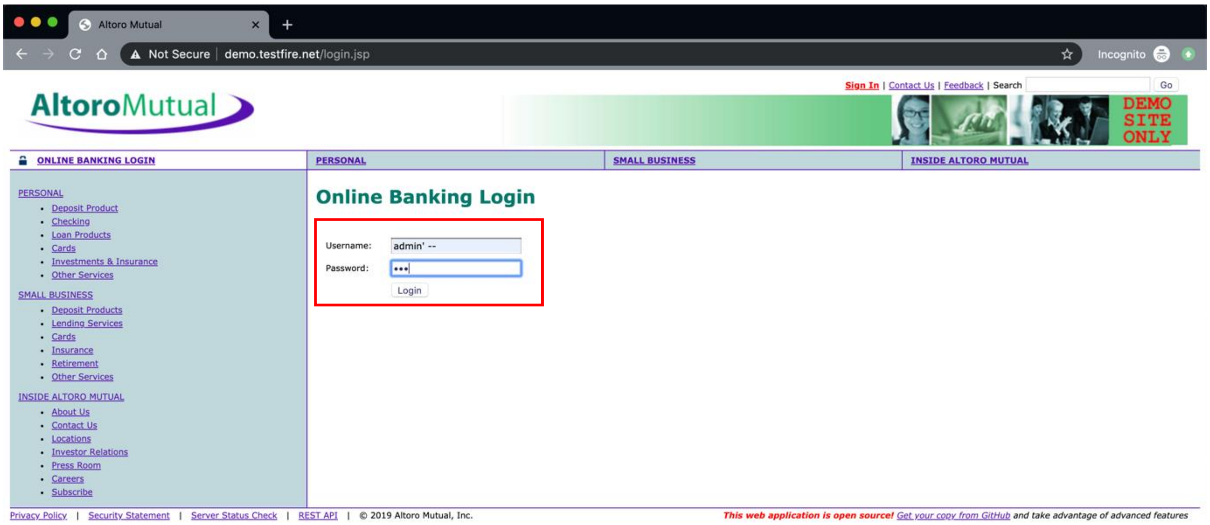
Exercise-1: SQL Injection

1. Circumventing the check for a correct password:

   In order to skip the check for password, we can add SQL comment i.e. '--' at the end of username field. If the SQL query is formed by concatenation, all the code after '-- ' will not be executed. Hence, the database won't equate the password field.

   Following screenshots explain the before mentioned working of circumventing password check for the user **'admin'**. Here, few random characters are added in the password field to overcome client side **null value** validation.

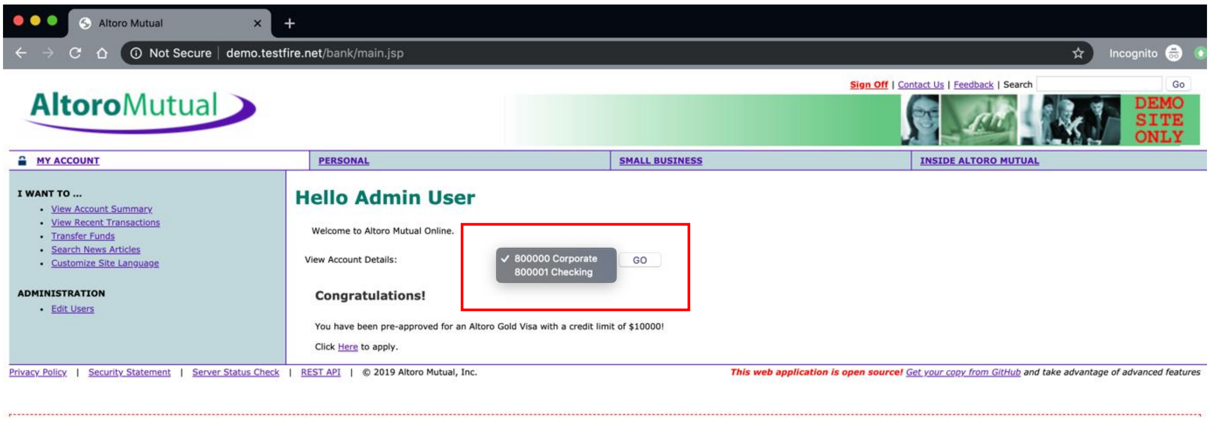


Online Banking Login

Username: admin' --

Password: •••

Login



Altoro Mutual
Not Secure | demo.testfire.net/bank/main.jsp
Incognito
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
Privacy Policy | Security Statement | Server Status Check | REST API | © 2019 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: ✓ 800000 Corporate
800001 Checking GO

Congratulations!

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

Click Here to apply.

After login we can view the account details for the accounts 800000 and 800001 that belong to user 'admin'.