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

Problem: This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you first need to determine the number of columns returned by the query. You can do this using a technique you learned in a [previous lab](https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns). The next step is to identify a column that is compatible with string data.

Goal: perform a [SQL injection UNION](https://portswigger.net/web-security/sql-injection/union-attacks) attack that returns an additional row containing the value provided. This technique helps you determine which columns are compatible with string data.

Solve:

1-try to know the number of column

A screenshot of a computer

Description automatically generated

2-number of column that contain null🡪3

A screenshot of a computer

Description automatically generated

3-we try to know what is the column that didn’t null

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

4- category=Lifestyle'+union+select+NULL,'lx6o1i',NULL--

A screenshot of a computer

Description automatically generated