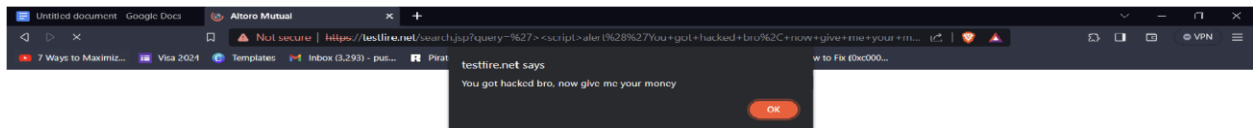


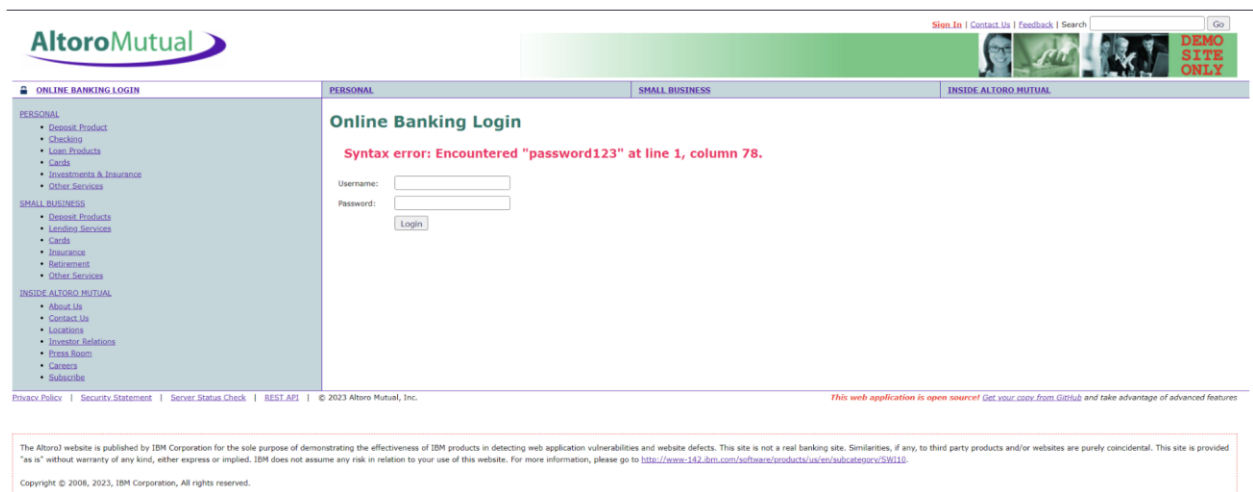
## Assignment-1

### 1)Injection

Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. For example, an attacker could enter SQL database code into a form that expects a plaintext username. If that form input is not properly secured, this would result in that SQL code being executed. This is known as an SQL injection attack.



As we can see, This website is vulnerable to HTML Injections This error shows that the website is vulnerable to SQL injections.



Basically if the query returns true, we can log in, but since this db is vulnerable to sql injection, we can write a basic statement that is true, inorder to get a true response and trick system into authenticating us.

– is comment.

## 2. Broken Authentication

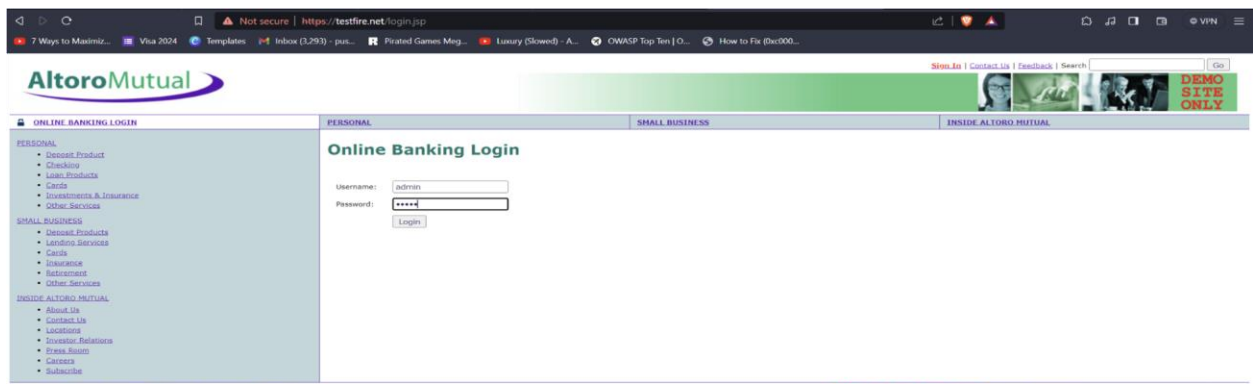
If the users identity is able to be spoofed or jeopardized.

Permitting wellknown passwords..

Permitting Automated Attacks like credential stuffing.

Permitting bruteforce attacks.

Wellknown common passwords are used here.



The screenshot shows the AltoroMutual website's login page. The browser address bar indicates the URL is <https://testfire.net/login.jsp>. The page has a navigation bar with links for 'Sign In', 'Contact Us', 'Feedback', and 'Search'. Below the navigation bar, there are tabs for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is selected, and the 'Online Banking Login' form is displayed. The form has fields for 'Username' (containing 'admin') and 'Password' (containing 'admin'). A 'Login' button is at the bottom of the form. The left sidebar contains links for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The footer contains a disclaimer and copyright information.

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

Online Banking Login

Username: admin

Password: admin

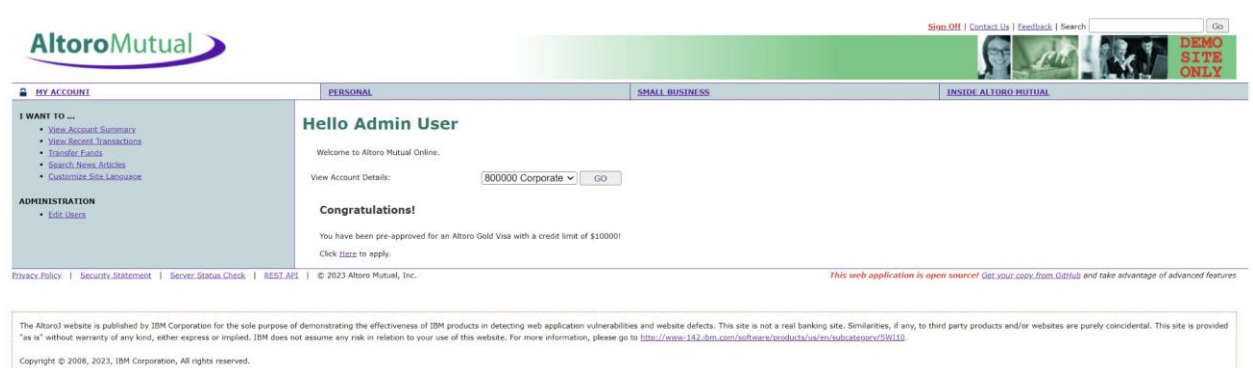
Login

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

This web application is open source! Get your copy from [Github](https://github.com) 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/subcategory506145>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.



The screenshot shows the AltoroMutual website's account page. The browser address bar indicates the URL is <https://testfire.net/login.jsp>. The page has a navigation bar with links for 'Sign Out', 'Contact Us', 'Feedback', and 'Search'. Below the navigation bar, there are tabs for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is selected, and the 'Hello Admin User' page is displayed. The page shows the account details for 'Admin User' with a balance of '800000 Corporate'. A 'GO' button is next to the balance. The left sidebar contains links for 'MY ACCOUNT' and 'ADMINISTRATION'. The footer contains a disclaimer and copyright information.

AltoroMutual

Sign Out | Contact Us | Feedback | Search

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

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](https://github.com) 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/subcategory506145>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Using wellknown password as Admin/Admin we logged in easily.

### 3) Cross Site Scripting (XSS)

By using HTML we can see that this website is vulnerable to XSS attacks.

Ex: `'><script>alert('You got hacked bro, now give me your money')</script>`



### 4) Broken Access Control

If user is able to go outside of their intended permissions we have a case of Broken Access Control. Ex is modifying the URL of page to get there.

<https://testfire.net/bank/showAccount?listAccounts=4539082039396>

[288](https://testfire.net/bank/showAccount?listAccounts=4485983356242) OR <https://testfire.net/bank/showAccount?listAccounts=4485983356242>

Even though i am not logged into this different users account. I can still access by just pasting the URL alone.

Not secure | https://testfire.net/bank/showAccount?listAccounts=4485983356242217

7 Ways to Maximiz... Visa 2024 Templates Inbox (3,293) - pus... Pirated Games Meg... Luxury (Slowed) - A... OWASP Top Ten | O... How to Fix (huc000...

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

**Account History - 4485983356242217 Credit Card**

**Balance Detail**

| 4485983356242217 Credit Card         | Select Account | Amount     |
|--------------------------------------|----------------|------------|
| Ending balance as of 8/28/23 7:28 AM |                | \$10000.97 |
| Available balance                    |                | \$10000.97 |

**10 Most Recent Transactions**

| Date | Description | Amount |
|------|-------------|--------|
|      |             |        |
|      |             |        |
|      |             |        |
|      |             |        |
|      |             |        |
|      |             |        |
|      |             |        |
|      |             |        |
|      |             |        |
|      |             |        |

**Credits**

| Account    | Date       | Description | Amount |
|------------|------------|-------------|--------|
| 1001180140 | 12/29/2004 | Paycheck    | 1200   |
| 1001180140 | 01/12/2005 | Paycheck    | 1200   |
| 1001180140 | 01/29/2005 | Paycheck    | 1200   |
| 1001180140 | 02/12/2005 | Paycheck    | 1200   |
| 1001180140 | 03/01/2005 | Paycheck    | 1200   |
| 1001180140 | 03/15/2005 | Paycheck    | 1200   |