PROJECT

Date: 13-10-2023

Team ID: Team-593479 (2.9)

Team Members:

Ramar Priya Maha Lakshmi

Chevala Syam Sai

Panchada Varun

Mulumudi Prabhas

1. Exploring the Vulnerabilities of Practice website.

a. **Vulnerability:** SQL injection

CWE: CWE-89

OWASP Category: A03 2021-Injection

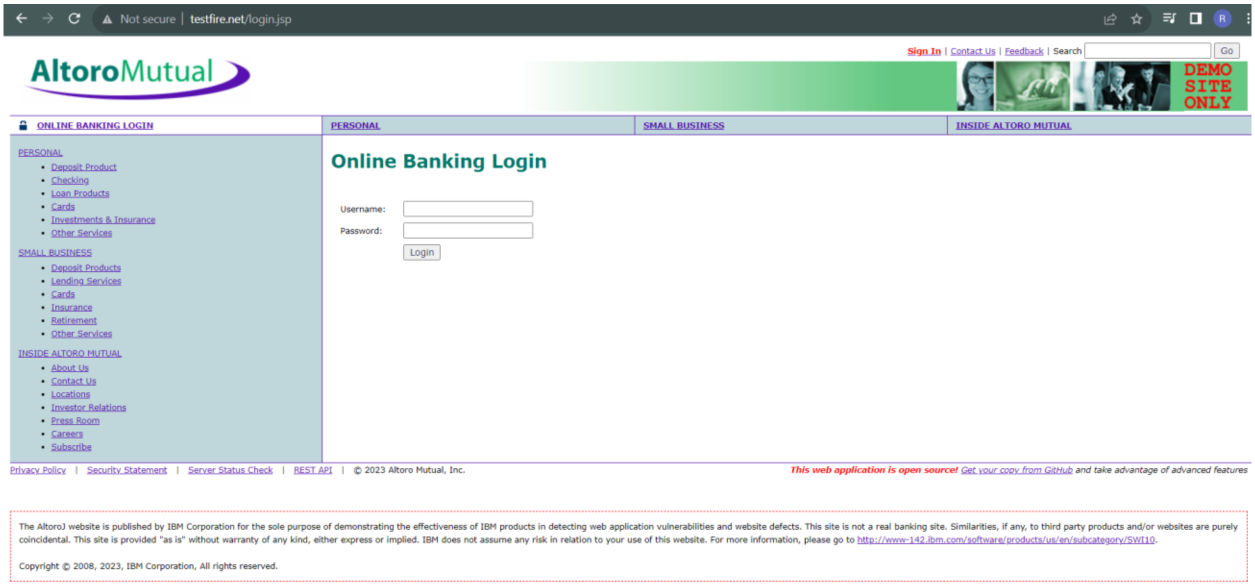
Description: The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Business Impact: SQL injection can have severe consequences, including data breaches, financial losses, damaged reputation, and legal repercussions for businesses. Attackers exploit vulnerabilities to gain unauthorized access to databases, steal sensitive information, and disrupt operations. The fallout often includes financial liabilities, regulatory fines, loss of customer trust, and the cost of remediation efforts to fix the vulnerabilities and recover from the breach.

Vulnerability Path: http://testfire.net/login.jsp

Steps to Reproduce:

1. Access the URL.



Online Banking Login

Username:

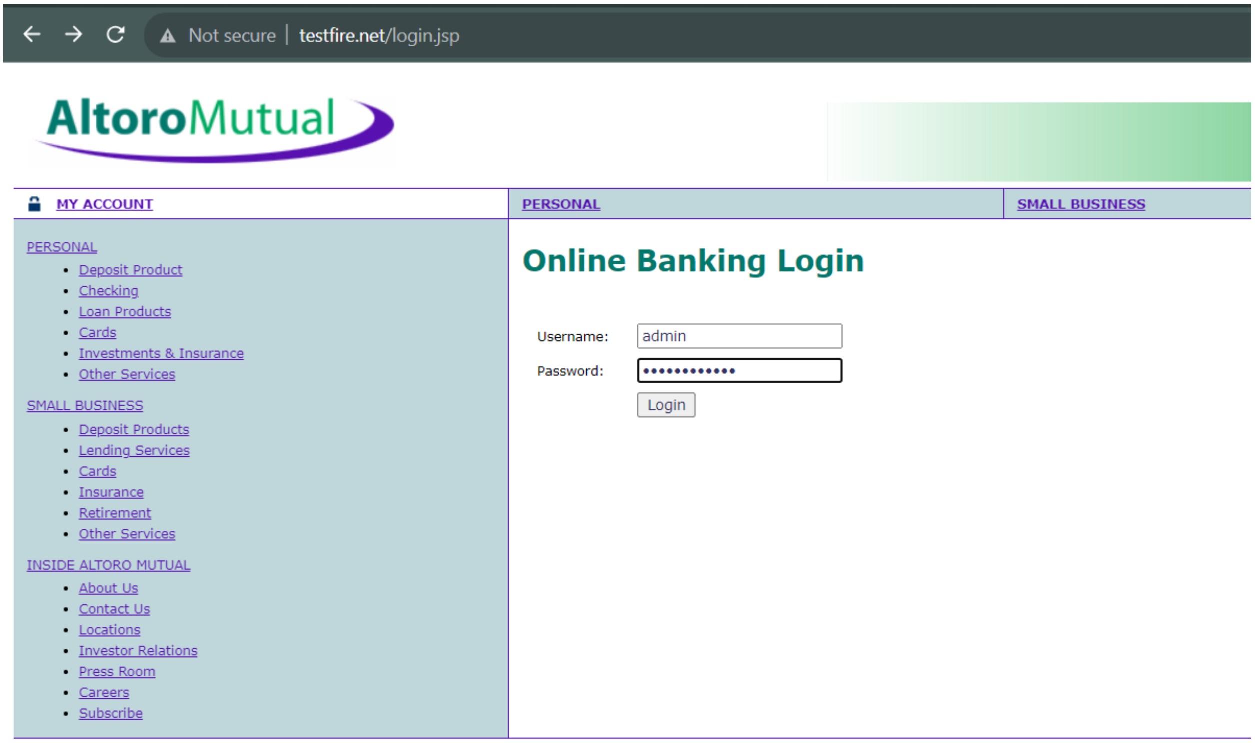
Password:

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/SWI10.

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

2. Enter the Username with “admin” and Password with “ ‘or 1=1--+".



Online Banking Login

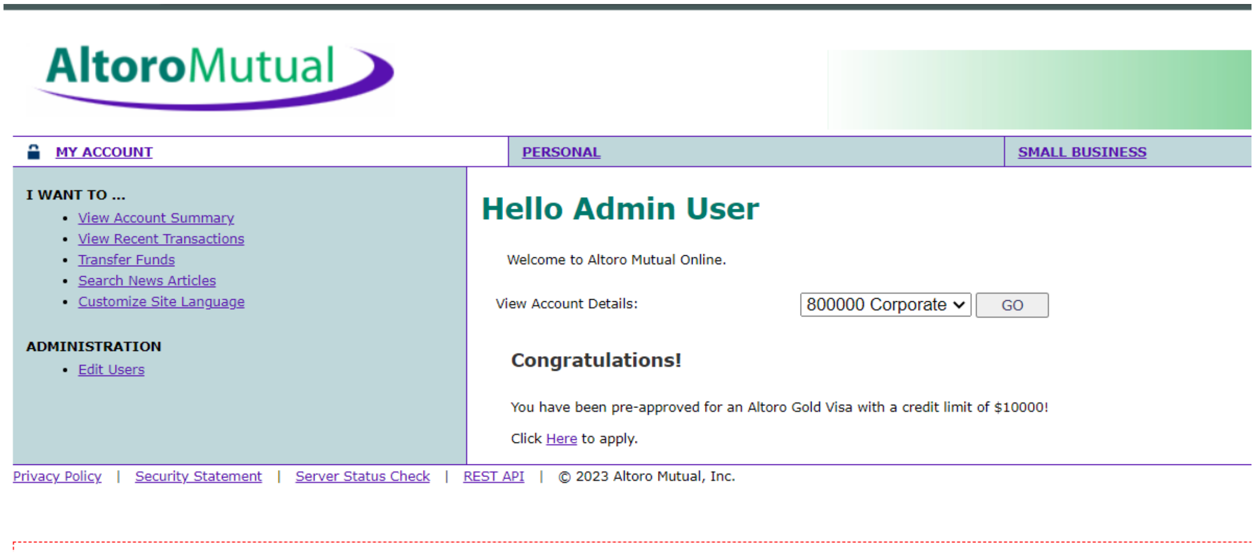
Username: admin

Password: ••••••••••••

In the above screenshot, when the user enters unanticipated input (i.e. payload) as **‘ or 1=1 --+** , the dynamically generated SQL query will be generated as below:

- Select * from Users where username= **admin** and password = **‘ or 1=1--+.**

3. Admin credentials are acquired.



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

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

Click Here to apply.

Recommendation:

- Use Prepared Statements and Parameterized Queries.
- Input Validation and Whitelisting.

b. **Vulnerability:** Cross Site Scripting (XSS)

CWE: CWE-87

OWASP Category: A03 2021-Injection

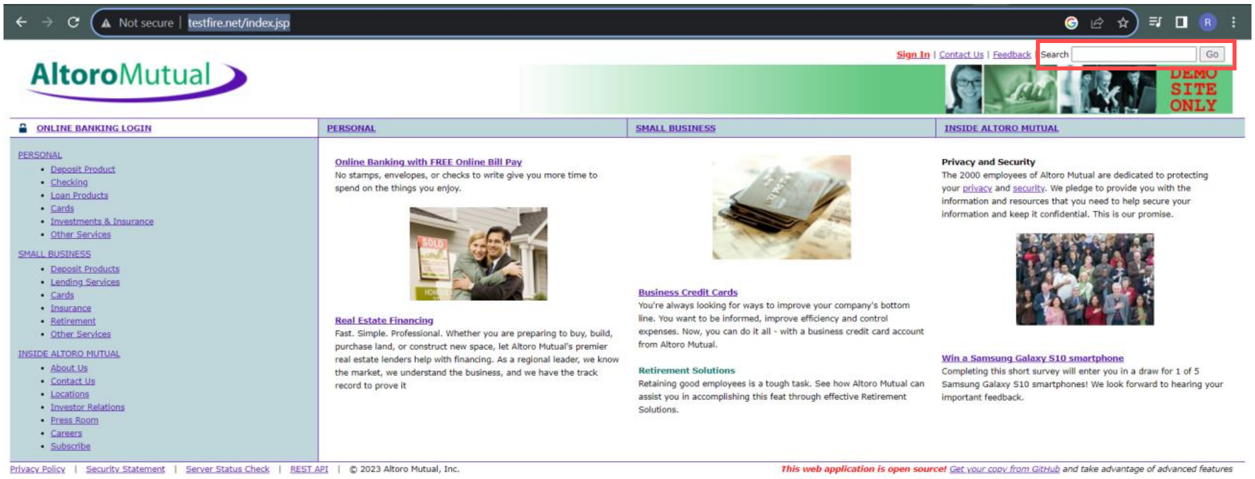
Description: The product does not neutralize or incorrectly neutralizes user-controlled input for alternate script syntax.

Business Impact: Attackers can use XSS to execute malicious scripts on the users in this case victim browsers. Since the browser cannot know if the script is trusty or not, the script will be executed, and the attacker can hijack session cookies, deface websites, or redirect the user to an unwanted and malicious website.

Vulnerability Path: http://testfire.net/index.jsp

Steps to Reproduce:

1. Go to the search bar of the given URL.



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.

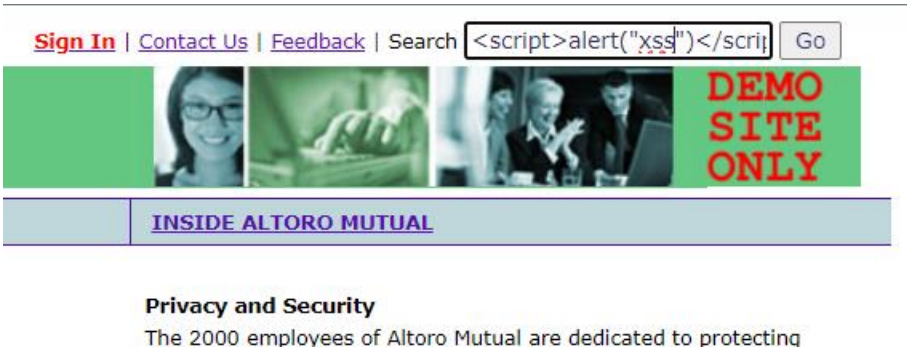
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

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.

© 2023 Altoro Mutual, Inc.

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

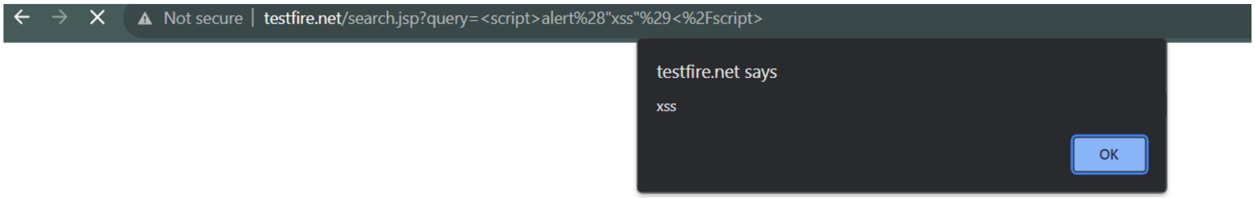
2. Execute any javascript code.



<script>alert("xss")</scri

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting

3. Click on Go.


Not secure | testfire.net/search.jsp?query=<script>alert%28"xss"%29<%2Fscript>

testfire.net says

xss

The entered code has been executed in the website.

Recommendations:

- Whitelisting input fields.
- Input Output encoding.

c. **Vulnerability:** Insecure Direct Object Reference (IDOR)

CWE: CWE-639

OWASP Category: A01 Broken Access Control

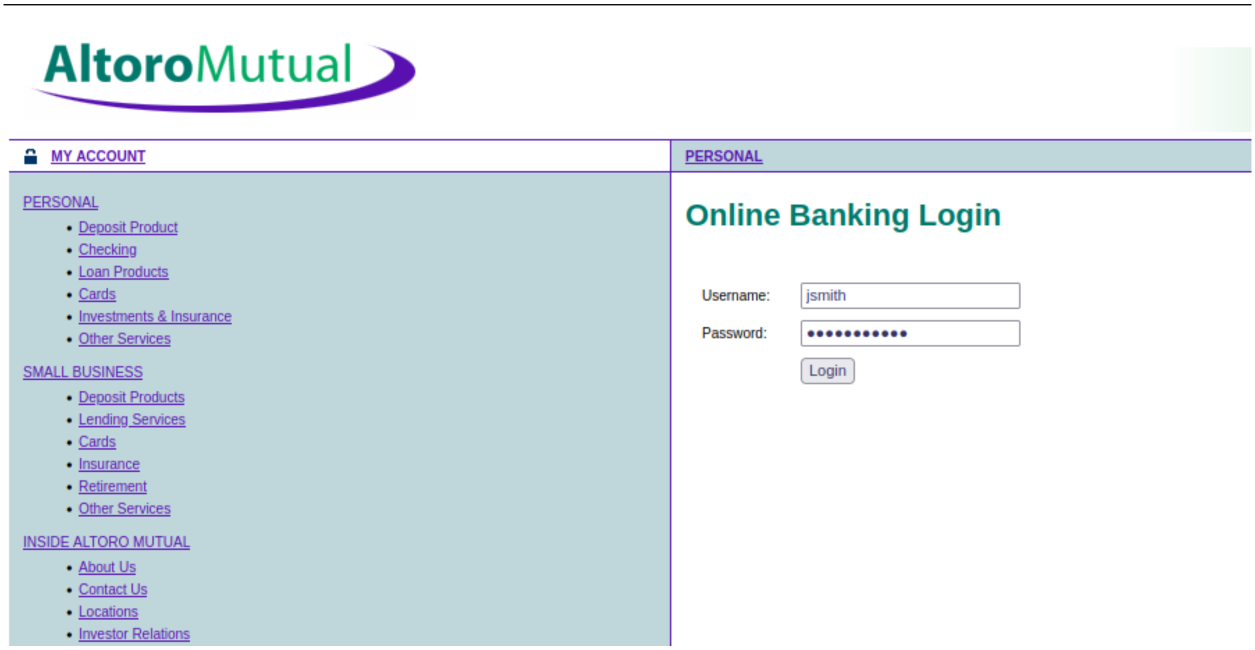
Description: The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data.

Business Impact: IDOR can lead to unauthorized access to sensitive data or resources, potentially resulting in data breaches, privacy violations, financial losses, and damage to an organization's reputation. It can also lead to legal and regulatory consequences, impacting the overall trust and confidence in the business.

Vulnerability path: http://testfire.net/login.jsp

Steps to Reproduce:

1. Navigate into the given URL and login using john smith credentials.



AltoroMutual

MY ACCOUNT

PERSONAL

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

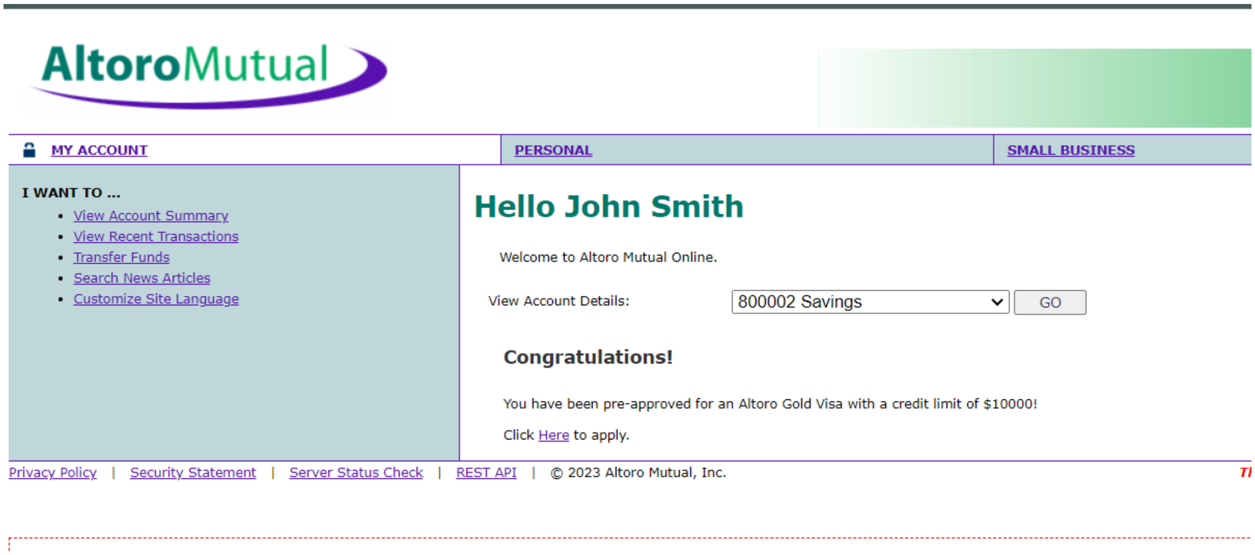
Online Banking Login

Username: jsmith

Password: ●●●●●●●●●●●

Login

2. Click on “Go” to view John Smith’s savings.



AltoroMutual

MY ACCOUNT | PERSONAL | SMALL BUSINESS

I WANT TO ...
- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

Hello John Smith

Welcome to Altoro Mutual Online.

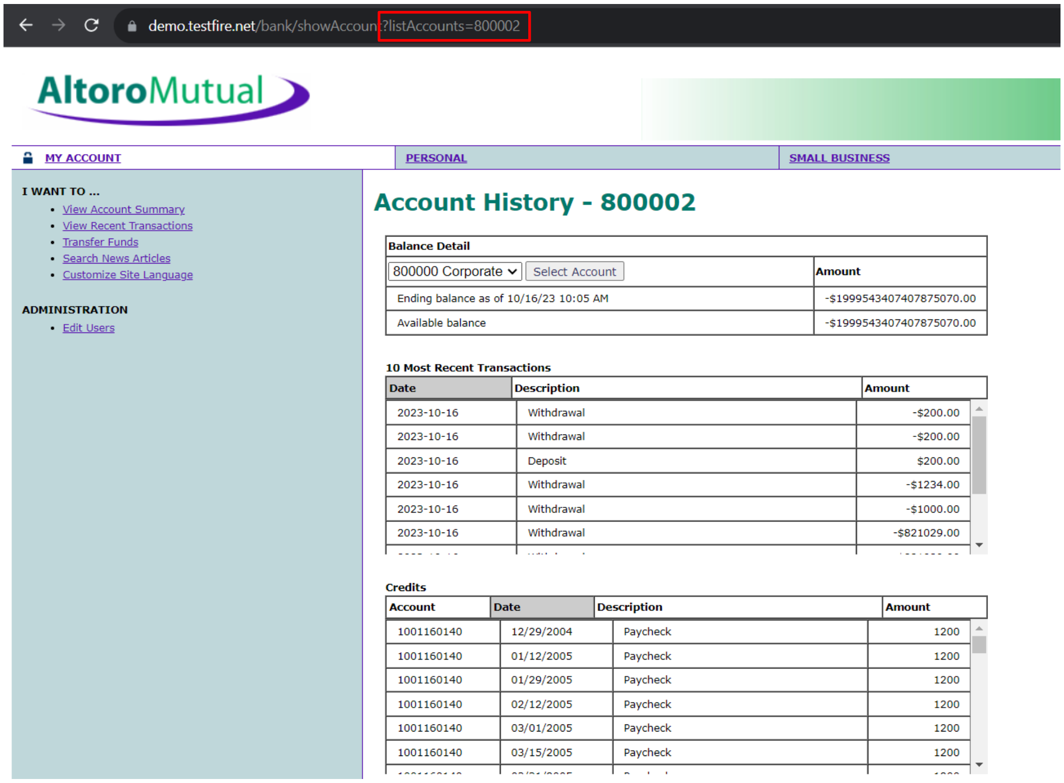
View Account Details: 800002 Savings GO

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. Th



demo.testfire.net/bank/showAccount?listAccounts=800002

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Account History - 800002

Balance Detail	
800000 Corporate ⌄ Select Account	**Amount**
Ending balance as of 10/16/23 10:05 AM	-$1999543407407875070.00
Available balance	-$1999543407407875070.00

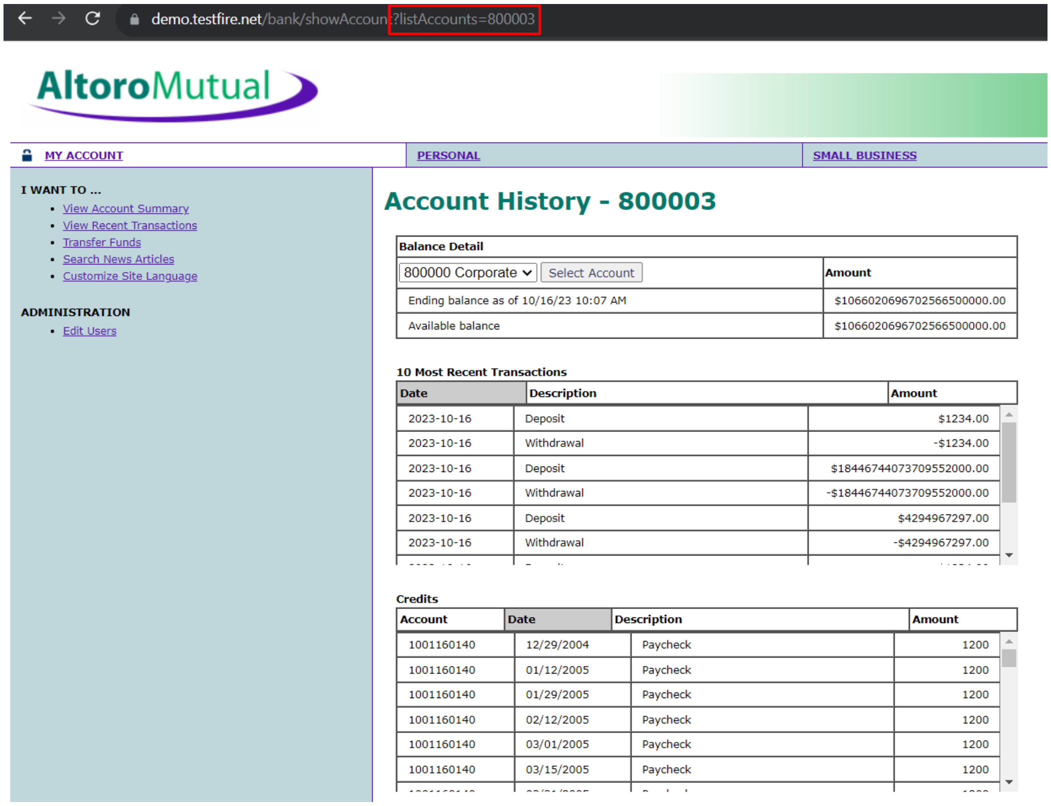
10 Most Recent Transactions

Date	Description	Amount
2023-10-16	Withdrawal	-$200.00
2023-10-16	Withdrawal	-$200.00
2023-10-16	Deposit	$200.00
2023-10-16	Withdrawal	-$1234.00
2023-10-16	Withdrawal	-$1000.00
2023-10-16	Withdrawal	-$821029.00

Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200
1001160140	03/01/2005	Paycheck	1200
1001160140	03/15/2005	Paycheck	1200

3. Change the listAccount=800002 to 800003 to view account history of other customers.



demo.testfire.net/bank/showAccount?listAccounts=800003

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Account History - 800003

Balance Detail	
800000 Corporate ⌄ Select Account	**Amount**
Ending balance as of 10/16/23 10:07 AM	$1066020696702566500000.00
Available balance	$1066020696702566500000.00

10 Most Recent Transactions

Date	Description	Amount
2023-10-16	Deposit	$1234.00
2023-10-16	Withdrawal	-$1234.00
2023-10-16	Deposit	$18446744073709552000.00
2023-10-16	Withdrawal	-$18446744073709552000.00
2023-10-16	Deposit	$4294967297.00
2023-10-16	Withdrawal	-$4294967297.00

Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200
1001160140	03/01/2005	Paycheck	1200
1001160140	03/15/2005	Paycheck	1200

Recommendations:

- Implement Proper Access Controls.
- Employ Session Management and Authentication.

d. **Vulnerability:** Personal Identifiable Information (PII)

CWE: CWE-319

OWASP Category: A02:2021 Cryptographic Failures

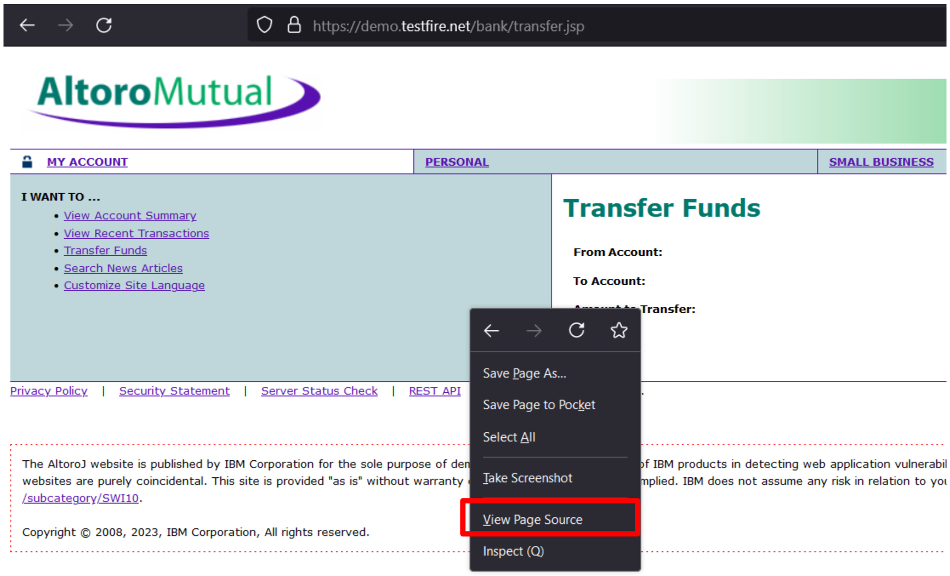
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Exposure of Personal Identifiable Information (PII) can lead to legal fines, reputation damage, financial losses, operational disruption, customer churn, cybersecurity costs, competitive disadvantage, and long-term legal liability, underscoring the importance of robust data protection.

Vulnerability Path: https://testfire.net/bank/transfer.jsp

Steps to Reproduce:

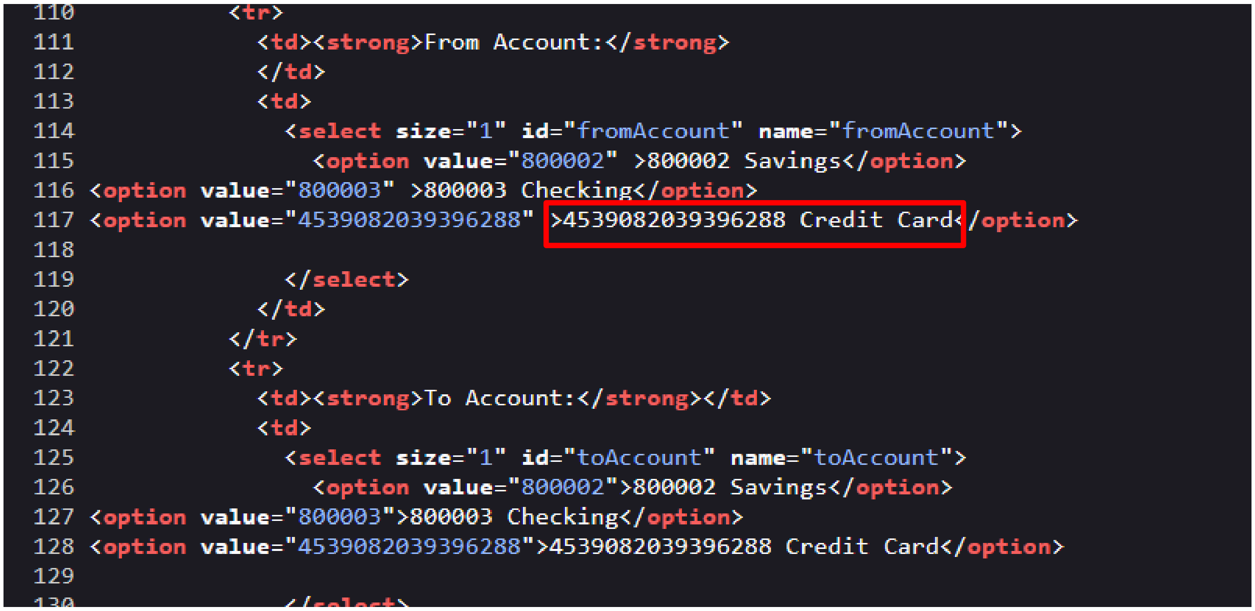
1. Navigate to the given URL. Then, view page source.



The AltoroJ website is published by IBM Corporation for the sole purpose of den of IBM products in detecting web application vulnerabil websites are purely coincidental. This site is provided "as is" without warranty mplied. IBM does not assume any risk in relation to you /subcategory/SWI10.

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

2. Scroll down. Credit card details are shown explicitly.



```
          <tr>
            <td><strong>From Account:</strong>
            </td>
            <td>
              <select size="1" id="fromAccount" name="fromAccount">
                <option value="800002" >800002 Savings</option>
<option value="800003" >800003 Checking</option>
<option value="4539082039396288" >4539082039396288 Credit Card</option>

              </select>
            </td>
          </tr>
          <tr>
            <td><strong>To Account:</strong></td>
            <td>
              <select size="1" id="toAccount" name="toAccount">
                <option value="800002">800002 Savings</option>
<option value="800003">800003 Checking</option>
<option value="4539082039396288">4539082039396288 Credit Card</option>

              </select>
```

Recommendations:

- Data Encryption.
- Data Minimization.
- Limit access to authorized people.

e. **Vulnerability:** Information Disclosure

CWE: CWE-200

OWASP Category: A03:2017 Sensitive Data Exposure.

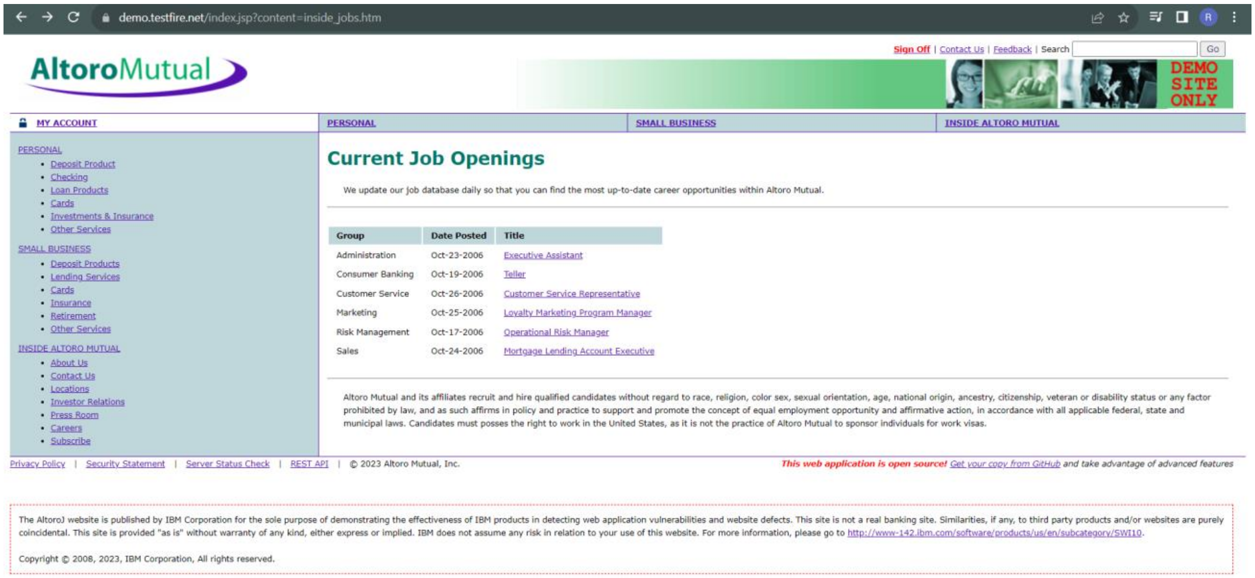
Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business Impact: Information disclosure jeopardizes privacy, competitive standing, and trust, potentially resulting in legal actions, financial losses, and reputational harm, undermining an organization's security, prosperity, and image.

Vulnerability Path:
https://demo.testfire.net/index.jsp?content=inside_jobs.htm

Steps to Reproduce:

1. Navigate to the given URL.



Current Job Openings

We update our job database daily so that you can find the most up-to-date career opportunities within Altoro Mutual.

Group	Date Posted	Title
Administration	Oct-23-2006	Executive Assistant
Consumer Banking	Oct-19-2006	Teller
Customer Service	Oct-26-2006	Customer Service Representative
Marketing	Oct-25-2006	Loyalty Marketing Program Manager
Risk Management	Oct-17-2006	Operational Risk Manager
Sales	Oct-24-2006	Mortgage Lending Account Executive

Altoro Mutual and its affiliates recruit and hire qualified candidates without regard to race, religion, color sex, sexual orientation, age, national origin, ancestry, citizenship, veteran or disability status or any factor prohibited by law, and as such affirms in policy and practice to support and promote the concept of equal employment opportunity and affirmative action, in accordance with all applicable federal, state and municipal laws. Candidates must posses the right to work in the United States, as it is not the practice of Altoro Mutual to sponsor individuals for work visas.

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/SWI10.

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

The details of the company are clearly visible.

Recommendations:

- The information must not be in clear text.
- Classify the data into "sensitive" and "non-sensitive".

f. **Vulnerability:** Outdated Server

CWE: CWE-1352

OWASP Category: A06:2021 Vulnerable and Outdated Components

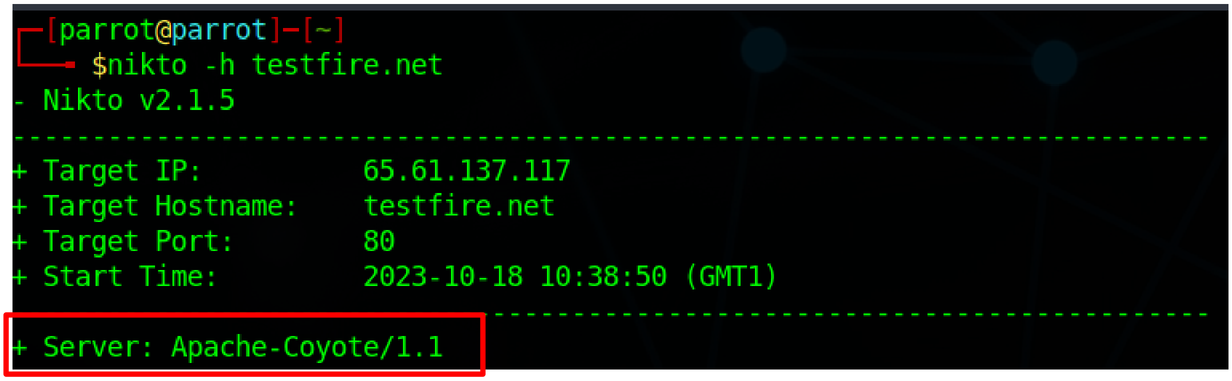
Description: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact: Using outdated or vulnerable components may result in non-compliance with data protection and security regulations, leading to fines and legal penalties. Security incidents and breaches can disrupt day-to-day operations, leading to downtime, increased support costs, and decreased productivity. Exploitable vulnerabilities in components can lead to data breaches, potentially resulting in loss of sensitive information, legal consequences, and damage

Vulnerability Path: https://testfire.net/bank/transfer.jsp

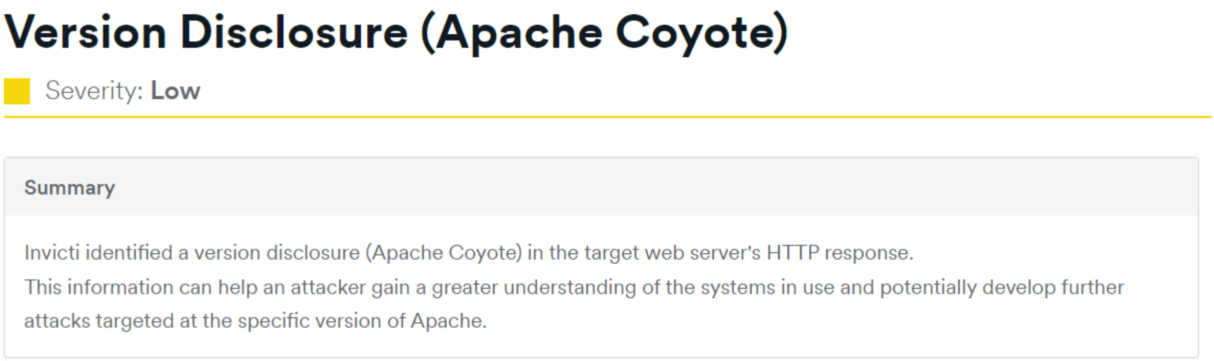
Steps to Reproduce:

1. Tool Used: **Nikto.** Type the following Command.



```
┌─[parrot@parrot]─[~]
└──╼ $nikto -h testfire.net
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2023-10-18 10:38:50 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
```

2. Search vulnerabilities in web.



Version Disclosure (Apache Coyote)

🟨 Severity: **Low**

Summary

Invicti identified a version disclosure (Apache Coyote) in the target web server's HTTP response.
This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of Apache.

Recommendations:

- Configure your web server to prevent information leakage from the SERVER header of its HTTP response.
- Conduct frequent vulnerable scans.

g. **Vulnerability:** Transmission of Cleartext Credentials

CWE: CWE-319

OWASP Category: A05:2021 Security Misconfiguration

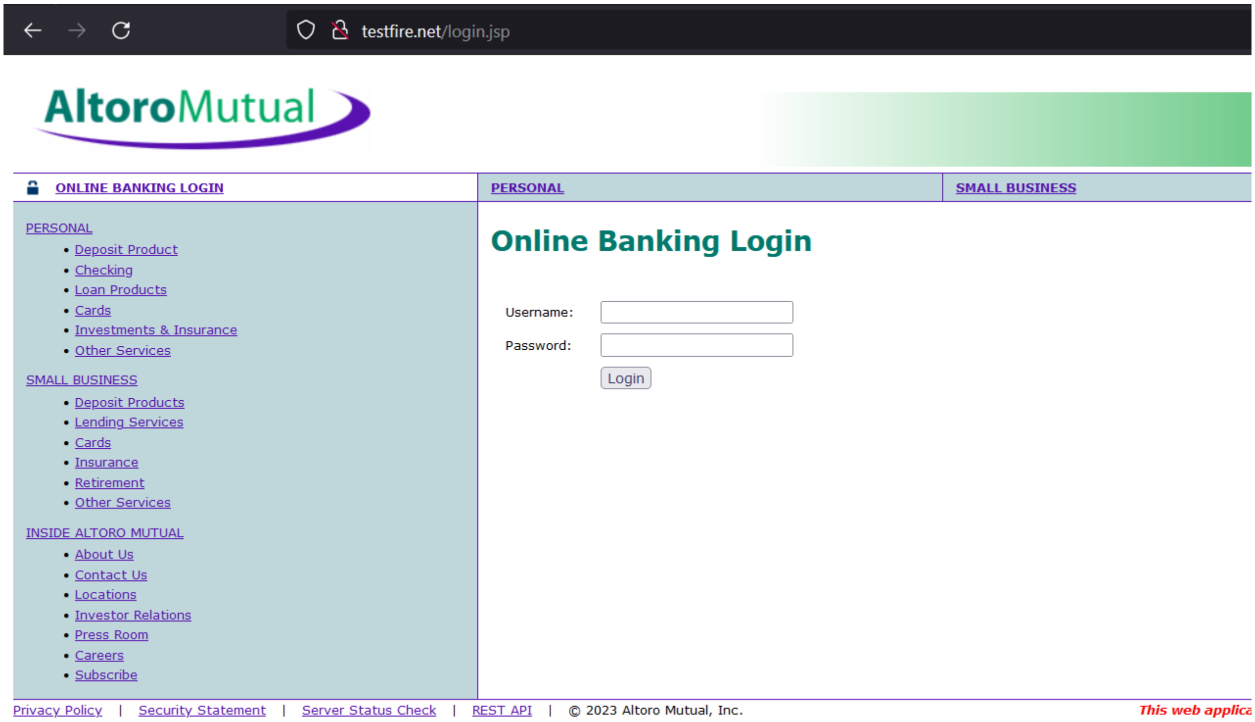
Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Transmitting credentials in cleartext can result in unauthorized access, data breaches, loss of customer trust, legal and regulatory consequences, and reputation damage, impacting an organization's security and financial standing.

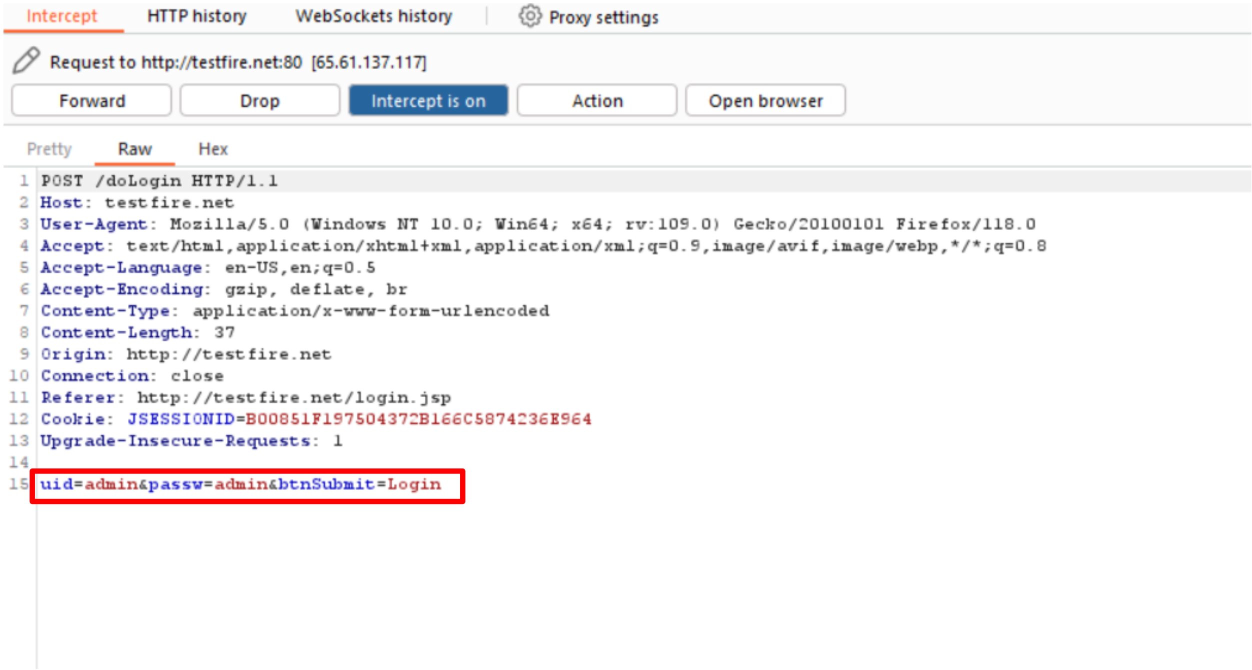
Vulnerability Path: http://testfire.net/login.jsp

Steps to Reproduce:

1. Navigate to the above mentioned URL.



2. Login using admin credentials with "**Burp Suite"** intercept turned on.



Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=B00851F197504372B166C5874236E964
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=Login
```

It is clearly visible that the credentials are transmitted in cleartext.

Recommendations:

- Hash and Salt credentials.
- Implement Secure Protocols.

h. **Vulnerability**: Clickjacking

CWE: CWE-451

OWASP Category: A04:2021 Insecure Design

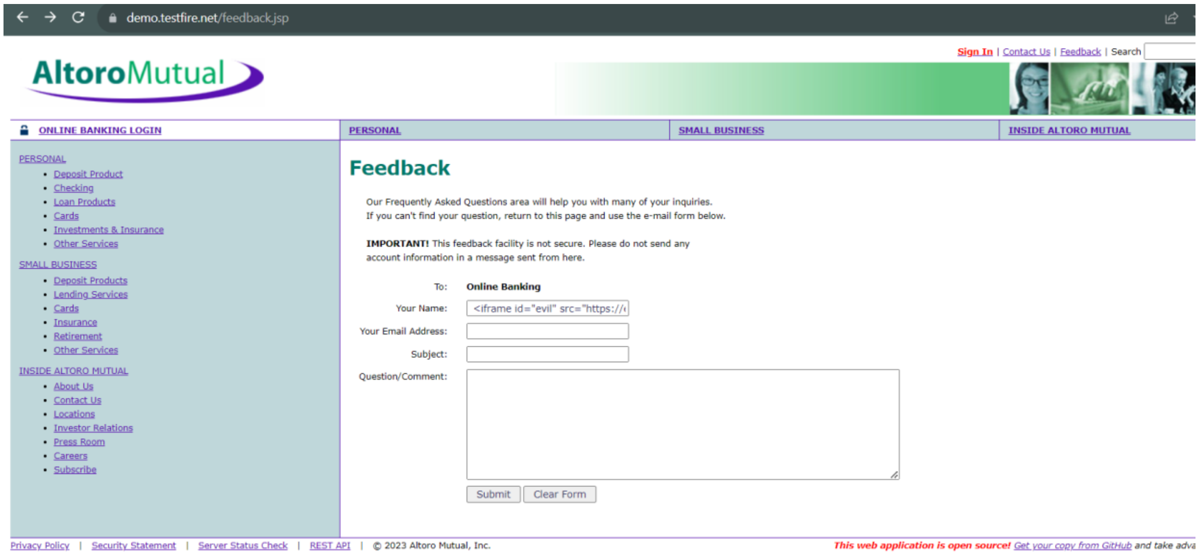
Description: The user interface (UI) does not properly represent critical information to the user, allowing the information - or its source - to be obscured or spoofed. This is often a component in phishing attacks.

Business Impact: The Impact of Clickjacking The hacker has several ways they can use the redirected clicks for their own gain. A common form of clickjacking involves mirroring a login and password form on a website.

Vulnerability Path: https://demo.testfire.net/feedback.jsp

Steps to reproduce:

1. Navigate to the above-mentioned URL. Enter the payload "<iframe id="evil" src=https://evil.com sandbox="allow-forms"></iframe>



Feedback

Our Frequently Asked Questions area will help you with many of your inquiries.
If you can't find your question, return to this page and use the e-mail form below.

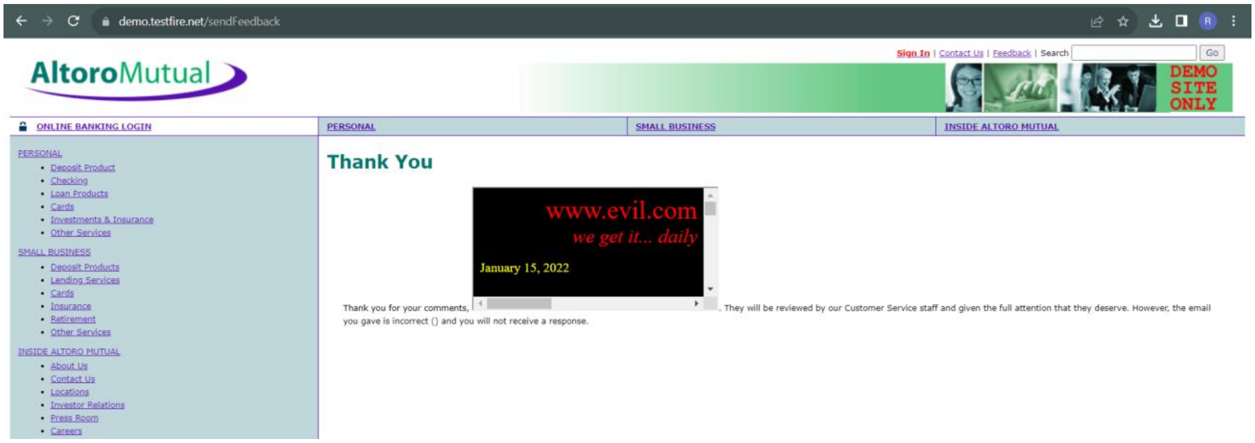
IMPORTANT! This feedback facility is not secure. Please do not send any account information in a message sent from here.

To: **Online Banking**
Your Name: <iframe id="evil" src="https://
Your Email Address:
Subject:
Question/Comment:

| © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take adva

2. Click on submit.



Thank You

Thank you for your comments, . They will be reviewed by our Customer Service staff and given the full attention that they deserve. However, the email you gave is incorrect () and you will not receive a response.

Recommendations:

- Implement X-Frame Options Header.
- Utilize Content Security Policy.
- Employ frame-busting JavaScript code.

i. **Vulnerability:** Cookie with Insecure or Improper or Missing SameSite attribute

CWE: CWE-1275

OWASP Category: A01:2021 Broken Access Control

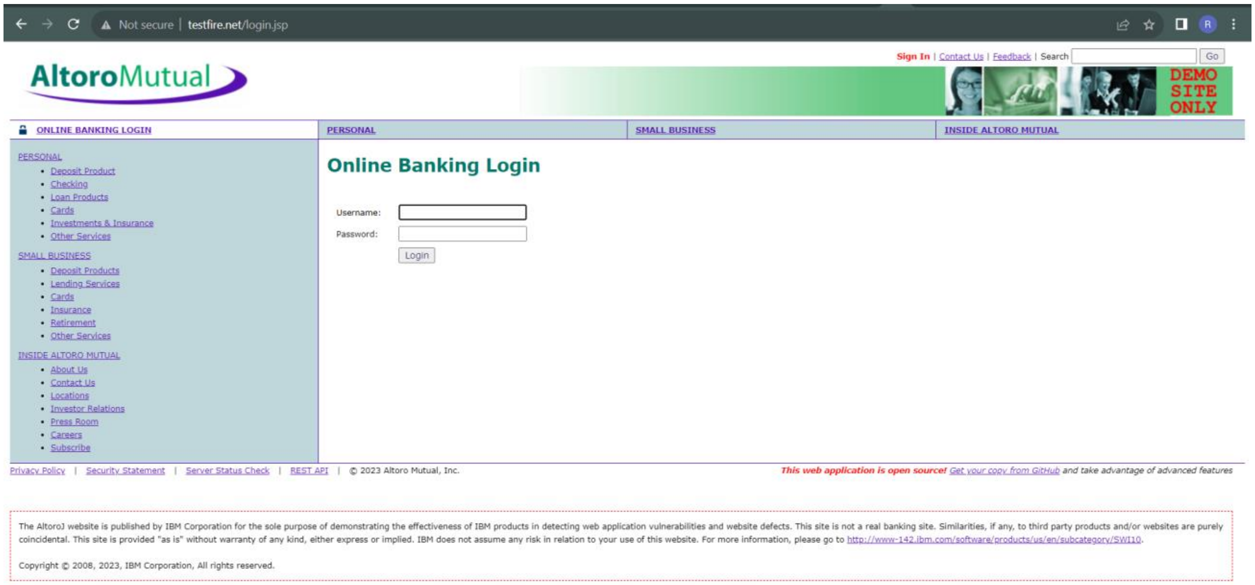
Description: The SameSite attribute for sensitive cookies is not set, or an insecure value is used.

Business Impact: Inadequate SameSite attribute settings on cookies can lead to security vulnerabilities, enabling Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS) attacks, potentially resulting in data breaches, loss of customer trust, legal consequences, and financial damage.

Vulnerability Path: http://testfire.net/login.jsp

Steps to Reproduce:

1. Navigate to the above-mentioned URL.



Online Banking Login

Username:

Password:

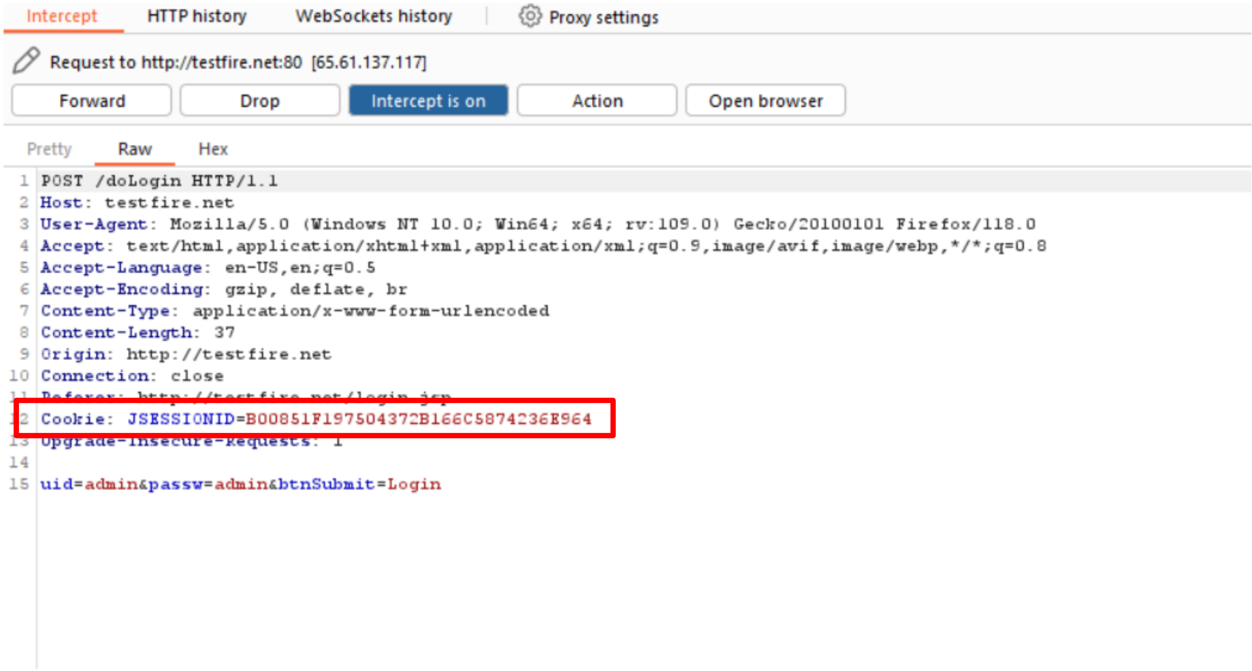
© 2023 Altoro Mutual, Inc.

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/SWI10.

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

2. Login using admin credentials with “**Burp Suite”** intercept turned on.



```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=B00851F197504372B166C5874236E964
Upgrade-Insecure-Requests: 1

uid=admin&passw=admin&btnSubmit=Login
```

Recommendations:

- Implement proper SameSite settings.
- Regular Security Audits.