

CYBER SECURITY JULY MINOR PROJECT

PROBLEM STATEMENT

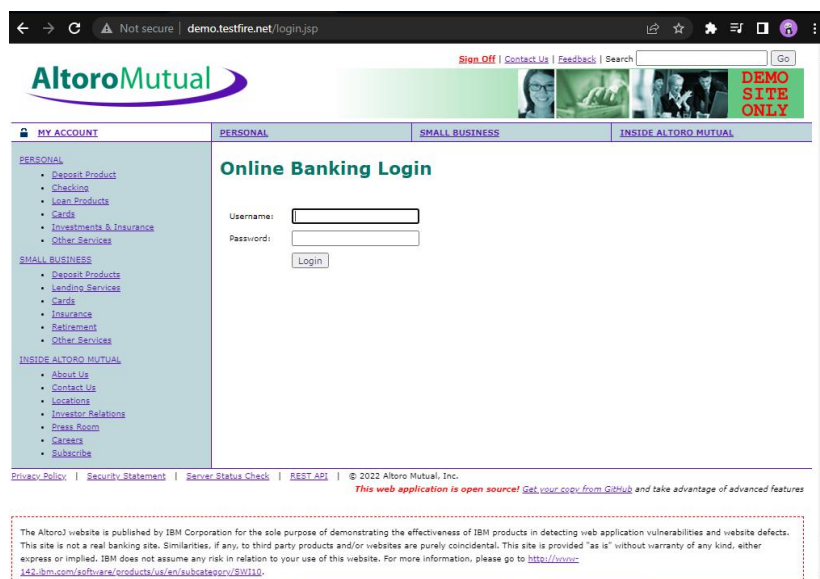
4.

Perform Bypass Authentication on <http://demo.testfire.net> website with different payloads and make report along with screenshots and mention to mitigation steps to protect.

INTRODUCTION

Bypass authentication refers to an attacker gaining access equivalent to an authenticated user without ever going through an authentication procedure. This is usually the result of the attacker using an unexpected access procedure that does not go through the proper checkpoints where authentication should occur.

REPORT



i)

← → ↻ ⚠ Not secure | demo.testfire.net/login.jsp

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

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:

Password:

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 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-142.ibm.com/software/products/us/en/subcategory/SW110>.

← → ↻ ⚠ Not secure | demo.testfire.net/bank/main.jsp

Sign Off | Contact Us | Feedback | Search Go

AltoroMutual

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: 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 | © 2022 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-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2022, IBM Corporation. All rights reserved.

In above screenshots the username and password is same.

ii)

← → ↻ ⚠ Not secure | demo.testfire.net/login.jsp

Sign In | Contact Us | Feedback | Search Go

AltoroMutual

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

Syntax error: Encountered "\'" at line 1, column 79.

Username:

Password:

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features

← → ↻ ⚠ Not secure | demo.testfire.net/bank/main.jsp

Sign Off | Contact Us | Feedback | Search Go

AltoroMutual

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: 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 | © 2022 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-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

In above screenshots the password is 'foo'.

iii)

The screenshot shows the AltoroMutual login page. The browser address bar indicates the URL is `demo.testfire.net/login.jsp`. The page features the AltoroMutual logo and a navigation menu with links for [Sign Off](#), [Contact Us](#), [Feedback](#), and a search bar. A banner on the right side of the header reads "DEMO SITE ONLY". The main content area is titled "Online Banking Login" and displays a red error message: "Syntax error: Encountered '\ ' AND PASSWORD='\ ' at line 1, column 60." Below the message are input fields for "Username:" (containing "' or 1=1--+") and "Password:" (containing "*****"), followed by a "Login" button. The left sidebar contains links for "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The footer includes a disclaimer stating the site is published by IBM Corporation for testing purposes and a copyright notice for 2022 Altoro Mutual, Inc.

The screenshot shows the AltoroMutual main page after a successful login. The browser address bar indicates the URL is `demo.testfire.net/bank/main.jsp`. The page features the AltoroMutual logo and a navigation menu with links for [Sign Off](#), [Contact Us](#), [Feedback](#), and a search bar. A banner on the right side of the header reads "DEMO SITE ONLY". The main content area is titled "Hello Admin User" and displays a welcome message: "Welcome to Altoro Mutual Online." Below the message is a "View Account Details:" section with a dropdown menu showing "800000 Corporate" and a "GO" button. The page also displays a "Congratulations!" message and a notification: "You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply." The left sidebar contains links for "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The footer includes a disclaimer stating the site is published by IBM Corporation for testing purposes and a copyright notice for 2008, 2022, IBM Corporation, All rights reserved.

In above screenshots the password is 'foo'.

MITIGATION STEPS FOR PROTECTION:

This vulnerability can be eliminated by fixing the SQL injection vulnerability in the application's authentication mechanism.

The authentication bypass vulnerability is a special case of SQL injection, specifically located in your authentication routines.

The following recommendations will help to mitigate the risk of Authentication Bypass attacks:

- Keep up to date on patches and security fixes as they are released by the vendor or maintainer

- You always check for all vulnerabilities and always install the best antivirus software and are always free from bugs.

- To Avoid the special character '=' 'or' to bypass authentication, you can use the "mysql_real_escape_string()".

- It is best to have a secure and strong authentication policy in place.

- Avoid using external SQL interpreters.

- It is best to ensure all systems, folders, apps, are password protected.

- Audit your applications frequently for points where HTML input can access interpreters.

- Security experts recommend resetting default passwords with unique strong passwords and periodically rotate passwords.

- It is suggested to not expose authentication protocol in the client-side web browser script.

- They suggest ensuring that user session IDs and cookies are encrypted.

- It is recommended to validate all user input on the server side.

- Avoid the use of dynamic SQL or PL/SQL and use bound variables whenever possible.

Enforce strict limitations on the rights to database access.

Remove any sample applications or demo scripts that allow remote database queries.
