Assignment- 1

Black Box Penetration Testing

On

demo.testfire.net

By: - Parth Pathak

Scope of Work: -

This assignment covers the remote penetration testing of demo.testfire.net. The assignment was carried out from a black box perspective, with the only supplied information being the domain name. No other information was assumed at the start of the assignment.

I used the following tools only:

- Burp Suite (Proxy)

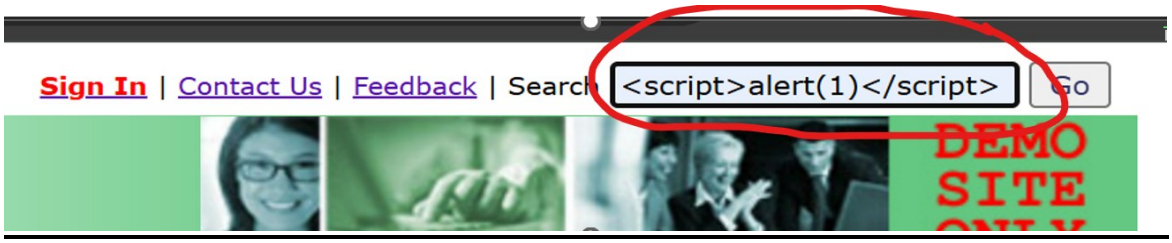
Summary of Findings: -

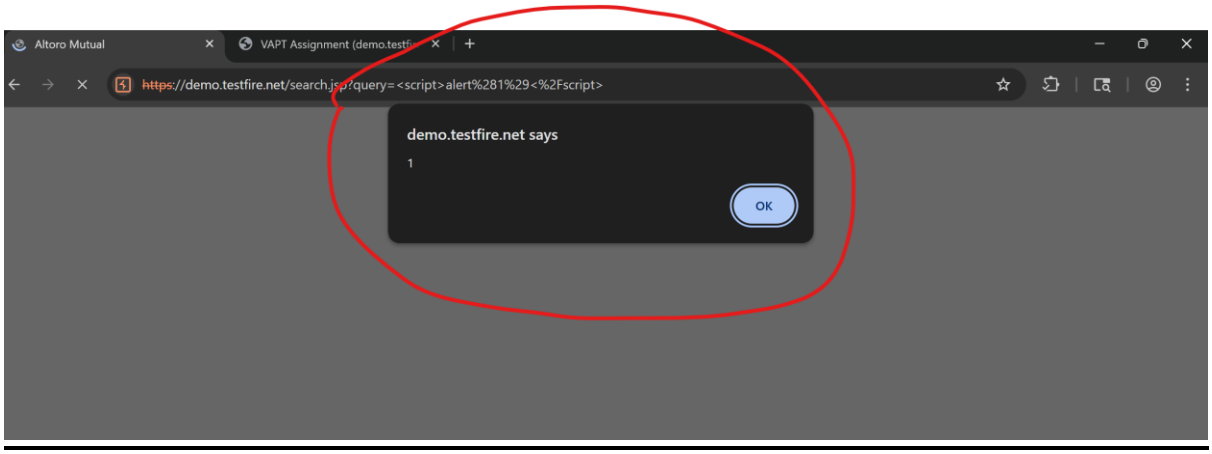
Category	Vulnerability	Count
Injection Attacks	XSS	3
	SQL Injection	1
	Host Header Injection	1
Authentication & Authorization	Broken Authentication	2
	Broken Access Control	1
	Authorization Handling Bug	1
Input Validation Issues	Improper Input Validation	1
	Client-Side Validation Bypass	1
Information Exposure	Information Disclosure	4
	Clipboard Data Exposure	1

Category	Vulnerability	Count
Application Logic / Functional	Broken Functionality	1
	Broken Confirmation Logic	1
	Incorrect Backend Mapping	1
	Non-Functional Submit Button	1
Error Handling & Configuration	Incorrect Error Handling	1
UI / Navigation Issues	Broken Link / Dead Link	4
Total		**25**

1. Reflected XSS 1:-

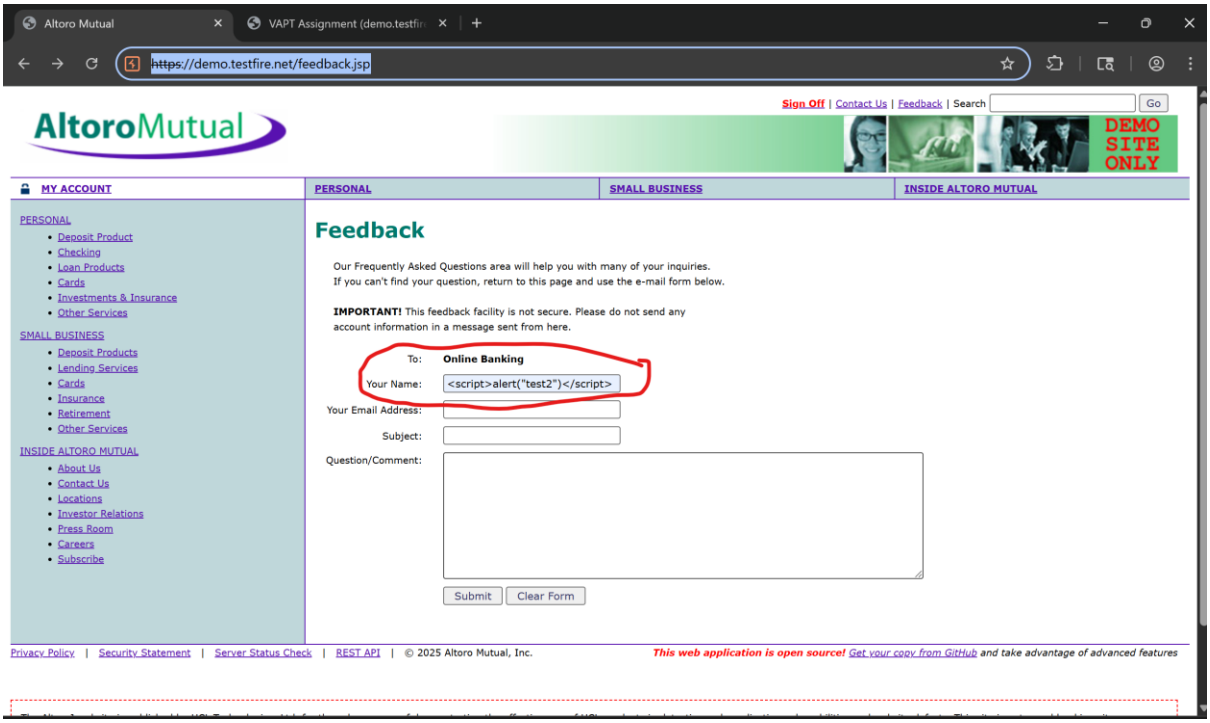
After opening the website https://demo.testfire.net the search field was tested first. So, the following JavaScript code was entered which resulted in immediate **Reflected XSS**:
<script> alert(1) </script>

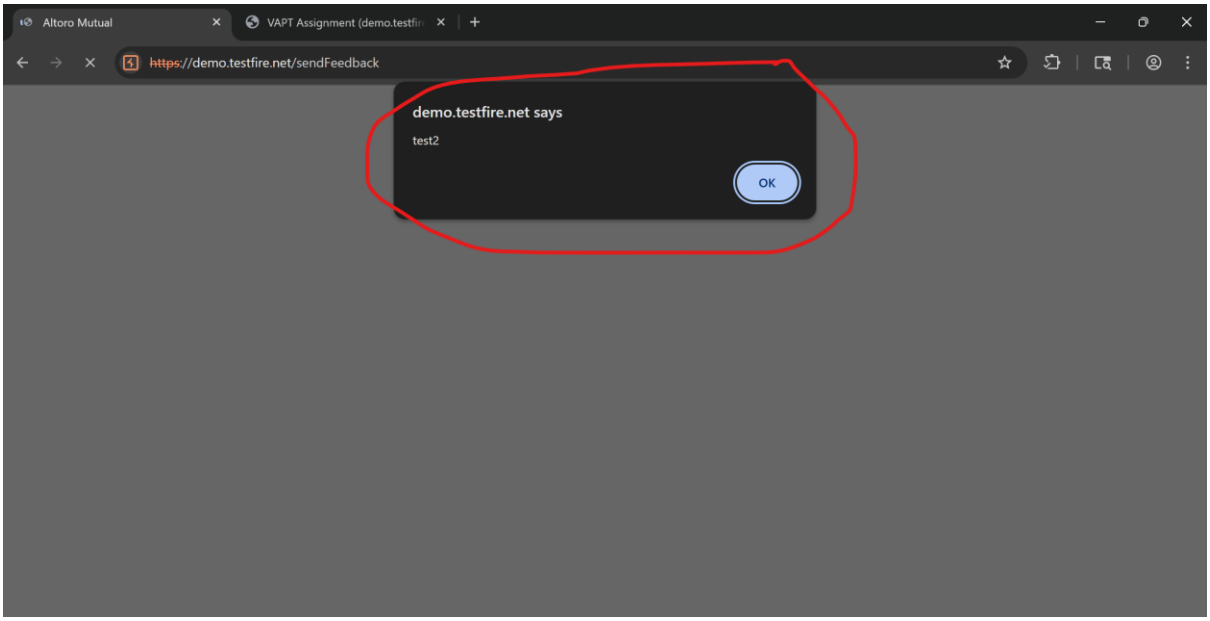




2. Reflected XSS 2:-

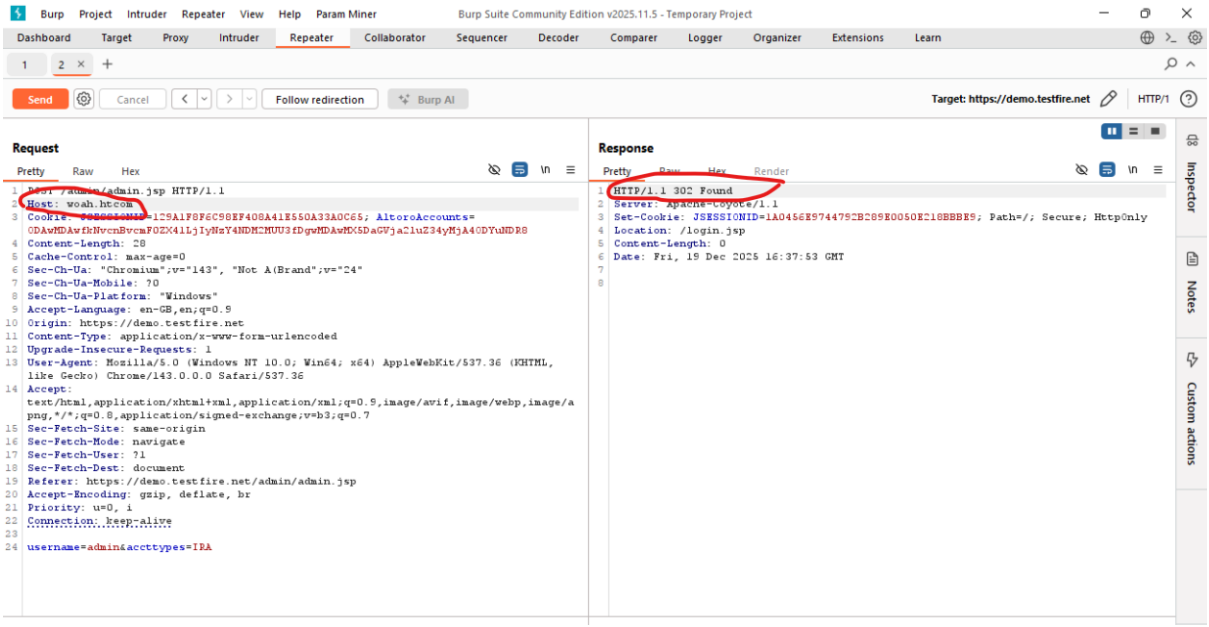
In the Feedback page on link https://demo.testfire.net/feedback.jsp, the name field was entered with the following JavaScript code which resulted in immediate **Reflected XSS**:
<script> alert(“test2”) </script>





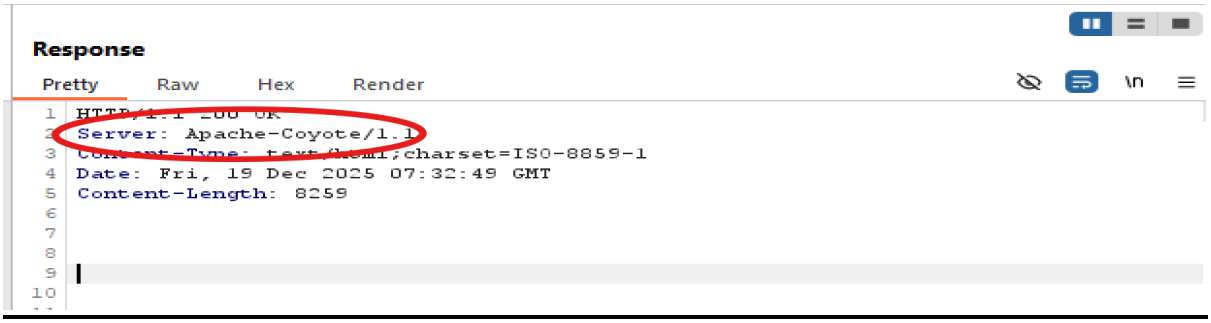
3. Host Header Injection:-

Server responses were received for all hosts even those which maybe do not exist:



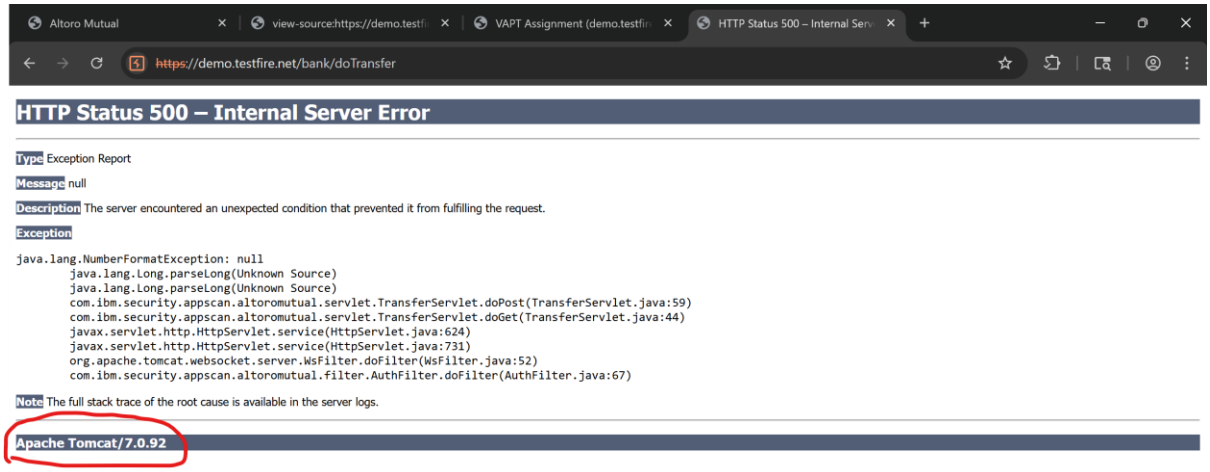
4. Information Disclosure 1:-

Every server response revealed the **http version** it supports along with **server name**:



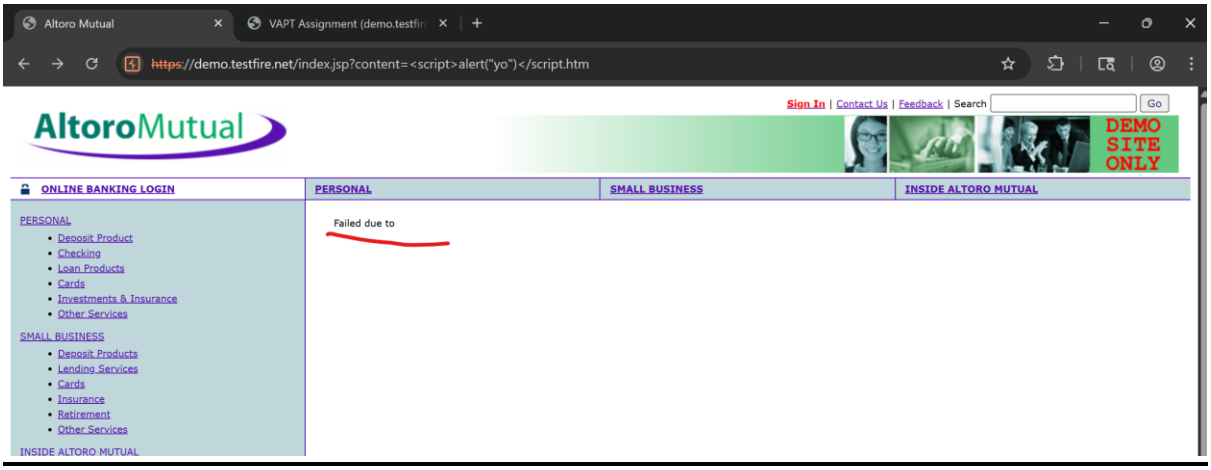
5. Information Disclosure 2:-

Server version was revealed during error handling:



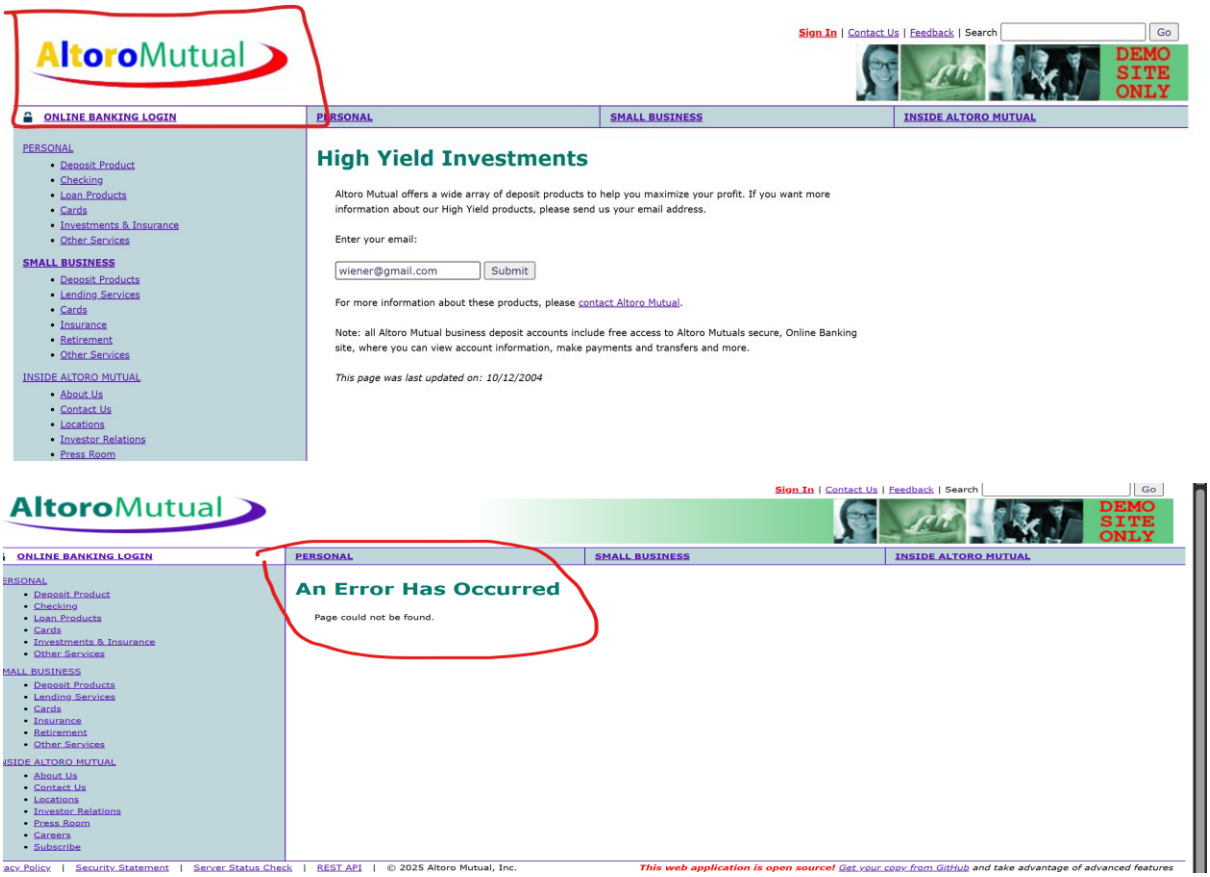
6. Incorrect Error Handling:-

7. **<script> alert("yo") </script>**
   was injected in URL https://demo.testfire.net/index.jsp?content=personal_deposit.htm and was not met with an appropriate error response:



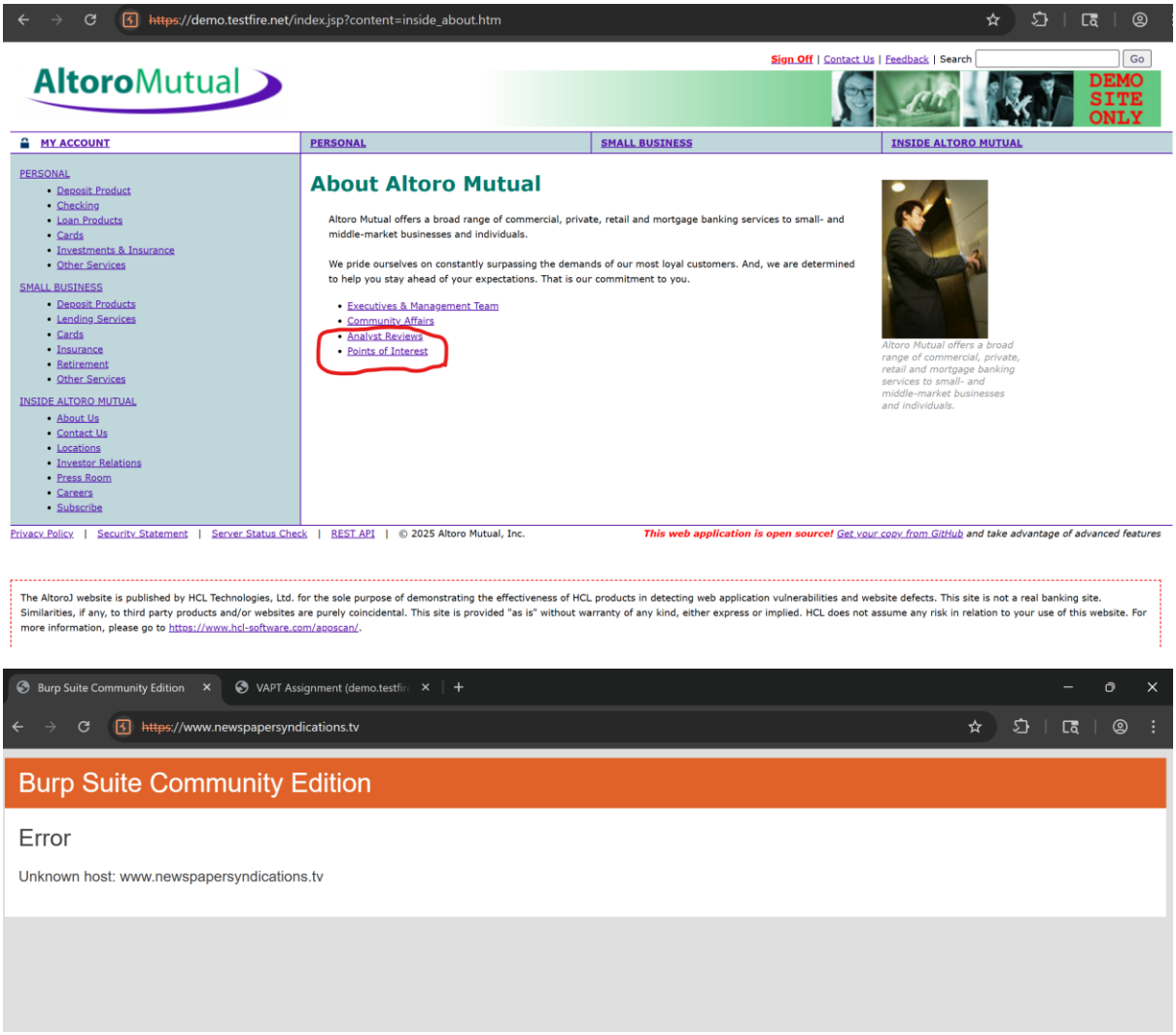
8. Broken Link/Dead Link 1:-

This image on the link https://demo.testfire.net/high_yield_investments.htm was clickable. When it was clicked site returned a **404 error** saying page could not be found:



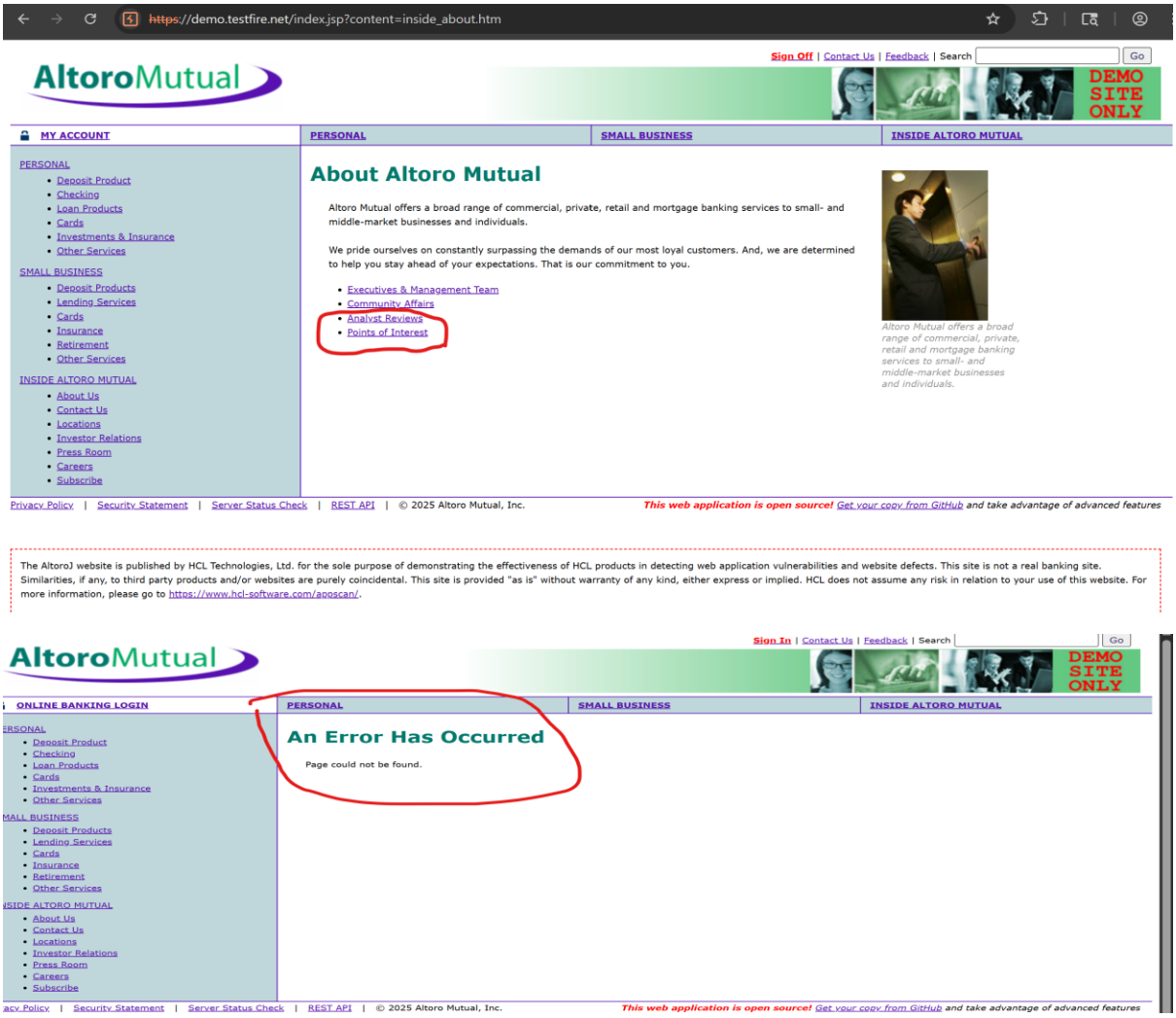
9. Broken Link/Dead Link 2:-

The **Analyst Reviews** page on the link https://demo.testfire.net/index.jsp?content=inside_about.htm was selected but host was not recognised:



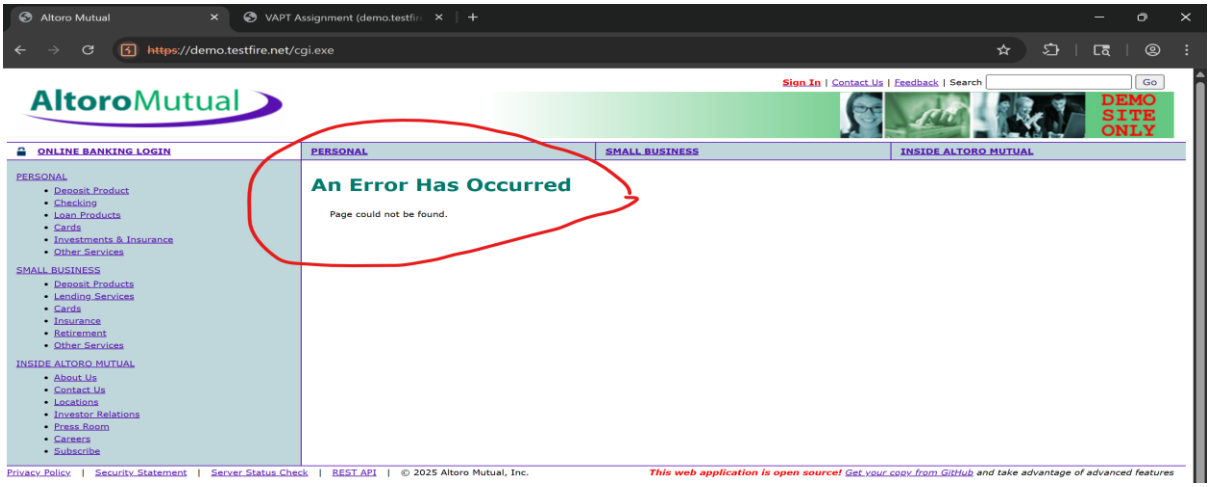
10. Broken Link/Dead Link 3:-

The **Points of interest** page on the link https://demo.testfire.net/index.jsp?content=inside_about.htm was selected and met with **404 error**:



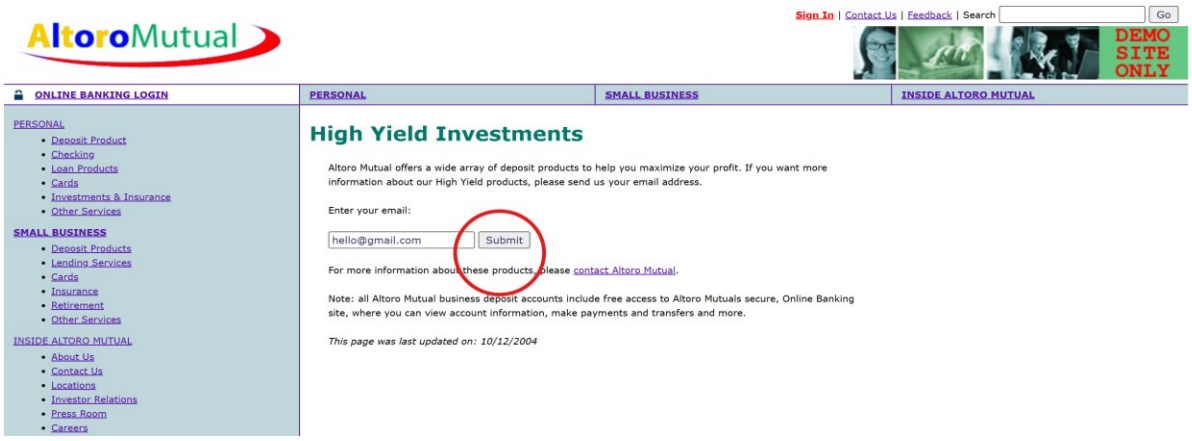
11. Broken Link/Dead Link 4:-

The **Locations** page on https://demo.testfire.net/cgi.exe was selected and met with **404 error**:



12. Non-Functional Submit Button:-

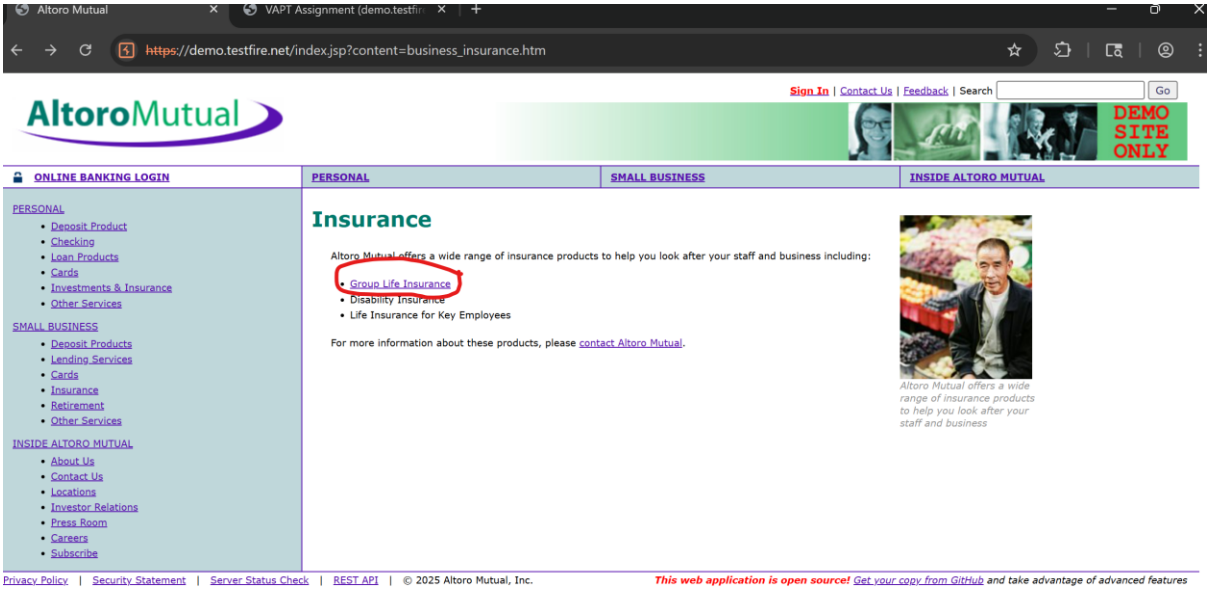
The **Submit** button on the link https://demo.testfire.net/high_yield_investments.htm for entering email was clicked but there was no response. Upon inspection it was found that there was no **<form>** tag in the html:

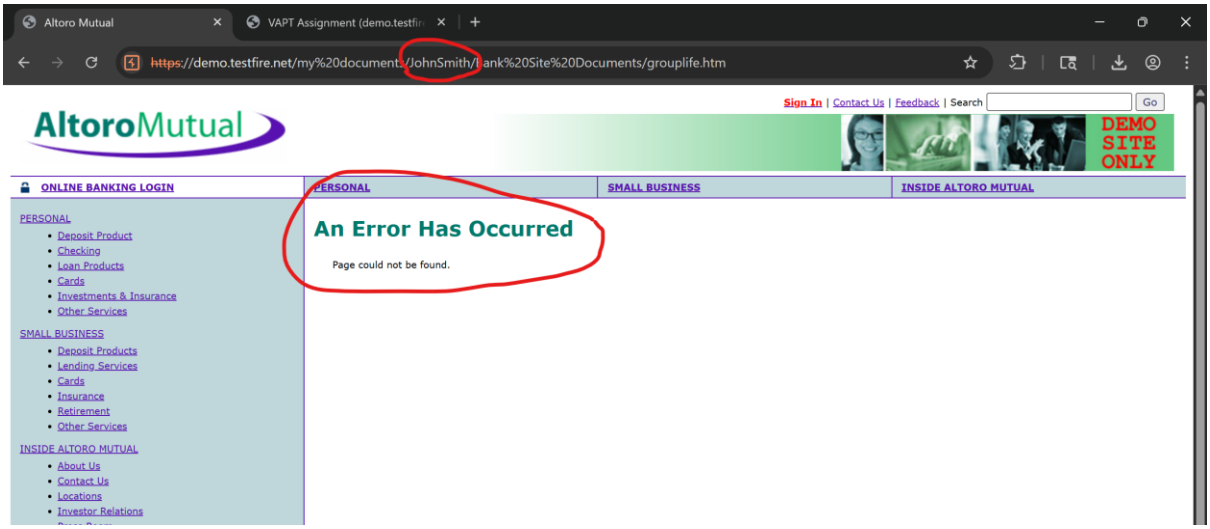


13. Information Disclosure 3:-

This page was found: https://demo.testfire.net/index.jsp?content=business_insurance.htm
On this page there was a hyperlink “Group Life Insurance” which was leading to: https://demo.testfire.net/my%20documents/JohnSmith/Bank%20Site%20Documents/grouplife.htm

The document showed an error when it was accessed however the name “John Smith” was found in the URL:





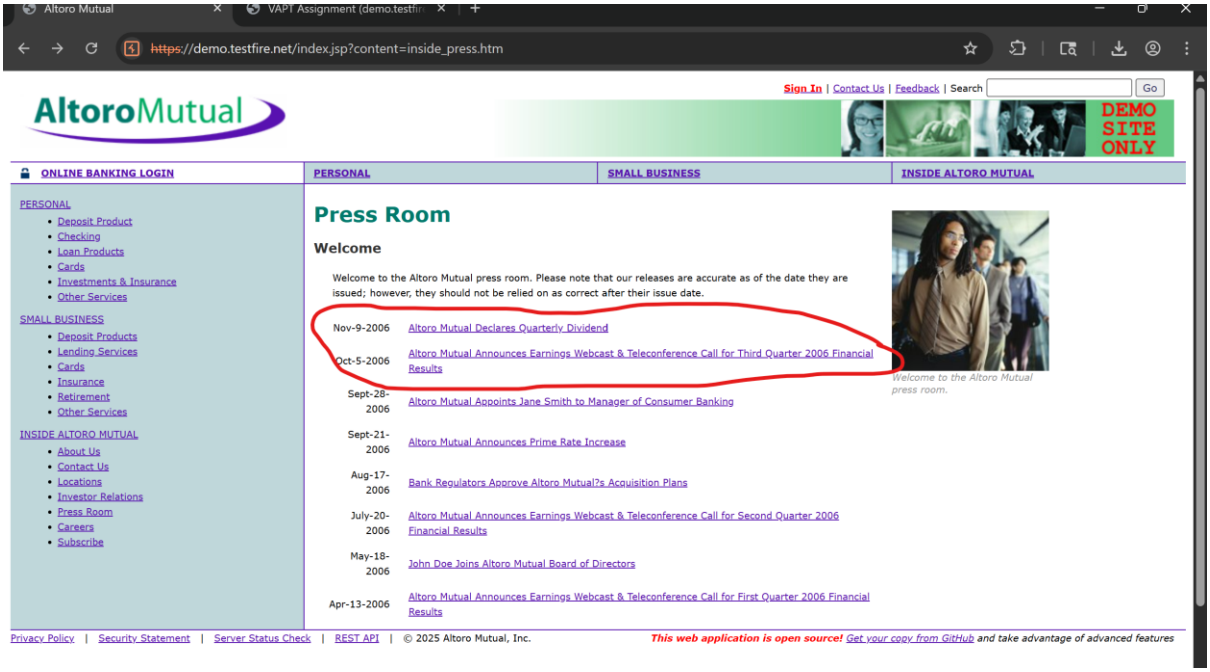
14. Incorrect Backend Mapping:-

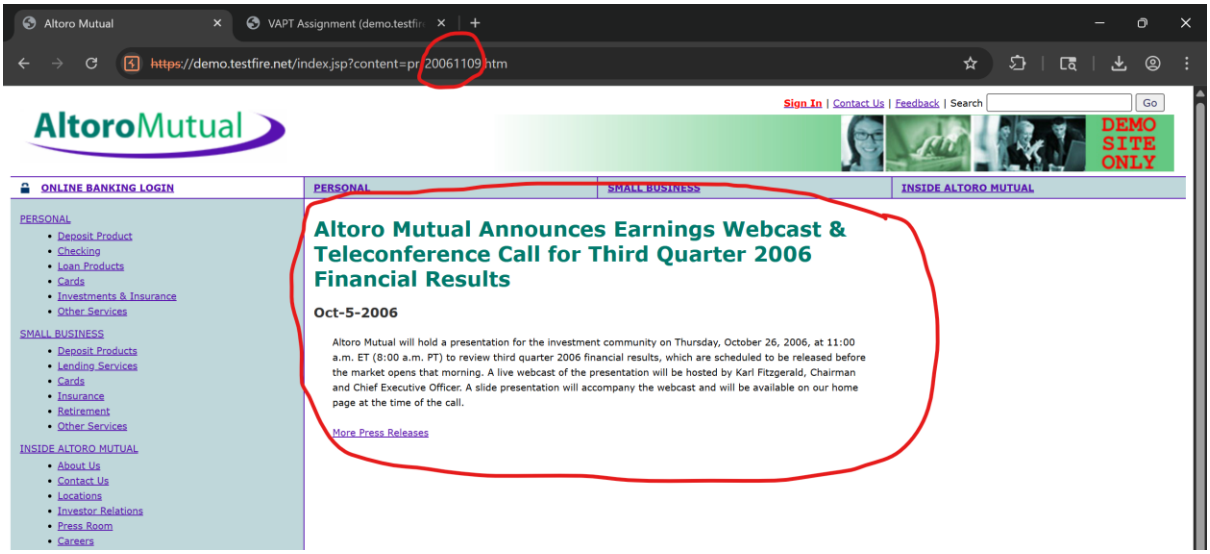
In the **Press Room** section on the link https://demo.testfire.net/index.jsp?content=inside_press.htm, the first two press release links behave inconsistently compared to the rest:

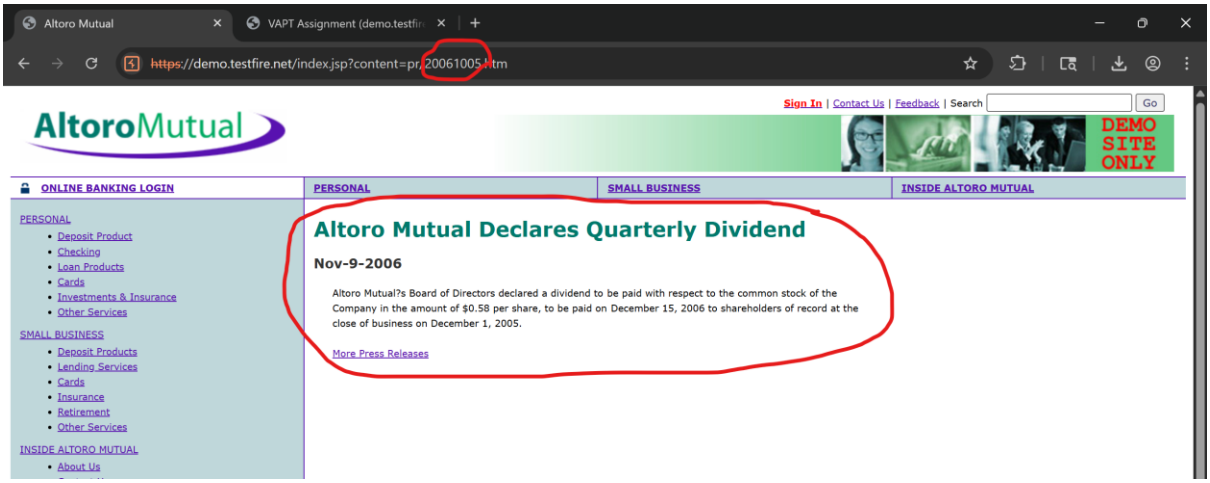
- Clicking “Nov-9-2006” shows content for Oct-5-2006, even though the URL still corresponds to Nov-9-2006.
- Clicking “Oct-5-2006” shows content for Nov-9-2006, while the URL remains Oct-5-2006.

- All subsequent links (Sept 28, Sept 21, Aug 17, etc.) correctly display content that matches both the URL parameter and the selected date.

This indicates that only the first two records are incorrectly mapped on the server side:







15. Information Disclosure 4: -

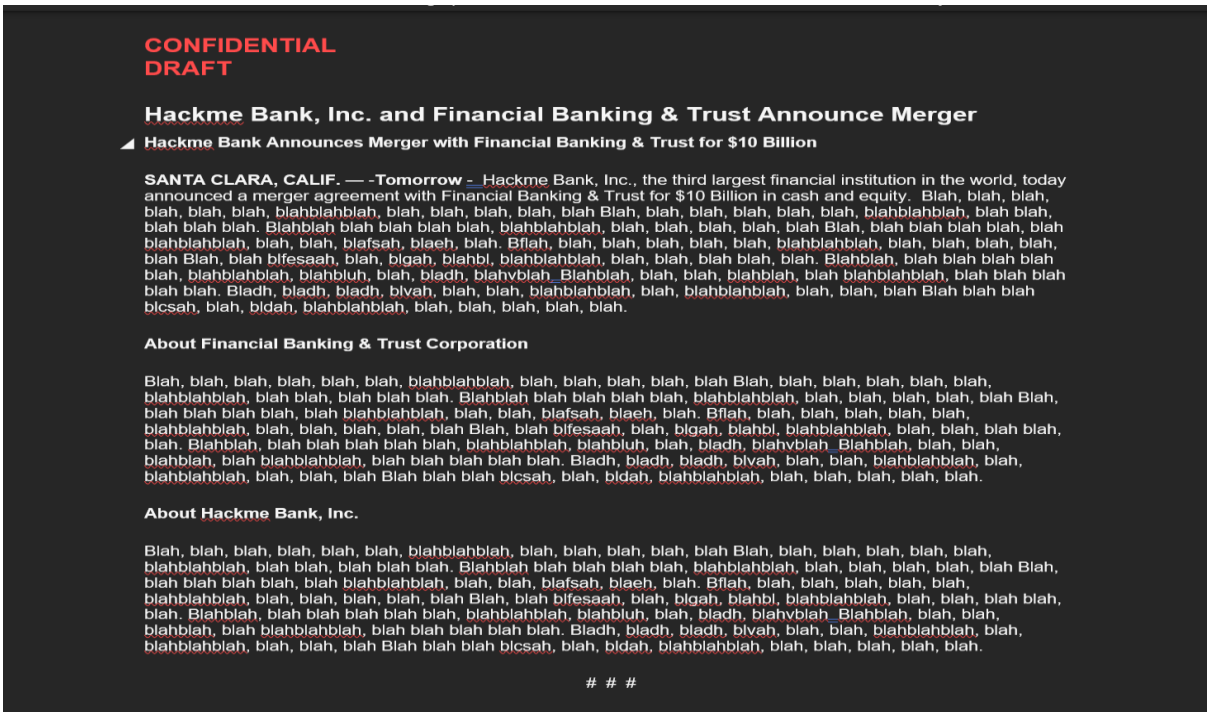
Directory listing was not disabled on this link:

https://demo.testfire.net/pr/

There was a confidential document:

https://demo.testfire.net/pr/Draft.rtf

It disclosed some names and there contact details:



CONFIDENTIAL
DRAFT

Hackme Bank, Inc. and Financial Banking & Trust Announce Merger

Hackme Bank Announces Merger with Financial Banking & Trust for $10 Billion

SANTA CLARA, CALIF. — -Tomorrow - Hackme Bank, Inc., the third largest financial institution in the world, today announced a merger agreement with Financial Banking & Trust for $10 Billion in cash and equity. Blah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah, blah, blah, blah, blah, blahblahblah, blah blah, blah blah blah. Blahblah blah blah blah blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah blah blah blah blah, blah blahblahblah, blah, blah, blafsah, blaeh, blah. Bflah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah blfesaah, blah, blgah, blahbl, blahblahblah, blah, blah, blah blah, blah. Blahblah, blah blah blah blah blah, blahblahblah, blahbluh, blah, bladh, blahvblah Blahblah, blah, blah, blahblah, blah blahblahblah, blah blah blah blah blah. Bladh, bladh, bladh, blvah, blah, blah, blahblahblah, blah, blahblahblah, blah, blah, blah Blah blah blah blah blcsah, blah, bldah, blahblahblah, blah, blah, blah, blah, blah.

About Financial Banking & Trust Corporation

Blah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah blah blah. Blahblah blah blah blah blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah blah blah blah, blah blahblahblah, blah, blah, blafsah, blaeh, blah. Bflah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah blfesaah, blah, blgah, blahbl, blahblahblah, blah, blah, blah blah, blah. Blahblah, blah blah blah blah blah, blahblahblah, blahbluh, blah, bladh, blahvblah Blahblah, blah, blah, blahblah, blah blahblahblah, blah blah blah blah blah. Bladh, bladh, bladh, blvah, blah, blah, blahblahblah, blah, blahblahblah, blah, blah, blah Blah blah blah blah blcsah, blah, bldah, blahblahblah, blah, blah, blah, blah, blah.

About Hackme Bank, Inc.

Blah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah blah blah. Blahblah blah blah blah blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah blah blah blah, blah blahblahblah, blah, blah, blafsah, blaeh, blah. Bflah, blah, blah, blah, blah, blah, blahblahblah, blah, blah, blah, blah, blah Blah, blah blfesaah, blah, blgah, blahbl, blahblahblah, blah, blah, blah blah, blah. Blahblah, blah blah blah blah blah, blahblahblah, blahbluh, blah, bladh, blahvblah Blahblah, blah, blah, blahblah, blah blahblahblah, blah blah blah blah blah. Bladh, bladh, bladh, blvah, blah, blah, blahblahblah, blah, blahblahblah, blah, blah, blah Blah blah blah blah blcsah, blah, bldah, blahblahblah, blah, blah, blah, blah, blah.

# # #

Not For Immediate Release
Contact:

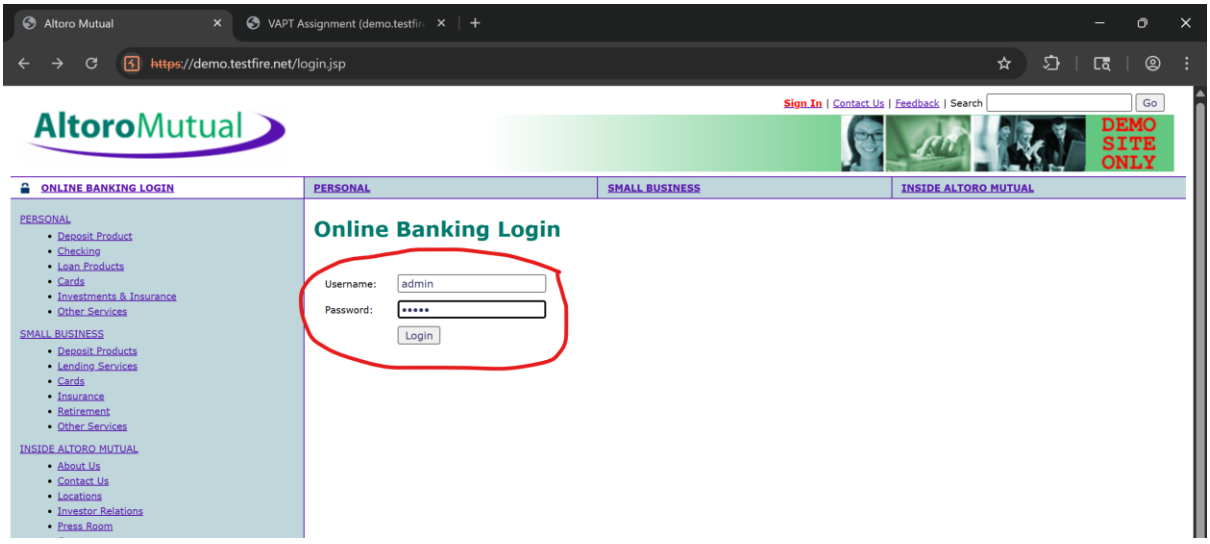
Joan Esposito
Hackme Bank, Inc.
(408) 123-4567

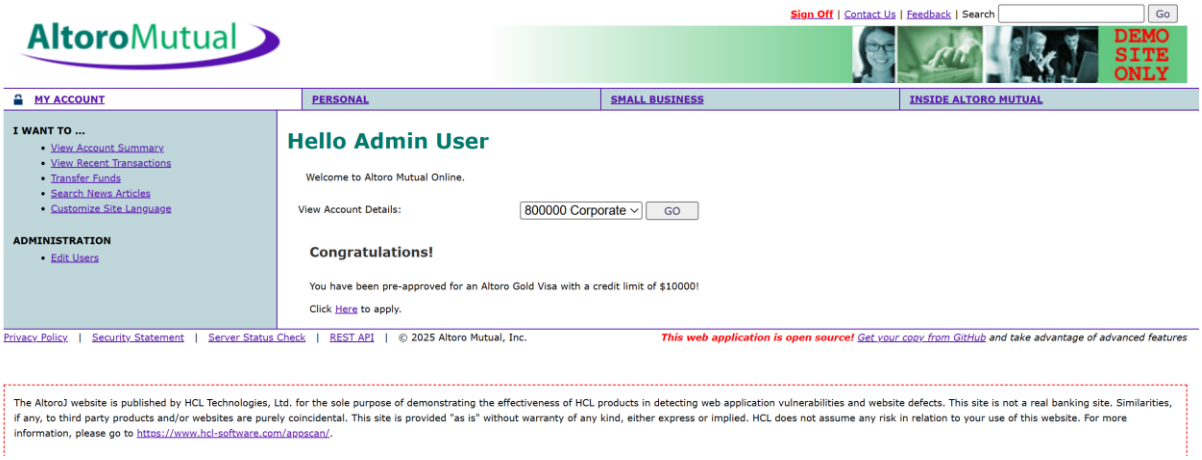
Jean Enerson
PR Communications, Inc.
(415) 123-4567
Hackme Bank@prcommunications.com

Mike James
Financial Banking & Trust Corporation
212.123.4567
mike.james@finbankandtrust.com

16. Broken Authentication 1:-

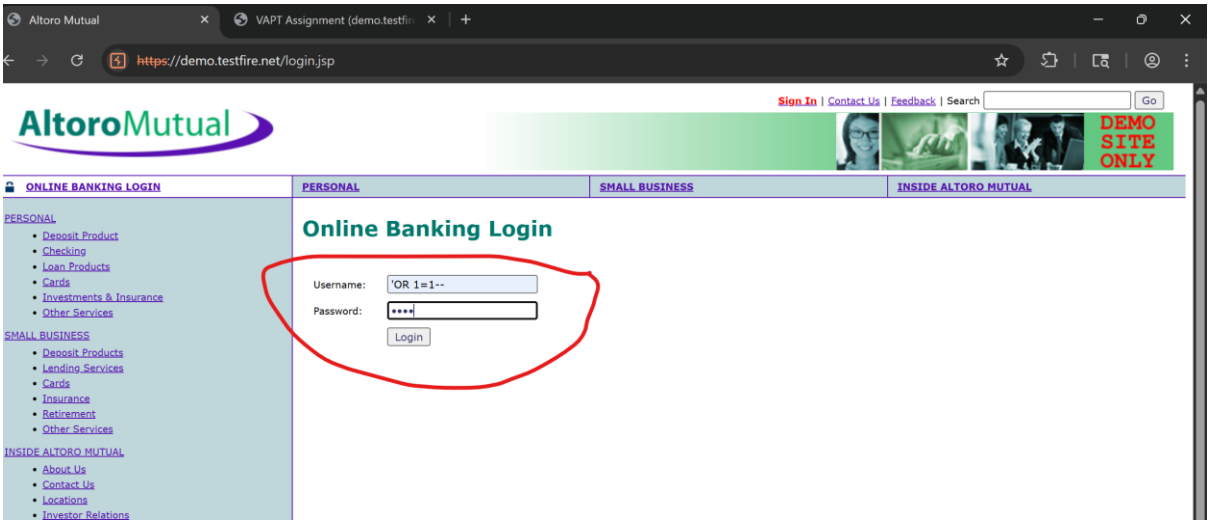
The **Sign In** page was on https://demo.testfire.net/login.jsp. **'admin'** was entered as "username" and "password" and the login system was easily broken providing **admin rights.**

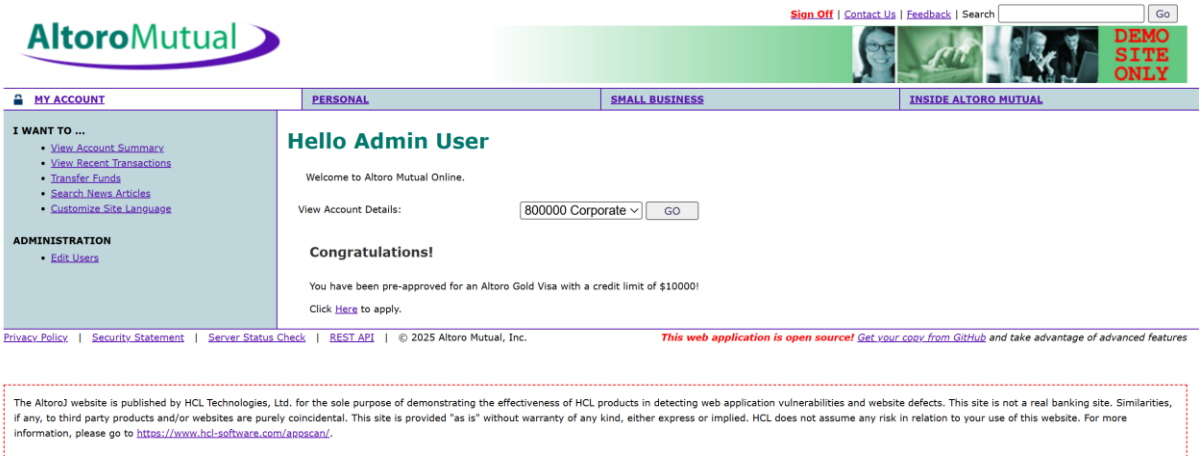




17. Broken Authentication 2 Through SQL Injection:-

The query **'OR 1=1--** was injected in "username", and "password" was entered randomly. This resulted in **authentication bypass** and admin rights were successfully gained.



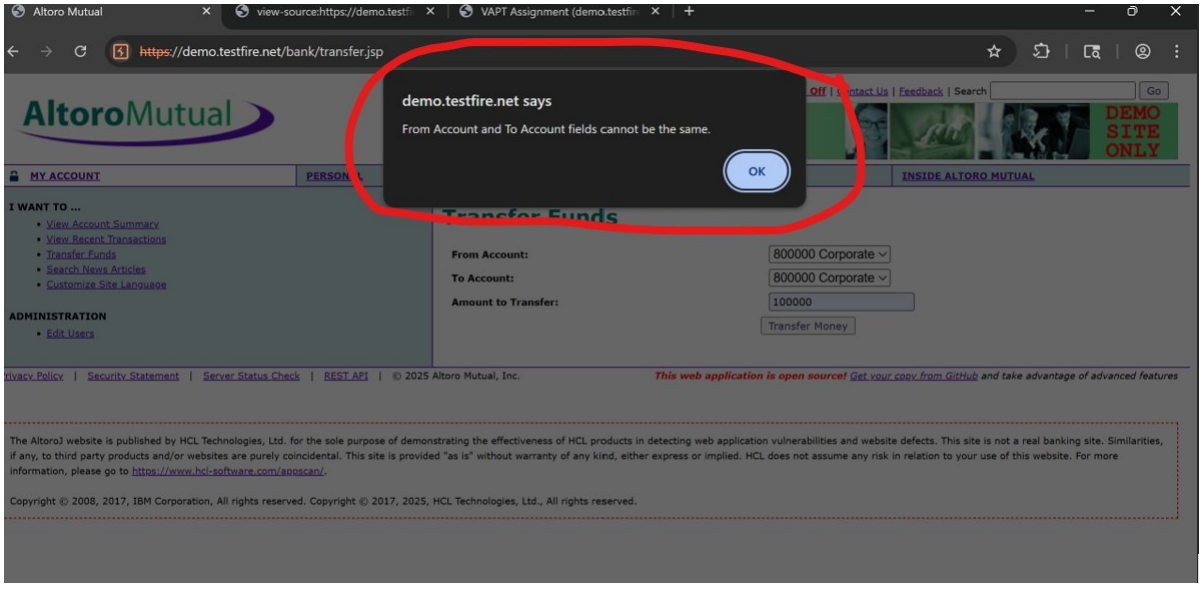


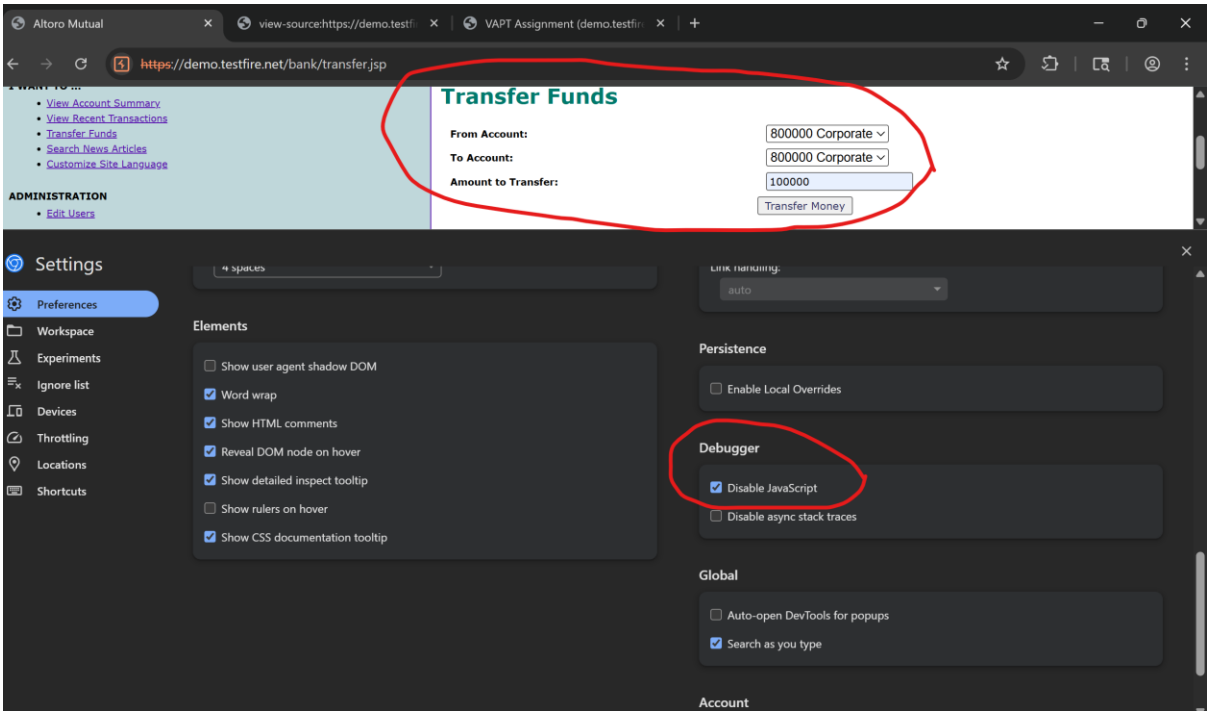
18. Clipboard Data Exposure:-

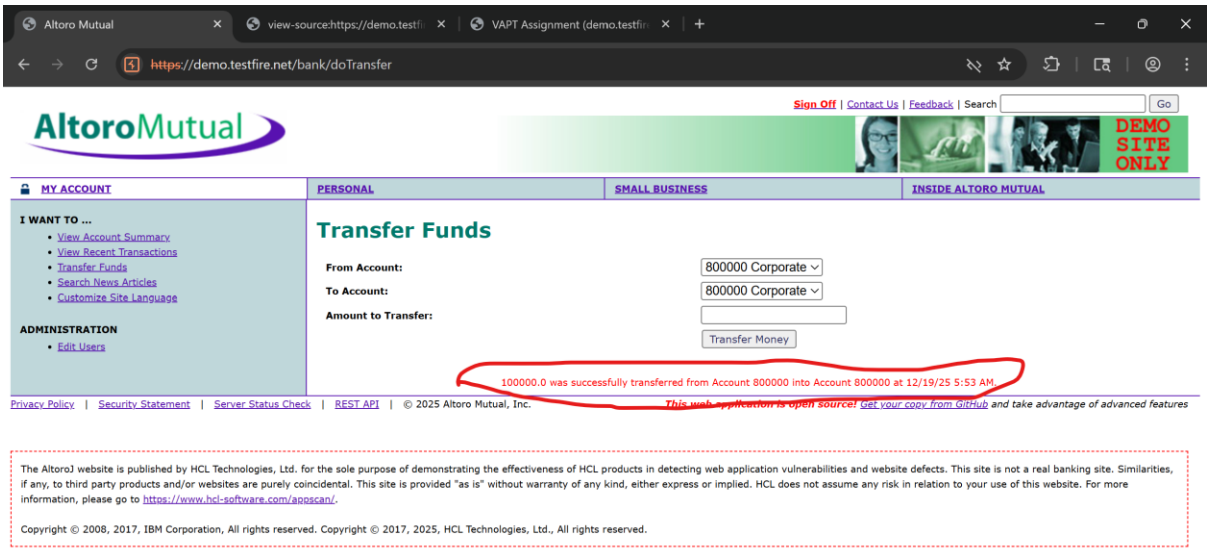
The website allowed copy pasting password in the “password” field.

19. Client-Side Validation Bypass:-

The **‘admin’** is the only one with the rights to transfer funds from one account to another. The javascript in the page https://demo.testfire.net/bank/transfer.jsp is validated such that it prevents transfer of funds in the wrong way such as from one account to itself. So, the javascript was disabled and funds were transferred from one account to itself which in turn generated the regular response as well. Hence, **client-side validation was bypassed**:



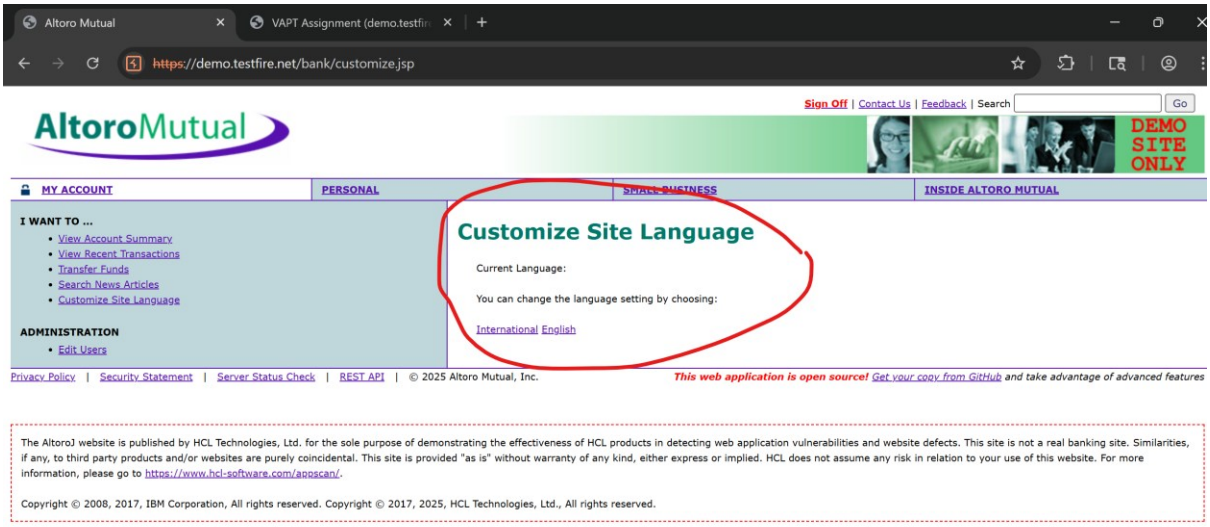


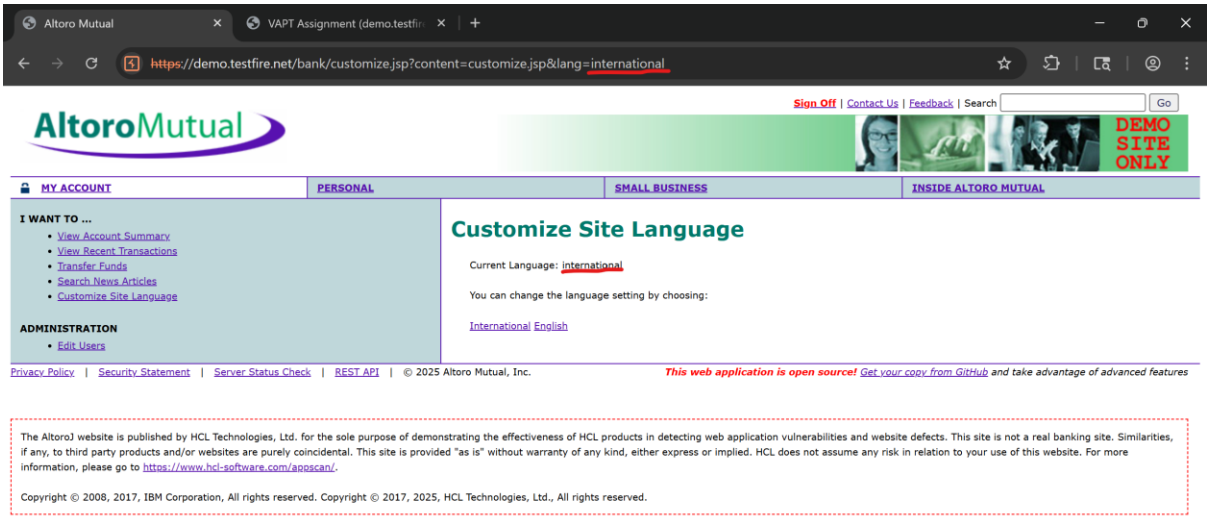


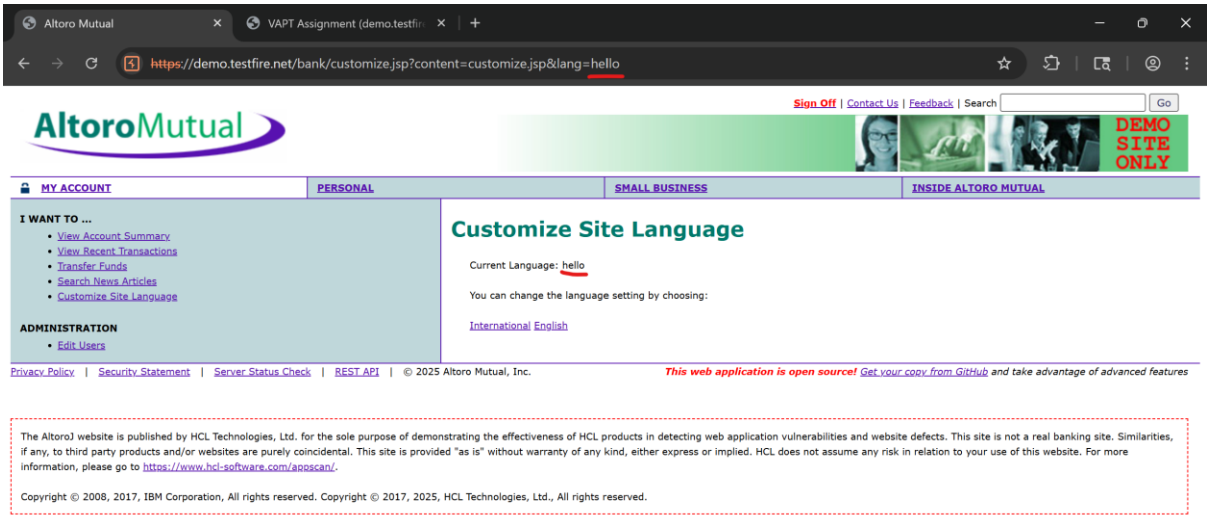
20. Improper Input Validation:-

The **Customize Size Language** page on the URL https://demo.testfire.net/bank/customize.jsp?content=customize.jsp&lang=international reflects whatever value is provided in the **lang** URL parameter as the “Current Language” without validating whether it is a supported language. Although the input is properly encoded and no XSS or SQL injection was possible, this indicates missing server-side input validation and can lead to incorrect

display or potential risk if validation is weakened in the future:

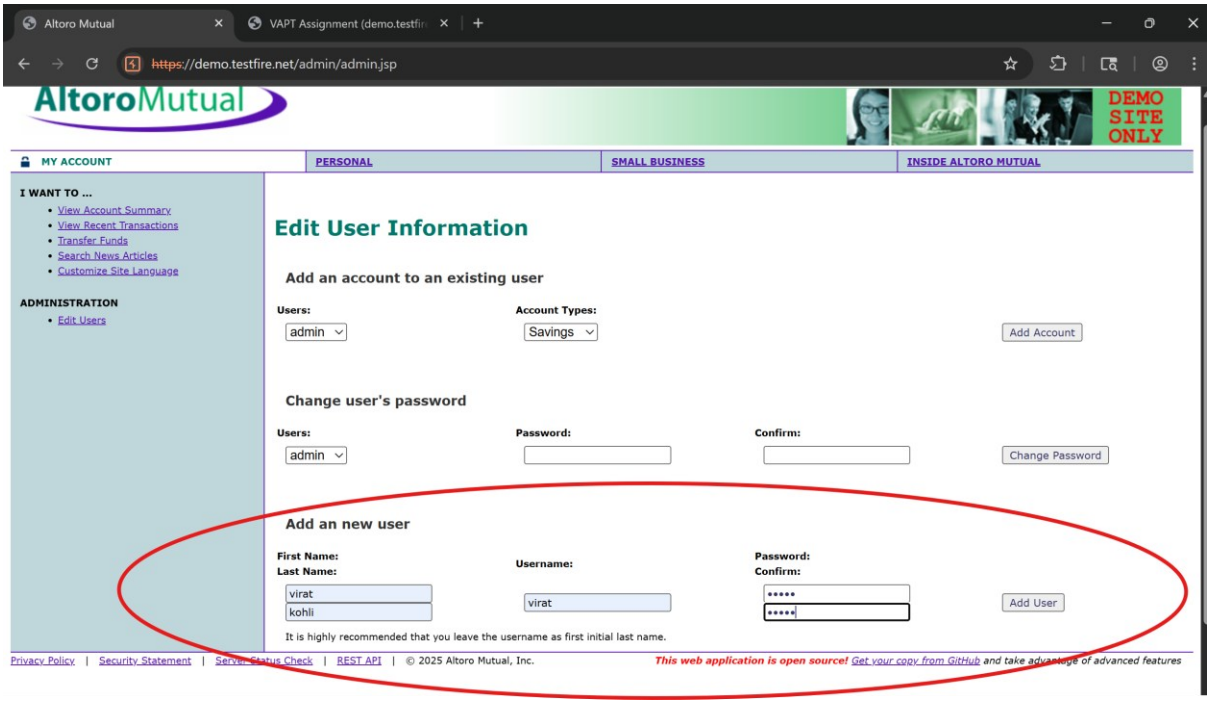


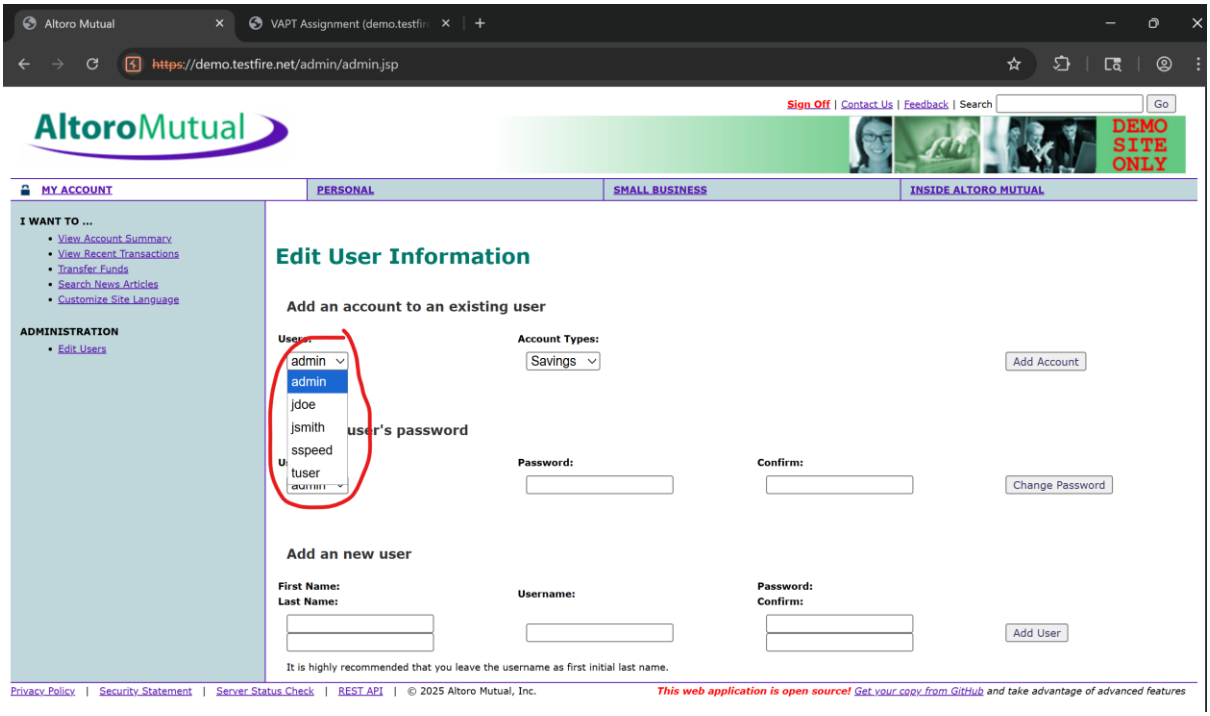




21. Broken Functionality:-

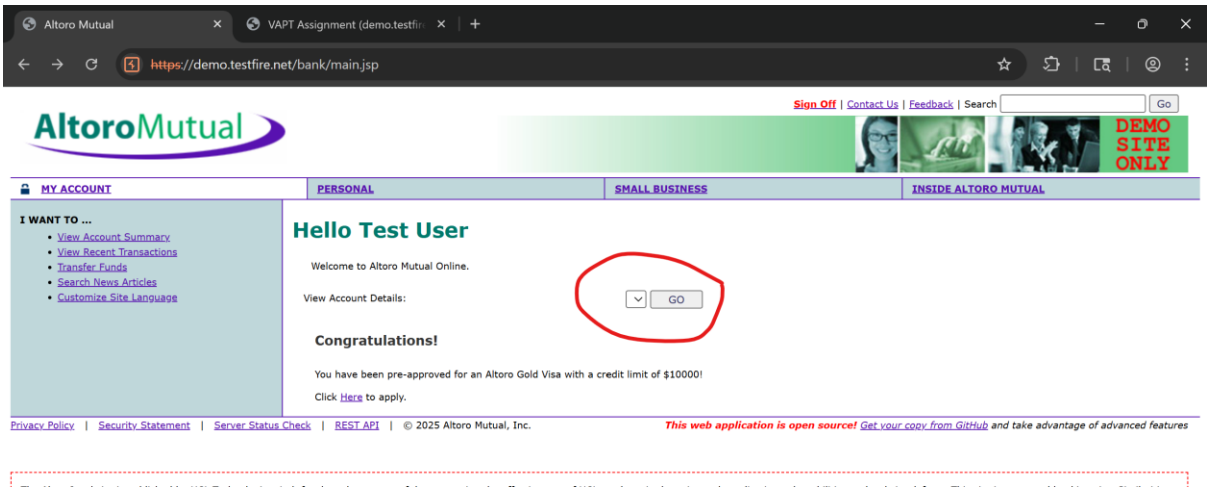
The **Edit Users** page is on https://demo.testfire.net/admin/admin.jsp. Even with admin rights one can't add a new user or add an account to an existing user. After submitting the details the user is not added in the drop down menu of "Users":





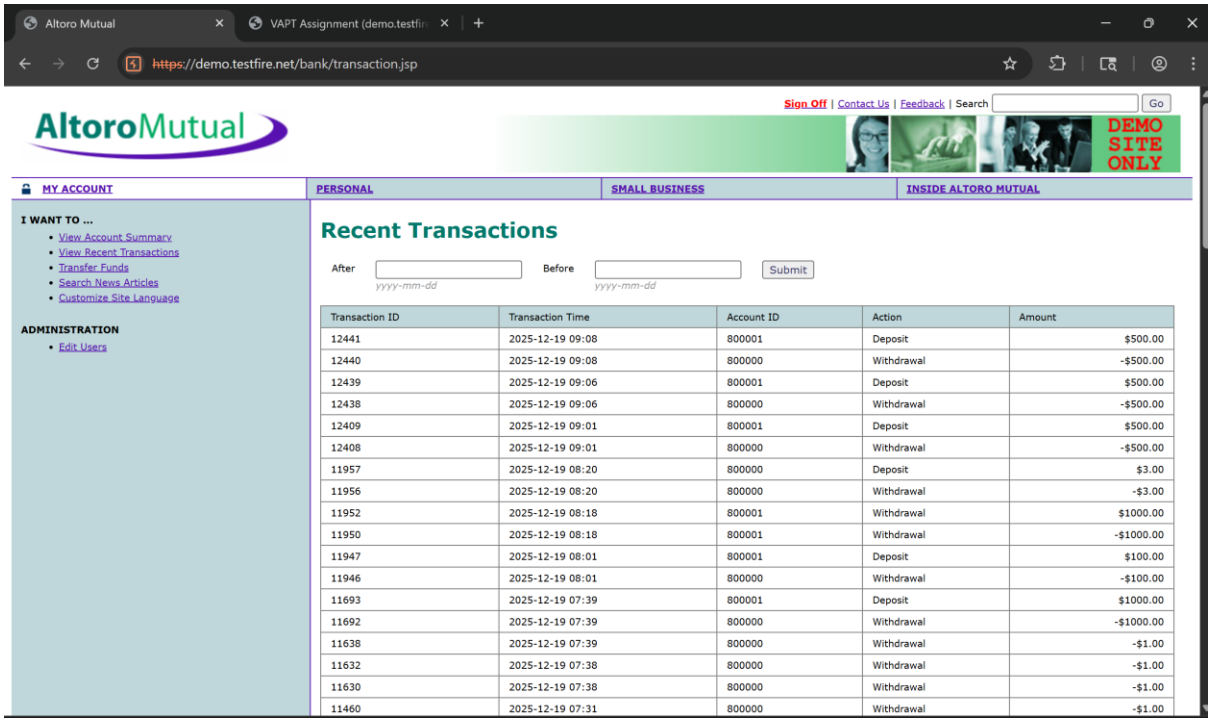
22. Broken Access Control:-

Password can be changed by **'admin'** for all users on https://demo.testfire.net/login.jsp. But only "tuser" can login using this method. Test user himself can't view his account details on **View Account Summary** running on https://demo.testfire.net/bank/main.jsp:



23. Authorization Handling Bug:-

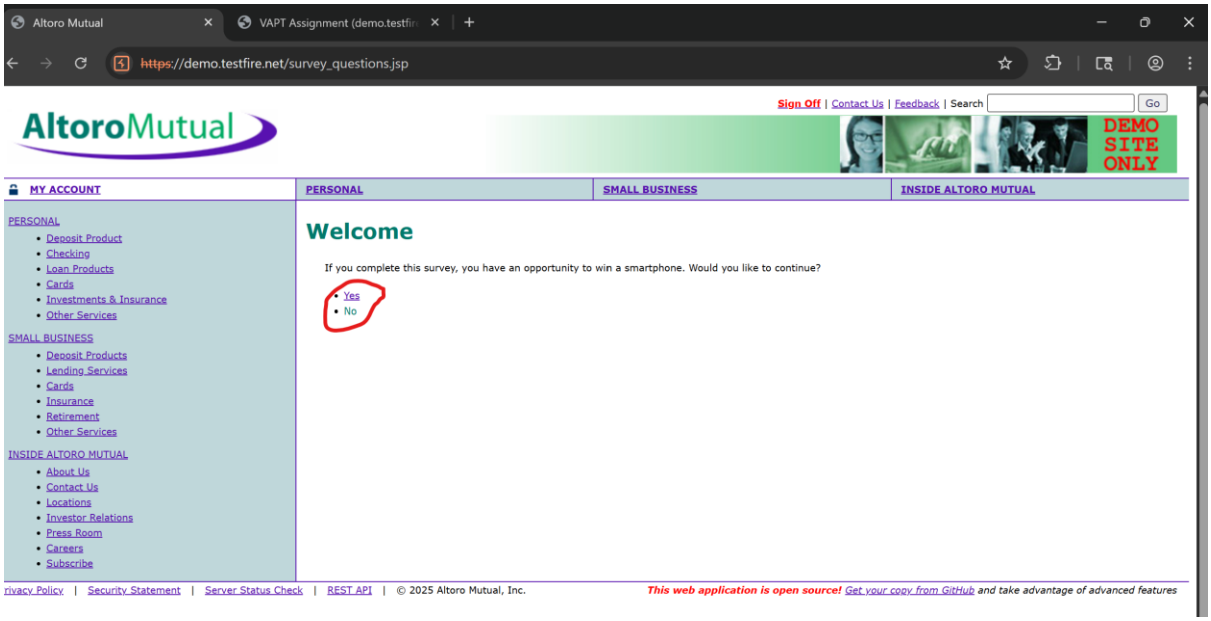
The **View Recent Transactions** page on https://demo.testfire.net/bank/transaction.jsp can be accessed by **'admin'** but gives an error for other users:



24. Broken Confirmation Logic:-

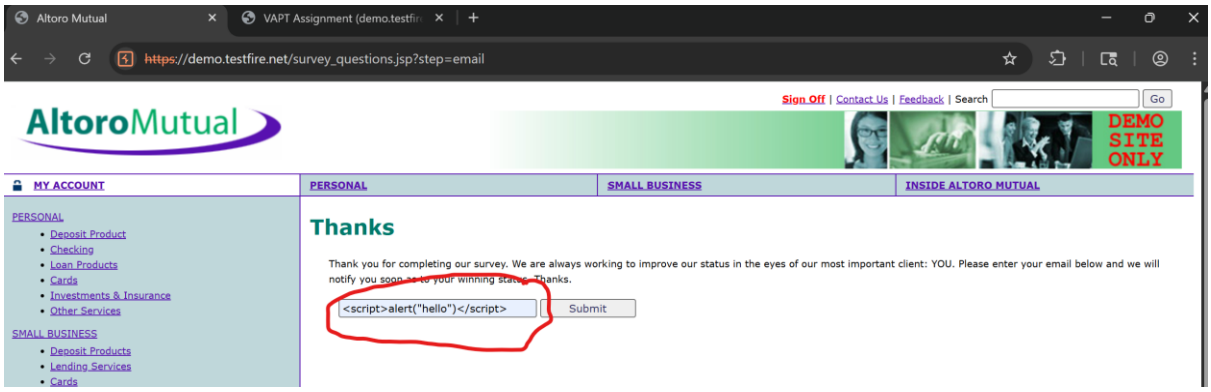
A survey was found on this link: https://demo.testfire.net/survey_questions.jsp.

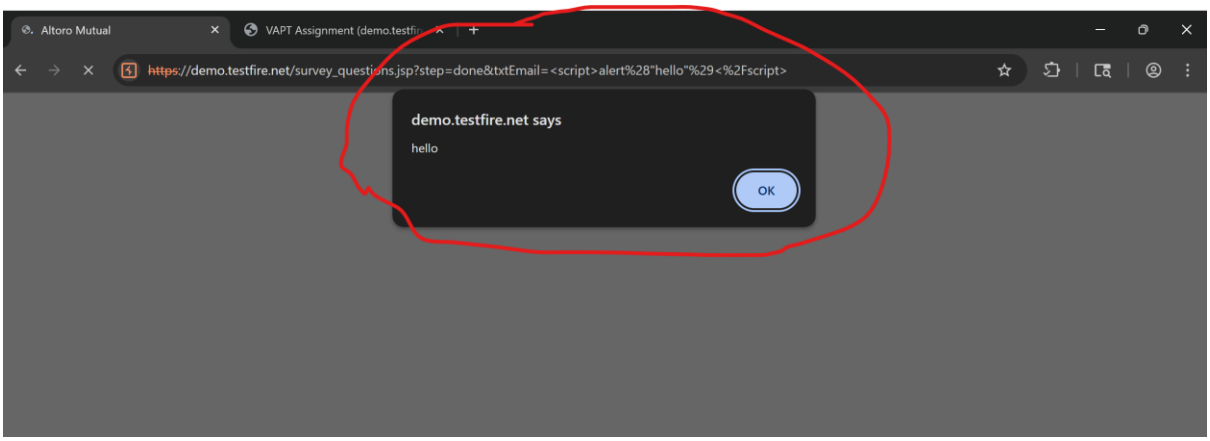
Even if a user selects the “No” option the survey still continues as if user selected “Yes”:



25. Reflected XSS 3:-

The final page of the survey is on the link https://demo.testfire.net/survey_questions.jsp?step=email.
The following JavaScript code was entered which resulted in immediate **Reflected XSS**:
<script>alert("hello")</script>




Altoro Mutual
VAPT Assignment (demo.testfir
https://demo.testfire.net/survey_questions.jsp?step=done&txtEmail=<script>alert%28"hello"%29<%2Fscript>
demo.testfire.net says
hello
OK