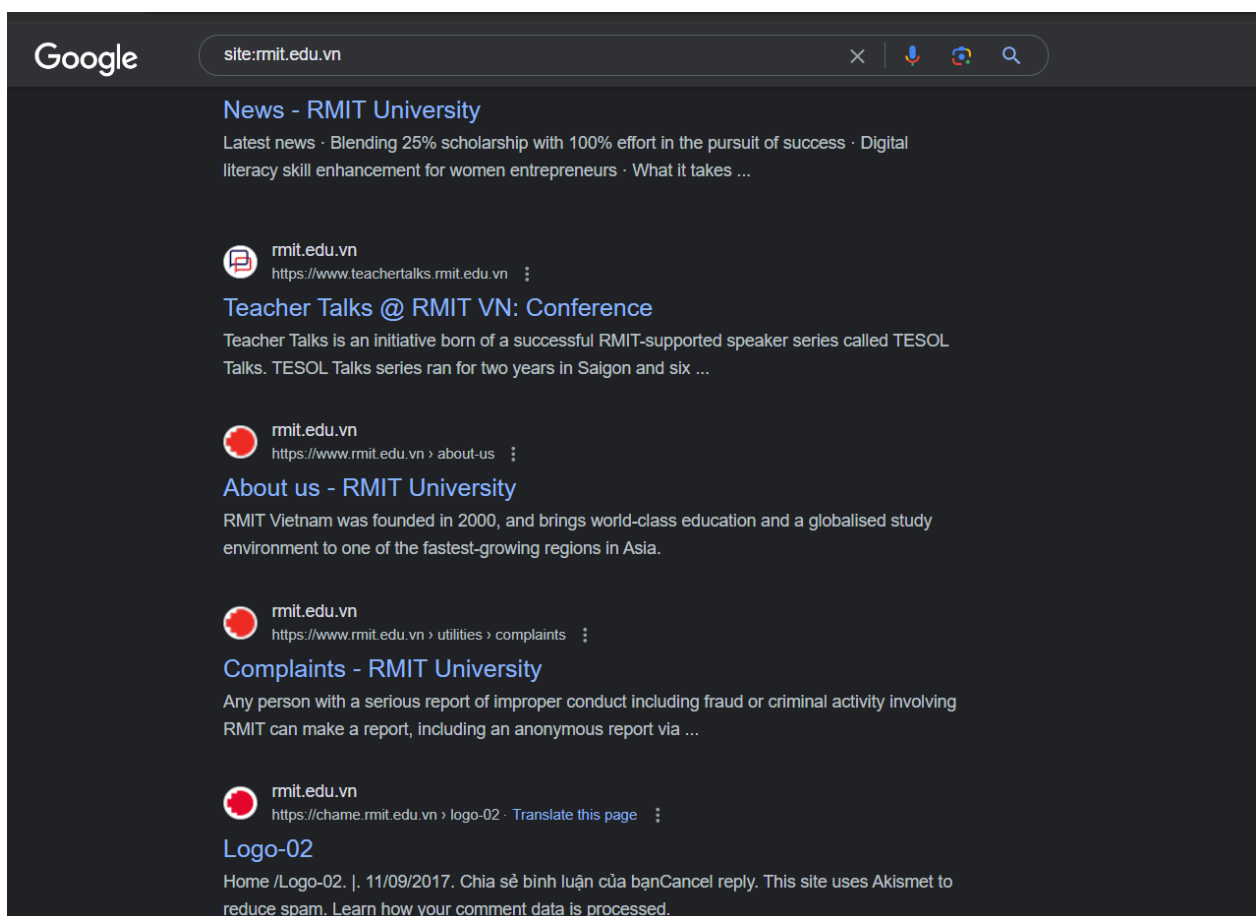
BÁO CÁO CHI TIẾT

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

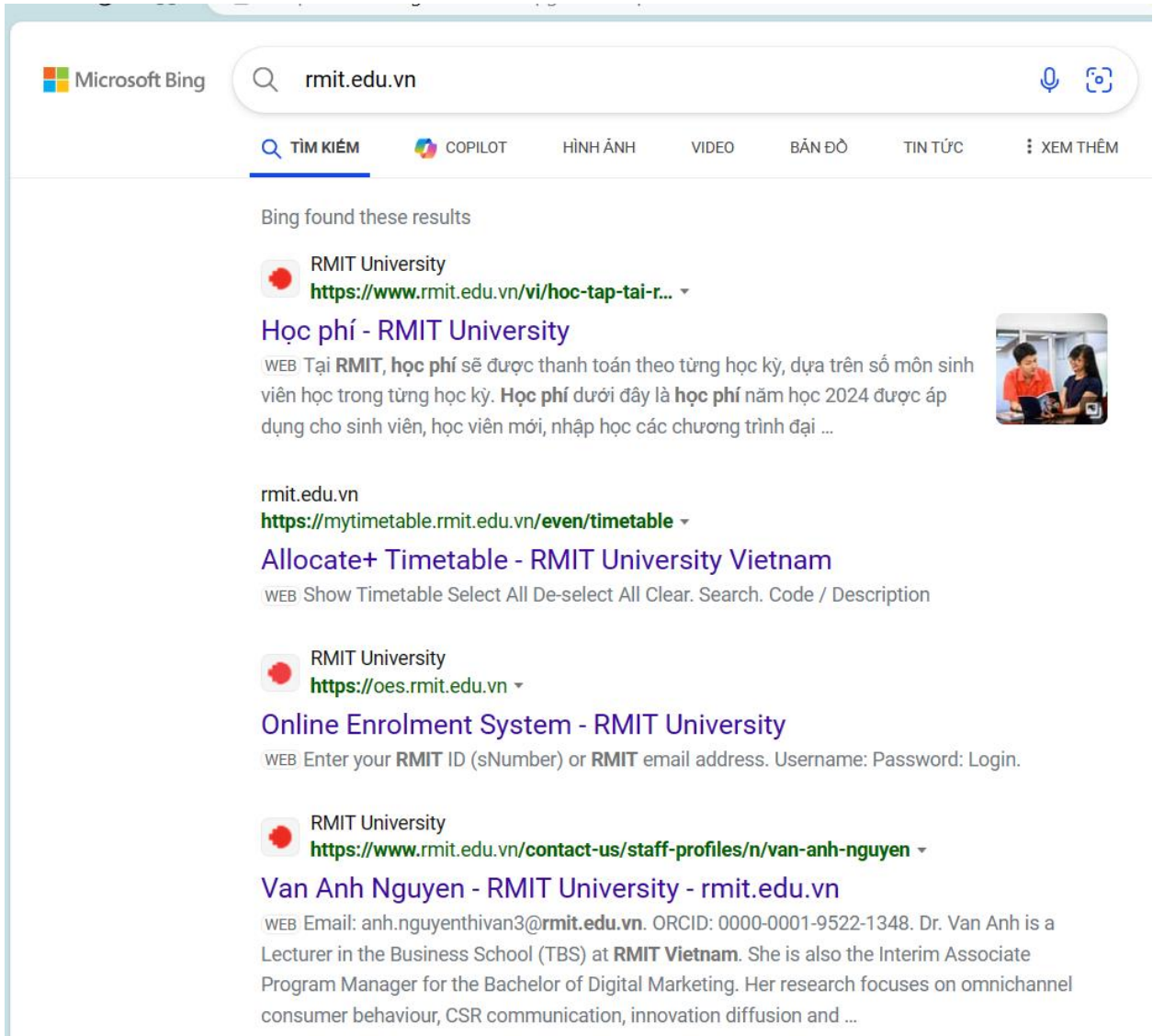
Các nguồn có thể tìm kiếm dữ liệu công khai tên miền phụ: Foca, Sublist3r, Amass, Virustotal, Nmap, Subfinder, Recon-ng.

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 google với từ khóa site:rmit.edu.vn

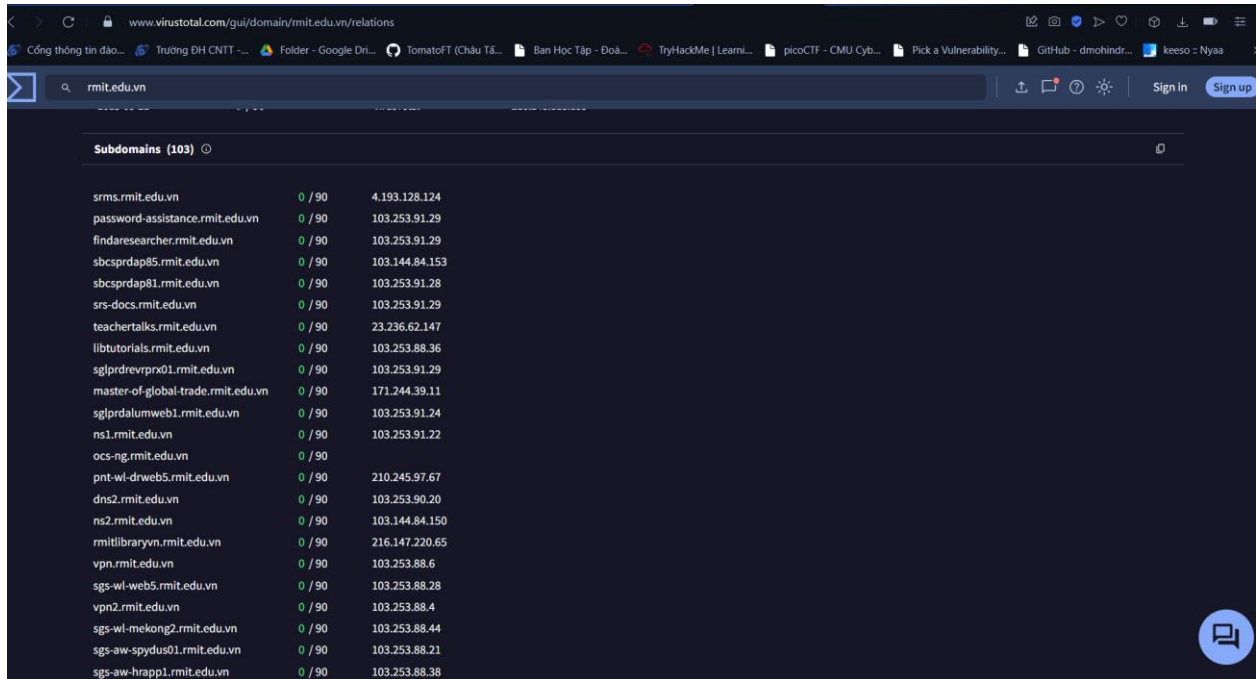


Sử dụng bing



The screenshot shows a Microsoft Bing search interface. The search bar contains 'rmit.edu.vn'. Below the search bar, there are navigation links: TÌM KIẾM, COPILOT, HÌNH ẢNH, VIDEO, BẢN ĐỒ, TIN TỨC, and XEM THÊM. The search results are displayed below, starting with 'Bing found these results'. The first result is 'RMIT University' with the URL 'https://www.rmit.edu.vn/vi/hoc-tap-tai-r...'. Below this is a link 'Học phí - RMIT University' with a description: 'WEB Tại RMIT, học phí sẽ được thanh toán theo từng học kỳ, dựa trên số môn sinh viên học trong từng học kỳ. Học phí dưới đây là học phí năm học 2024 được áp dụng cho sinh viên, học viên mới, nhập học các chương trình đại ...'. To the right of this result is a small image of two students. The second result is 'rmit.edu.vn' with the URL 'https://mytimetable.rmit.edu.vn/even/timetable'. Below this is a link 'Allocate+ Timetable - RMIT University Vietnam' with a description: 'WEB Show Timetable Select All De-select All Clear. Search. Code / Description'. The third result is 'RMIT University' with the URL 'https://oes.rmit.edu.vn'. Below this is a link 'Online Enrolment System - RMIT University' with a description: 'WEB Enter your RMIT ID (sNumber) or RMIT email address. Username: Password: Login.'. The fourth result is 'RMIT University' with the URL 'https://www.rmit.edu.vn/contact-us/staff-profiles/n/van-anh-nguyen'. Below this is a link 'Van Anh Nguyen - RMIT University - rmit.edu.vn' with a description: 'WEB Email: anh.nguyenthivan3@rmit.edu.vn. ORCID: 0000-0001-9522-1348. Dr. Van Anh is a Lecturer in the Business School (TBS) at RMIT Vietnam. She is also the Interim Associate Program Manager for the Bachelor of Digital Marketing. Her research focuses on omnichannel consumer behaviour, CSR communication, innovation diffusion and ...'.

Sử dụng virustotal



Sử dụng subdomainfinder



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.

Ta sử dụng burp suite để can thiệp vào các gói tin gửi đi.

The screenshot displays the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with icons for Intercept, HTTP history, WebSockets history, and Options. The main window is divided into several panes. The left pane shows a list of HTTP requests, with the first request selected. The middle pane shows the details of the selected request, including the raw HTTP data and the response. The right pane shows the response details, including the status code, headers, and body. The response body contains HTML code for the RMIT University homepage.

- Chuột phải vào 1 http request của rmit.edu.vn và chọn send to intruder để tiến hành tìm các tên miền phụ.
- Tại mục Intruder/Positions phần Target, ta đổi thành 1 kí tự bất kì, tô đen kí tự và ấn vào “Add §”, điều này thay thế các kí tự giữa 2 dấu § thành các cụm từ trong list sub domain mà ta có ở câu 1 hoặc ở các list mặc định của burp suite.

The screenshot shows the Burp Suite Intruder/Positions tab. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with icons for Positions, Payloads, Resource Pool, and Options. The main window is divided into several panes. The left pane shows a list of positions, with the first position selected. The middle pane shows the details of the selected position, including the raw HTTP data and the response. The right pane shows the response details, including the status code, headers, and body. The response body contains HTML code for the RMIT University homepage.

- Tiếp theo tại mục Intruder/Payloads phần Payload Option, ta load list các subdomain đã ghi nhận ở câu 1 và “start attack” để bắt đầu.

The screenshot shows the Burp Suite Intruder tab with the 'Payloads' sub-tab selected. The 'Payload Sets' section is active, displaying a list of payload sets. The 'Payload set' is set to '1' and the 'Payload count' is '230'. The 'Payload type' is set to 'Simple list'. Below this, the 'Payload Options [Simple list]' section is visible, showing a list of URLs used as payloads, including 'www.rmit.edu.vn', 'CNC3HN77D8.rmit.edu.vn', 'CNF2HN70NB.rmit.edu.vn', 'CNF2HN70PB.rmit.edu.vn', 'HAN-RADSPRDAP01.rmit.edu.vn', 'HAN-RADSPRDAP02.rmit.edu.vn', 'SGS-RADSPRDAP01.rmit.edu.vn', 'SIP.rmit.edu.vn', 'SgwPrdPrApp01.rmit.edu.vn', and 'WCE.rmit.edu.vn'. The 'Add' button is visible at the bottom of the list.

- Sau 1 khoảng thời gian chạy, ta có được các tên miền có trả về kết quả status code 200(trang web tương ứng tồn tại và có thể truy cập được mà không gặp phải lỗi nào) và các tên miền có trả về kết quả khác như :

- + **301/302 (Redirect):** Trang web được chuyển hướng đến một URL khác.
- + **403 (Forbidden):** Truy cập vào trang web bị cấm.
- + **404 (Not Found):** Trang web không tồn tại.
- + **500 (Internal Server Error):** Lỗi máy chủ nội bộ.

...

10. Intruder attack of https://\$x\$ - Temporary attack - Not saved to project file							
Attack Save Columns							
Results Positions Payloads Resource Pool Options							
Filter: Showing all items							
Request	Payload	Target	Status ^	Error	Timeout	Length	Comment
1	www.rmit.edu.vn	https://www.rmit.edu.vn	200			404440	
12	alumninetwork.rmit.edu.vn	https://alumninetwork.rmit.edu.vn	200			145071	
21	chame.rmit.edu.vn	https://chame.rmit.edu.vn	200			203688	
27	democlass.rmit.edu.vn	https://democlass.rmit.edu.vn	200			35801	
28	design.rmit.edu.vn	https://design.rmit.edu.vn	200			1764	
40	english.rmit.edu.vn	https://english.rmit.edu.vn	200			35801	
41	etal.rmit.edu.vn	https://etal.rmit.edu.vn	200			2117	
43	www.event.rmit.edu.vn	https://www.event.rmit.edu.vn	200			762865	
71	www.infosession.rmit.edu.vn	https://www.infosession.rmit.edu.vn	200			793362	
99	learning.rmit.edu.vn	https://learning.rmit.edu.vn	200			219256	
125	pe.rmit.edu.vn	https://pe.rmit.edu.vn	200			4146	
128	rbpc.rmit.edu.vn	https://rbpc.rmit.edu.vn	200			3530	
134	www.rmitenglishevent.rmit.edu.vn	https://www.rmitenglishevent.rmit.edu.vn	200			834337	
155	sglprdstudlab01.rmit.edu.vn	https://sglprdstudlab01.rmit.edu.vn	200			267	
205	studentlab1.rmit.edu.vn	https://studentlab1.rmit.edu.vn	200			267	
207	www.teachertalks.rmit.edu.vn	https://www.teachertalks.rmit.edu.vn	200			366077	
42	event.rmit.edu.vn	https://event.rmit.edu.vn	301			724	
70	infosession.rmit.edu.vn	https://infosession.rmit.edu.vn	301			650	
133	rmitenglishevent.rmit.edu.vn	https://rmitenglishevent.rmit.edu.vn	301			867	
206	teachertalks.rmit.edu.vn	https://teachertalks.rmit.edu.vn	301			864	
124	payments.rmit.edu.vn	https://payments.rmit.edu.vn	302			732	
132	rivf2020.rmit.edu.vn	https://rivf2020.rmit.edu.vn	302			237	
141	results-stg.seup.rmit.edu.vn	https://results-stg.seup.rmit.edu.vn	302			1842	
102	libtutorials.rmit.edu.vn	https://libtutorials.rmit.edu.vn	400			490	
116	omeka.rmit.edu.vn	https://omeka.rmit.edu.vn	400			490	
216	typographyvn.rmit.edu.vn	https://typographyvn.rmit.edu.vn	400			529	
175	srms.rmit.edu.vn	https://srms.rmit.edu.vn	403			334	
197	srms.staging.rmit.edu.vn	https://srms.staging.rmit.edu.vn	403			334	
20	careers.rmit.edu.vn	https://careers.rmit.edu.vn	404			1021	
112	mytimetable.rmit.edu.vn	https://mytimetable.rmit.edu.vn	410			136	
13	apps.rmit.edu.vn	https://apps.rmit.edu.vn	505			354	
18	blackboard.rmit.edu.vn	https://blackboard.rmit.edu.vn	505			354	
36	emedia.rmit.edu.vn	https://emedia.rmit.edu.vn	505			354	
38	ems-forwarder.rmit.edu.vn	https://ems-forwarder.rmit.edu.vn	505			354	
44	experienceday.rmit.edu.vn	https://experienceday.rmit.edu.vn	505			354	
45	findaresearcher.rmit.edu.vn	https://findaresearcher.rmit.edu.vn	505			354	
57	helpdesk.rmit.edu.vn	https://helpdesk.rmit.edu.vn	505			354	
69	industryhub.rmit.edu.vn	https://industryhub.rmit.edu.vn	505			354	
100	learninglab.rmit.edu.vn	https://learninglab.rmit.edu.vn	505			354	
101	library.rmit.edu.vn	https://library.rmit.edu.vn	505			354	
103	lms.rmit.edu.vn	https://lms.rmit.edu.vn	505			354	
114	oes.rmit.edu.vn	https://oes.rmit.edu.vn	505			354	

Request

Finished

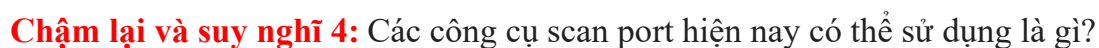
Chậm lại và suy nghĩ 3: Sử dụng cách nào để nhận được địa chỉ IP khi có được tên miền?

Khi có được tên miền muốn nhận địa chỉ IP ta có thể sử dụng lệnh ping, nslookup, sử dụng một số web như whatismyip, iplocation, các công cụ quét tên miền như Nmap, Subfinder, Recon-ng

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.

Ta sẽ thực hiện dò tìm IP của các subdomain mà ta tìm được, thực hiện tạo shell code, ở đây chương trình sẽ lấy mỗi subdomain sau đó thực hiện resolve IP để trả về kết quả IP.

Cấp quyền và thực thi file



1 số công cụ scan port phổ biến :

- 1.Nmap: Nmap là một trong những công cụ quét port mạng phổ biến nhất và mạnh mẽ nhất. Nó cung cấp nhiều tính năng như quét port, phát hiện hệ thống, phân tích bảo mật, vv.
- 2.Masscan: Masscan là một công cụ quét port mạng nhanh chóng và hiệu quả. Nó được thiết kế để quét một lượng lớn các địa chỉ IP trong thời gian ngắn.
- 3.Angry IP Scanner: Đây là một công cụ quét port mạng đơn giản nhưng mạnh mẽ dành cho các hệ điều hành Windows, macOS và Linux. Nó cho phép bạn quét các thiết bị trong mạng LAN của mình.
- 4.ZMap: ZMap cũng là một công cụ quét port mạng nhanh chóng và hiệu quả. Nó được thiết kế để quét toàn bộ không gian địa chỉ IPv4 một cách nhanh chóng.
- 5.Netcat (nc): Netcat không chỉ là một công cụ quét port mạng mà còn là một công cụ đa năng có thể tạo và kết nối với các kết nối TCP và UDP.

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.

- IP của các sub domain rmit.edu.vn sau khi loại bỏ các IP trùng nhau.

```
(cuong@kali)-[~]  
$ cat new_ip_rmit.txt  
  
167.89.123.204  
103.253.91.29  
192.0.78.13  
192.0.78.153  
52.62.164.158  
108.157.38.41  
103.253.88.45  
23.236.62.147  
173.203.204.123  
103.253.88.35  
34.149.87.45  
103.253.88.47  
103.253.91.24  
103.253.88.38  
4.193.128.124  
210.245.97.71  
171.244.39.11  
210.245.97.72  
216.147.220.65  
103.144.84.150  
103.253.88.6  
103.253.88.4  
103.253.88.36  
103.253.91.28  
103.253.91.23  
108.157.38.126  
20.225.187.144  
103.144.84.153  
103.253.88.40  
103.253.91.22
```

- Ta sử dụng tùy chọn `-iL` trong Nmap là một tùy chọn dùng để chỉ định một tệp chứa danh sách các mục tiêu (IP hoặc tên miền) muốn quét.

```
(cuong@kali)-[~]  
$ nmap -p 80,23,443,21,22,25,3389,110,445,139,143,53,135,3306,8080,1723,111,995,993,5900,1025,587,8888,199,1720,465,5  
5631,631,49153,8081,2049,88,79,5800,106,2121,1110,49155,6000,513,990,5357,427,49156,543,544,5101,144,7,389,8009,3128,44  
1,82,10010,1030,9090,2107,1024,2103,6004,1801,5050,19,8031,1041,255,1049,1048,2967,1053,3703,1056,1065,1064,1054,17,808  
4000,1993,1761,5003,2002,2005,1998,1032,1050,6112,3690,1521,2161,6002,1080,2401,4045,902,7937,787,1058,2383,32771,1033,  
,6543,1352,24,3269,1111,407,500,20,2006,3260,15000,1218,1034,4444,264,2004,33,1042,42510,999,3052,1023,1068,222,7100,88  
010,42,9535,2602,3333,161,5100,5002,2604,4002,6059,1047,8192,8193,2702,6789,9595,1051,9594,9593,16993,16992,5226,5225,3  
828,1311,1060,4443,730,731,709,1067,13782,5902,366,9050,1002,85,5500,5431,1864,1863,8085,51103,49999,45100,10243,49,349  
,648,146,1666,901,83,9207,8001,8083,5004,3476,8084,5214,14238,12345,912,30,2605,2030,6,541,8007,3005,4,1248,2500,880,30  
69,3071,5269,5222,1085,1046,5987,5989,5988,2190,11967,8600,3766,7627,8087,30000,9010,7741,14000,3367,1099,1098,3031,271  
1,5718,8086,3998,2607,11110,4126,5911,5910,9618,2381,1096,3300,3351,1073,8333,3784,5633,15660,6123,3211,1078,3659,3551,  
,60020,5962,5961,5960,5959,5925,5877,5825,5810,58080,57294,50800,50006,50003,49160,49159,49158,48080,40193,34573,34572,  
,1783,16018,16016,15003,14442,13456,10629,10628,10626,10621,10617,10616,10566,10025,10024,10012,1169,5030,5414,1057,678  
,20000,8400,1272,6389,7777,1072,1079,1082,8402,89,691,1001,32776,1999,212,2020,6003,7002,2998,50002,3372,898,5510,32,20  
3371,3370,3369,7402,5054,3918,3077,7443,3493,3828,1186,2179,1183,19315,19283,3995,5963,1124,8500,1089,10004,2251,1087,5  
1532,5922,5915,5904,5822,56738,55055,51493,50636,50389,49175,49165,49163,3546,32784,27355,27353,27352,24444,19780,18988  
,1112,49400,84,38292,2040,32780,3006,2111,1084,1600,2048,2638,6699,9111,16080,6547,6007,1533,5560,2106,1443,667,720,203  
6566,9081,5678,3800,4550,5080,1201,3168,3814,1862,1114,6510,3905,8383,3914,3971,3809,5033,7676,3517,4900,3869,9418,2909  
,4445,9917,9575,9099,9003,8290,8099,8093,8045,7921,7920,7496,6839,6792,6779,6692,6565,60443,5952,5950,5907,5906,5862,58  
1,32785,32783,30951,27356,26214,25735,19350,18101,18040,17877,16113,15004,14441,12265,12174,10215,10180,4567,6100,4004,  
301,524,668,2041,6009,1417,1434,259,44443,1984,2068,7004,1007,4343,416,2038,6006,109,4125,1461,9103,911,726,1010,2046,2  
6060,6051,1145,3916,9443,9444,1875,7272,4252,4200,7024,1556,13724,1141,1233,8765,1137,3963,5938,9191,3808,8686,3981,271  
,8019,10160,4658,7878,3304,3307,1259,1092 -iL new_ip_rmit.txt > rmit_result.txt  
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
```



- Kết quả sau khi quét.

```
(cuong@kali)-[~]
$ cat rmit_result.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 08:03 EDT
Nmap scan report for 103.253.91.29
Host is up (0.016s latency).
Not shown: 992 filtered tcp ports (no-response), 4 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.0.78.13
Host is up (1.7s latency).
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.0.78.153
Host is up (0.031s latency).
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for server-108-157-38-41.sgn50.r.cloudfront.net (108.157.38.41)
Host is up (0.0085s latency).
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 103.253.88.45
Host is up (0.016s latency).
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 103.253.88.35
Host is up (0.015s latency).
Not shown: 993 filtered tcp ports (no-response), 3 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 45.87.149.34.bc.googleusercontent.com (34.149.87.45)
```



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.

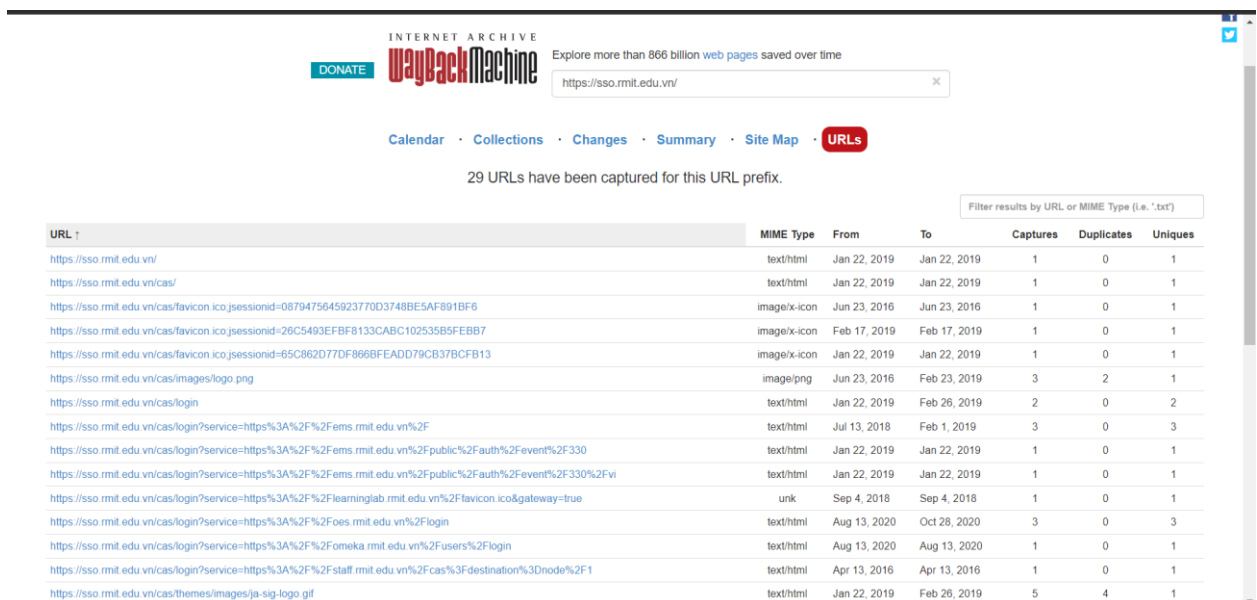
Dùng subdomainfinder để tìm các subdomain sau đó check xem các subdomain đó còn hoạt động không.

Ta kiểm tra thử 2 subdomain là sso.rmit.edu.vn và staff.rmit.edu.vn.



Subdomain	Last seen
admgprdap01.rmit.edu.vn	29-05-2024 01:59:59
alumninetwork.rmit.edu.vn	23-10-2024 01:59:59
api-staging.virtualcase.rmit.edu.vn	02-04-2025 01:59:59
apps.rmit.edu.vn	03-01-2025 00:59:59
apps.itsdev.rmit.edu.vn	19-07-2023 01:59:59
apps.staging.rmit.edu.vn	18-07-2024 01:59:59
appsdr.rmit.edu.vn	07-04-2022 01:39:00
ave.rmit.edu.vn	29-06-2021 10:09:00
ave-prov-test.gapps.rmit.edu.vn	19-07-2021 02:52:00
ave.prov-test.gapps.rmit.edu.vn	19-07-2021 04:29:00
bis-exam.rmit.edu.vn	04-07-2020 05:45:00
blackboard.rmit.edu.vn	22-02-2023 05:25:13
burpsuite.its.rmit.edu.vn	12-07-2024 01:59:59
careerhub.rmit.edu.vn	03-11-2022 00:25:00

Để kiểm dữ liệu trong quá khứ thì ta sẽ dùng trang web wayback machine.
Ta kiểm tra thử 2 subdomain là sso.rmit.edu.vn và staff.rmit.edu.vn.



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=26C5493EFB8133CABC102535B5FEBB7	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%2Ffomeka.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
https://sso.rmit.edu.vn/cas/themes/images/ja-sig-logo.gif	text/html	Jan 22, 2019	Feb 26, 2019	5	4	1

web.archive.org/web/"https://staff.rmit.edu.vn/"

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
https://staff.rmit.edu.vn/	text/html	Jun 21, 2020	Aug 30, 2022	10	9	1
https://staff.rmit.edu.vn/favicon.ico	image/vnd.microsoft.icon	Apr 29, 2016	Jan 8, 2022	5	4	1
https://staff.rmit.edu.vn/misc/drupal.js	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/drupal.js?pbdyeq	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/jquery.js	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/jquery.js?v=1.4.4	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/jquery.once.js	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/jquery.once.js?v=1.2	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.css?pbdyeq	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.min.js?v=1.8.7	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.css?pbdyeq	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.min.js?v=1.8.7	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.draggable.min.js?v=1.8.7	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.mouse.min.js?v=1.8.7	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.position.min.js?v=1.8.7	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.resizable.css?pbdyeq	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.resizable.min.js?v=1.8.7	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.theme.css?pbdyeq	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.widget.min.js?v=1.8.7	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1
https://staff.rmit.edu.vn/modules/book/book.css?pbdyeq	warc/visit	Jan 22, 2019	Jan 22, 2019	1	0	1

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

Ở đây ta sẽ thực hiện việc vào google dork và tìm kiếm thì ta có cách tìm bên dưới:
site:alumninetwork.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls

site:alumninetwork.rmit.edu.vn

https://www.google.com/search?q=site%3Aalumninetwork.rmit.edu.vn+filetype%3Apdf+OR+filetype%3Adoc+OR+filetype%3Axls&rlz=1C1CHBD_v...&btnG=Google

Google

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

Tất cả Mua sắm Hình ảnh Video Sách Thêm Công cụ Tìm kiếm an toàn

Khoảng 4 kết quả (0,10 giây)

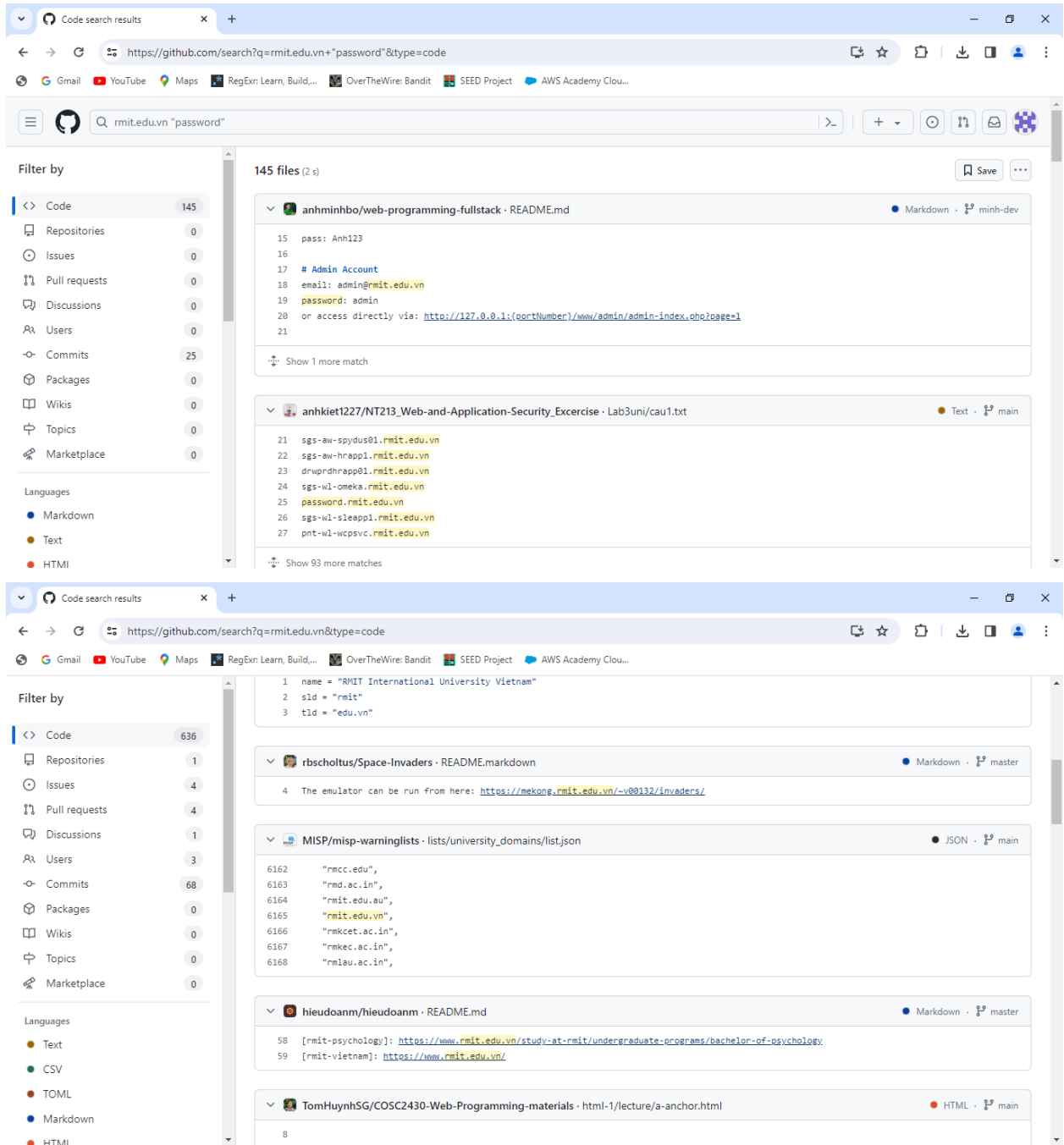
rmit.edu.vn
https://alumninetwork.rmit.edu.vn/ RMIT_PAR... PDF
Welcome to our Partnership Program
Becoming our partner provides you a range of new possibilities to grow the brand love. Let's build together the best-in-class experience and discount.

rmit.edu.vn
https://alumninetwork.rmit.edu.vn/ 2022/06/ B... PDF
RMIT Vietnam Alumni Connecting the dots
In conducting holistic research to understand people's desires and interests, we have segmented the alumni cohort into three groups - the junior group (...

rmit.edu.vn
https://alumninetwork.rmit.edu.vn/ 2022/01/ A... PDF
RMIT Alumni 2021 - Beyond the Borders
It is such a helpful platform that enables us (alumni) to navigate our daily lives with as much normality as possible where social distancing requires.

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).

Thông tin tìm kiếm được bằng phương pháp thủ công



Bài tập thực hành :

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

Sử dụng bing

 <http://courses.uit.edu.vn/course/view.php?id=8>

courses.uit.edu.vn

WEB Nếu bạn muốn học cách phát triển ứng dụng trên mobile, bạn có thể đăng ký khóa học này tại courses.uit.edu.vn. Bạn sẽ được hướng dẫn bởi các giảng viên chuyên môn, thực ...

KHÁM PHÁ THÊM


 UIT English Practice Online

i-english.uit.edu.vn

 Cổng thông tin đào tạo | Trường Đại Học Công Nghệ ...


student.uit.edu.vn

Đề xuất cho bạn dựa trên những gì phổ biến • Phản hồi

 Trường Đại học Công nghệ Thông tin - UIT
<https://www.uit.edu.vn/thong-tin-thong-bao> ▾


[Thông tin - thông báo | Trường Đại học Công nghệ Thông tin](#)

WEB Sinh viên kiểm tra tình trạng tốt nghiệp tại <https://student.uit.edu.vn/> (đăng nhập và kiểm tra... 03-04-2024 Thông báo đăng ký xét cấp các loại học bổng Học kỳ 2 – Năm học 2023 ...

 Cổng thông tin đào tạo
<https://student.uit.edu.vn/sinhvien> ▾

[Sinh Viên | Cổng thông tin đào tạo](#)


WEB Cập nhật kết quả xét miễn anh văn - Thông báo về việc xét miễn các môn anh văn 1, 2 và 3 đợt 1 trong học kỳ 2 năm học 2023-2024 cho sinh viên chính quy chương trình đào tạo ...

 Thông tin tuyển sinh Đại học - UIT
<https://tuyensinh.uit.edu.vn/2023-phuo...> ▾

[\[2023\] Phương thức tuyển sinh 2023 - UIT](#)

WEB 31 thg 1, 2023 · Phương thức 1: Tuyển thẳng và ưu tiên xét tuyển. 1.Phương thức Xét tuyển thẳng theo quy định của Quy chế tuyển sinh (Điều 8) - Mã phương thức xét tuyển: 301 (Tuyển thẳng, ưu tiên xét tuyển theo ...



 Thông tin tuyển sinh Đại học - UIT
<https://tuyensinh.uit.edu.vn/tuyen-sinh-uit> ▾

[Tuyển sinh IIT | Thông tin tuyển sinh Đại học](#)

Sử dụng google với từ khóa site:uit.edu.vn

site:uit.edu.vn

Tp.Hồ Chí Minh. Điện thoại: (028) 372 52002 Fax: (028) 372 52148 Email: info@uit.edu.vn Website...

www.uit.edu.vn > tin-uit >

Tin UIT | Trường Đại học Công nghệ Thông tin

Tiếp nối thành công của UIT JOB FAIR liên tục suốt nhiều năm qua, Trường Đại học Công nghệ Thông tin tiếp tục tổ chức Ngày hội Sinh viên và Doanh nghiệp - UIT JOB FAIR 2024. Thông tin về...

coures.uit.edu.vn >

Trường Đại học Công nghệ Thông tin - UIT

Trường Đại học Công nghệ Thông tin, Đại học Quốc gia Thành phố Hồ Chí Minh (ĐHQG-HCM) là trường đại học công lập đào tạo về công nghệ thông tin và truyền thông (CNTT&TT) được thành lậ...

tuyensinh.uit.edu.vn > 2023-phuong-thuc-tuyen-sinh-nam-2023 >

[2023] Phương thức tuyển sinh 2023 - Trường Đại học Công ...

31 thg 1, 2023 - - Điểm ưu tiên: điểm UIT Code Contest Lưu ý: Điểm UIT Code Contest là điểm quy đổi theo quy định của Trường dành cho thí sinh có tham gia cuộc thi UIT Code Contest do Trường...

student.uit.edu.vn > danh-muc-mon-hoc-dai-hoc >

Danh mục môn học | Cổng thông tin đào tạo

PHÒNG ĐÀO TẠO ĐẠI HỌC Phòng A120, Trường Đại học Công nghệ Thông tin. Khu phố 6, P.Linh Trung, Tp.Thủ Đức, Tp.Hồ Chí Minh.

student.uit.edu.vn > sinhvien >

Sinh Viên | Cổng thông tin đào tạo

Cập nhật kết quả xét miễn anh văn - Thông báo về việc xét miễn các môn anh văn 1, 2 và 3 đợt 2 trong học kỳ 1 năm học 2023-2024 cho sinh viên chính quy chương trình đào tạo đại trà và chương...

Sử dụng subdomainfinder

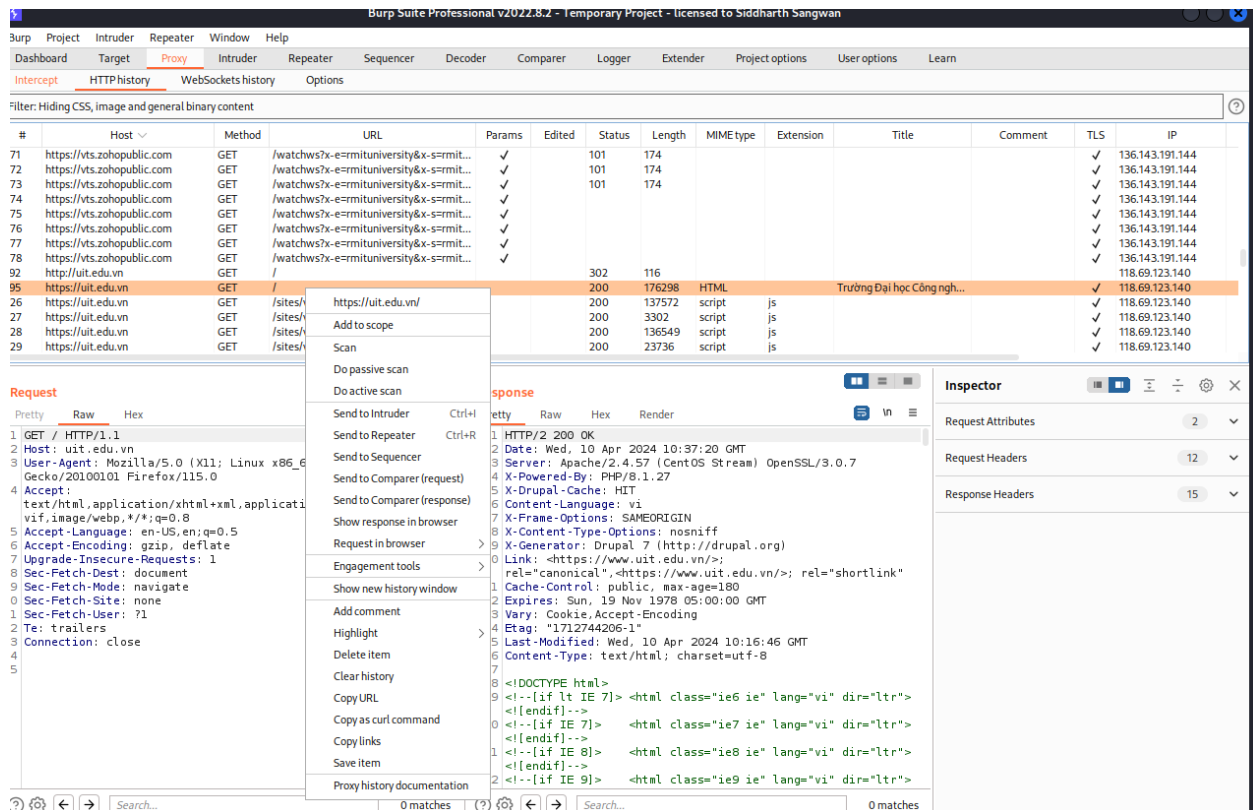
Subdomain	Last seen
519bb137df6144dcbda18e87d53ad8a-0-s-80.vlab.uit.edu.vn	15-11-2021 13:42:38
a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn	20-08-2022 06:05:31
annotation.mmlab.uit.edu.vn	05-07-2024 05:54:40
api.mmlab.uit.edu.vn	12-05-2024 21:47:37
app.tech4covid.uit.edu.vn	21-09-2021 04:31:07
app1.iot.uit.edu.vn	21-10-2020 09:19:36
app2.iot.uit.edu.vn	21-10-2020 09:11:38
cbsv1.uit.edu.vn	12-06-2024 02:27:23
competitions.uit.edu.vn	07-02-2022 08:13:09
console-cloud.vlab.uit.edu.vn	10-06-2024 17:22:55
console-cloud.vlab2.uit.edu.vn	08-10-2022 15:42:43
cs.uit.edu.vn	25-10-2019 23:30:20
dsc.uit.edu.vn	15-06-2024 11:57:56
eth2.uit.edu.vn	07-04-2022 10:35:15

Sử dụng virustotal

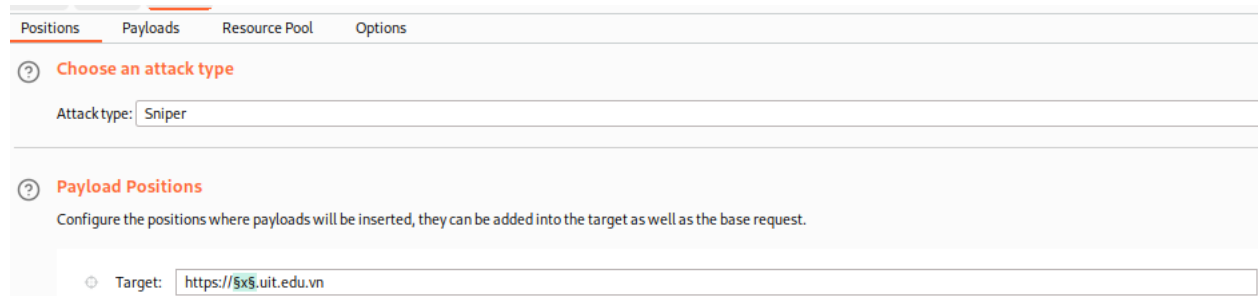
Subdomains (140) ⓘ					
cd.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78		
smtp.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78		
live.uit.edu.vn	0 / 90	42.116.11.16			
uhongdl.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78		
gaingon.uit.edu.vn	0 / 90	45.122.249.78	118.69.123.140		
traibao.uit.edu.vn	0 / 90	45.122.249.78	118.69.123.140		
daa1.uit.edu.vn	0 / 90	45.122.249.78	118.69.123.140		
dkhpapi.uit.edu.vn	0 / 90	45.122.249.75	118.69.123.137		
dsc.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78		
elearning.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78		
aiclubcs.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78		
rmit.uit.edu.vn	0 / 90	118.69.123.140			
state.uit.edu.vn	0 / 90	118.69.123.140			
cfl.uit.edu.vn	0 / 90	118.69.123.142	45.122.249.78		
dev.uit.edu.vn	0 / 90	118.69.123.142	45.122.249.78		
bandl.uit.edu.vn	0 / 90	118.69.123.142	45.122.249.78		
huongnghiep.uit.edu.vn	0 / 90	45.122.249.78	118.69.123.142		
cc62e73f33af4d5vlab2.uit.edu.vn	0 / 90	118.69.123.142	45.122.249.78		
vlab2.uit.edu.vn	0 / 90	45.122.249.78	118.69.123.142		
ucpc.uit.edu.vn	0 / 90	45.122.249.78	118.69.123.142		
post.uit.edu.vn	0 / 90	45.122.249.78	118.69.123.142		
fce.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.77	45.122.249.78	...
ttpcdbcl.uit.edu.vn	0 / 90	118.69.123.142	45.122.249.78		
link.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.77	45.122.249.78	...

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.

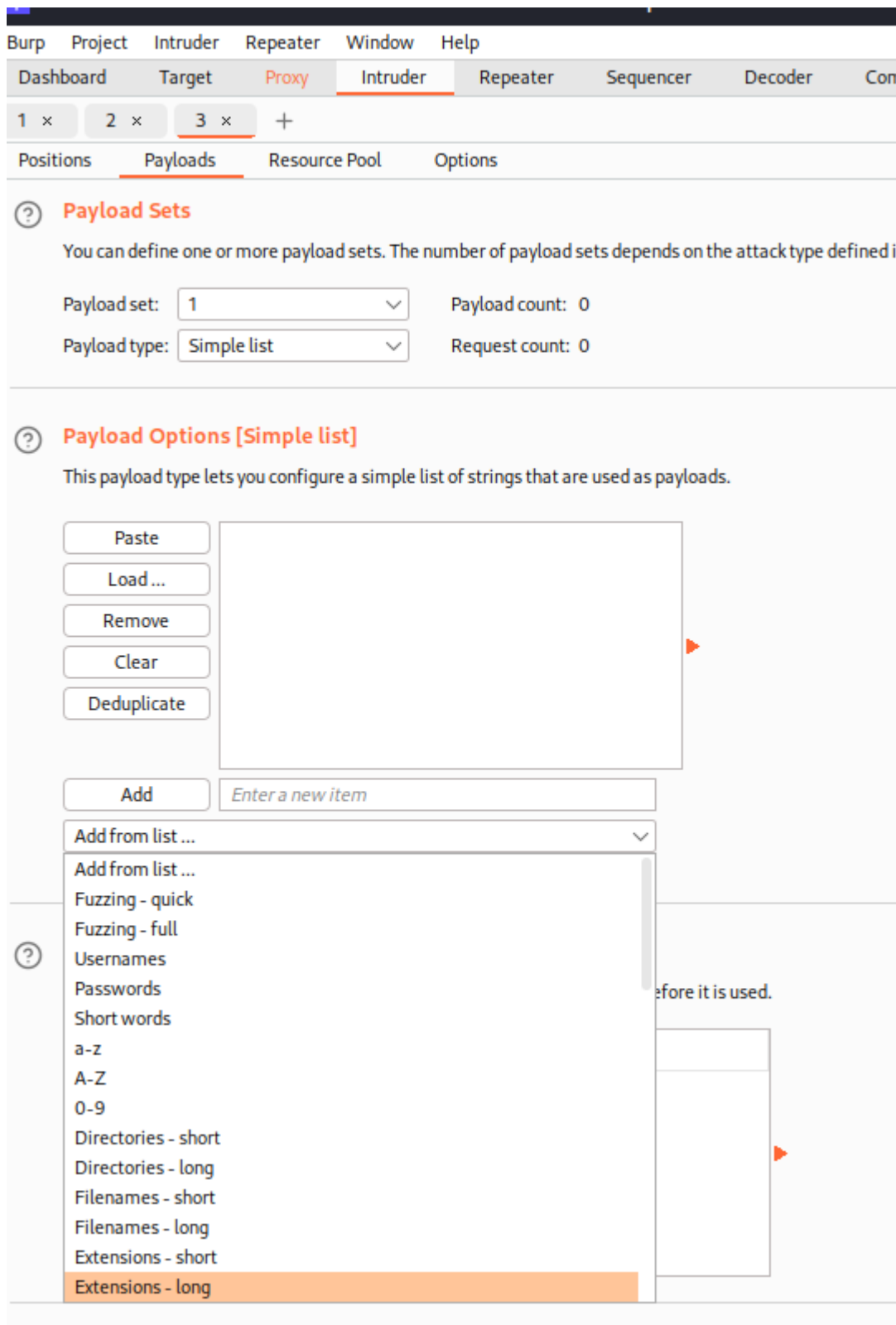
Tương tự với tên miền rmit.edu.vn, ta làm tương tự với uit.edu.vn.



- Brute force các sub domain của uit.edu.vn.



- Thêm list mặc định của burp suite để tiến hành brute force. Như hình dưới là list extensions-long.



- Kết quả sau khi brute force ta có 2 sub domain với status code 200 là drl.uit.edu.vn và conf.uit.edu.vn.

14. Intruder attack of https://\$x\$.uit.edu.vn - Temporary attack - Not saved to project file							
Attack Save Columns							
Results Positions Payloads Resource Pool Options							
Filter: Showing all items							
Request	Payload	Target	Status ^	Error	Timeout	Length	Comment
09	drl	https://drl.uit.edu.vn	200	<input type="checkbox"/>	<input type="checkbox"/>	17469	
051	conf	https://conf.uit.edu.vn	200	<input type="checkbox"/>	<input type="checkbox"/>	12509	
		https://x.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
	0	https://0.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
	000	https://000.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
	123	https://123.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
	1pe	https://1pe.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
	1ph	https://1ph.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
0	3dr	https://3dr.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
1	3dt	https://3dt.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
2	3me	https://3me.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
3	3pe	https://3pe.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
4	4dl	https://4dl.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
5	4dv	https://4dv.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
6	7z	https://7z.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
7	8xk	https://8xk.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
8	a00	https://a00.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
9	a01	https://a01.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
0	a02	https://a02.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
1	a3l	https://a3l.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
2	a3m	https://a3m.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
3	a3w	https://a3w.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
4	a4l	https://a4l.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
5	a4m	https://a4m.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
6	a4w	https://a4w.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
7	a5l	https://a5l.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
8	a5w	https://a5w.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
9	a65	https://a65.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
0	aa0	https://aa0.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
1	ab	https://ab.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
2	ab1	https://ab1.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
3	ab2	https://ab2.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
4	ab3	https://ab3.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
5	abcd	https://abcd.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
6	abi	https://abi.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
7	abp	https://abp.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
8	aby	https://aby.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
9	aca	https://aca.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
0	acc	https://acc.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
1	accdb	https://accdb.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
2	ace	https://ace.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
3	acf	https://acf.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	

- Với list username, ta có sub domain student.uit.edu.vn trả về status code 200.

15. Intruder attack of https://\$x\$.uit.edu.vn - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Target	Status ^	Error	Timeout	Length	Comment
214	STUDENT	https://student.uit.edu.vn	200	<input type="checkbox"/>	<input type="checkbox"/>	47196	
0		https://x.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
4	1	https://1.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
5	1.1	https://1.1.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
6	11111111	https://11111111.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
7	2	https://2.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
8	22222222	https://22222222.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
9	30	https://30.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
10	4dgifts	https://4dgifts.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
11	5	https://5.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
12	7	https://7.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
13	ADAMS	https://adams.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
14	ADMIN	https://admin.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
15	ADMN	https://adm.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
16	ADVMAIL	https://advmail.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
17	ALLIN1	https://allin1.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
18	ALLIN1MAIL	https://allin1mail.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
19	ALLINONE	https://allinone.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
20	AP2SVP	https://ap2svp.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
21	APL2PP	https://apl2pp.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
22	APPLSYS	https://applsys.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
23	APPS	https://apps.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
24	AQDEMO	https://aqdemo.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
25	AQUSER	https://aquser.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
26	ARCHIVIST	https://archivist.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
27	AUTOLOG1	https://autolog1.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
28	Administrator	https://administrator.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
29	Anonymous	https://anonymous.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
30	Any	https://any.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
31	BACKUP	https://backup.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
32	BATCH	https://batch.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
33	BATCH1	https://batch1.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
34	BATCH2	https://batch2.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
35	BLAKE	https://blake.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
36	CATALOG	https://catalog.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
37	CCC	https://ccc.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
38	CDEMO82	https://cdemo82.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
39	CDEMOCOR	https://cdemocr.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
40	CDEMORID	https://cdemorid.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
41	CDEMOUCB	https://cdemouc.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
42	CHEY_ARCHSVR	https://chey_archsvr.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	
43	CLARK	https://clark.uit.edu.vn	302	<input type="checkbox"/>	<input type="checkbox"/>	98	

8893 of 8894

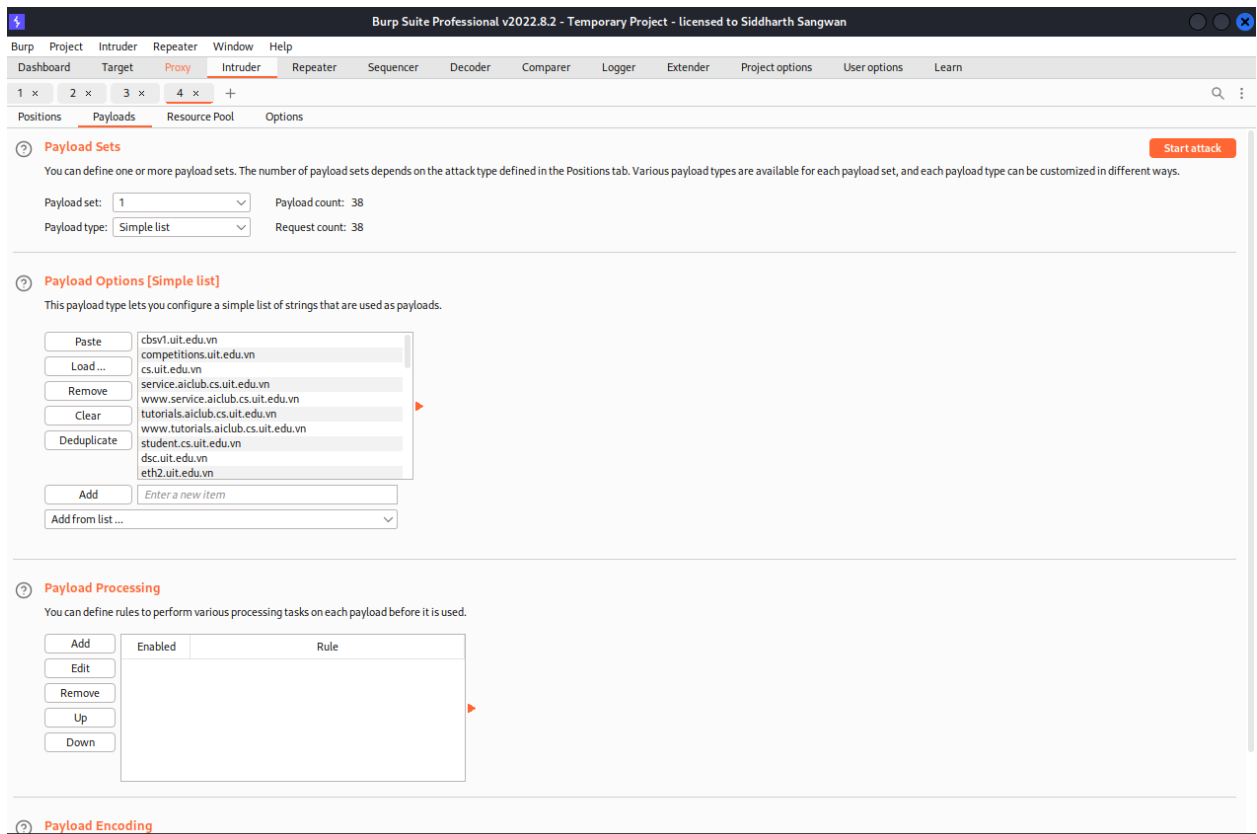
Sau khi có các sub domain của uit.edu.vn từ câu 1 cũng như các sub domain ta vừa tìm được thông qua burp suite, ta tiến hành quét các sub domain này để kiểm tra kết quả trả về status code là gì.

Target:

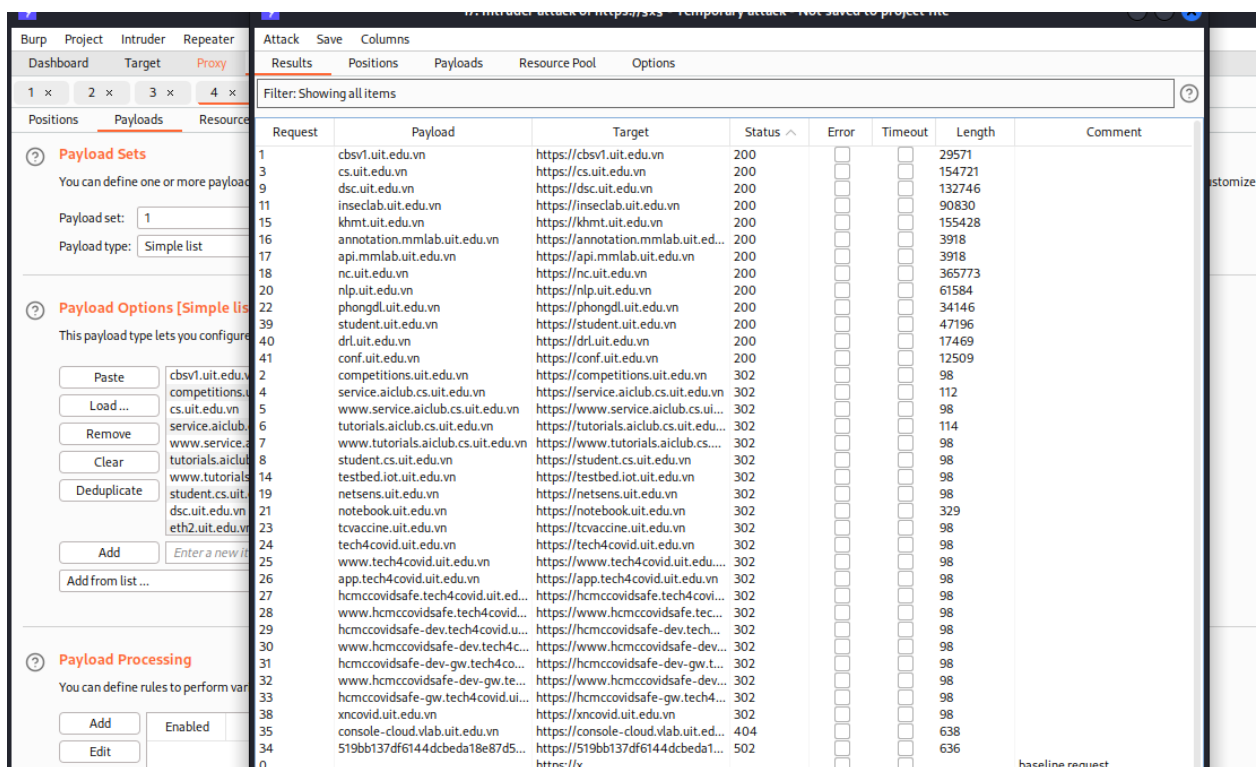
- Load list các sub domain của uit.edu.vn đã tìm được ở câu 1 để tiến hành tấn công.

Session 01: Tổng quan các lỗ hổng bảo mật web thường gặp

Nhóm 07 23



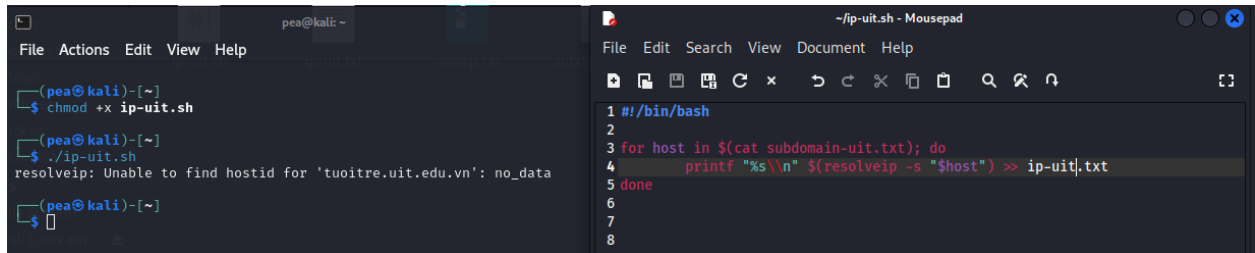
- Kết quả sau khi tấn công ta có các sub domain trả về status 200.



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

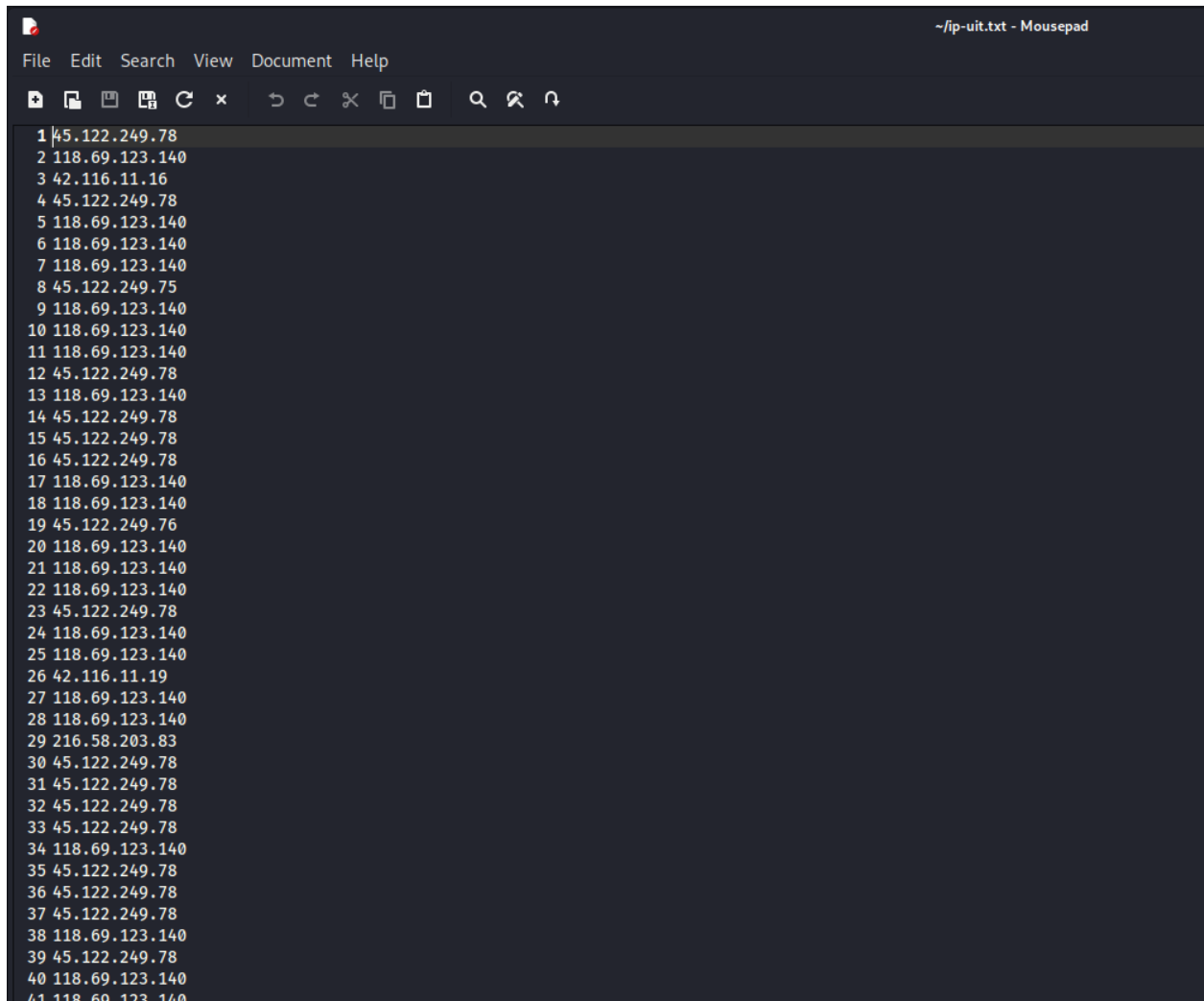
Ta sẽ thực hiện dò tìm IP của các subdomain mà ta tìm được, thực hiện tạo shell code, ở đây chương trình sẽ lấy mỗi subdomain sau đó thực hiện resolve IP để trả về kết quả IP.

Cấp quyền và thực thi file



```
pea@kali: ~  
$ chmod +x ip-uit.sh  
pea@kali: ~  
$ ./ip-uit.sh  
resolveip: Unable to find hostid for 'tuoitre.uit.edu.vn': no_data  
pea@kali: ~  
$  
~ip-uit.sh - Mousepad  
1 #!/bin/bash  
2  
3 for host in $(cat subdomain-uit.txt); do  
4     printf "%s\\n" $(resolveip -s "$host") >> ip-uit.txt  
5 done  
6  
7  
8
```

Sau khi chạy xong ta có kết quả là dãy IP bên dưới



```
~ip-uit.txt - Mousepad  
1 45.122.249.78  
2 118.69.123.140  
3 42.116.11.16  
4 45.122.249.78  
5 118.69.123.140  
6 118.69.123.140  
7 118.69.123.140  
8 45.122.249.75  
9 118.69.123.140  
10 118.69.123.140  
11 118.69.123.140  
12 45.122.249.78  
13 118.69.123.140  
14 45.122.249.78  
15 45.122.249.78  
16 45.122.249.78  
17 118.69.123.140  
18 118.69.123.140  
19 45.122.249.76  
20 118.69.123.140  
21 118.69.123.140  
22 118.69.123.140  
23 45.122.249.78  
24 118.69.123.140  
25 118.69.123.140  
26 42.116.11.19  
27 118.69.123.140  
28 118.69.123.140  
29 216.58.203.83  
30 45.122.249.78  
31 45.122.249.78  
32 45.122.249.78  
33 45.122.249.78  
34 118.69.123.140  
35 45.122.249.78  
36 45.122.249.78  
37 45.122.249.78  
38 118.69.123.140  
39 45.122.249.78  
40 118.69.123.140  
41 118.69.123.140
```

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

- IP của các sub domain uit.edu.vn sau khi loại bỏ các IP trùng nhau.

```
(cuong@kali)-[~]  
$ cat new_ip UIT.txt  
  
42.116.11.19  
45.122.249.78  
45.122.249.74  
216.58.203.83  
118.69.123.140  
45.122.249.75  
45.122.249.76  
42.116.11.16
```

- Ta sử dụng tùy chọn `-iL` trong Nmap là một tùy chọn dùng để chỉ định một tệp chứa danh sách các mục tiêu (IP hoặc tên miền) muốn quét.

```
(cuong@kali)-[~]  
$ nmap -p 80,23,443,21,22,25,3389,110,445,139,143,53,135,3306,8080,1723,111,995,993,5900,1025,587,8888,199,1720,465,5  
5631,631,49153,8081,2049,88,79,5800,106,2121,1110,49155,6000,513,990,5357,427,49156,543,544,5101,144,7,389,8009,3128,44  
1,82,10010,1030,9090,2107,1024,2103,6004,1801,5050,19,8031,1041,255,1049,1048,2967,1053,3703,1056,1065,1064,1054,17,808  
4000,1993,1761,5003,2002,2005,1998,1032,1050,6112,3690,1521,2161,6002,1080,2401,4045,902,7937,787,1058,2383,32771,1033,  
,6543,1352,24,3269,1111,407,500,20,2006,3260,15000,1218,1034,4444,264,2004,33,1042,42510,999,3052,1023,1068,222,7100,88  
010,42,9535,2602,3333,161,5100,5002,2604,4002,6059,1047,8192,8193,2702,6789,9595,1051,9594,9593,16993,16992,5226,5225,3  
828,1311,1060,4443,730,731,709,1067,13782,5902,366,9050,1002,85,5500,5431,1864,1863,8085,51103,49999,45100,10243,49,349  
,648,146,1666,901,83,9207,8001,8083,5004,3476,8084,5214,14238,12345,912,30,2605,2030,6,541,8007,3005,4,1248,2500,880,30  
69,3071,5269,5222,1085,1046,5987,5989,5988,2190,11967,8600,3766,7627,8087,30000,9010,7741,14000,3367,1099,1098,3031,271  
1,5718,8086,3998,2607,11110,4126,5911,5910,9618,2381,1096,3300,3351,1073,8333,3784,5633,15660,6123,3211,1078,3659,3551,  
,60020,5962,5961,5960,5959,5925,5877,5825,5810,58080,57294,50800,50006,50003,49160,49159,49158,48080,40193,34573,34572,  
,1783,16018,16016,15003,14442,13456,10629,10628,10626,10621,10617,10616,10566,10025,10024,10012,1169,5030,5414,1057,678  
,20000,8400,1272,6389,7777,1072,1079,1082,8402,89,691,1001,32776,1999,212,2020,6003,7002,2998,50002,3372,898,5510,32,20  
3371,3370,3369,7402,5054,3918,3077,7443,3493,3828,1186,2179,1183,19315,19283,3995,5963,1124,8500,1089,10004,2251,1087,5  
1532,5922,5915,5904,5822,56738,55055,51493,50636,50389,49175,49165,49163,3546,32784,27355,27353,27352,24444,19780,18988  
,1112,49400,84,38292,2040,32780,3006,2111,1084,1600,2048,2638,6699,9111,16080,6547,6007,1533,5560,2106,1443,667,720,203  
6566,9081,5678,3800,4550,5080,1201,3168,3814,1862,1114,6510,3905,8383,3914,3971,3809,5033,7676,3517,4900,3869,9418,2909  
,4445,9917,9575,9099,9003,8290,8099,8093,8045,7921,7920,7496,6839,6792,6779,6692,6565,60443,5952,5950,5907,5906,5862,58  
1,32785,32783,30951,27356,26214,25735,19350,18101,18040,17877,16113,15004,14441,12265,12174,10215,10180,4567,6100,4004,  
301,524,668,2041,6009,1417,1434,259,44443,1984,2068,7004,1007,4343,416,2038,6006,109,4125,1461,9103,911,726,1010,2046,2  
6060,6051,1145,3916,9443,9444,1875,7272,4252,4200,7024,1556,13724,1141,1233,8765,1137,3963,5938,9191,3808,8686,3981,271  
,8019,10160,4658,7878,3304,3307,1259,1092 -iL new_ip UIT.txt > uit_result.txt  
WARNING: Duplicate port number(s) specified. Are you alert enough to be using Nmap? Have some coffee or Jolt(tm).
```

- Kết quả các cổng đang mở của từng địa chỉ IP sau khi quét.

```
(cuong@kali)-[~]
$ cat uit_result.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 07:40 EDT
Nmap scan report for static.cmcti.vn (45.122.249.78)
Host is up (0.0085s latency).
Not shown: 990 filtered tcp ports (no-response), 7 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for static.cmcti.vn (45.122.249.74)
Host is up (0.0087s latency).
Not shown: 994 filtered tcp ports (no-response), 3 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for kul09s03-in-f19.1e100.net (216.58.203.83)
Host is up (0.054s latency).
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 118.69.123.140
Host is up (0.010s latency).
Not shown: 990 filtered tcp ports (no-response), 5 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
541/tcp   open  uucp-rlogin

Nmap scan report for static.cmcti.vn (45.122.249.75)
Host is up (0.0088s latency).
Not shown: 993 filtered tcp ports (no-response), 4 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for 42.116.11.16
Host is up (0.0092s latency).
Not shown: 993 filtered tcp ports (no-response), 2 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
80/tcp    open  http
541/tcp   open  uucp-rlogin
8080/tcp  open  http-proxy

Nmap done: 8 IP addresses (6 hosts up) scanned in 633.42 seconds
```

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 *.uit.edu.vn.

Dùng subdomainfinder để tìm các subdomain sau đó check xem các subdomain đó còn hoạt động không.

Subdomain	Last seen
519bb137df6144dcbeda18e87d53ad8a-0-s-80.vlab.uit.edu.vn	15-11-2021 13:42:38
a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn	20-08-2022 06:05:31
annotation.mmlab.uit.edu.vn	05-07-2024 05:54:40
api.mmlab.uit.edu.vn	12-05-2024 21:47:37
app.tech4covid.uit.edu.vn	21-09-2021 04:31:07
app1.iot.uit.edu.vn	21-10-2020 09:19:36
app2.iot.uit.edu.vn	21-10-2020 09:11:38
cbsv1.uit.edu.vn	12-06-2024 02:27:23
competitions.uit.edu.vn	07-02-2022 08:13:09
console-cloud.vlab.uit.edu.vn	10-06-2024 17:22:55
console-cloud.vlab2.uit.edu.vn	08-10-2022 15:42:43
cs.uit.edu.vn	25-10-2019 23:30:20
dsc.uit.edu.vn	15-06-2024 11:57:56
eth2.uit.edu.vn	07-04-2022 10:35:15

Để kiểm dữ liệu trong quá khứ thì ta sẽ dùng trang web wayback machine.

Ta sẽ kiểm tra thử với subdomain testbed.iot.uit.edu.vn

INTERNET ARCHIVE
DONATE WayBackMachine Explore more than 866 billion web pages saved over time

https://testbed.iot.uit.edu.vn/

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

3 URLs have been captured for this URL prefix.

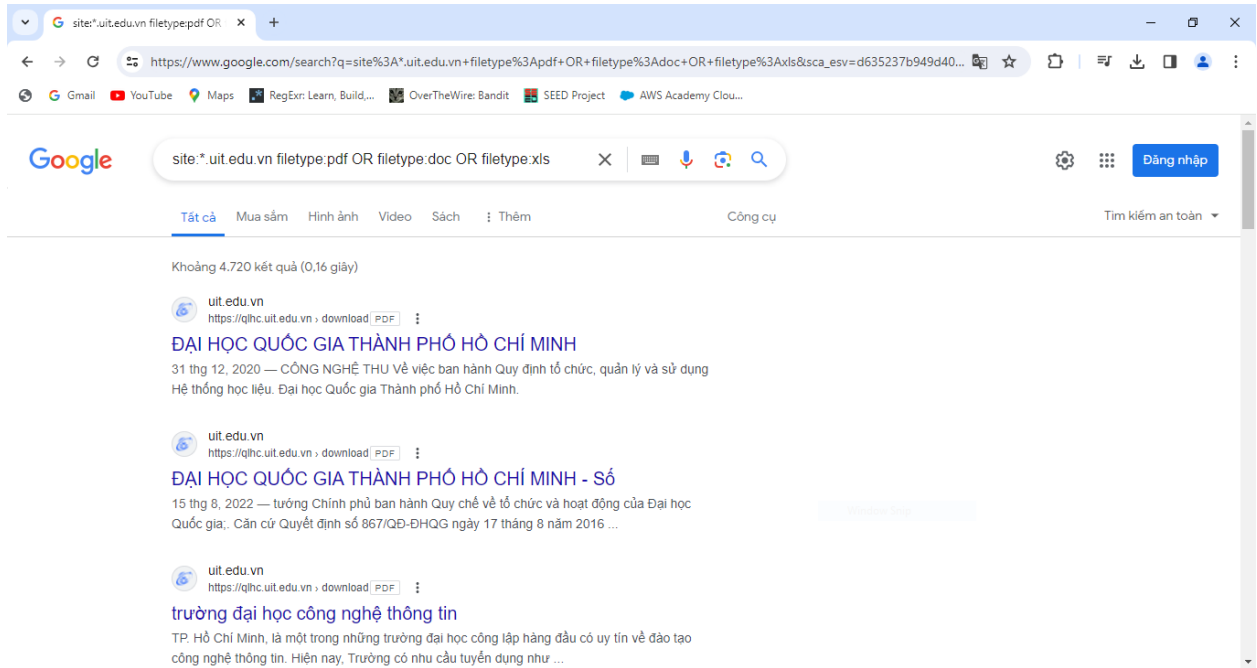
Filter results by URL or MIME Type (i.e. ".txt")

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://testbed.iot.uit.edu.vn/80/login	text/html	Aug 11, 2019	Sep 10, 2019	2	1	1
http://testbed.iot.uit.edu.vn/80/ver1	text/html	Apr 16, 2018	Apr 16, 2018	2	0	2
http://testbed.iot.uit.edu.vn/80/ver1/login.php	text/html	Apr 14, 2018	Apr 21, 2019	14	13	1

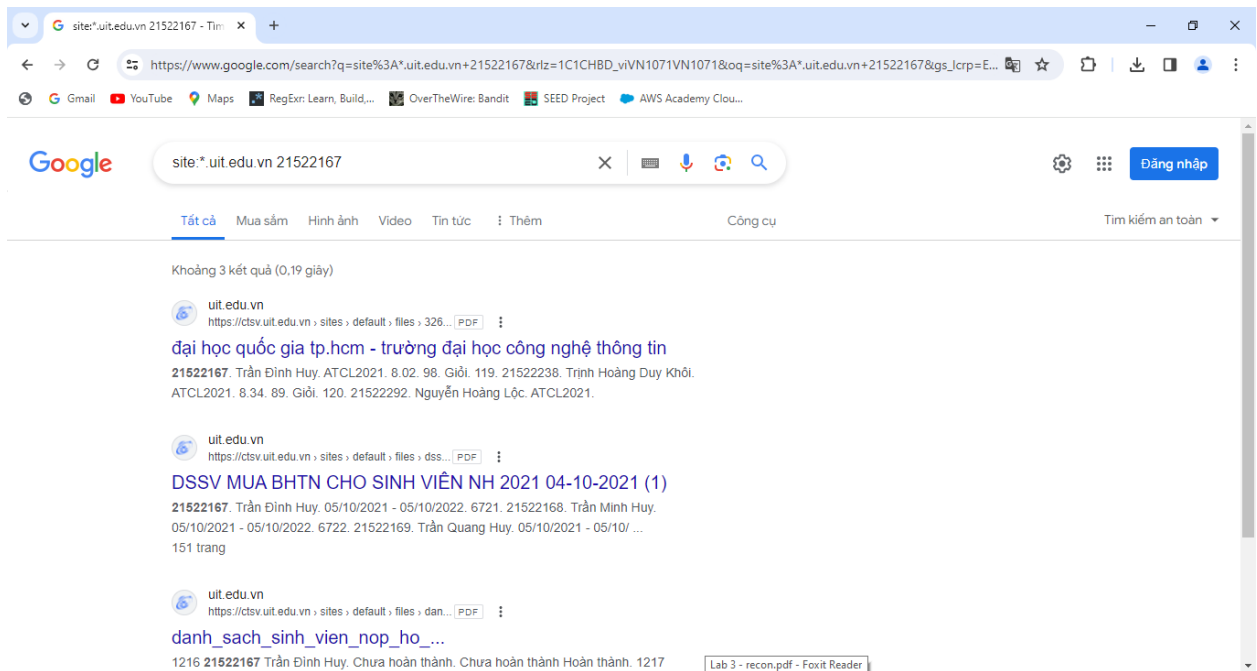
Showing 1 to 3 of 3 entries

First Previous **1** Next Last

Bài tập 6: Tìm kiếm các dữ liệu nhạy cảm của *.uit.edu.vn thông qua google dork và github



- Truy cập vào các trang trên, ta thu được tên, MSSV, ... Từ đó, có thể tiến hành khai thác sâu hơn vào thông tin cá nhân



Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).
Ví dụ: [NT101.K11.ATCL]-Session1_Group3.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

HẾT