SCENARIO

A vulnerable product category filter in the application leaves an opening for SQL injection. The system constructs a SQL query based on the selected category, like:

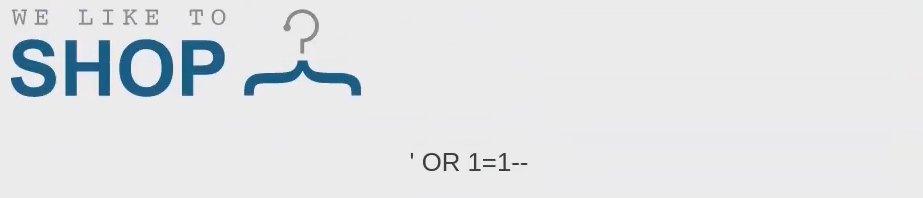
SELECT \* FROM products WHERE category = 'Gifts' AND released = 1

**PROCEDURE**

1. Initiate Burp Suite and intercept the request that sets the product category filter.
2. Alter the category parameter, replacing its value with '+OR+1=1--.
3. Forward the modified request and observe the response, looking for any unreleased products.

**PAYLOAD**

'+OR+1=1--

**PROOF OF CONCEPT**

**REMEDIATION**

1. Utilize parameterized SQL queries or prepared statements.
2. Implement strict input validation for all user inputs.
3. Use a web application firewall (WAF) to detect and block SQL injection attempts.
4. Regularly audit and review code, especially sections dealing with database operations.
5. Educate developers about the risks of SQL injection and how to code defensively against them.