

# BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và ứng dụng

## Lab 3: Reconnaissance

GVHD: Ngô Đức Hoàng Sơn

### 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT132.012.ATCL.2- Nhóm 4

STT	Họ và tên	MSSV	Email
1	Đỗ Thị Yến Ly	21520337	<a href="mailto:21520337@gm.uit.edu.vn">21520337@gm.uit.edu.vn</a>
2	Lê Hoàng Oanh	21521253	21521253@gm.uit.edu.vn
3	Nguyễn Đại Bảo Duy	21520772	<a href="mailto:21520772@gm.uit.edu.vn">21520772@gm.uit.edu.vn</a>

### 2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%
4	Yêu cầu 4	100%
5	Yêu cầu 5	100%
6	Yêu cầu 6	100%
7	Yêu cầu 7	100%
8	Chậm lại và suy nghĩ 1	100%
9	Chậm lại và suy nghĩ 2	100%
10	Chậm lại và suy nghĩ 3	100%
11	Chậm lại và suy nghĩ 4	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

## BÁO CÁO CHI TIẾT

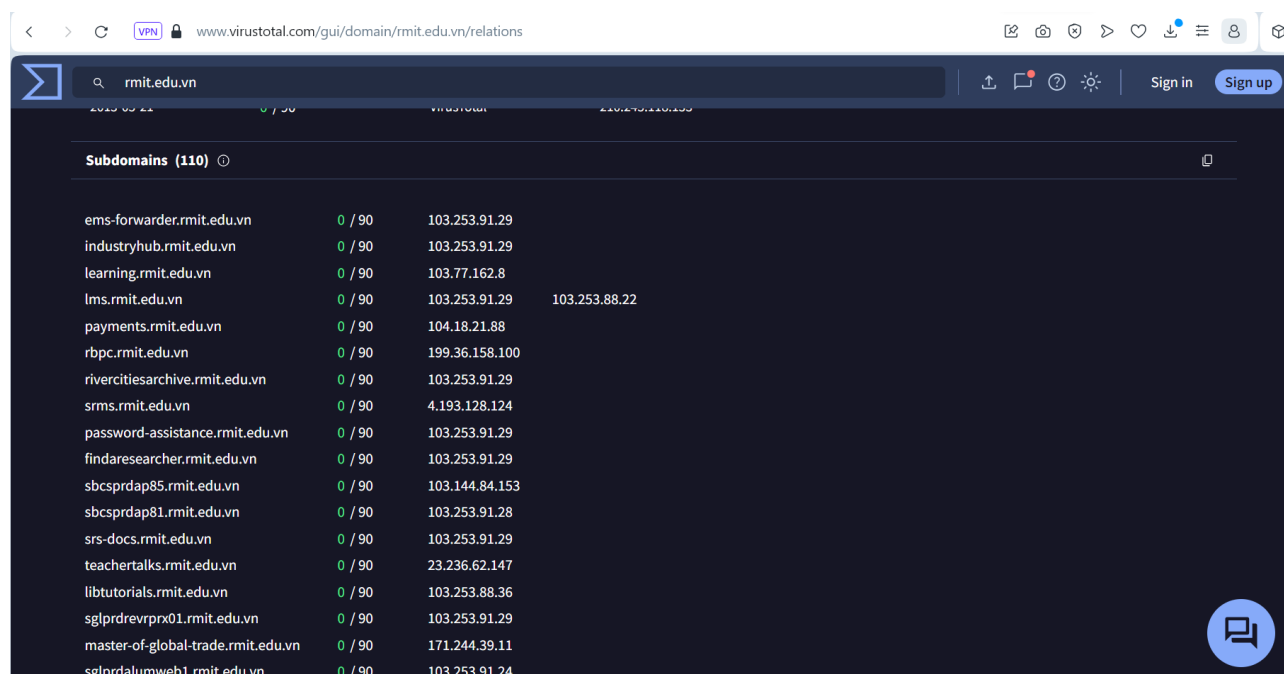
**Chậm lại và suy nghĩ 1: Các nguồn có thể tìm kiếm dữ liệu công khai tên miền phụ ở đâu?**

Các nguồn có thể tìm kiếm dữ liệu công khai tên miền phụ là Virustotal, Wayback Machine (<https://web.archive.org>), ...

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

Ở câu 1 ta sẽ sử dụng virustotal.com để thực hiện kiểm tra các domain thì ta có thể lấy được 110 domain

<https://www.virustotal.com/gui/domain/rmit.edu.vn/relations>



Sau đó ta sẽ copy kết quả bỏ vào file csv.

**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?**

Có các công cụ như dnsdumpster, dnsrecon, amass, sublist3r, fierce,... mà bạn có thể sử dụng để tìm kiếm các tên miền phụ của một tên miền cụ thể.

Cách để đưa tên miền phụ vào burpsuite để tìm kiếm:

- Ta mở trang web trong trình duyệt của Burpsuite và ta chọn Send to Intruder

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	https://www.rmit.edu.vn	GET	/			200	404442	HTML		Home - RMIT University	
4	https://www.rmit.edu.vn	GET	https://www.rmit.edu.vn/			200	196317	script	js		
6	https://www.rmit.edu.vn	GET				200	114247	script	jpg		
7	https://assets.adobedtm.com	GET				200	548983	script	js		
10	https://www.rmit.edu.vn	GET				200	163992	script	js		
11	https://www.rmit.edu.vn	GET				200	149729	script	js		
13	https://www.rmit.edu.vn	GET				200	252044	script	is		

- Trong Target, sửa đường dẫn thành <http://x.portswigger-labs.net> và chọn Add §

**Choose an attack type**

Attack type:

**Payload positions**

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

Target:  ☒ Update Host header to match target

- Trong mục Payloads, chọn Add from list và chọn Dictionary – short, chọn Start Attack

**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 customized in different ways.

Payload set:  Payload count: 372

Payload type:  Request count: 372

**Payload settings [Simple list]**

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

Add from list ...

- Sau khi Attack, ta có những tên miền phụ sau

Attack Save 4. Intruder attack of https://x.rmit.edu.vn

4. Intruder attack of https://x.rmit.edu.vn Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Target	Status code	Response received	Error	Timeout	Length	Comment
322	design	https://design.rmit.edu.vn	200	341			1764	
381	english	https://english.rmit.edu.vn	200	118			35801	
382	English	https://english.rmit.edu.vn	200	160			35801	
525	helpdesk	https://helpdesk.rmit.edu.vn	200	137			5143	
1793	www	https://www.rmit.edu.vn	200	76			404441	
398	event	https://event.rmit.edu.vn	301	394			857	
1615	library	https://library.rmit.edu.vn	301	112			377	
805	payments	https://payments.rmit.edu.vn	302	681			732	
1469	apps	https://apps.rmit.edu.vn	302	143			826	
171	careers	https://careers.rmit.edu.vn	404	447			1021	
1548	email	https://email.rmit.edu.vn	404	476			712	
0		https://x.rmit.edu.vn		0				baseline request
1	A	https://a.rmit.edu.vn		0				
2	About	https://about.rmit.edu.vn		0				

**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.

- Chỉnh sửa file csv đã lấy ở câu 1, giữ lại tên miền phụ rồi lưu file

	A	B	C	D	E	F	G	H	I
1	ems-forwarder								
2	industryhub								
3	learning								
4	lms								
5	payments								
6	rbpc								
7	rivercitiesarchive								
8	srms								
9	password-assistance								
10	findaresearcher								
11	sbcspredap85								
12	sbcspredap81								
13	srs-docs								
14	teachertalks								
15	libtutorials								
16	sglprdrevrprx01								
17	master-of-global-trade								
18	sglprdalumweb1								
19	ns1								

- Vào mục Payload, load file tên miền phụ của file trên và chọn Start Attack.

1 x 2 x 3 x +

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 customized in different ways.

Payload set: 1 Payload count: 110

Payload type: Simple list Request count: 110

**Start attack**

**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 Enter a new item

ams-forwarder  
industryhub  
learning  
lms  
payments  
rbpc  
rivercitiesarchive  
sims  
password-assistance  
findaresearcher

Add from list ... [Pro version only]

## - Các tên miền có kết quả trả về 200

5. Intruder attack of https://sx9.rmit.edu.vn

Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Target	Status code	Response received	Error	Timeout	Length	Comment
1	ems-forwarder	https://ems-forwarder.rmit.edu.vn	200	176			235	
3	learning	https://learning.rmit.edu.vn	200	3080			219256	
6	rbpc	https://rbpc.rmit.edu.vn	200	67			3534	
7	rivercitiesarchive	https://rivercitiesarchive.rmit.edu.vn	200	304			1764	
10	findaresearcher	https://findaresearcher.rmit.edu.vn	200	175			1106	
15	libtutorials	https://libtutorials.rmit.edu.vn	200	41			2090	
18	sglprdalumweb1	https://sglprdalumweb1.rmit.edu.vn	200	118			329	
37	english	https://english.rmit.edu.vn	200	90			35801	
39	alumninetwork	https://alumninetwork.rmit.edu.vn	200	927			145071	
41	sglprdstudlab01	https://sglprdstudlab01.rmit.edu.vn	200	38			267	
43	studentlab1	https://studentlab1.rmit.edu.vn	200	47			267	
45	democlass	https://democlass.rmit.edu.vn	200	88			35801	
46	experienceday	https://experienceday.rmit.edu.vn	200	163			139868	
56	helpdesk	https://helpdesk.rmit.edu.vn	200	209			5143	
80	sas	https://sas.rmit.edu.vn	200	131			2142	
83	pe	https://pe.rmit.edu.vn	200	508			4140	
84	omeka	https://omeka.rmit.edu.vn	200	181			31655	
98	design	https://design.rmit.edu.vn	200	299			1764	
100	chame	https://chame.rmit.edu.vn	200	80			204735	
103	etal	https://etal.rmit.edu.vn	200	315			2117	
107	learninglab	https://learninglab.rmit.edu.vn	200	547			56991	
110	www	https://www.rmit.edu.vn	200	119			404442	

## - Các tên miền có kết quả trả về khác

5. Intruder attack of https://sx9.rmit.edu.vn

Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Target	Status code	Response received	Error	Timeout	Length	Comment
42	mytimetable	https://mytimetable.rmit.edu.vn	410	274			136	
38	email	https://email.rmit.edu.vn	404	219			712	
51	careers	https://careers.rmit.edu.vn	404	504			1021	
8	sims	https://sims.rmit.edu.vn	403	56			736	
32	sgs-wi-omeka	https://sgs-wi-omeka.rmit.edu.vn	403	33			456	
96	emedia	https://emedia.rmit.edu.vn	403	133			4324	
2	industryhub	https://industryhub.rmit.edu.vn	302	259			483	
5	payments	https://payments.rmit.edu.vn	302	670			732	
9	password-assistance	https://password-assistance.rmit.edu.vn	302	131			901	
16	sglprdrexp01	https://sglprdrexp01.rmit.edu.vn	302	152			881	
24	rmitlibrary	https://rmitlibrary.rmit.edu.vn	302	200			608	
47	apps	https://apps.rmit.edu.vn	302	145			826	
63	oes	https://oes.rmit.edu.vn	302	179			755	
85	typographyvn	https://typographyvn.rmit.edu.vn	302	197			610	
101	riv2020	https://riv2020.rmit.edu.vn	302	223			237	
4	lms	https://lms.rmit.edu.vn	301	111			367	
14	teachertalks	https://teachertalks.rmit.edu.vn	301	326			731	
49	blackboard	https://blackboard.rmit.edu.vn	301	125			367	
87	event	https://event.rmit.edu.vn	301	516			723	
99	infosession	https://infosession.rmit.edu.vn	301	323			1034	
104	rmitenglishevent	https://rmitenglishevent.rmit.edu.vn	301	356			868	
109	library	https://library.rmit.edu.vn	301	120			377	

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

Ta có thể sử dụng nslookup, dig, host, hoặc là sử dụng code python mở socket.

### 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 sử dụng socket.gethostbyname(subdomain) để thực hiện truy vấn dns để tìm địa chỉ ip của tên miền được cung cấp (subdomain).

```
cau3.py
1 import csv
2 import socket
3
4 def get_ip(subdomain):
5     try:
6         ip = socket.gethostbyname(subdomain)
7         return ip
8     except socket.gaierror:
9         return "Unknown"
10
11 def main(input_csv, output_txt):
12     with open(input_csv, 'r') as csv_file:
13         csv_reader = csv.reader(csv_file)
14         with open(output_txt, 'w') as txt_file:
15             for row in csv_reader:
16                 subdomain = row[0]
17                 ip = get_ip(subdomain)
18                 txt_file.write(f"{subdomain}: {ip}\n")
19
20 if __name__ == "__main__":
21     input_csv = "cau1.csv"
22     output_txt = "output.txt"
23     main(input_csv, output_txt)
```

Ta có file địa chỉ ip như sau

```
ems-forwarder.rmit.edu.vn: 103.253.91.29
industryhub.rmit.edu.vn: 103.253.91.29
learning.rmit.edu.vn: 103.77.162.8
lms.rmit.edu.vn: 103.253.91.29
payments.rmit.edu.vn: 104.18.20.88
rbpc.rmit.edu.vn: 199.36.158.100
rivercitiesarchive.rmit.edu.vn: 103.253.91.29
srms.rmit.edu.vn: 4.193.128.124
password-assistance.rmit.edu.vn: 103.253.91.29
findaresearcher.rmit.edu.vn: 103.253.91.29
sbcsprdap85.rmit.edu.vn: 103.144.84.153
sbcsprdap81.rmit.edu.vn: 103.253.91.28
srs-docs.rmit.edu.vn: Unknown
teachertalks.rmit.edu.vn: 23.236.62.147
libtutorials.rmit.edu.vn: 103.253.88.36
sglprdevrpx01.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: Unknown
pnt-wl-drweb5.rmit.edu.vn: Unknown
dns2.rmit.edu.vn: Unknown
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: Unknown
vpn2.rmit.edu.vn: 103.253.88.4
sgs-wl-mekong2.rmit.edu.vn: Unknown
sgs-aw-spydus01.rmit.edu.vn: Unknown
sgs-aw-hrapp1.rmit.edu.vn: 103.253.88.38
drwprdrhapp01.rmit.edu.vn: 210.245.97.71
sgs-wl-omeka.rmit.edu.vn: 103.253.88.36
password.rmit.edu.vn: Unknown
sgs-wl-sleapp1.rmit.edu.vn: 103.253.88.40
pnt-wl-wcpsvc.rmit.edu.vn: 210.245.97.72
pnt-wl-drweb3.rmit.edu.vn: Unknown
english.rmit.edu.vn: 103.253.88.35
```

### Chậm lại và suy nghĩ 4: Các công cụ scan port hiện nay có thể sử dụng là gì?

Các công cụ scan port hiện nay có thể sử dụng là nmap, naabu, masscan,...

### 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.

Ta sử dụng naabu để tìm port đang mở của từng ip trong câu 3 và gán giá trị vào file cau4.txt

```
#!/bin/bash
for ip in $(cat cau3.txt); do
    printf "%s\n" $(naabu "$ip") >> cau4.txt
done
```

Sau khi chạy xong ta có kết quả như sau:

```
64 103.253.91.29:80
65 103.253.91.29:443
```

Lưu kết quả vào file csv.

### 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.

Các tên miền không còn được sử dụng của \*.rmit.edu.vn

web.archive.org/web/7/https://staff.rmit.edu.vn

Explore more than 600 billion web pages saved over time

https://staff.rmit.edu.vn

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

70 URLs have been captured for this URL prefix.

Filter results by URL or MIME T

URL ↑	MIME Type	From	To	Captures	Duplicates
https://staff.rmit.edu.vn/	text/html	Jun 21, 2020	Aug 30, 2022	10	9
https://staff.rmit.edu.vn/favicon.ico	image/vnd.microsoft.icon	Apr 29, 2016	Jan 8, 2022	5	4
https://staff.rmit.edu.vn/misc/drupal.js	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/drupal.js?pbdeq	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/jquery.js	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/jquery.js?v=1.4.4	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/jquery.once.js	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/jquery.once.js?v=1.2	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.css?pbdeq	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.core.css?pbdeq	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.core.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.css?pbdeq	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.dialog.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.draggable.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.mouse.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.position.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.resizable.css?pbdeq	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.resizable.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.theme.css?pbdeq	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0
https://staff.rmit.edu.vn/misc/ui/jquery.ui.widget.min.js?v=1.8.7	warcrevisit	Jan 22, 2019	Jan 22, 2019	1	0

## Dữ liệu của một url được capture

web.archive.org/web/2019122182550/https://staff.rmit.edu.vn/misc/drupal.js?pbdeq

1 capture

22 Jan 2019

```
var __$wombat$assignFunction = function(name) { return (self._wombat && self._wombat.local_init && self._wombat.local_init(name)) || self[name]; };
if (self._wombat) { self._wombat = function(obj) { this._wombat = obj; return this; }; }

let window = __$wombat$assignFunction("window");
let self = __$wombat$assignFunction("self");
let document = __$wombat$assignFunction("document");
let location = __$wombat$assignFunction("location");
let top = __$wombat$assignFunction("top");
let parent = __$wombat$assignFunction("parent");
let frames = __$wombat$assignFunction("frames");
let opener = __$wombat$assignFunction("opener");

var Drupal = Drupal || { 'settings': {}, 'behaviors': {}, 'locale': {} };

// Allow other JavaScript libraries to use $.
jQuery.noConflict();

(function ($) {

  /**
   * Override jQuery.fn.init to guard against XSS attacks.
   *
   * See http://bugs.jquery.com/ticket/1921
   */
  var jquery_init = $.fn.init;
  $.fn.init = function(selector, context, rootjQuery) {
    // If the string contains a "<" before a ">", treat it as invalid HTML.
    if (selector && typeof selector === 'string') {
      var hash_position = selector.indexOf('#');
      if (hash_position > 0) {
        var bracket_position = selector.indexOf('<');
        if (bracket_position > hash_position) {
          throw 'Syntax error, unrecognized expression: ' + selector;
        }
      }
    }
    return jquery_init.call(this, selector, context, rootjQuery);
  };
  $.fn.init.prototype = jquery_init.prototype;

  /**
   * Attach all registered behaviors to a page element.
   *
   * Behaviors are event-triggered actions that attach to page elements, enhancing
   * default non-javascript UIs. Behaviors are registered in the Drupal.behaviors
   * object using the method 'attach' and optionally also 'detach' as follows:
   *
   * @code
   * Drupal.behaviors.behaviorName = {
   *   attach: function (context, settings) {
   *     ...
   *   },
   *   detach: function (context, settings, trigger) {
   *     ...
   *   }
   * }
  
```

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




Google

site:rmit.edu.vn filetype:pdf

×

All Shopping Images Videos News More Tools

About 701 results (0.35 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 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

⋮

. In Physics we commonly use SI units (kilograms, metres, ...

In Physics we commonly use SI units (kilograms, metres, seconds) and prefixes, and we assume that you can convert between them. It is also assumed that you ...


Google

site:rmit.edu.vn filetype:xls OR filetype:xlsx

×

All Shopping Images Videos News More Tools

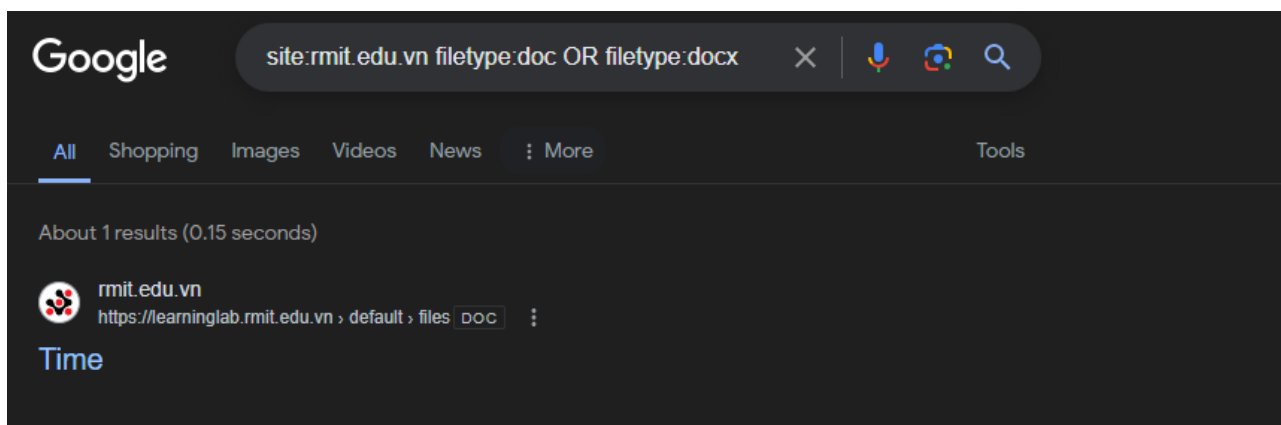
About 1 results (0.14 seconds)

 rmit.edu.vn

https://www.rmit.edu.vn > pdfs > atn-exchange XLS

⋮

Student input here



## Bài tập 7: Ghi nhận một vài thông tin tìm được trên github với domain \*.rmit.edu.vn.

Tìm được một vài thông tin các nhân liên quan đến miền \*.rmit.edu.vn

