SCENARIO

Our application's product category filter is not immune to SQL injection. A UNION attack could retrieve results from an injected query, revealing sensitive data.

**PROCEDURE**

1. Intercept the request that modifies the product category filter using Burp Suite.
2. Confirm the number of columns returned by the query by setting the category parameter to: '+UNION+SELECT+'abc','def'#.
3. To retrieve the database version, adjust the payload to: '+UNION+SELECT+@@version,+NULL#.

**PAYLOAD**

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

**PROOF OF CONCEPT**

**REMEDIATION**

1. Adopt parameterized queries or prepared statements.
2. Implement rigorous input validation.
3. Utilize a WAF to detect malicious input patterns.
4. Keep the database and associated software updated.
5. Monitor database logs for unusual query patterns and act accordingly.