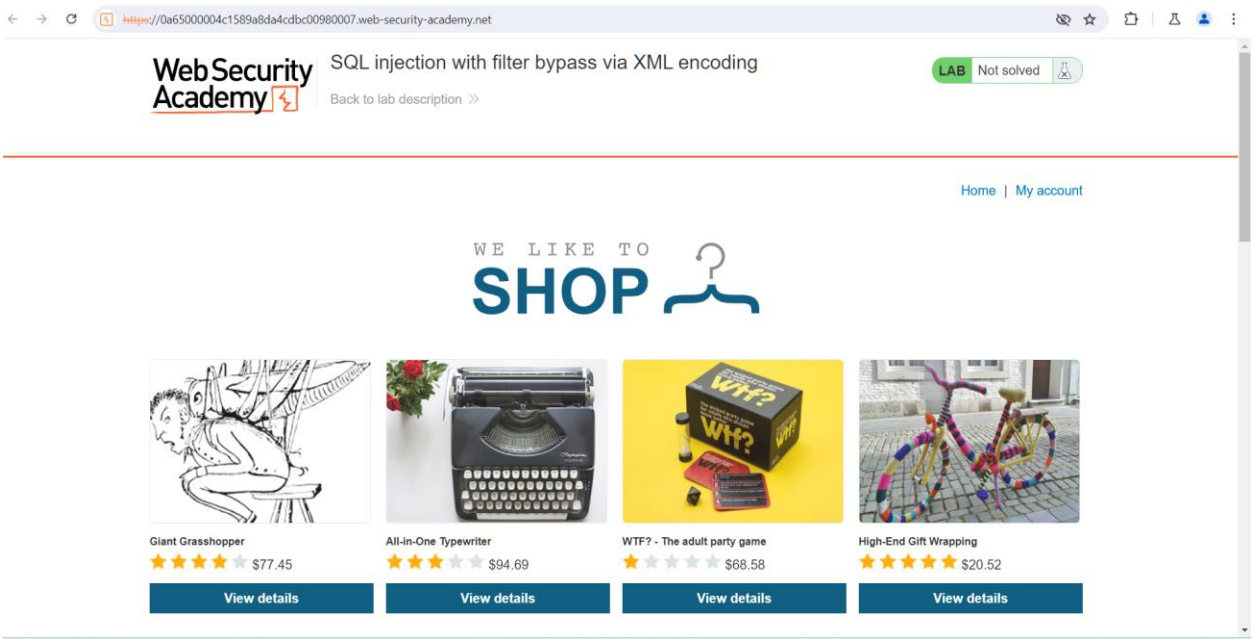
Lab: SQL injection with filter bypass via XML encoding

Scenario:

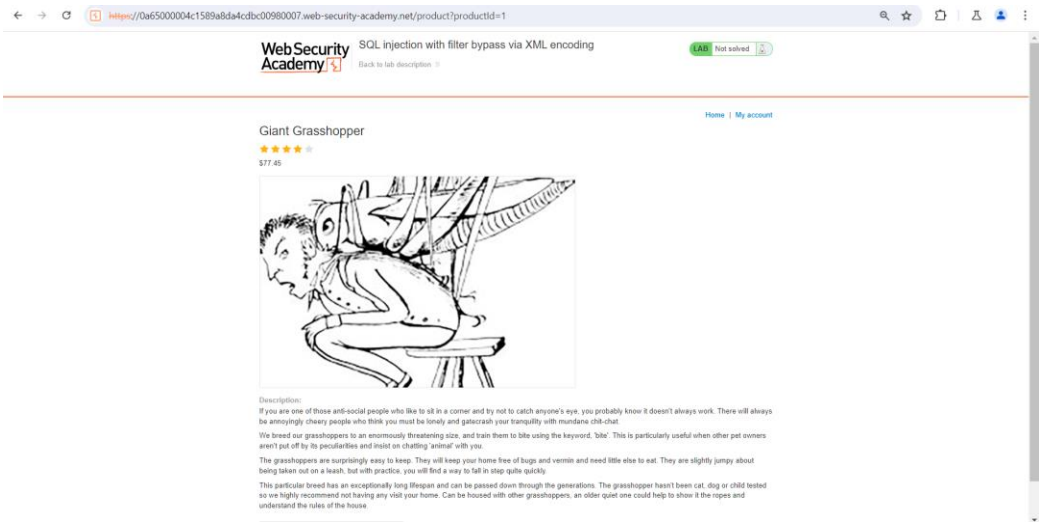
The stock check feature in this lab is vulnerable to SQL injection, allowing for a UNION attack to retrieve data from other tables. To solve the lab, exploit this vulnerability to obtain the admin user's credentials from the users table and log into their account.

Before Testing the Exploit:

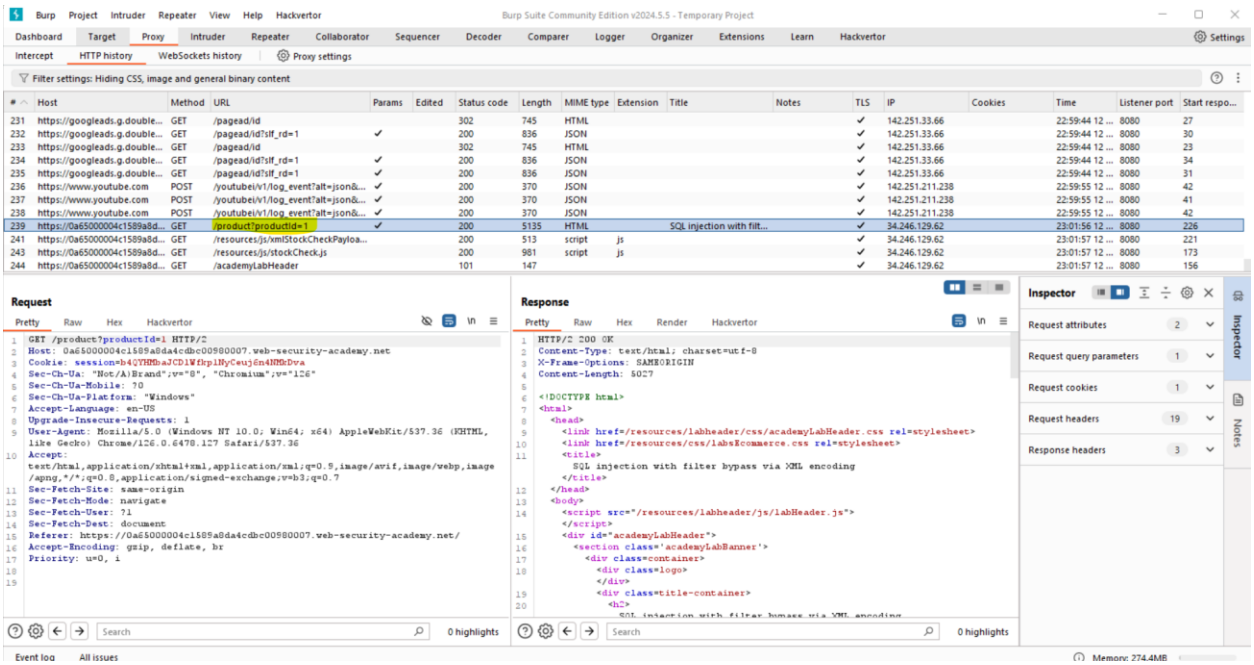
Web Application Page:



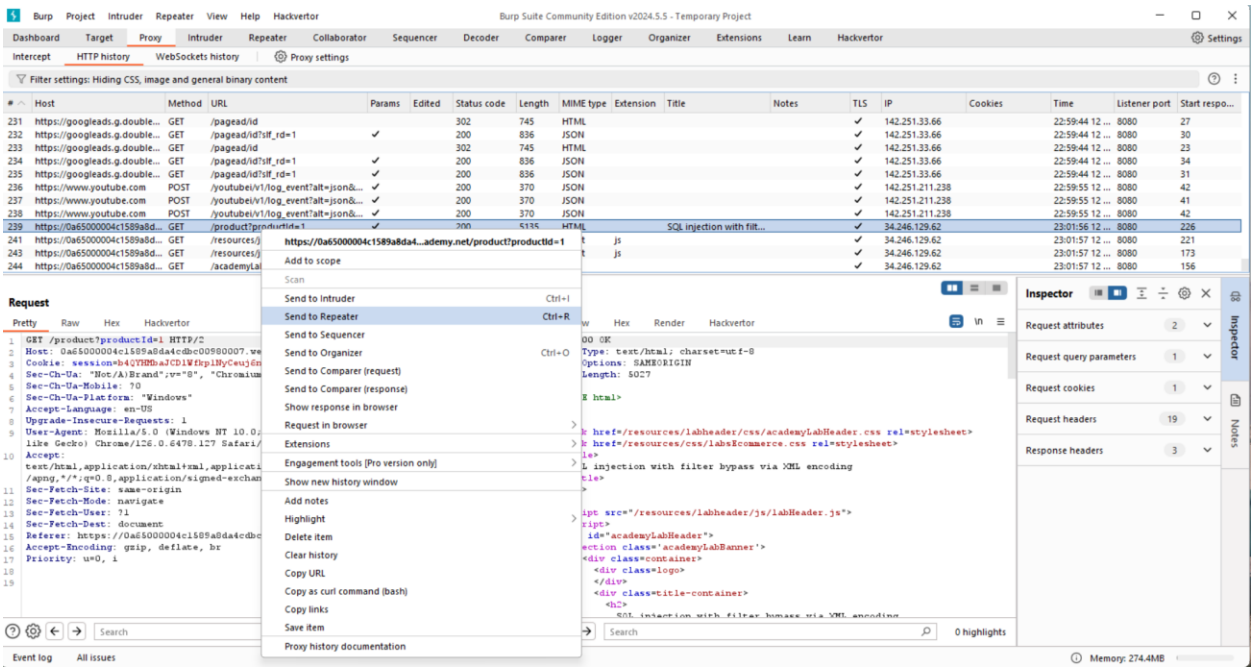
Clicked on the product from the left



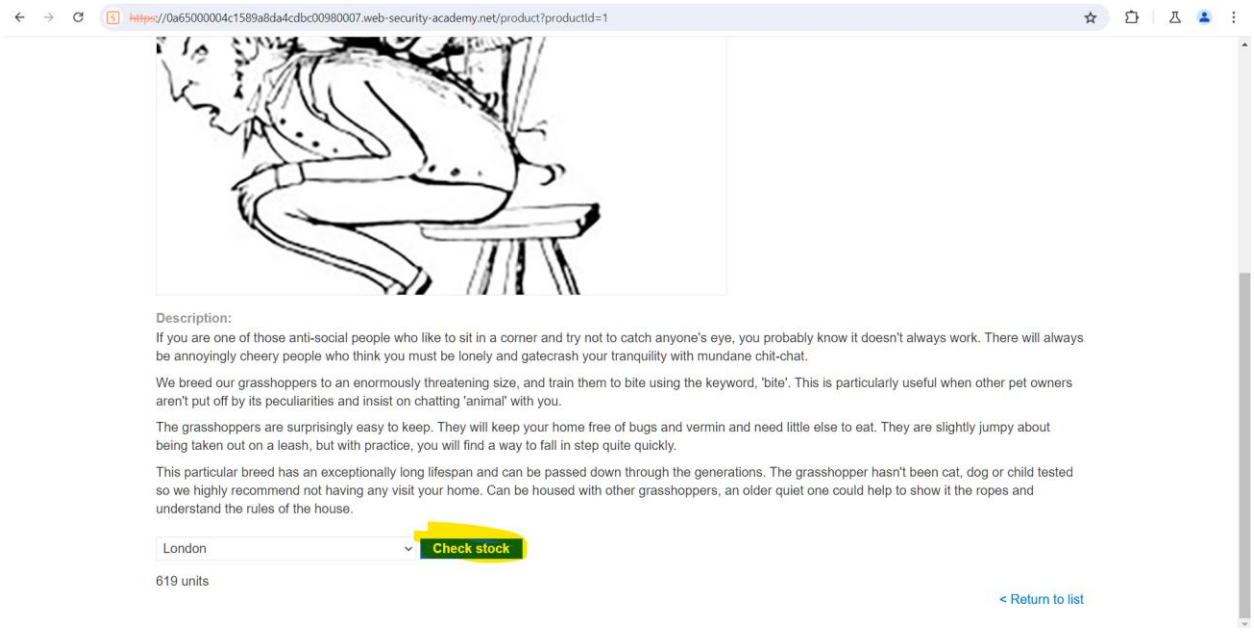
Under BurpSuite, the website requests will be passed to the proxy when I click on the product with the ID "1".



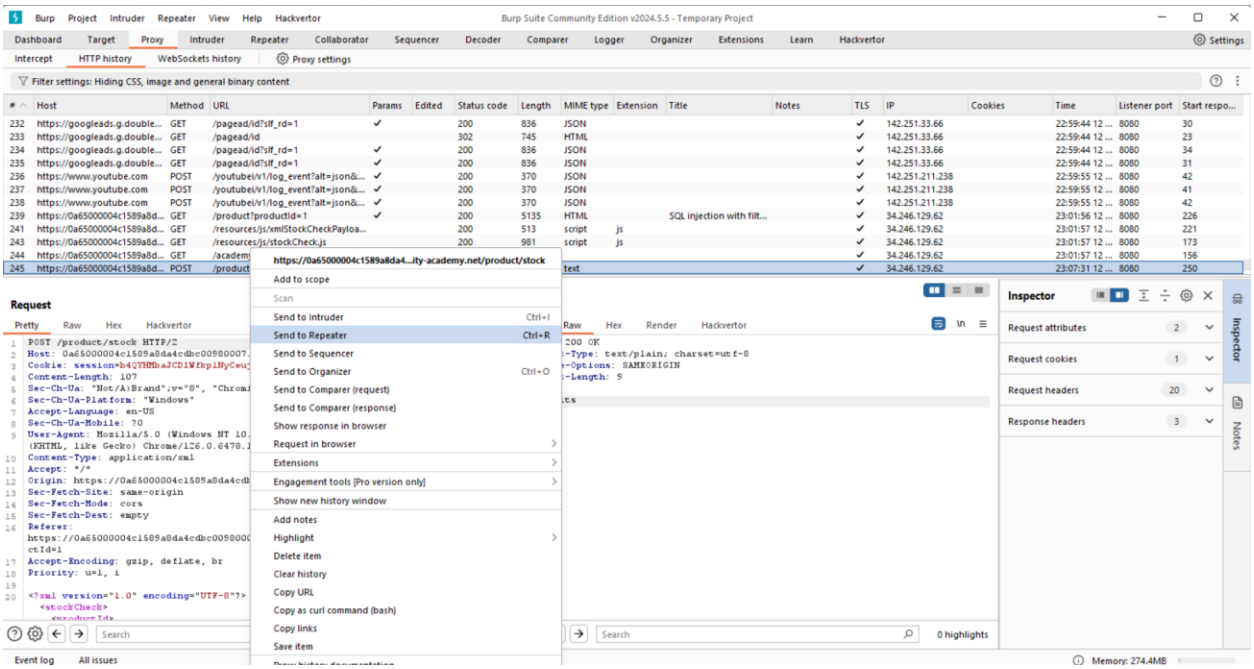
To modify the web request, send the selected request to the Repeater.



After that, click on "Check Stock" on the webpage.

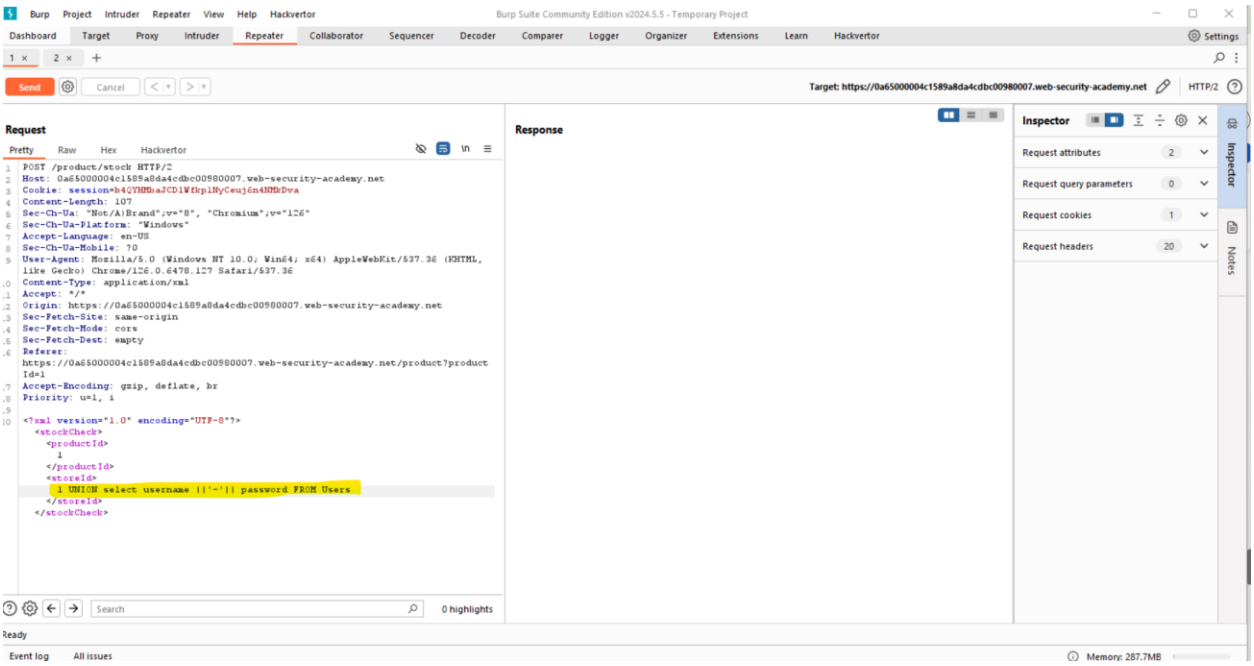


Now, under BurpSuite, send the "Check Stock" web POST request to the Repeater to modify it.



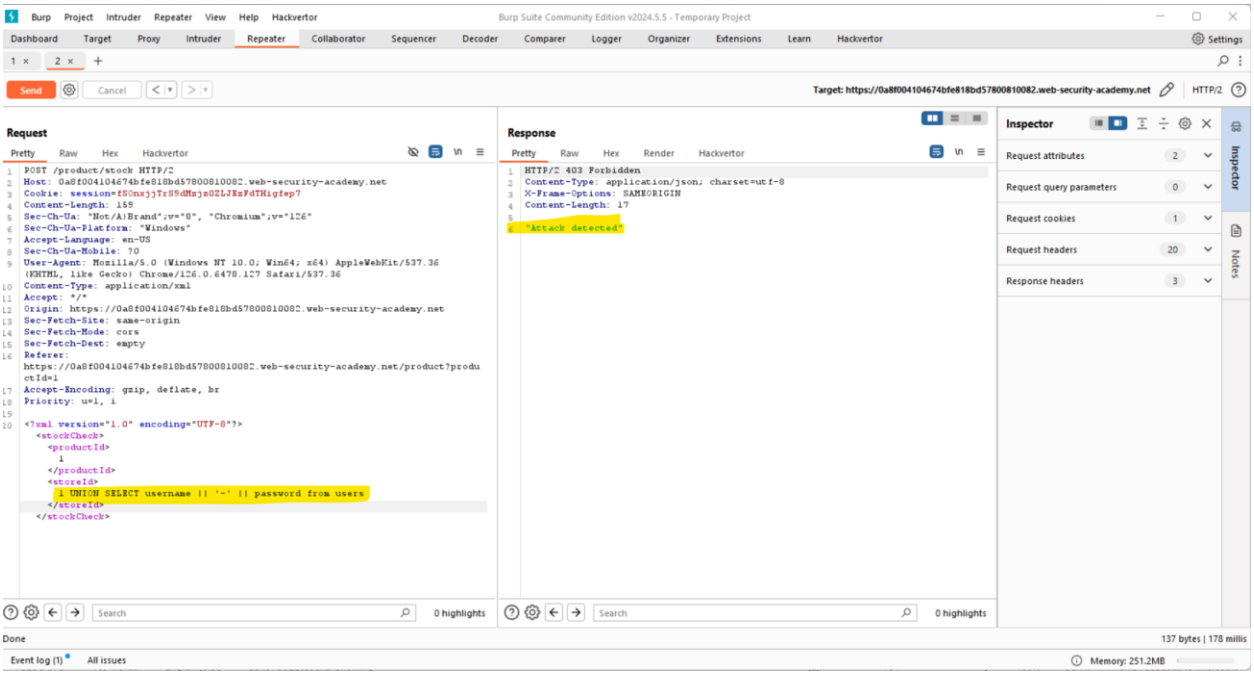
There is a vulnerability in the "Check Stock" feature, so I modified the POST request with an SQL query to fetch user credentials:

SQL query: SELECT 'some_column' UNION SELECT username || '~' || password FROM users;

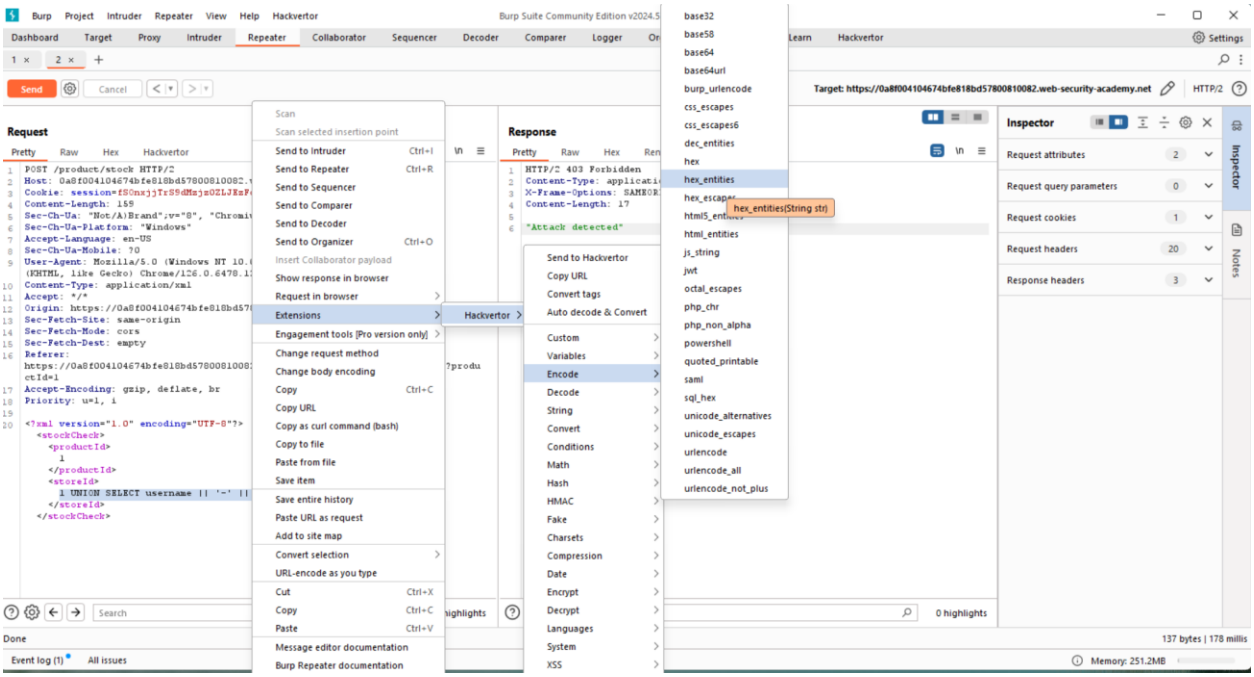


After encoding the query payload using the Hackvertor extension, we can fetch the user credentials of the application, as a basic SQL query payload would be blocked by the Web Application Firewall.

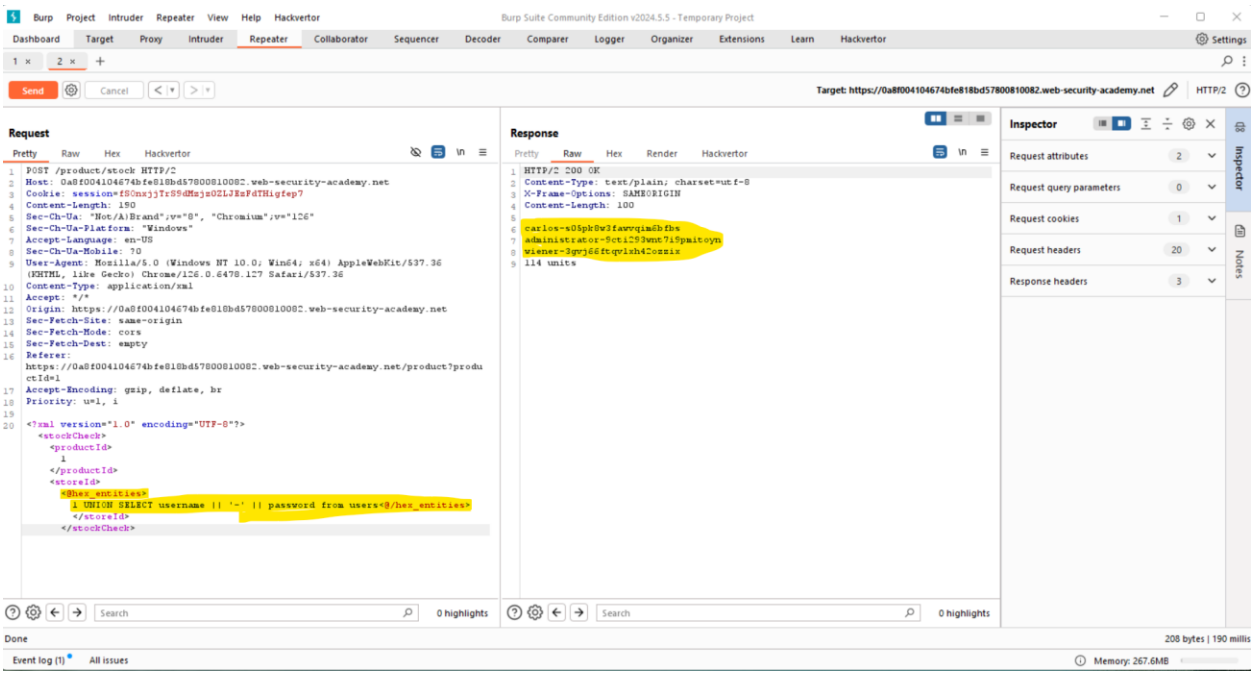
Basic SQL query payload:



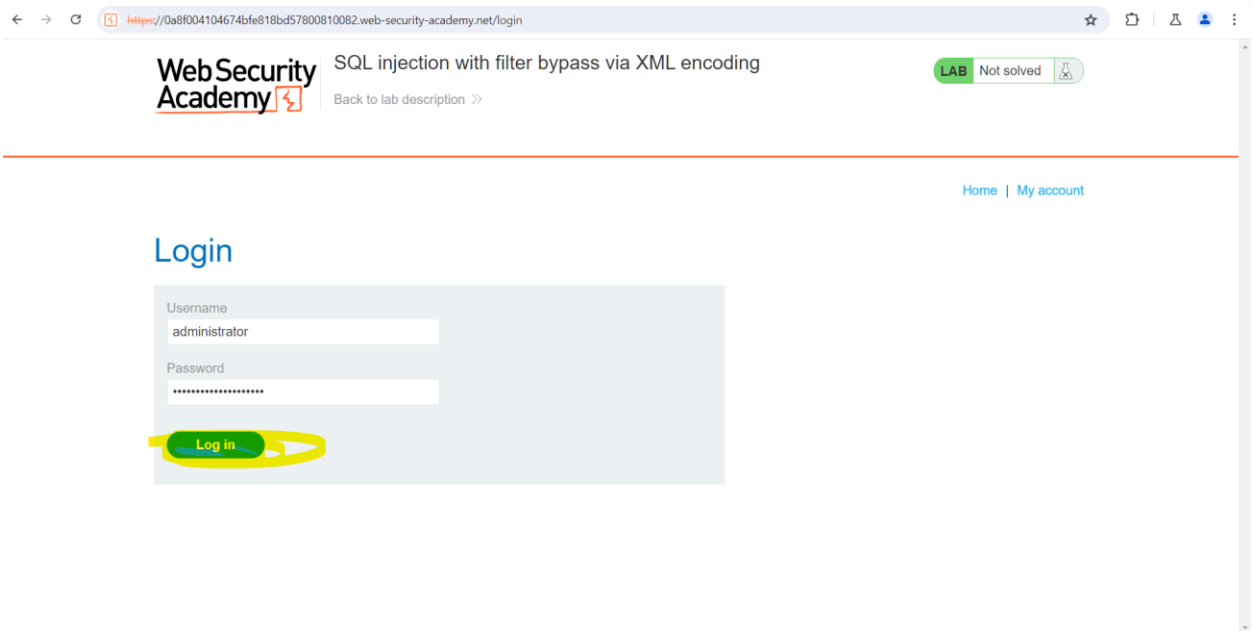
SQL payload after encoding

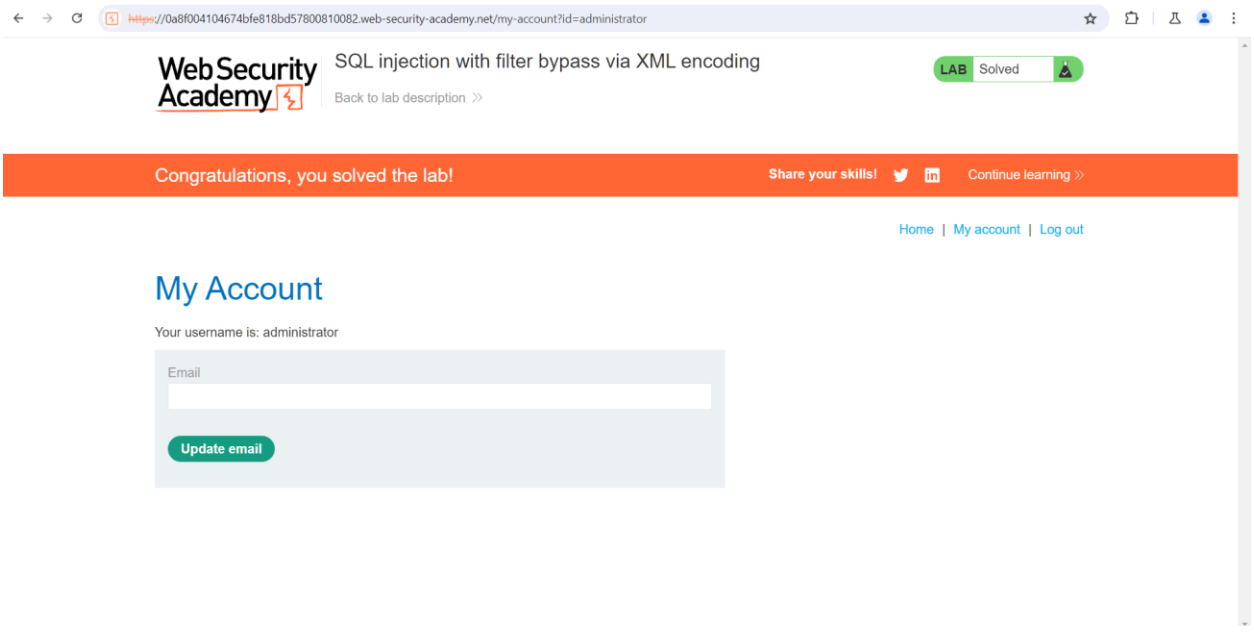


After encoding the payload , you can see the user credentials to access the web application



Finally performed SQL injection by logging with admin credentials
(username :administrator, password: 9cti293wnt7i9pmitoyn)




https://0a8f004104674bfe818bd57800810082.web-security-academy.net/my-account?id=administrator
Web Security Academy
SQL injection with filter bypass via XML encoding
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