SCENARIO

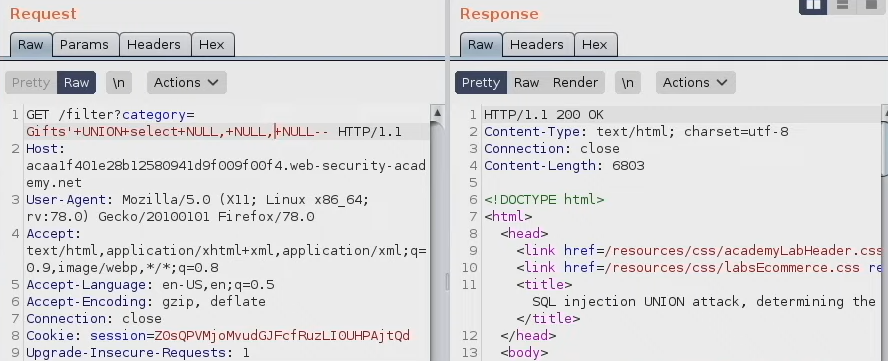
A SQL injection vulnerability is present in the application's product category filter. Using a UNION attack, we aim to detect the number of columns being returned and then explore a column compatible with string data.

**PROCEDURE**

1. Run Burp Suite and snare the request changing the product category filter.
2. By altering the category parameter to '+UNION+SELECT+NULL,NULL,NULL--, verify that the query is returning three columns.
3. Begin replacing each NULL with a random value provided by the lab until a successful response is received.

**PAYLOAD**

'+UNION+SELECT+'randomValue',NULL,NULL--

**PROOF OF CONCEPT**

**REMEDIATION**

1. Limit the permissions associated with database accounts, ensuring they can only perform necessary tasks.
2. Deploy an intrusion detection system to monitor traffic for signs of malicious activity.
3. Implement output encoding to neutralize any potentially harmful characters.
4. Regularly review and update the application codebase to address potential vulnerabilities.
5. Use web proxies to detect and mitigate SQL injection attacks in real-time.