Solution and logic of Lab 1: UNION attack using SQL injection, determining the number of columns returned by a query

Understanding UNION Attack:

The UNION attack allows you to combine the results of two SQL queries. For a successful attack:

1. The number of columns in both queries must be the same.
2. The data types in the columns must be compatible.

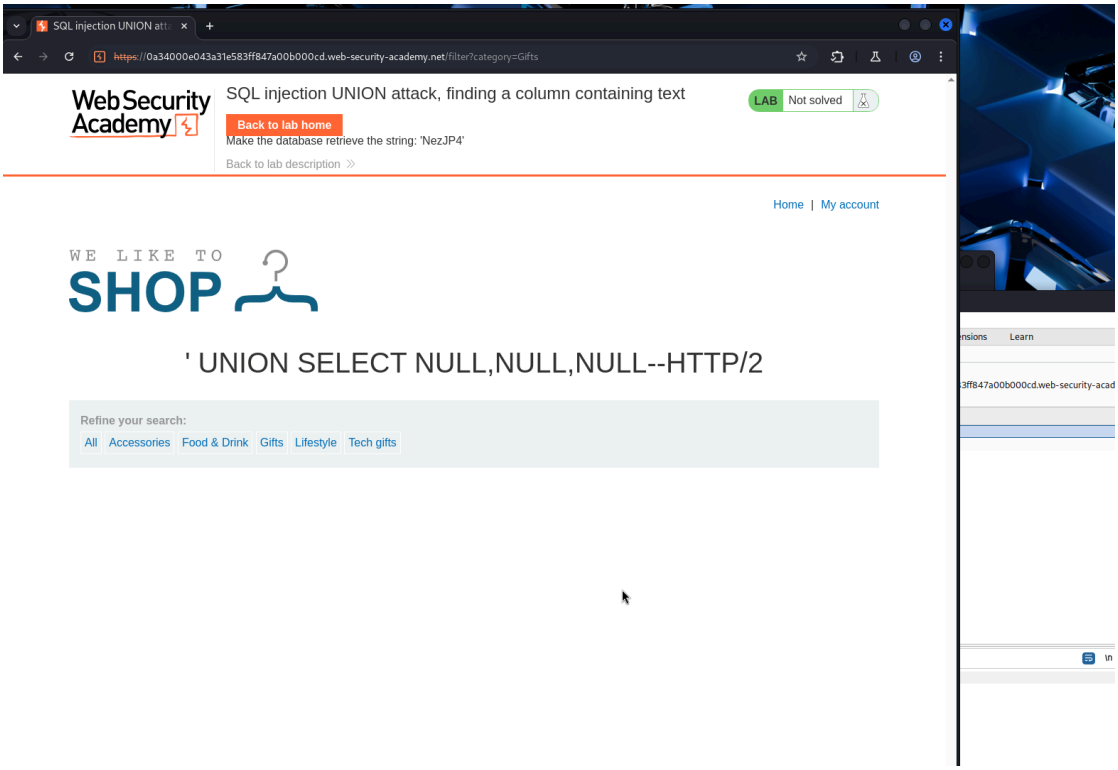
Task — determine how many columns the original query returns in order to properly construct a UNION attack.

Error checking

If the number of columns in the original query does not match the number of columns in the UNION attack, the server will return an error.

A query was entered '+UNION+SELECT+NULL,NULL,NULL–, as a result of which it became clear that:

The server returns a response without an error. This means that the original request returns 3 columns..



2 Lab: UNION attack using SQL injection, find column containing text

The next step is to define a column that is compatible with string data.

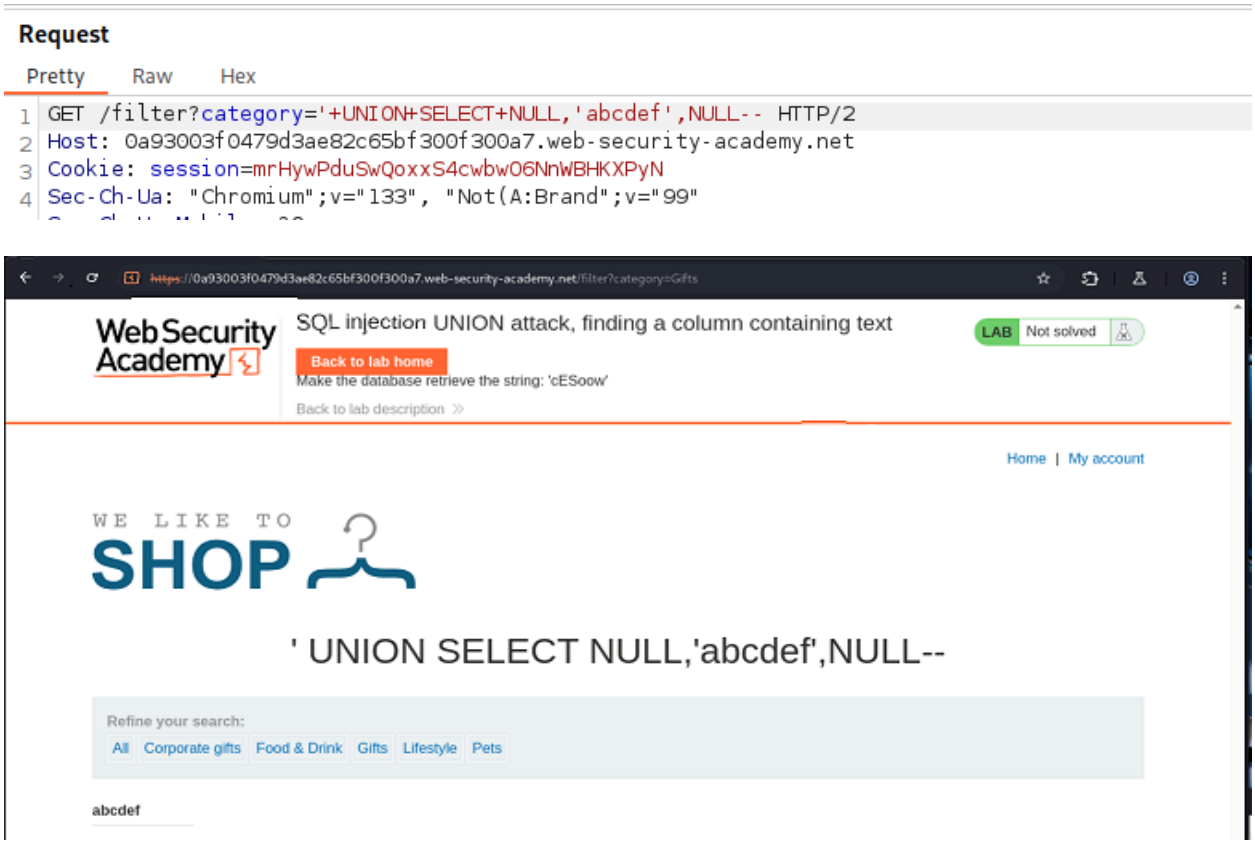
Let's determine the number of columns returned by the query. The query returns three columns using the following payload in the category parameter. To do this, replace each zero with a random value, for example (The lab provided a random value 'cESoow'):

'+UNION+SELECT+'cESoow',NULL,NULL--

'+UNION+SELECT+NULL,'cESoow',NULL--

'+UNION+SELECT+NULL,NULL,'cESoow'--

I have identified which columns are compatible with string data. The column that supports text data is 2:



3 Lab: UNION attack using SQL injection, extracting data from other tables

To solve the lab, a UNION attack using SQL injection is performed which will extract all usernames and passwords and use this information to login as the administrator user.

Used Burp Suite to intercept and modify the query, and also determined the number of columns returned by the query (1 and 2):

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

The payload was used to extract the contents of the users table.:

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

Next, authorization was required, information: