
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:



AltoroMutual

Online Banking Login

Username:

Password:

Login

DEMO SITE ONLY

Privacy Policy | Security Statement | Service Status Check | BEE7 API | © 2022 Altoro Mutual, Inc.

2. Fill Username and Password:

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

Online Banking Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username:

Password:

Login

DEMO SITE ONLY

3. After applying the SQL injection.

AltoroMutual

MY ACCOUNT PERSONAL SMALL BUSINESS

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [here](#) to apply.

DEMO SITE ONLY

4. Access to the accounts (Database).

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Learning Outcomes:

1. We have learned how to find SQL Injection attack.
2. An overview of how these attacks 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 code on the user's system.
4. As a result, the attacker can steal the user's active session cookie and can be the harmful for the website.