SCENARIO

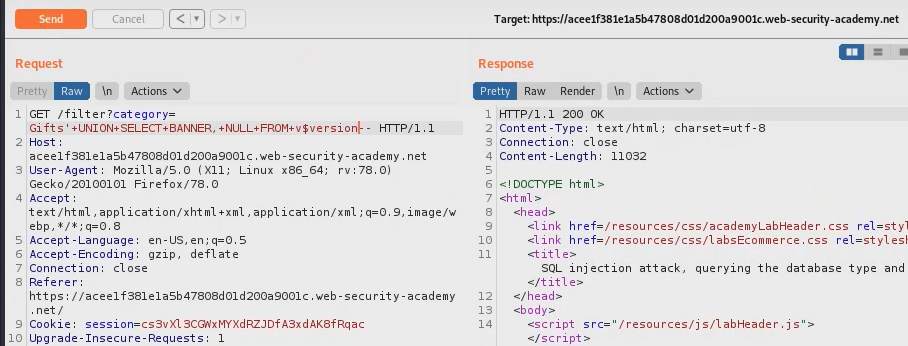
The product category filter in the application is susceptible to SQL injection. Given the use of an Oracle database, we aim to perform a UNION attack to retrieve specific data.

**PROCEDURE**

1. Use Burp Suite, capturing the request modifying the product category filter.
2. Determine the number of columns returned by the query. Confirm it by setting the category parameter to: '+UNION+SELECT+'abc','def'+FROM+dual--.
3. To unveil the database version, adjust the payload to: '+UNION+SELECT+BANNER,+NULL+FROM+v$version--.

**PAYLOAD**

'+UNION+SELECT+BANNER,+NULL+FROM+v$version--

**PROOF OF CONCEPT**

**REMEDIATION**

1. Always use parameterized SQL queries or prepared statements.
2. Deploy strict input validation rules.
3. Apply least privilege principles, ensuring database users have minimal necessary permissions.
4. Use a WAF to identify and block SQL injection attempts.
5. Regularly patch and update the database system to fix known vulnerabilities.