COURSE: Ethical Hacking/Penetration Testing & Bug Bounty Hunting v2

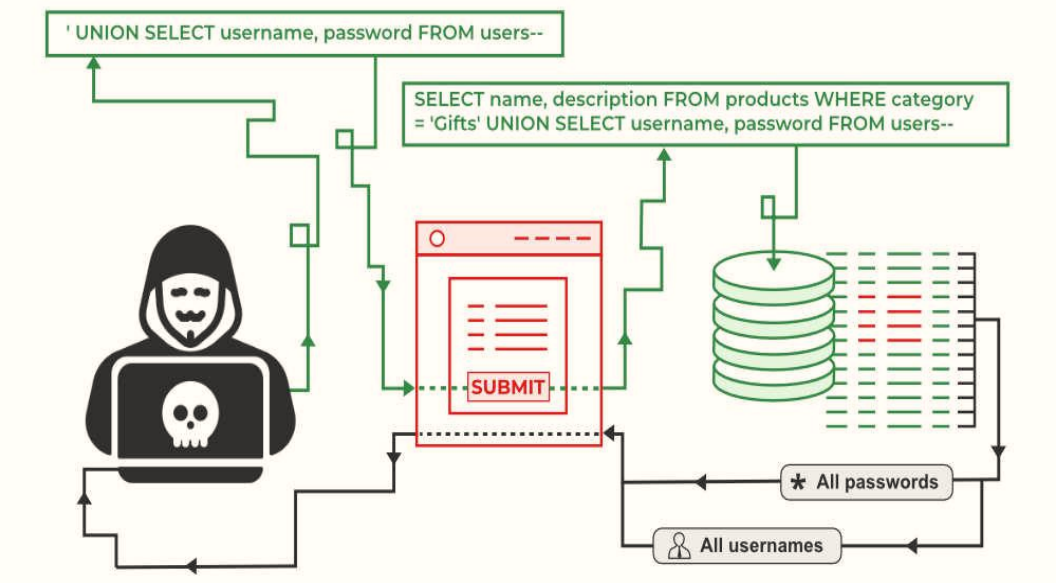
Unleash Your Cybersecurity Potential with Ethical Hacking, Penetration Testing & Bug Bounty Hunting v2

Introduction:

In a digital landscape teeming with complexities and vulnerabilities, the role of ethical hackers and penetration testers has never been more crucial. The relentless surge of cyber threats demands a new breed of cybersecurity professionals who are not only equipped with technical prowess but also possess an unyielding commitment to safeguarding digital assets. Welcome to the transformative Udemy course "Ethical Hacking / Penetration Testing & Bug Bounty Hunting v2." This article serves as your guide to understanding the rich tapestry of topics covered in this course, enabling you to embark on a journey that combines technical mastery with ethical responsibility.

❖ *Introduction to SQL Injection*

SQL injection is a cyberattack technique where malicious SQL code is inserted into input fields to manipulate or extract data from a database, potentially compromising its security.



❖ Lab from Portswigger for SQL Injection.

Link to the lab:
https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns

1. Lab Information.

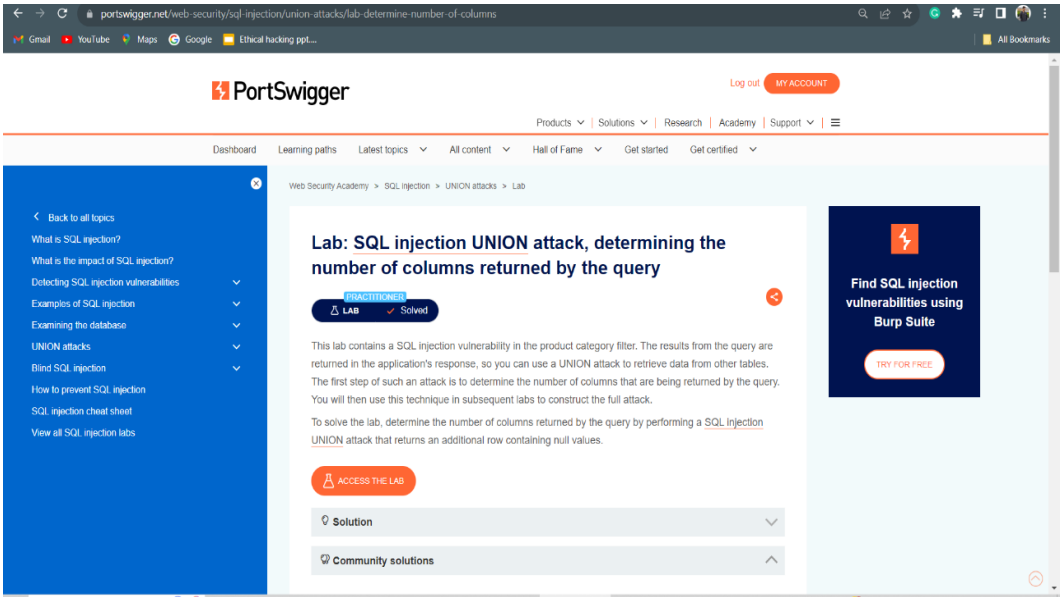


Figure 1 :-
The above figure shows the Description of the Lab

2. Modify the request that sets the product category filter using Burp Suite to intercept and alter it.

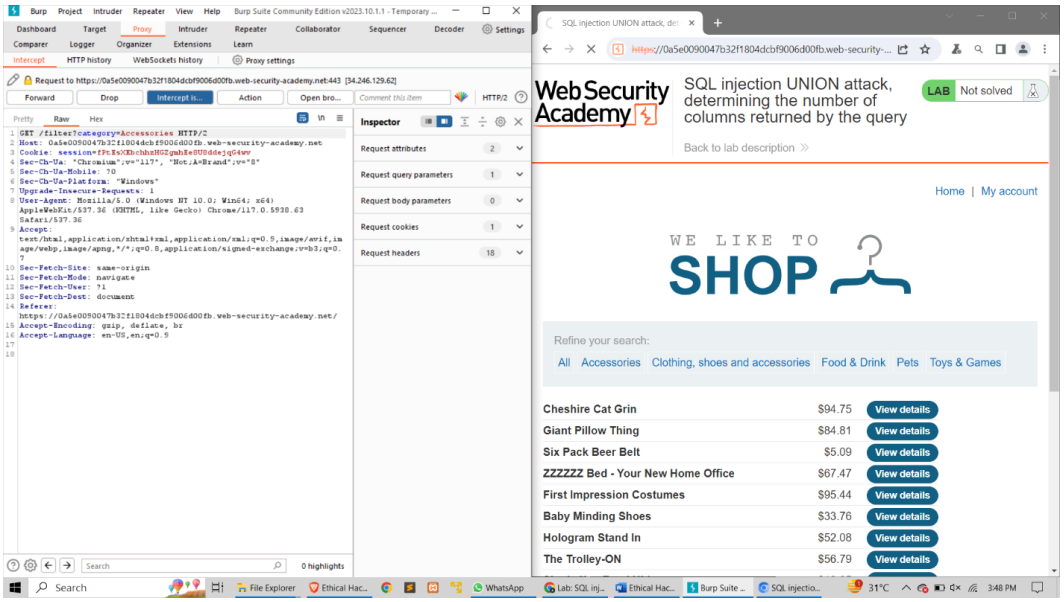


Figure 2 :-
The above figure shows that we have to change the product filter category after intercepting the request using the burp suite

3. **Change the category parameter by setting its value to '+UNION+SELECT+NULL-- and observe an error occurring.**

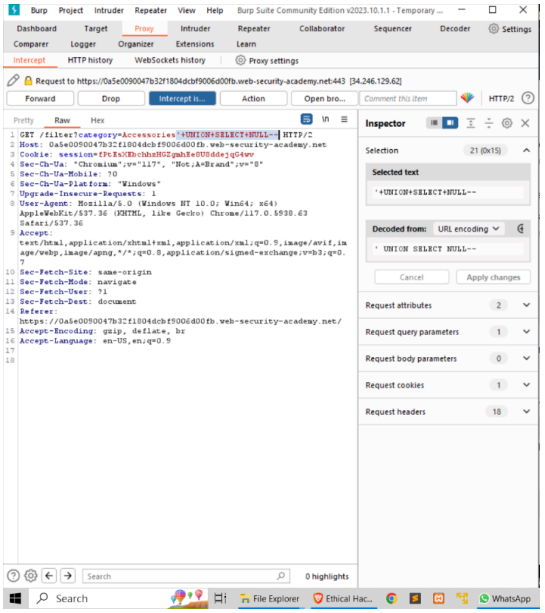


Figure 3 :-

The above figure shows that in the category parameter, we have to add our Union payload to manipulate the server

4. **To inject a null value into an additional column within the "category" parameter, you can use the following SQL injection payload: '+UNION+SELECT+NULL,NULL--**

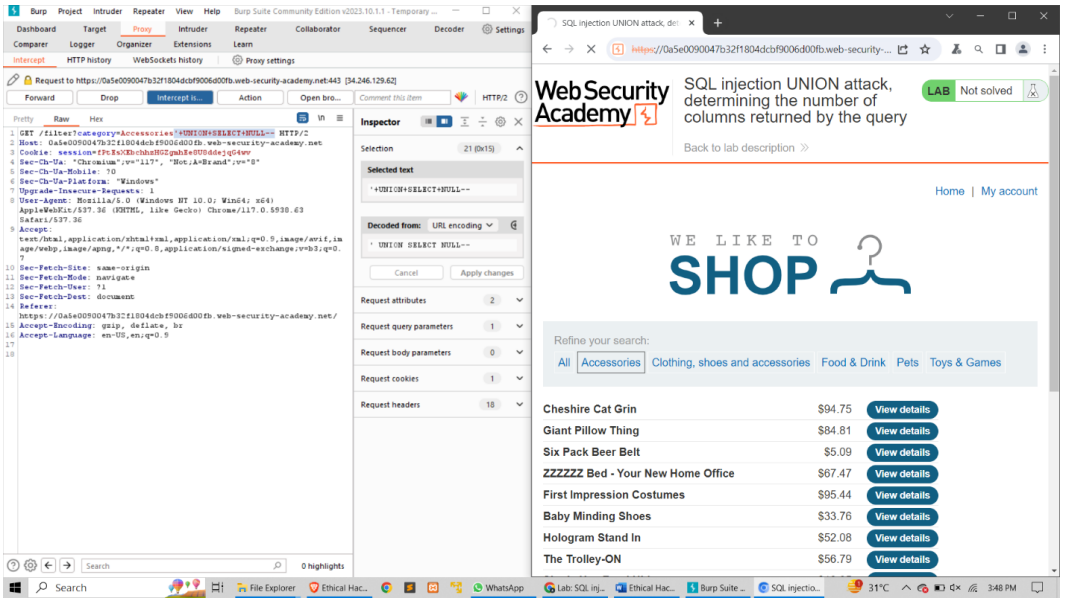


Figure 4 :-

The above figure shows that the payload injects a null value into an additional column within the "category" parameter.

5. ***Continue adding null values until the error disappears and the response includes additional content that contains the null values.***

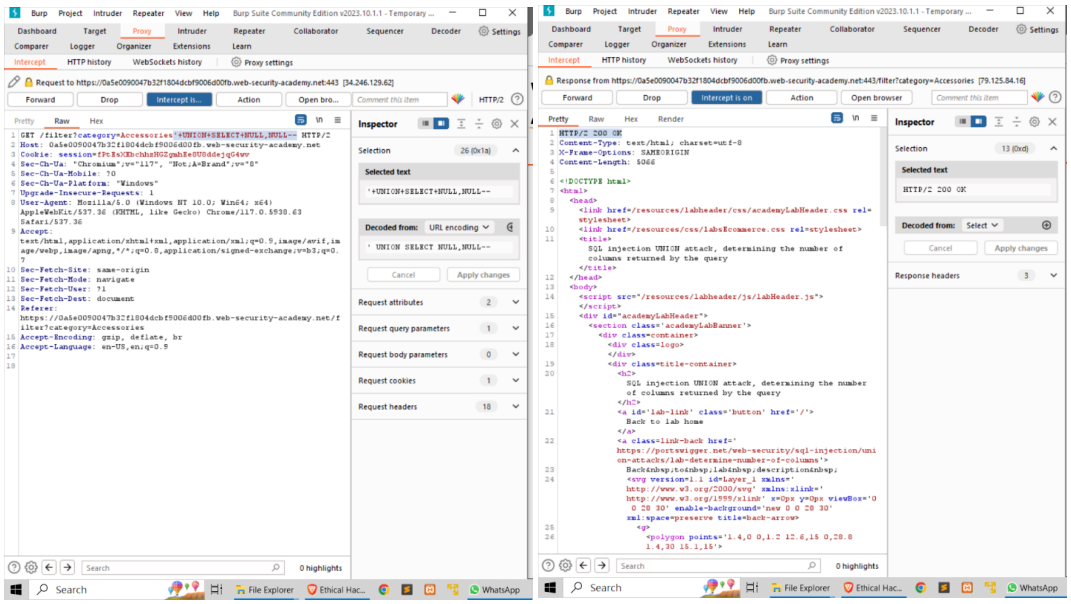


Figure 5 *:-*
The above figure shows that we have to add NULL value until we get a response of 200 Ok

For More Details:-
https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns