**Lab: SQL injection with filter bypass via XML encoding**

Problem: This lab contains a [SQL injection](https://portswigger.net/web-security/sql-injection) vulnerability in its stock check feature. 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

Goal: The database contains a users table, which contains the usernames and passwords of registered users. To solve the lab, perform a SQL injection attack to retrieve the admin user's credentials, then log in to their account.

Solve:

1-

A close up of a puppet

Description automatically generated

2- we try to access users table

A screenshot of a computer

Description automatically generated

3-

A screenshot of a computer

Description automatically generated

4-

A screenshot of a computer

Description automatically generated

5-

A screenshot of a computer

Description automatically generated

6- we will use hackvector to change the char

A screenshot of a computer

Description automatically generated

7-

A screenshot of a computer

Description automatically generated

8-

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Note:

And 🡪 encode🡪 hexa🡪 || '~' ||