Experiment: 1.4

Student Name: Yash Kumar
UID: 20BCS9256
Branch: BE-CSE
Section/Group: 616 –B
Semester: 5
Subject Code: 20CSP-338
Subject Name: Web and Mobile Security

Aim: Working of SQL Injection attack.

Software/Hardware Requirements:

a) Windows 7 or any version above.
b) AltoroMutual-Login (Database)

Steps:

1. Submitting the single quote character ' and looking for errors or other anomalies.
2. Submitting some SQL-specific syntax that evaluates to the base (original) value of the entry point, and to a different value, and looking for systematic differences in the resulting application responses.
3. Submitting Boolean conditions such as OR 1=1 and OR 1=2, and looking for differences in the application's responses.

Submitting payloads designed to trigger time delays when executed within anSQL query, and

looking for differences in the time taken to respond.

4. Submitting OAST payloads designed to trigger an out-of-band network interaction when executed within an SQL query, and monitoring for any resulting interactions.

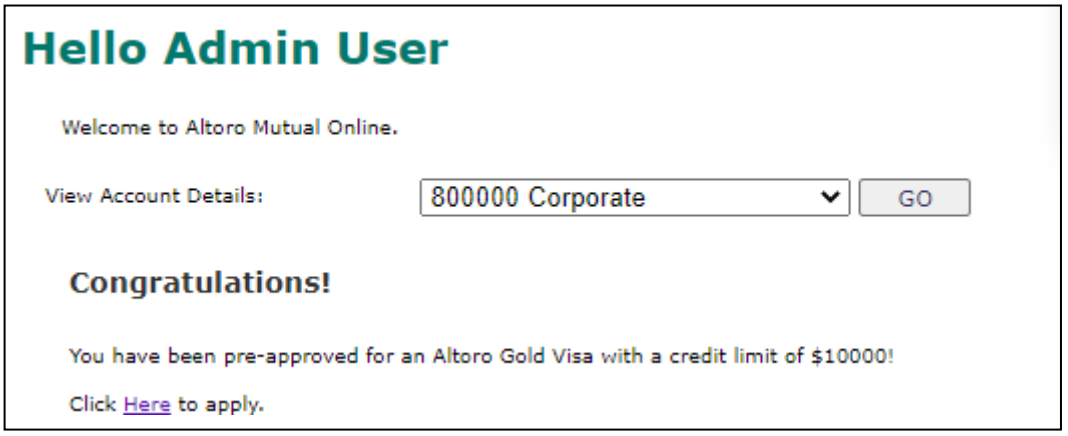
Output:

1. Opening Online Banking Login page:

2. Fill Username and Password:

3. After applying the SQL injection.

4. Access to the accounts (Database).



Learning Outcomes:

1. We have learned how to find SQL Injection attack.
2. An overview of how theseattacks are constructed and applied to real system.
3. If the app or website lacks proper data sanitization, the malicious link executes the attacker's chosen codeon the user's system.
4. As a result, the attacker can steal the user's active sessioncookie and can be the harmful for the website.