Lab: SQL injection attack, querying the database type and version on MySQL and Micros

This lab demonstrates a SQL injection vulnerability in the product category filter.

The objective is to extract the database version string using a UNION-based SQL injection.

Solution Summary:

- Determine the number of columns returned and which columns accept string data.

- Use UNION SELECT payload to extract the database version from the server.

1. Access the lab environment. (Screenshot: 1-access-lab.png)

2. Navigate to the product category filter by clicking a category. (Screenshot: 2-click-category.png)

3. Intercept the filter request in Burp Suite. (Screenshot: 3-intercepted-request.png)

4. Modify the intercepted request to test columns:

   `'+UNION+SELECT+'abc','def'#`

   (Screenshot: 4-column-test.png)

5. Then modify the request to get DB version:

   `'+UNION+SELECT+@@version,NULL#`

   (Screenshot: 5-db-version.png)

6. Confirm that the lab is solved by checking for the version string. (Screenshot: 6-lab-solved.png)

Completed and documented by panpalli - May 2025