



BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Kỳ báo cáo: Buổi 03

GVHD: Ngô Khánh Khoa

1. THÔNG TIN CHUNG:

STT	Họ và tên	MSSV	Email
1	Phạm Nguyễn Hải Anh	21520586	21520586@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 01	10%
2	Bài tập 02	10%
3	Bài tập 03	90%
4	Bài tập 04	90%
5	Bài tập 05	90%
6	Bài tập 06	90%
7	Bài tập 07	80%
8	Bài tập thực hành 01	90%
9	Bài tập thực hành 02	90%
10	Bài tập thực hành 03	90%
11	Bài tập thực hành 04	90%

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

Link các file kết quả: https://github.com/PNg-HA/BMW_Lab3

1. Bài tập 01

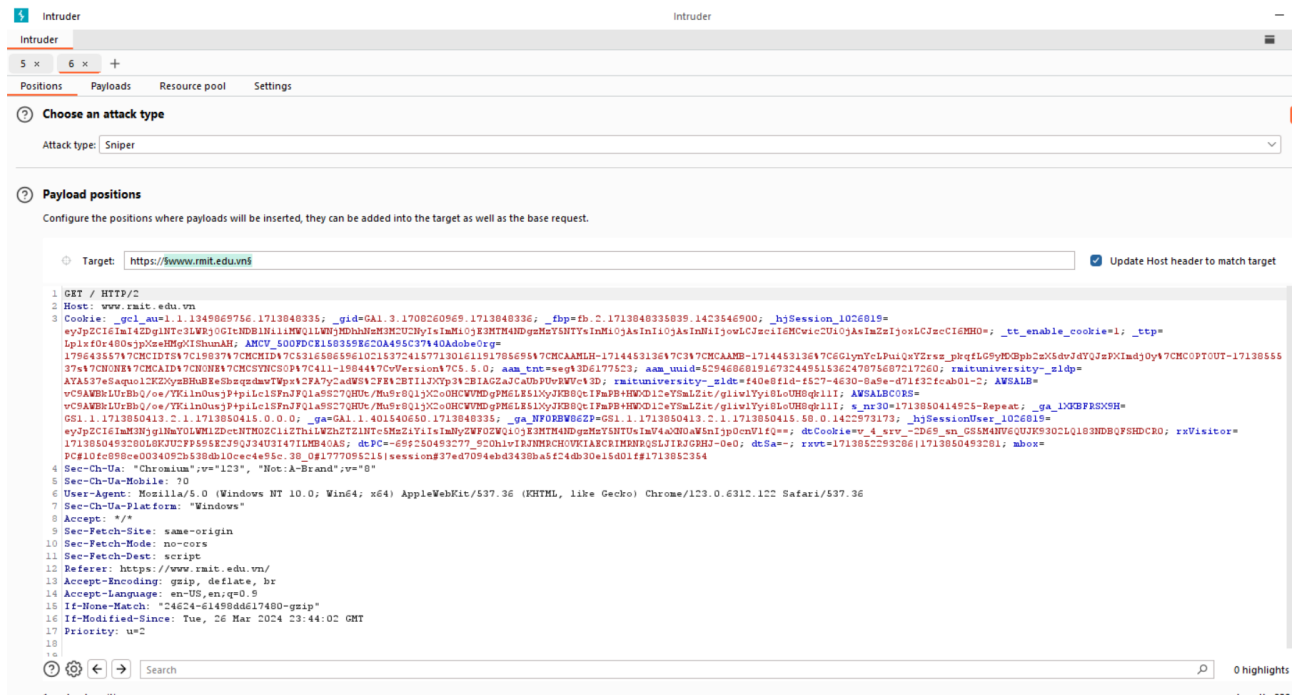
Sử dụng virustotal, mục subdomain, ta có thể xem các subdomain của tên miền:

 https://www.virustotal.com/gui/domain/rmit.edu.vn/relation			
rmit.edu.vn			
Subdomains (110) ⓘ			
ems-forwarder.rmit.edu.vn	0 / 90	103.253.91.29	
industryhub.rmit.edu.vn	0 / 90	103.253.91.29	
learning.rmit.edu.vn	0 / 90	103.77.162.8	
lms.rmit.edu.vn	0 / 90	103.253.91.29	103.253.88.22
payments.rmit.edu.vn	0 / 90	104.18.21.88	
rbpc.rmit.edu.vn	0 / 90	199.36.158.100	
rivercitiesarchive.rmit.edu.vn	0 / 90	103.253.91.29	
srms.rmit.edu.vn	0 / 90	4.193.128.124	
password-assistance.rmit.edu.vn	0 / 90	103.253.91.29	
findaresearcher.rmit.edu.vn	0 / 90	103.253.91.29	

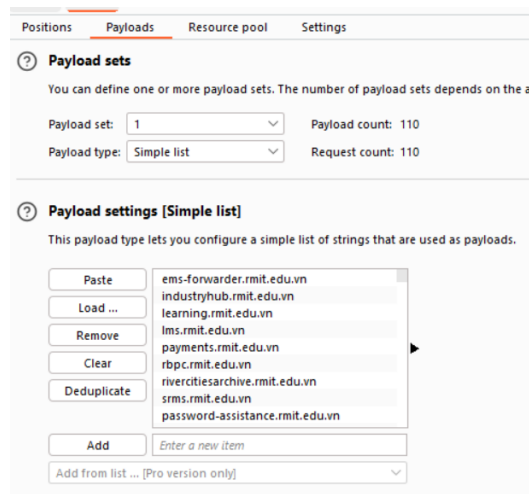
Kết quả được lưu thành bt1.csv

2. Bài tập 02

Thêm tên miền target 2 dấu \$ để thay thành các giá trị trong từ điển để liệt kê, tương tự như bruteforce:



Thêm danh sách ở bài 1 vào từ điển:



Thực hiện tấn công. Bấm cột “Status” để hiển thị những response 200 lên đầu:

- Hàm `resolve_domain()`: dùng hàm `gethostbyname()` của thư viện `socket` của Python để phân giải tên miền thành ip. Dòng 31 gọi hàm `resolve_domain` để phân giải tên miền thành ip, tạo thành 1 mảng `domain-ip` (biến `results`). Từng phần tử của biến này sẽ được viết thành từng hàng trong file `bt3.csv`, thực thi bởi hàm `write_results()`.

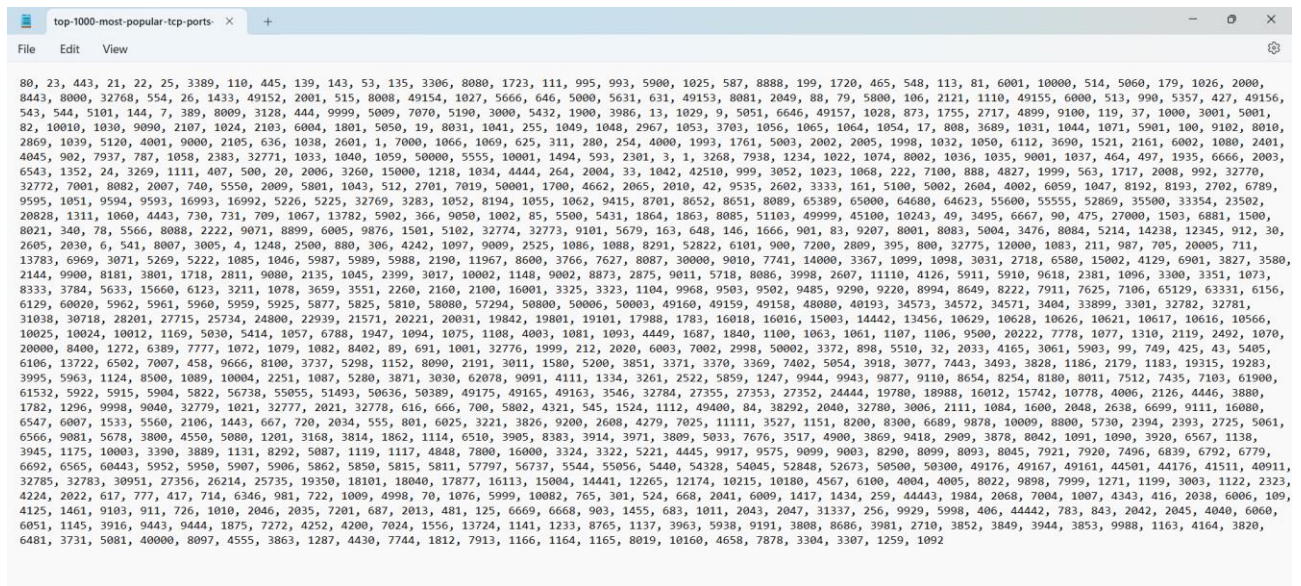
Thực thi chương trình:

```
(kali@kali)-[/mnt/hgfs]
$ python bt3.py
DNS resolution completed. Results saved to bt3.csv

(kali@kali)-[/mnt/hgfs]
$ cat bt3.csv
Domain,IP Address
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
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,Resolution Failed
teachertalks.rmit.edu.vn,23.236.62.147
libtutorials.rmit.edu.vn,103.253.88.36
sglprdrevrprx01.rmit.edu.vn,103.253.91.29
master-of-global-trade.rmit.edu.vn,171.244.39.11
sglprdalumweb1.rmit.edu.vn,103.253.91.24
ns1.rmit.edu.vn,103.253.91.22
ocs-ng.rmit.edu.vn,Resolution Failed
pnt-wl-drweb5.rmit.edu.vn,Resolution Failed
dns2.rmit.edu.vn,Resolution Failed
ns2.rmit.edu.vn,103.144.84.150
rmitlibraryvn.rmit.edu.vn,216.147.220.65
vpn.rmit.edu.vn,103.253.88.6
sgs-wl-web5.rmit.edu.vn,Resolution Failed
```

4. Bài tập 04

Sửa lại file `port csv` được cấp để thêm khoảng trắng sau dấu phẩy:



Việc chỉnh này sẽ phù hợp với option -pf của lệnh naabu. Ngoài ra, file csv ở bài tập 3 có 2 cột, em trích xuất cột ip và lưu nó dưới tên “bt3_for_bt4.csv” để dùng cho lệnh naabu. Để tiện thì em đã tạo 1 script:

```
1 #!/bin/bash
2
3 for host in $(cat bt3_for_bt4.txt); do
4     naabu -host $host -pf top-1000-most-popular-tcp-ports-nmap-sorted.csv | grep : >> bt4.csv
5 done
6
```

giải thích:

- Chạy 1 vòng lặp với mỗi giá trị ip (mỗi hàng) trong bt3, thực hiện quét tất cả port được liệt kê trong file được cung cấp, những output có dấu 2 chấm sẽ được lọc bởi grep (vì nó là ip:port) và lưu vào bt4.csv

Chạy script:

5. Bài tập 05

Biết được domain `staff.rmit.edu.vn` không còn hoạt động, ta dựa vào những thông số của nó trong kết quả của bt2 => lựa ra những domain không trả về status (và có thể cũng không có error (những response 505 HTTP Version Not Supported vẫn còn hoạt động, vì hoạt động thì mới báo phiên bản HTTP không phù hợp):

Request	Payload	Target	Status code	Response received	Error ^	Timeout	Length	Comment
53	dialin.rmit.edu.vn	https://dialin.rmit.edu.vn		0				
86	dns1.rmit.edu.vn	https://dns1.rmit.edu.vn		0				
22	dns2.rmit.edu.vn	https://dns2.rmit.edu.vn		0				
54	election.rmit.edu.vn	https://election.rmit.edu.vn		0				
55	ems.rmit.edu.vn	https://ems.rmit.edu.vn		0				
82	ielts.rmit.edu.vn	https://ielts.rmit.edu.vn		0				
57	itop.rmit.edu.vn	https://itop.rmit.edu.vn		0				
58	lyncdiscover.rmit.edu.vn	https://lyncdiscover.rmit.edu.vn		0				
59	mekong.rmit.edu.vn	https://mekong.rmit.edu.vn		0				
60	mekong1.rmit.edu.vn	https://mekong1.rmit.edu.vn		0				
20	ocs-ng.rmit.edu.vn	https://ocs-ng.rmit.edu.vn		0				
92	oesdr.rmit.edu.vn	https://oesdr.rmit.edu.vn		0				
44	online-archived.rmit.edu.vn	https://online-archived.rmit.edu.vn		0				
64	orsee.rmit.edu.vn	https://orsee.rmit.edu.vn		0				
33	password.rmit.edu.vn	https://password.rmit.edu.vn		0				
36	pnt-wl-drweb3.rmit.edu.vn	https://pnt-wl-drweb3.rmit.edu.vn		0				
21	pnt-wl-drweb5.rmit.edu.vn	https://pnt-wl-drweb5.rmit.edu.vn		0				
29	sgs-aw-spydus01.rmit.edu.vn	https://sgs-aw-spydus01.rmit.edu.vn		0				
40	sgs-wl-dis.rmit.edu.vn	https://sgs-wl-dis.rmit.edu.vn		0				
28	sgs-wl-mekong2.rmit.edu.vn	https://sgs-wl-mekong2.rmit.edu.vn		0				
66	sgs-wl-web3.rmit.edu.vn	https://sgs-wl-web3.rmit.edu.vn		0				
26	sgs-wl-web5.rmit.edu.vn	https://sgs-wl-web5.rmit.edu.vn		0				
67	sgs-www-livesiv.rmit.edu.vn	https://sgs-www-livesiv.rmit.edu.vn		0				
58	sip.rmit.edu.vn	https://sip.rmit.edu.vn		0				
69	skooprda81.rmit.edu.vn	https://skooprda81.rmit.edu.vn		0				
70	skooprda85.rmit.edu.vn	https://skooprda85.rmit.edu.vn		0				
71	skypeexternal81.rmit.edu.vn	https://skypeexternal81.rmit.edu.vn		0				
72	skypeexternal85.rmit.edu.vn	https://skypeexternal85.rmit.edu.vn		0				
13	srs-docs.rmit.edu.vn	https://srs-docs.rmit.edu.vn		0				
73	sso.rmit.edu.vn	https://sso.rmit.edu.vn		0				
88	ssodr.rmit.edu.vn	https://ssodr.rmit.edu.vn		0				
74	staff.rmit.edu.vn	https://staff.rmit.edu.vn		0				
77	sts.rmit.edu.vn	https://sts.rmit.edu.vn		0				
75	wce.rmit.edu.vn	https://wce.rmit.edu.vn		0				
76	webems.rmit.edu.vn	https://webems.rmit.edu.vn		0				
24	sgs-wl-umeka.rmit.edu.vn	https://sgs-wl-umeka.rmit.edu.vn	400	44			430	
8	srms.rmit.edu.vn	https://srms.rmit.edu.vn	403	41			736	
78	autodiscover.rmit.edu.vn	https://autodiscover.rmit.edu.vn		0				
48	ave.rmit.edu.vn	https://ave.rmit.edu.vn		0				
50	careerhub.rmit.edu.vn	https://careerhub.rmit.edu.vn		0				
52	crm.rmit.edu.vn	https://crm.rmit.edu.vn		0				
53	dialin.rmit.edu.vn	https://dialin.rmit.edu.vn		0				

Dùng web archive để xem những domain này còn hoạt động hay không.

careerhub.rmit.edu.vn:

99 URLs have been captured for this URL prefix.

Filter res

URL ↑	MIME Type	From	To
http://careerhub.rmit.edu.vn/favicon.ico	warc/visit	Jun 24, 2018	Dec 13, 2022
http://careerhub.rmit.edu.vn/80/	text/html	Apr 6, 2017	Dec 5, 2022
http://careerhub.rmit.edu.vn/80/content-console/scripts/?v=ubaKdbThWxRRogakcM-BZ9fPGC-8dLXIY-mJc6laUSs1	text/javascript	Apr 5, 2017	Apr 5, 2017
http://careerhub.rmit.edu.vn/80/employers	text/html	Apr 5, 2017	Aug 10, 2022
http://careerhub.rmit.edu.vn/80/Employers/ForgotLogin.aspx	text/html	Apr 6, 2017	Aug 10, 2022
http://careerhub.rmit.edu.vn/80/Employers/How_to_advertise_on_CareerHub.chpx	text/html	Apr 6, 2017	Jul 7, 2022
http://careerhub.rmit.edu.vn/80/Employers/Interviews_on_Campus.chpx	text/html	Apr 6, 2017	Oct 3, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?	text/html	Apr 5, 2017	Jul 7, 2022
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FInterviews_on_Campus.chpx	text/html	Apr 6, 2017	Apr 6, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FOn_campus_presentations.chpx	text/html	Apr 6, 2017	Apr 6, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FProtected%2FConfirmEmail.aspx%3F	text/html	Apr 15, 2017	Apr 15, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FProtected%2FContact.aspx	text/html	Apr 5, 2017	Apr 6, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FProtected%2FJob.aspx	text/html	Apr 5, 2017	Apr 6, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FProtected%2FJobPublishDetails.aspx%3F	text/html	Apr 5, 2017	Apr 6, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FProtected%2FOrganisation.aspx	text/html	Apr 5, 2017	Apr 6, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2Fprotected%2FPrelistedJobs.aspx	text/html	May 5, 2017	May 5, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2Fprotected%2FPublishJob.aspx%3F	text/html	Apr 5, 2017	Apr 6, 2017
http://careerhub.rmit.edu.vn/80/Employers/Login.aspx?ReturnUrl=%2FEmployers%2FProtected%2FSummary.aspx	text/html	Apr 4, 2017	Apr 6, 2017

election.rmit.edu.vn:

28 URLs have been captured for this URL prefix.

Filter results by URL or MIME Type (i.e.,

URL ↓	MIME Type	From	To	Captures	Duplicates	Unique
http://election.rmit.edu.vn/robots.txt	text/plain	May 16, 2018	May 16, 2018	1	0	1
http://election.rmit.edu.vn/80/	text/html	Mar 9, 2013	Jun 18, 2016	8	7	1
http://election.rmit.edu.vn/80/candidate	text/html	Mar 12, 2013	Mar 12, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/1	text/html	Apr 10, 2016	May 12, 2016	2	1	1
http://election.rmit.edu.vn/80/candidate/17	text/html	Mar 19, 2013	Mar 19, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/2	text/html	Apr 22, 2016	Apr 22, 2016	1	0	1
http://election.rmit.edu.vn/80/candidate/22	text/html	Apr 7, 2013	Apr 7, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/27	text/html	Feb 18, 2016	Mar 21, 2016	3	2	1
http://election.rmit.edu.vn/80/candidate/28	text/html	Feb 18, 2016	Mar 19, 2016	2	1	1
http://election.rmit.edu.vn/80/candidate/29	text/html	Mar 18, 2013	Mar 18, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/3	text/html	Apr 22, 2016	Apr 22, 2016	1	0	1
http://election.rmit.edu.vn/80/candidate/30	text/html	Apr 22, 2016	Apr 22, 2016	1	0	1
http://election.rmit.edu.vn/80/candidate/34	text/html	Mar 18, 2013	Mar 18, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/4	text/html	Apr 11, 2013	Apr 11, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/44	text/html	Apr 7, 2013	Apr 7, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/48	text/html	Mar 21, 2013	Mar 21, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/5	text/html	Mar 18, 2013	May 15, 2016	3	2	1
http://election.rmit.edu.vn/80/candidate/53	text/html	Mar 19, 2013	Mar 19, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/56	text/html	Apr 6, 2013	Apr 6, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/57	text/html	Mar 21, 2013	Mar 21, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/61	text/html	Apr 7, 2013	Apr 7, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/9	text/html	Mar 18, 2013	Mar 18, 2013	1	0	1
http://election.rmit.edu.vn/80/candidate/status	text/html	Mar 12, 2013	Apr 21, 2016	6	4	1

ems.rmit.edu.vn:

SACAP **ՀԱՅԳԵՆՈՒԹՅԱՆ ՀԱՄԱԿԱՐԳԻ ՎԵԲ-ՊՈՐՏԱԼ**

ems.rmit.edu.vn x

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

61 URLs have been captured for this URL prefix.

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniqi
http://ems.rmit.edu.vn/	text/html	Apr 8, 2016	Jan 22, 2019	9	5	4
http://ems.rmit.edu.vn/favicon.ico	text/html	Jun 10, 2016	Mar 24, 2019	5	3	2
http://ems.rmit.edu.vn/public/event/52	text/html	Jul 23, 2014	Jul 23, 2014	1	0	1
http://ems.rmit.edu.vn/public/event/55	text/html	Jul 23, 2014	Jul 23, 2014	1	0	1
http://ems.rmit.edu.vn/robots.txt	text/html	Jul 23, 2014	Oct 21, 2021	99	96	3
http://ems.rmit.edu.vn:80/public/event/27/vi	text/html	Mar 13, 2014	Mar 13, 2014	1	0	1
http://ems.rmit.edu.vn:80/public/event/37/vi	text/html	Mar 13, 2014	Mar 13, 2014	1	0	1
http://ems.rmit.edu.vn:80/public/event/52/vi	text/html	Jun 25, 2014	Jun 25, 2014	1	0	1
http://ems.rmit.edu.vn:80/public/event/55/vi	text/html	Jun 25, 2014	Jun 25, 2014	1	0	1
http://ems.rmit.edu.vn:80/public/event/89/vi	text/html	Jan 4, 2015	Jan 4, 2015	1	0	1
http://ems.rmit.edu.vn:80/public/event/90/vi	text/html	Jan 6, 2015	Jan 6, 2015	1	0	1
https://ems.rmit.edu.vn/bootstrap/css/bootstrap-responsive.min.css	text/css	Oct 26, 2017	Oct 21, 2021	4	3	1
https://ems.rmit.edu.vn/bootstrap/css/bootstrap.min.css	text/css	Jan 22, 2019	Oct 22, 2021	3	2	1
https://ems.rmit.edu.vn/img/glyphicons-hallifrons-white.png	warc/revisit	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bootstrap/img/glyphicons-hallifrons.png	warc/revisit	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bundles/milems/connected/css/modules.css	text/css	Oct 26, 2017	Oct 21, 2021	4	3	1
https://ems.rmit.edu.vn/bundles/milems/connected/css/styles.css	text/css	Jan 22, 2019	Oct 21, 2021	3	2	1
https://ems.rmit.edu.vn/bundles/milems/connected/fonts/vnmuseo300-webfont.eot	application/vnd.ms-fontobject	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bundles/milems/connected/fonts/vnmuseo300-webfont.svg	image/svg+xml	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bundles/milems/connected/fonts/vnmuseo300-webfont.ttf	text/plain	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bundles/milems/connected/fonts/vnmuseo300-webfont.woff	text/plain	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bundles/milems/connected/fonts/vnmuseo500-webfont.eot	application/vnd.ms-fontobject	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bundles/milems/connected/fonts/vnmuseo500-webfont.svg	image/svg+xml	Jan 22, 2019	Mar 24, 2019	2	1	1
https://ems.rmit.edu.vn/bundles/milems/connected/fonts/vnmuseo500-webfont.ttf	text/plain	Jan 22, 2019	Mar 24, 2019	2	1	1

6. Bài tập 6

Tìm file doc:

Tìm file pdf:



site:rmit.edu.vn filetype:pdf



All

Shopping

Images

Videos

News

More

About 573 results (0.20 seconds)



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://typographyvn.rmit.edu.vn > files > original PDF

History of Sign in Hanoi Lịch sử của Bảng hiệu ở Hà Nội

1880 - 1920. -. Most common commerce activity was trading in bazaar. -. Most common type of signs were Flag Banner or Basket. -. Written in Chinese.



rmit.edu.vn

https://learninglab.rmit.edu.vn > default > files > A... PDF

AS1.1: ALGEBRAIC OPERATIONS

Like Terms. Like terms contain exactly the same pronumerals (letters, variables) . Like Terms. Unlike terms. $3x$, $5x$. $3x$, $4y$. $2a$, $-3a$. $3a$, 3 . $3m^2$, m^2 .



rmit.edu.vn

https://learninglab.rmit.edu.vn > default > files > st... PDF

Reflective Writing in Design

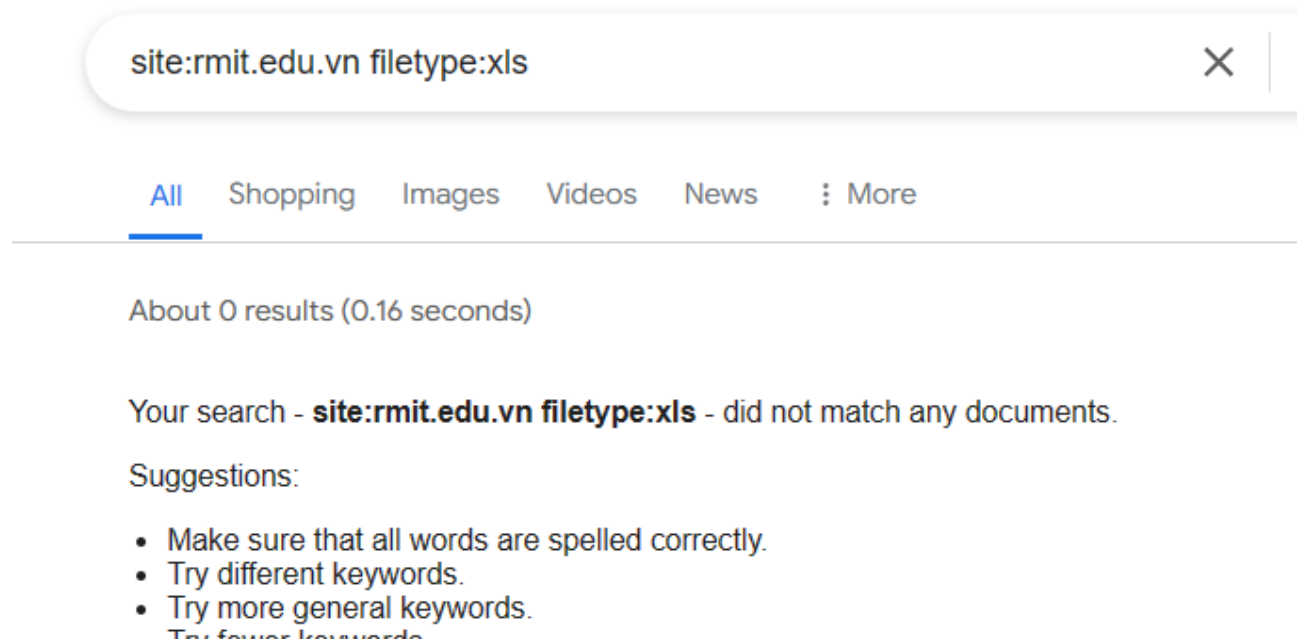
This resource provides a guide for writing a structured reflection in a studio knowledge object (SKO). The studio knowledge object.



rmit.edu.vn

https://learninglab.rmit.edu.vn > default > files > U... PDF

Tìm file xls:



7. Bài tập 7

Sử dụng google dork để search các thông tin liên quan "*.rmit.edu.vn" (dùng ngoặc kép để đảm bảo nội dung bài sẽ có) xuất hiện trên github với inurl:



inurl:github.com "rmit.edu.vn"



[All](#) [Images](#) [Videos](#) [News](#) [Shopping](#) [More](#)

T

About 90 results (0.30 seconds)



GitHub

<https://github.com/rmitvn>

RMIT University Vietnam rmitvn

www.rmit.edu.vn. Block or Report. Block or report rmitvn. Block user. Prevent this user from interacting with your repositories and sending you notifications ...



GitHub

<https://github.com/rmit-ncf>

RMIT Neo Culture Tech

Mar 27, 2024 — neoculturetechclub.sgs@rmit.edu.vn · Overview · Repositories 1 · Projects · Packages · People. More. Overview · Repositories · Projects ...



GitHub

<https://github.com/blob/hoi-dap> · [Translate this page](#)

mangmaytinh/hoi-dap at master

... rmit.edu.vn - Local hỏi máy chủ rmit.edu.vn và nhận được câu trả lời là địa chỉ ip của www.mathdept.rmit.edu.vn - Local trả lời cho client địa chỉ ip của ...



GitHub

<https://github.com/LaansDole>

Do Le Long An LaansDole

Do Le Long An LaansDole · <https://rbpc.rmit.edu.vn/> · <https://laansdole.github.io/LaansDole/> · <https://laansdole.github.io/random-dungeon-game/> · <https://www.credly.com> ...



GitHub

<https://gist.github.com/nhanb>

Scrape RMIT courses

```
start_page = 'https://online.rmit.edu.vn/enrolmentcopy'. full_data = {}. def get(url, cookie):. r = requests.get(url, headers={'Cookie': cookie}). return r ...
```



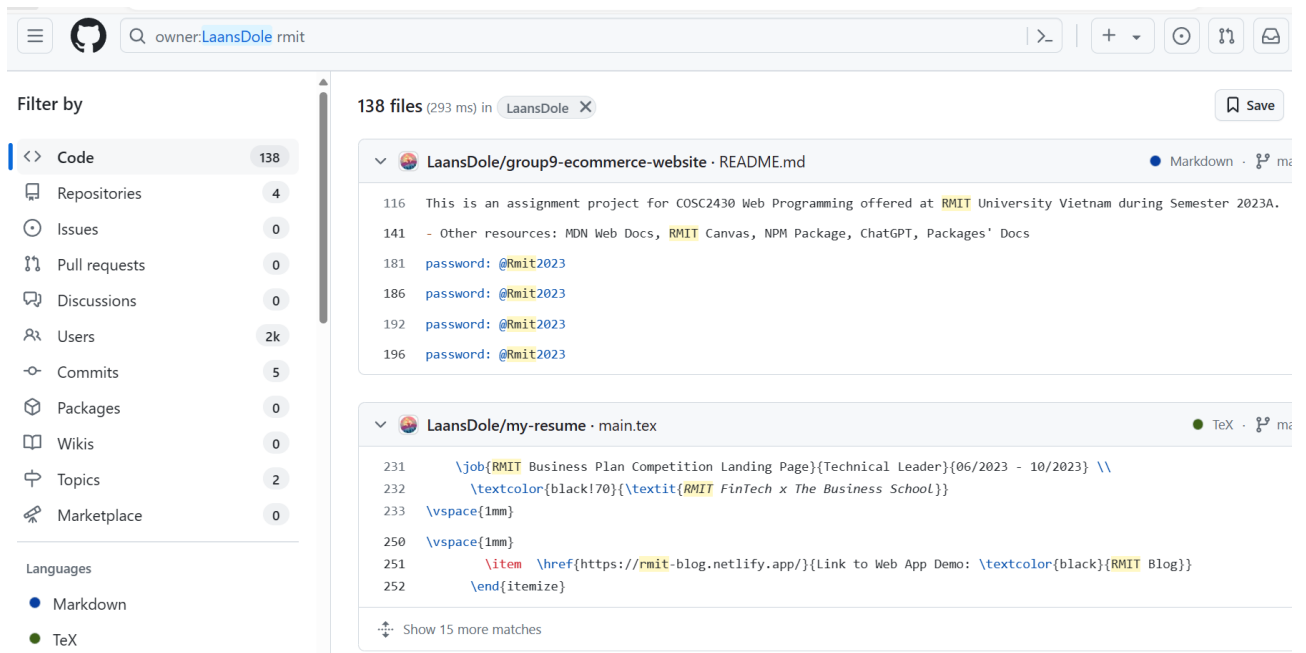
GitHub

<https://github.com/rcl1>

rcl1

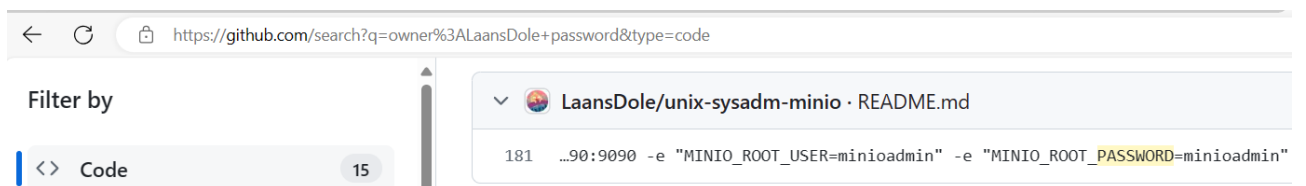
Sent from my VINASAT-1. Probably writing some bash that shouldn't be bash. Hanoi, Vietnam; emailto:s3818993@rmit.edu.vn. Block or Report ...

Vào 1 repository bất kỳ, search từ khóa rmit:

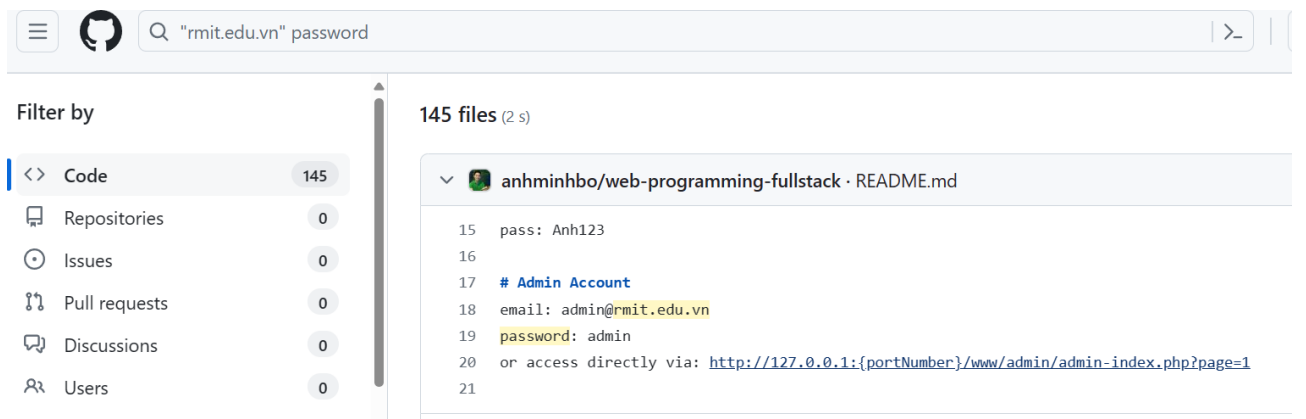


Có thể thấy password của 1 website nào đó.

Search keyword “password”:



Hoặc có thể ghép cả 2 lại:



8. Bài tập thực hành 1 – Tìm subdomain uit

Sử dụng virustotal như bài tập 1:

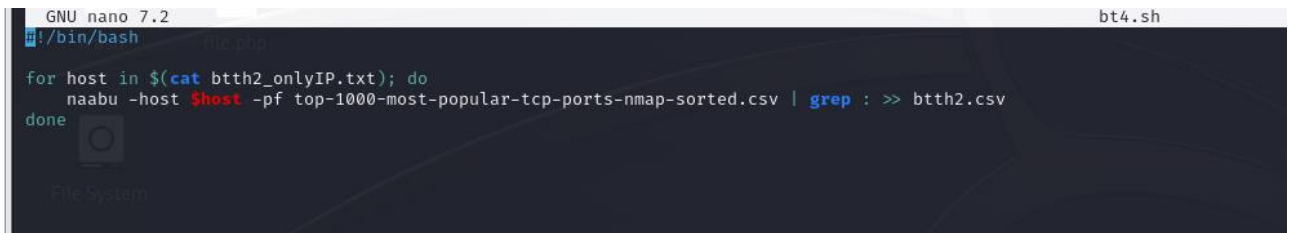
→ ↺ https://www.virustotal.com/gui/domain/uit.edu.vn/relations				
uit.edu.vn				
cd.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78	
smtp.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78	
live.uit.edu.vn	0 / 90	42.116.11.16		
uhongdl.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78	
gaingon.uit.edu.vn	0 / 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
tttdtt.uit.edu.vn	0 / 90	118.69.123.142		
eth2.uit.edu.vn	0 / 90	42.116.11.19		
aiclub.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78	118.69.123.142
sa.uit.edu.vn	0 / 90	118.69.123.140	45.122.249.78	118.69.123.142

Kết quả được lưu vào file btth1.csv.

9. Bài tập thực hành 2 – Tìm port và ip của subdomain uit

Sử dụng file bt3.py với input là btth1.csv, output là btth2_ip.csv. Output file btt2_ip.csv:

Và vì file này có 2 cột, nên cột ip sẽ được trích thành file riêng tên btth2_onlyIP.txt và được xử lý chỉ để còn IP, không có giá trị “Resolution Failed”. Sửa lại tên file input trong code bt4.py để tìm các port mở với ip tương ứng:



```
GNU nano 7.2 bt4.sh
#!/bin/bash

for host in $(cat btth2_onlyIP.txt); do
    naabu -host $host -pf top-1000-most-popular-tcp-ports-nmap-sorted.csv | grep : >> btth2.csv
done
```

Chạy script, được kết quả:



AutoSave



Off



btth2.c

File

Home

Insert

Page Layout

Formulas



Paste



Clipboard

Aptos Narrow

11

A[^]A[^]**B***I*U

Font



G17

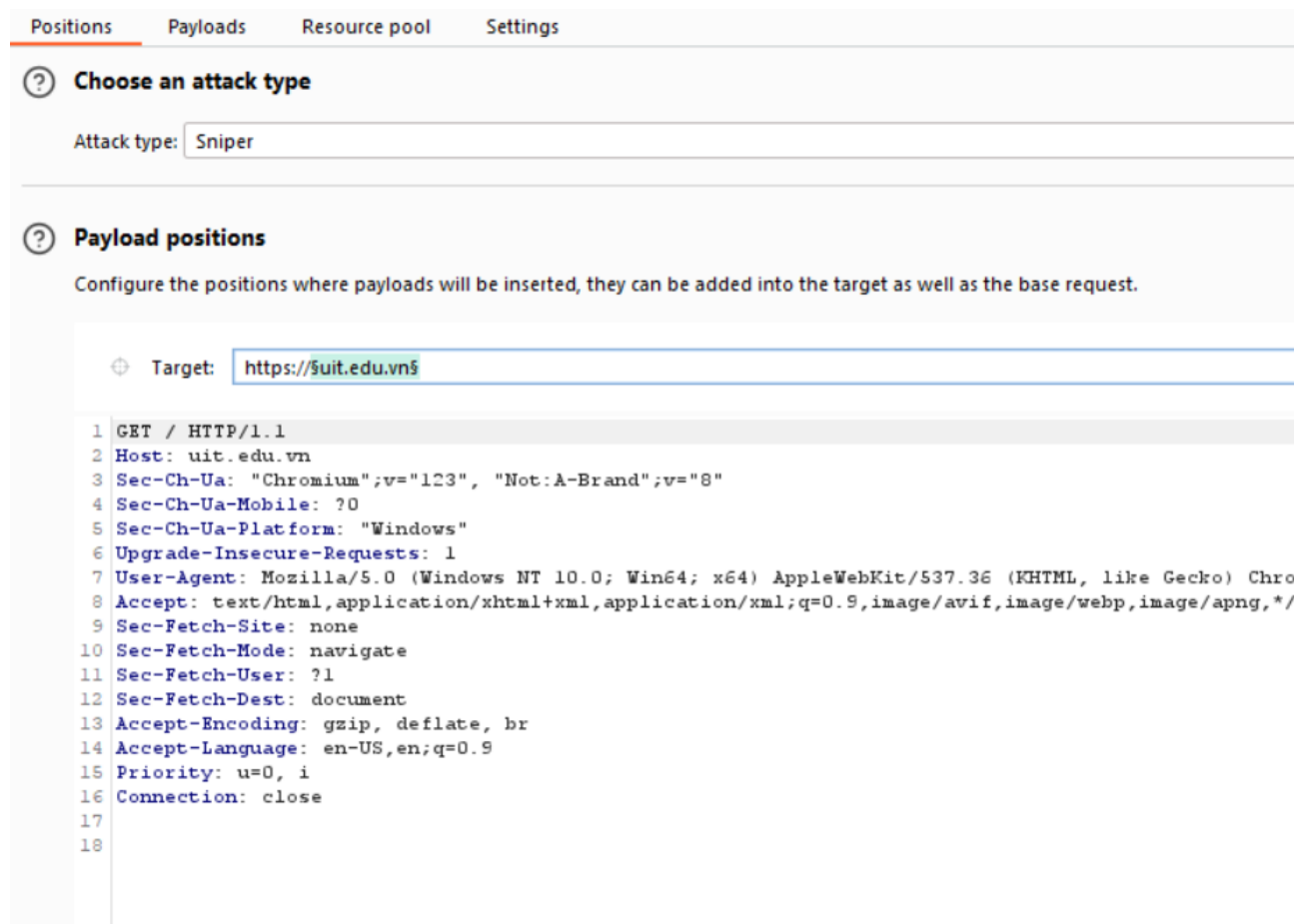
X ✓ *fx*

	A	B	C	D	E
1	192.168.20.87:110				
2	192.168.20.87:5060				
3	192.168.20.87:22				
4	10.204.2.4:443				
5	10.204.2.4:22				
6	10.204.2.4:5060				
7	10.204.2.4:80				
8	192.168.20.200:80				
9	192.168.20.200:22				
10	192.168.20.200:5060				
11	10.204.2.4:80				
12	10.204.2.4:5060				
13	10.204.2.4:443				
14	10.204.2.4:22				
15	10.204.2.4:443				
16	10.204.2.4:5060				
17	192.168.20.60:5060				
18	192.168.20.60:443				
19	192.168.20.60:22				
20	10.204.2.4:443				
21	10.204.2.4:8080				
22	10.204.2.4:80				
23	10.204.2.4:5060				
24	192.168.20.22:3389				
25	192.168.20.22:80				
26	192.168.20.22:5060				

10. Bài tập thực hành 3 – Tìm dữ liệu quá khứ của subdomain uit

Tương tự như bài tìm dữ liệu quá khứ của *.rmit.edu.vn. Ta dùng intruder để liệt kê các website không còn phản hồi.

Đầu tiên là thêm 2 dấu \$ vào Target:



The screenshot shows the Burp Suite Intruder configuration window. At the top, there are four tabs: "Positions", "Payloads", "Resource pool", and "Settings". The "Positions" tab is selected. Below the tabs, there is a section titled "Choose an attack type" with a question mark icon. Underneath, the "Attack type" is set to "Sniper". Below this, there is a section titled "Payload positions" with a question mark icon. It contains a description: "Configure the positions where payloads will be inserted, they can be added into the target as well as the base request." Below the description, there is a "Target" field with a plus icon on the left and the text "https://\$uit.edu.vn\$". Below the target field, there is a list of HTTP request headers and methods, numbered 1 through 18. The list includes: 1 GET / HTTP/1.1, 2 Host: uit.edu.vn, 3 Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8", 4 Sec-Ch-Ua-Mobile: ?0, 5 Sec-Ch-Ua-Platform: "Windows", 6 Upgrade-Insecure-Requests: 1, 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro, 8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/, 9 Sec-Fetch-Site: none, 10 Sec-Fetch-Mode: navigate, 11 Sec-Fetch-User: ?1, 12 Sec-Fetch-Dest: document, 13 Accept-Encoding: gzip, deflate, br, 14 Accept-Language: en-US,en;q=0.9, 15 Priority: u=0, i, 16 Connection: close, 17, and 18.

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://\$uit.edu.vn\$

```
1 GET / HTTP/1.1
2 Host: uit.edu.vn
3 Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Priority: u=0, i
16 Connection: close
17
18
```

Thêm danh sách từ điển từ bài tập thực hành 1:

Intruder

1 ×

2 ×

+

Positions

Payloads

Resource pool

Settings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of positions.

Payload set:

1

▼

Payload count:

140

Payload type:

Simple list

▼

Request count:

140

?

Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

cd.uit.edu.vn

smtp.uit.edu.vn

live.uit.edu.vn

uhongdl.uit.edu.vn

gaingon.uit.edu.vn

traibao.uit.edu.vn

daa1.uit.edu.vn

dkhpapi.uit.edu.vn

dsc.uit.edu.vn

Enter a new item

Add from list ... [Pro version only]

▼

Các tên miền cũ không còn dùng:

live.uit.edu.vn:

DONATE

WayBackMachine

Explore more than 866 billion web pages saved over time

live.uit.edu.vn

Calendar

Collections

Changes

Summary

Site Map

URLs

43 URLs have been captured for this URL prefix.

URL ↑	MIME Type	From	To
http://live.uit.edu.vn/baigiang	text/html	Mar 3, 2022	Mar 3, 2022
http://live.uit.edu.vn/css/flexslider.css	text/css	Nov 28, 2018	Mar 3, 2022
http://live.uit.edu.vn/css/images/active-nav-border.png	image/png	Dec 21, 2018	Dec 21, 2018
http://live.uit.edu.vn/css/images/baner.png	image/png	Mar 3, 2022	Mar 3, 2022
http://live.uit.edu.vn/css/images/blue-btn.png	image/png	Dec 13, 2018	Dec 13, 2018
http://live.uit.edu.vn/css/images/body.png	image/png	Dec 17, 2018	Dec 17, 2018
http://live.uit.edu.vn/css/images/bullet-footer-col.png	image/png	Dec 16, 2018	Dec 16, 2018
http://live.uit.edu.vn/css/images/bullet.png	image/png	Dec 21, 2018	Dec 21, 2018
http://live.uit.edu.vn/css/images/col-separator.png	image/png	Dec 21, 2018	Dec 21, 2018
http://live.uit.edu.vn/css/images/control-nav-bg.png	image/png	Dec 21, 2018	Dec 21, 2018
http://live.uit.edu.vn/css/images/control-nav.png	image/png	Dec 25, 2018	Dec 25, 2018
http://live.uit.edu.vn/css/images/DHCNTT.jpg	image/jpeg	Nov 27, 2018	Nov 27, 2018
http://live.uit.edu.vn/css/images/favicon.ico	image/x-icon	Nov 29, 2018	Mar 3, 2022
http://live.uit.edu.vn/css/images/footer-cols.png	image/png	Dec 13, 2018	Dec 13, 2018
http://live.uit.edu.vn/css/images/footer-nav-border.png	image/png	Dec 21, 2018	Dec 21, 2018
http://live.uit.edu.vn/css/images/header-@2x.png	image/png	Dec 12, 2018	Dec 12, 2018
http://live.uit.edu.vn/css/images/header-cnt.png	image/png	Dec 25, 2018	Dec 25, 2018
http://live.uit.edu.vn/css/images/header-tablet.png	image/png	Dec 20, 2018	Dec 20, 2018
http://live.uit.edu.vn/css/images/header.png	image/png	Dec 13, 2018	Dec 13, 2018
http://live.uit.edu.vn/css/images/logo-@2x.png	image/png	Dec 24, 2018	Dec 24, 2018
http://live.uit.edu.vn/css/images/logo-tablet.png	image/png	Dec 20, 2018	Dec 20, 2018

elearning.uit.edu.vn:

DONATE

WayBackMachine

Explore more than 866 billion web pages saved over time

elearning.uit.edu.vn

Calendar

Collections

Changes

Summary

Site Map

URLs

1,205 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	Unique
http://elearning.uit.edu.vn:80/phpmyadmin/tbl_structure.php?	text/html	Apr 16, 2011	Apr 16, 2011	1	0	1
http://elearning.uit.edu.vn:80/product.php?	text/html	Apr 9, 2013	Aug 26, 2014	6	2	4
http://elearning.uit.edu.vn:80/product.php?content=product	text/html	Apr 12, 2013	Jul 16, 2014	4	1	3
http://elearning.uit.edu.vn:80/security/index.php	text/html	Apr 16, 2011	Apr 16, 2011	1	0	1
http://elearning.uit.edu.vn:80/webalizer	text/html	Apr 16, 2011	Apr 16, 2011	2	0	2

Showing 1,201 to 1,205 of 1,205 entries

First

Previous

1

...

21

22

23

24

25

Next

huongnghiep.uit.edu.vn:



Explore more than 866 billion web pages saved over time

huongnghiep.uit.edu.vn



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

73 URLs have been captured for this URL prefix.

URL ↑	MIME Type	From	To
http://huongnghiep.uit.edu.vn/misc/draggable.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/gripple.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/help.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/menu-collapsed.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/menu-expanded.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/menu-leaf.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/message-24-error.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/message-24-ok.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/message-24-warning.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/progress.gif	image/gif	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/throbber-active.gif	image/gif	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/throbber-inactive.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/tree-bottom.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/misc/tree.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/robots.txt	text/plain	Jun 28, 2017	Aug 10, 2018
http://huongnghiep.uit.edu.vn/sites/all/modules/contrib/back_top/backtotop.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/sites/all/modules/contrib/back_top/backtotop2x.png	image/png	Jul 31, 2018	Jul 31, 2018
http://huongnghiep.uit.edu.vn/sites/all/themes/open_framework/js/html5shiv.js	text/javascript	Jun 13, 2018	Jun 13, 2018

Và có thể còn rất nhiều tên miền khác ở trong danh sách này:

Results	Positions	Payloads	Resource pool	Settings		
Filter: Showing all items						
Request	Payload	Target	Status code ^	Response received	Error	Ti
1	cd.uit.edu.vn	https://cd.uit.edu.vn	0	0		
2	smtp.uit.edu.vn	https://smtp.uit.edu.vn	0	0	✓	
3	live.uit.edu.vn	https://live.uit.edu.vn	0	0	✓	
4	uhongdl.uit.edu.vn	https://uhongdl.uit.edu.vn	0	0		
5	gaingon.uit.edu.vn	https://gaingon.uit.edu.vn	0	0		
6	traibao.uit.edu.vn	https://traibao.uit.edu.vn	0	0		
7	daa1.uit.edu.vn	https://daa1.uit.edu.vn	0	0		
10	elearning.uit.edu.vn	https://elearning.uit.edu.vn	0	0		
11	aiclubcs.uit.edu.vn	https://aiclubcs.uit.edu.vn	0	0		
12	rmit.uit.edu.vn	https://rmit.uit.edu.vn	0	0		
13	state.uit.edu.vn	https://state.uit.edu.vn	0	0		
17	huongnghiep.uit.edu.vn	https://huongnghiep.uit.edu.vn	0	0		
18	cc62e73f33af4d5vlab2.uit.edu.vn	https://cc62e73f33af4d5vlab2.uit.edu.vn	0	0		
19	vlab2.uit.edu.vn	https://vlab2.uit.edu.vn	0	0		
20	ucpc.uit.edu.vn	https://ucpc.uit.edu.vn	0	0	✓	
21	post.uit.edu.vn	https://post.uit.edu.vn	0	0		
25	tttdtt.uit.edu.vn	https://tttdtt.uit.edu.vn	0	0	✓	
26	eth2.uit.edu.vn	https://eth2.uit.edu.vn	0	0	✓	
29	momiji.uit.edu.vn	https://momiji.uit.edu.vn	0	0	✓	
30	competitions.uit.edu.vn	https://competitions.uit.edu.vn	0	0	✓	
34	host88.uit.edu.vn	https://host88.uit.edu.vn	0	0		
37	khcn2.uit.edu.vn	https://khcn2.uit.edu.vn	0	0		
38	tcvaccine.uit.edu.vn	https://tcvaccine.uit.edu.vn	0	0		
39	xncovid.uit.edu.vn	https://xncovid.uit.edu.vn	0	0		
40	tech4covid.uit.edu.vn	https://tech4covid.uit.edu.vn	0	0		
43	thilaptrinh.uit.edu.vn	https://thilaptrinh.uit.edu.vn	0	0	✓	
44	cncs.uit.edu.vn	https://cncs.uit.edu.vn	0	0		
45	ceday.uit.edu.vn	https://ceday.uit.edu.vn	0	0	✓	
47	cdn.uit.edu.vn	https://cdn.uit.edu.vn	0	0		
48	apigwqa.uit.edu.vn	https://apigwqa.uit.edu.vn	0	0		
49	135-208.uit.edu.vn	https://135-208.uit.edu.vn	0	0		
50	201-109.uit.edu.vn	https://201-109.uit.edu.vn	0	0		
51	225-160.uit.edu.vn	https://225-160.uit.edu.vn	0	0		
52	arbe.uit.edu.vn	https://arbe.uit.edu.vn	0	0		
53	hsts.uit.edu.vn	https://hsts.uit.edu.vn	0	0		

#	http://uit.edu.vn	https://uit.edu.vn	
54	log.uit.edu.vn	https://log.uit.edu.vn	0
55	service.uit.edu.vn	https://service.uit.edu.vn	0
56	com.uit.edu.vn	https://com.uit.edu.vn	0
58	vinhdanh.uit.edu.vn	https://vinhdanh.uit.edu.vn	0 ✓
61	mapr2019.uit.edu.vn	https://mapr2019.uit.edu.vn	0
63	acm.uit.edu.vn	https://acm.uit.edu.vn	0
65	cns.cuit.edu.vn	https://cns.cuit.edu.vn	0 ✓
66	coures.uit.edu.vn	https://coures.uit.edu.vn	0
68	cybertrain.uit.edu.vn	https://cybertrain.uit.edu.vn	0 ✓
73	extensivereading.uit.edu.vn	https://extensivereading.uit.edu.vn	0 ✓
74	gmail.uit.edu.vn	https://gmail.uit.edu.vn	0
75	htt.uit.edu.vn	https://htt.uit.edu.vn	0
77	isclub.uit.edu.vn	https://isclub.uit.edu.vn	0 ✓
81	lib.uit.edu.vn	https://lib.uit.edu.vn	0 ✓
85	netsens.uit.edu.vn	https://netsens.uit.edu.vn	0
87	quiz.uit.edu.vn	https://quiz.uit.edu.vn	0 ✓
90	sois2017.uit.edu.vn	https://sois2017.uit.edu.vn	0 ✓
91	speechlab1.uit.edu.vn	https://speechlab1.uit.edu.vn	0 ✓
95	yuyxcvplilit.uit.edu.vn	https://yuyxcvplilit.uit.edu.vn	0
98	maskolis.uit.edu.vn	https://maskolis.uit.edu.vn	0
109	zeroshell.uit.edu.vn	https://zeroshell.uit.edu.vn	0
139	kse2015.uit.edu.vn	https://kse2015.uit.edu.vn	0
140	www.uit.edu.vn	https://www.uit.edu.vn	200 16

11. Bài tập thực hành 4 - Tìm dữ liệu nhạy cảm liên quan subdomain uit bằng google dork và github

Dùng git dork password kết hợp với “uit.edu.vn”, khai thác được 1 số thông tin nhạy cảm như mật khẩu một số project:

filter by

- <> Code 384
- Repositories 0
- Issues 0
- Pull requests 0
- Discussions 0
- Users 0
- More

Languages

- Markdown
- JavaScript
- XML
- Shell
- YAML

384 files (2 s)

▼ Mann202/Museverse-Music-Web-FE · README.md

```

24 5.1 Front-end side
25 - Install NodeJS (Recommend for most user) from [NodeJS](https://nodejs.org/en)
26 - Login Spotify Premium account in Spotify
27   User: 21521115@gm.uit.edu.vn
28   Password: Truonggiaman.3012
29 - Clone the GitHub repository through the link or unzip the packaged web.
30 - After cloning or unzip, use Visual Code Studio and run the following commands:

```

Show 6 more matches

▼ duyet/node-rtb-server · config/config.js

```

8  user      : 'root',
9  password : '',
10 database : 'bgate_demo',
14 module.exports = {
15   domain: 'http://ptnhttp.uit.edu.vn',
16   port: process.env.PORT || 8899,

```

HẾT