

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: -

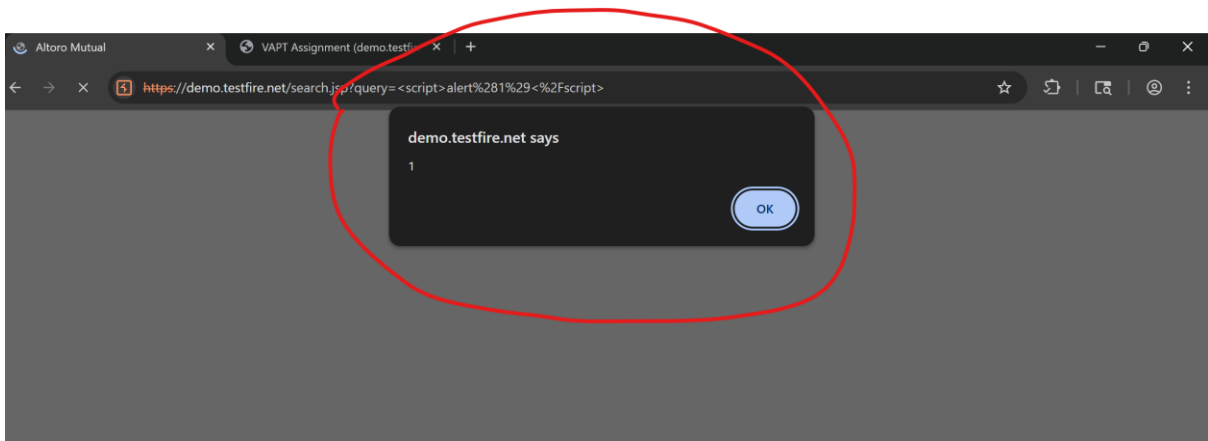
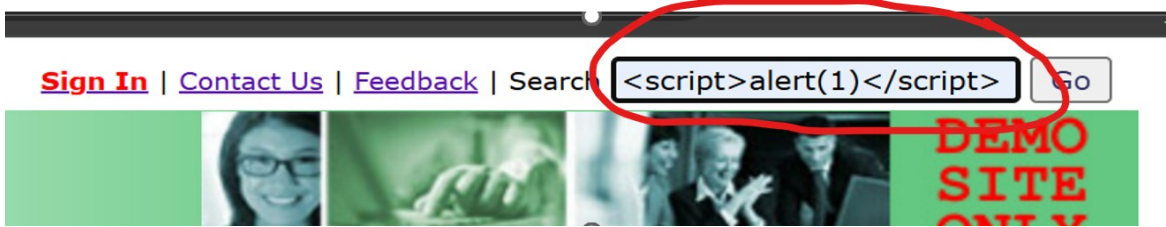
Category	Vulnerability	Count
Injection Attacks	XSS	3
	SQL Injection	1
	Host Header Injection	1
Authentication & Authorization	Broken Authentication	2
	Broken Access Control	1
	Authorization Handling Bug	1
Input Validation Issues	Improper Input Validation	1
	Client-Side Validation Bypass	1
Information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

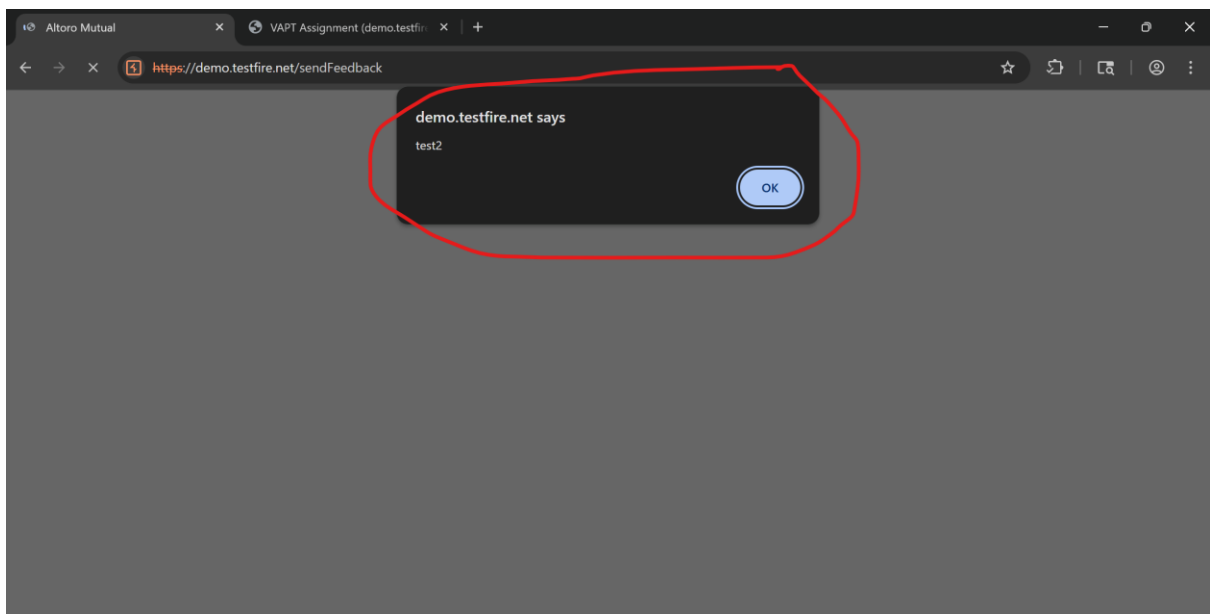
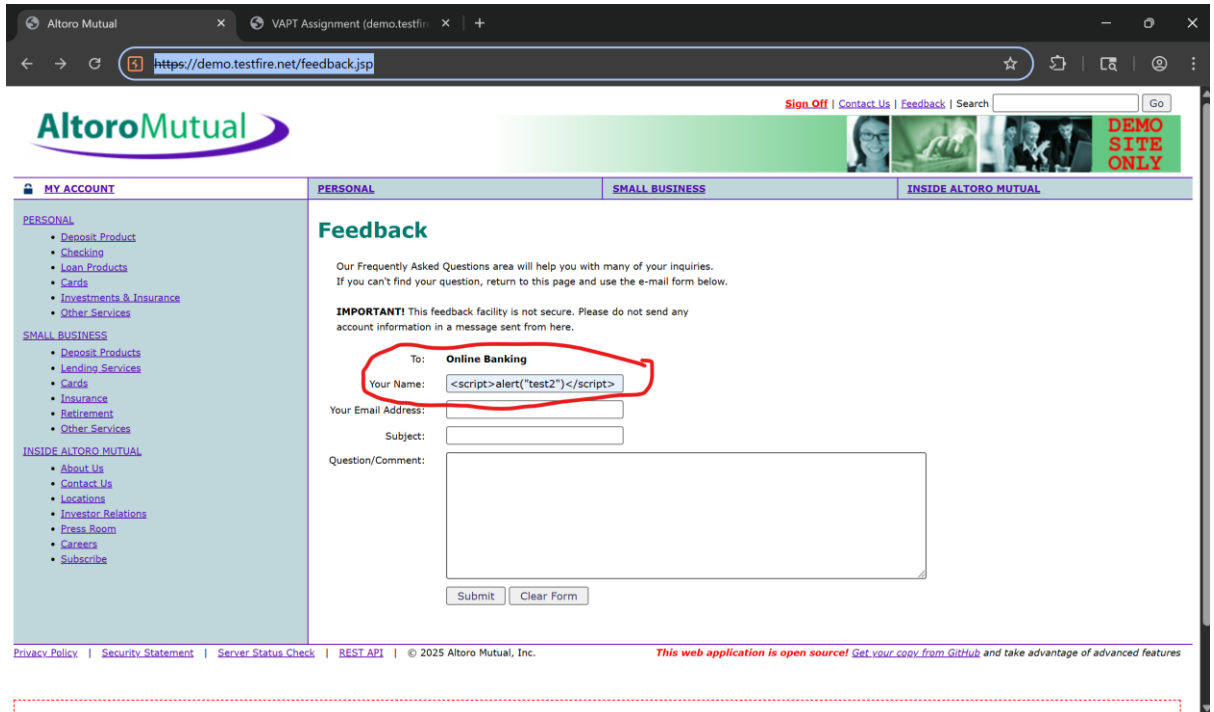
```
<script> alert(1) </script>
```



2. Reflected XSS 2:-

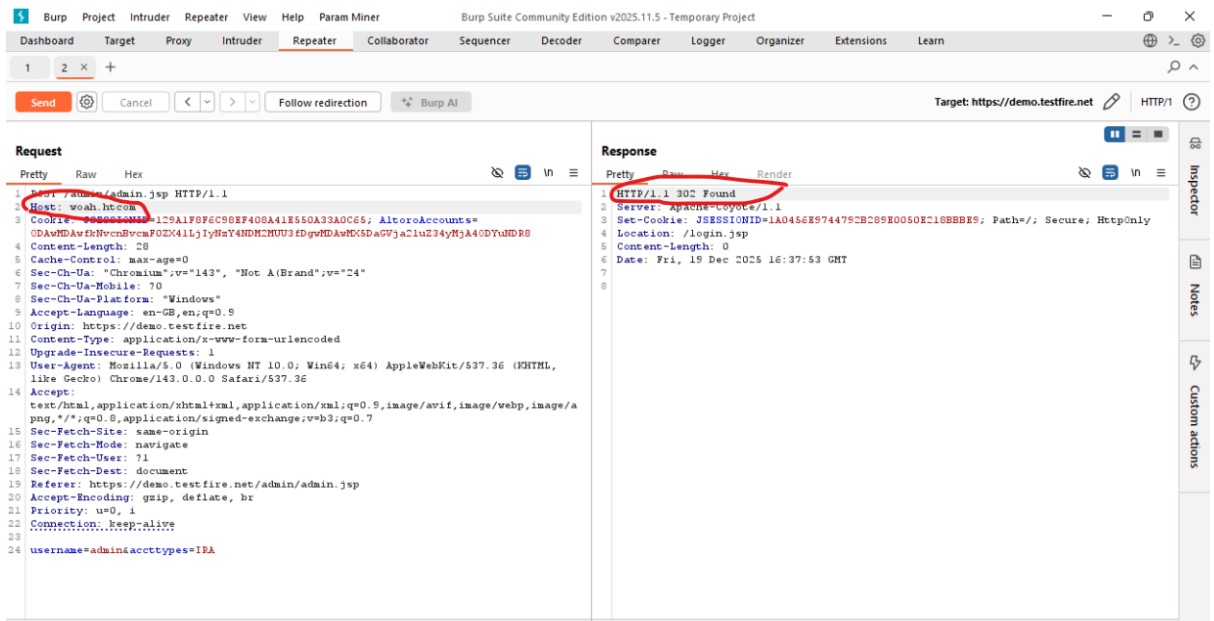
In the Feedback page on link <https://demo.testfire.net/feedback.jsp>, the name field was entered with the following JavaScript code which resulted in immediate **Reflected XSS**:

```
<script> alert("test2") </script>
```



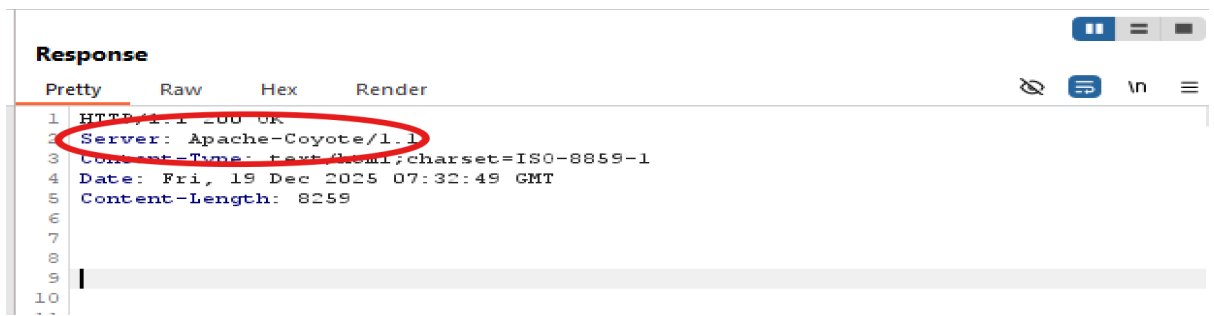
3. Host Header Injection:-

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



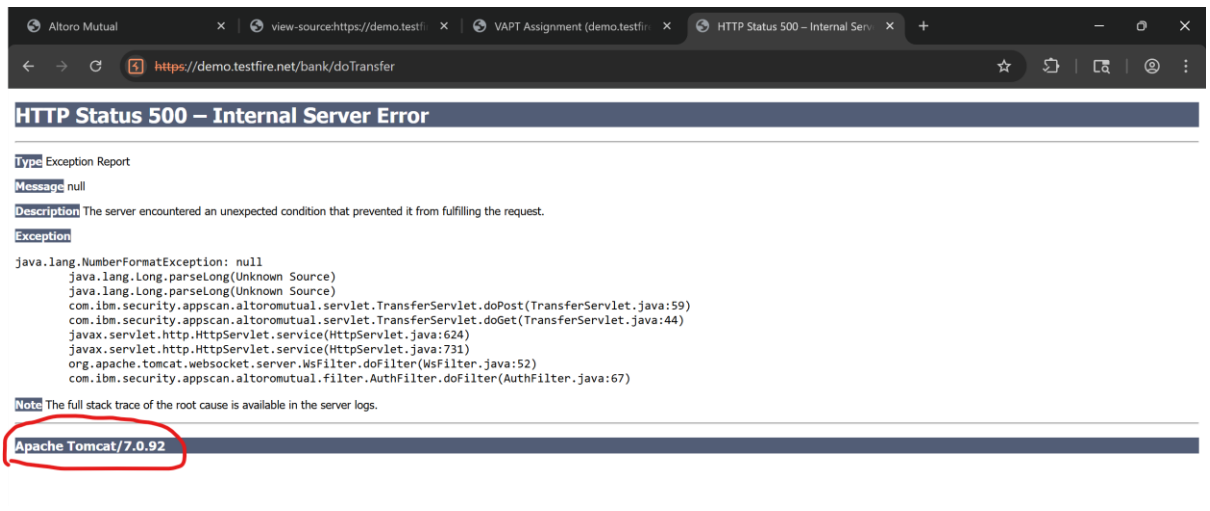
4. Information Disclosure 1:-

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



5. Information Disclosure 2:-

Server version was revealed during error handling:

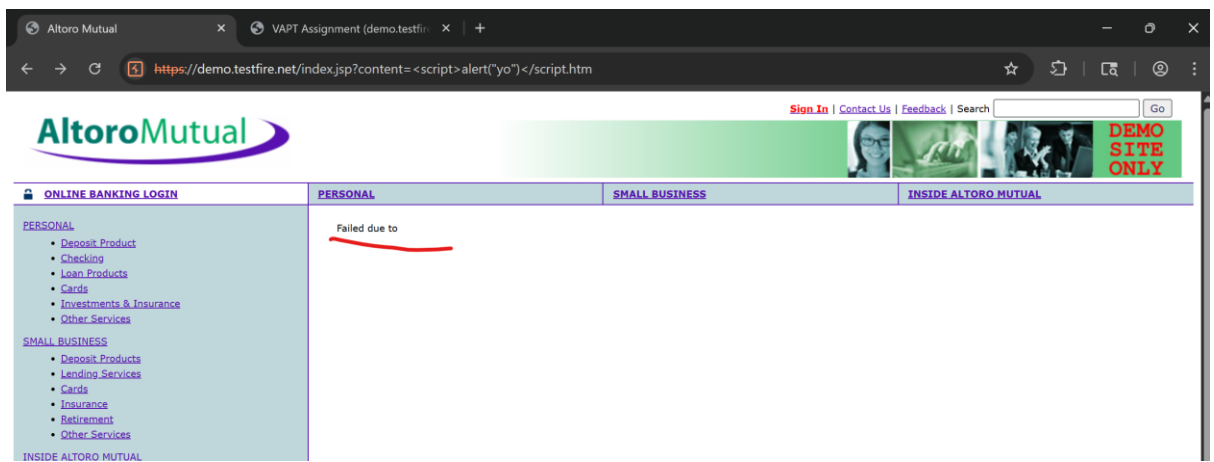


6. Incorrect Error Handling:-

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:

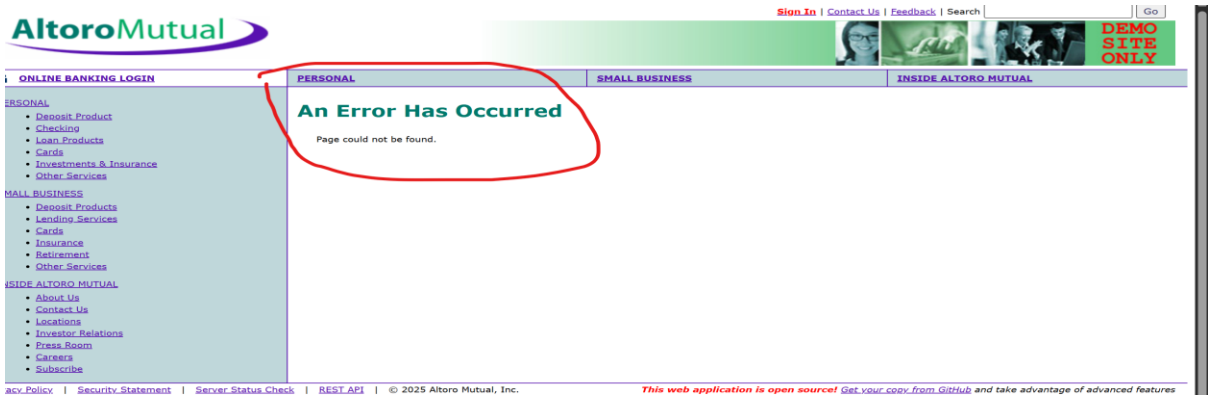
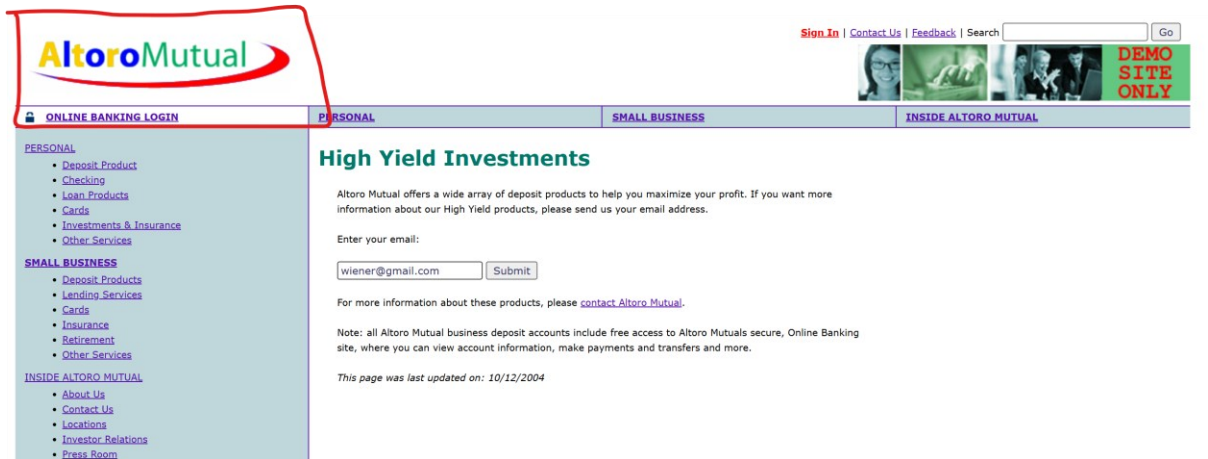


8. Broken Link/Dead Link 1:-

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:

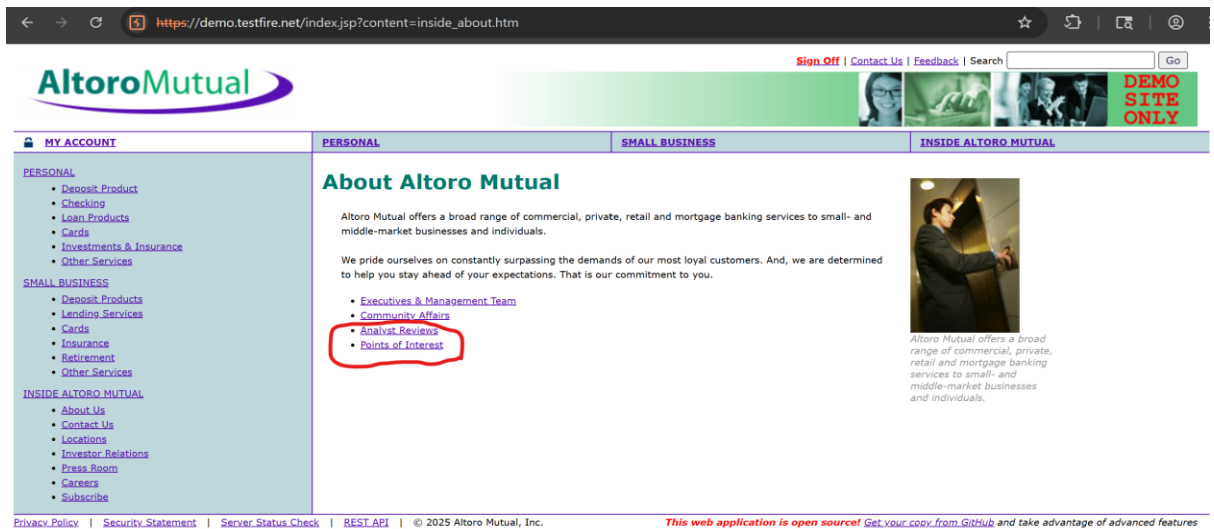
The screenshot shows the Altoro Mutual website. The URL in the browser is https://demo.testfire.net/index.jsp?content=inside_about.htm. The page has a header with the Altoro Mutual logo and navigation links: Sign Off, Contact Us, Feedback, and a search bar. A 'DEMO SITE ONLY' banner is visible on the right. The main content area is titled 'About Altoro Mutual' and includes a list of links: Executives & Management Team, Community Affairs, Analyst Reviews, and Points of Interest. The 'Points of Interest' link is circled in red. A sidebar on the left contains navigation menus for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. At the bottom, there is a footer with legal notices and a statement: 'This web application is open source! Get your copy from GitHub and take advantage of advanced features'.

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/amoscan/>.

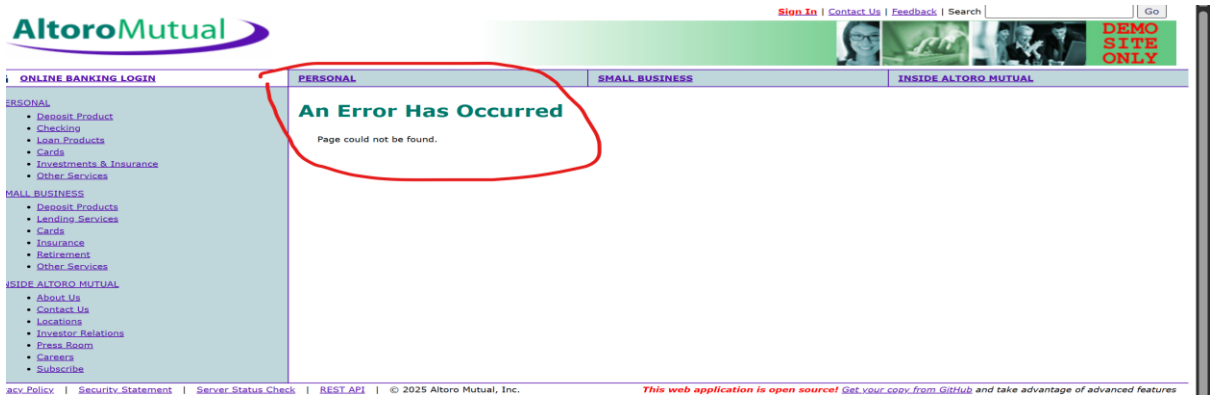
The screenshot shows a browser window with the URL <https://www.newspapersyndications.tv>. The browser title is 'Burp Suite Community Edition'. The page displays an error message: 'Error: Unknown host: www.newspapersyndications.tv'. This indicates a 404 error due to an unreachable host.

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**:

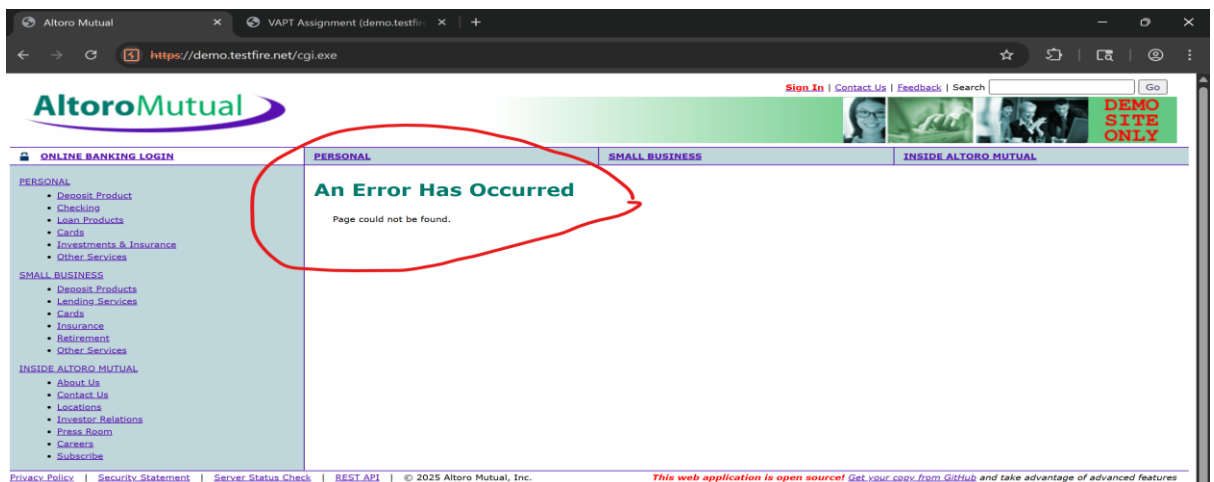


The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/aoscan/>.



11. Broken Link/Dead Link 4:-

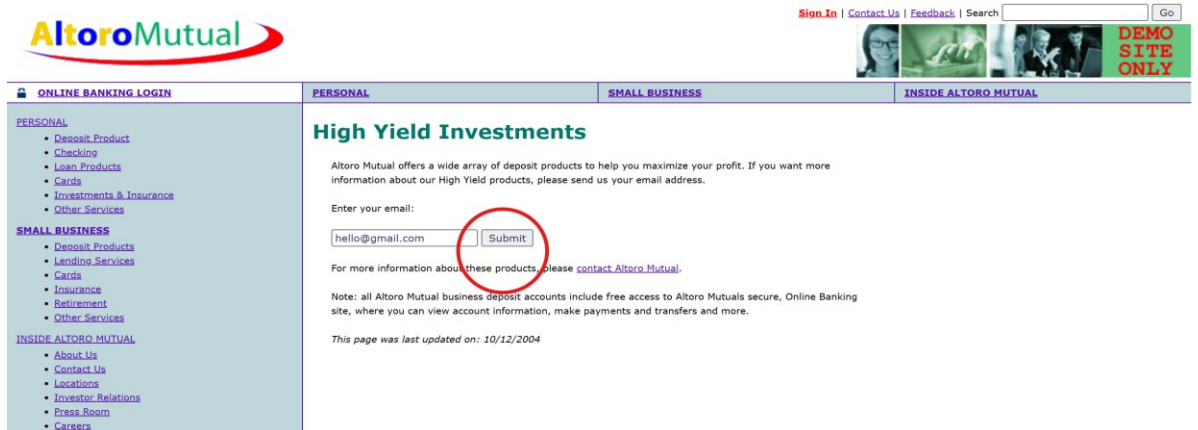
The **Locations** page on <https://demo.testfire.net/cgi.exe> was selected and met with **404 error**:



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:



The screenshot shows the Altoro Mutual website. The header includes the logo and navigation links: Sign In, Contact Us, Feedback, Search, and Go. Below the header is a navigation bar with three tabs: ONLINE BANKING LOGIN, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. The main content area is titled 'High Yield Investments' and contains a form for entering an email address. The 'Submit' button is circled in red. The form includes a text input field with the value 'hello@gmail.com' and a 'Submit' button. The page also contains a note about account security and a last updated date of 10/12/2004.

```
<body style="margin-top:5px;">
<div id="header" style="margin-bottom:5px; width: 99%;">
<div id="wrapper" style="width: 99%;">
  <table cellpadding="0" width="100%">
    <tbody>
      <tr>
        <td colspan="3">
          <div class="fl" style="width: 67%;">
            <h1>High Yield Investments</h1>
            <p></p>
            <p id="email">Enter your email:</p>
            <p>
              <input type="text" name="email">
              <input type="submit" name="submit" value="Submit">
            </p>
            <p></p>
            <p></p>
            <p></p>
            <script></script>
          </div>
        </td>
      </tr>
    </tbody>
  </table>
</div>
```

13. Information Disclosure 3:-

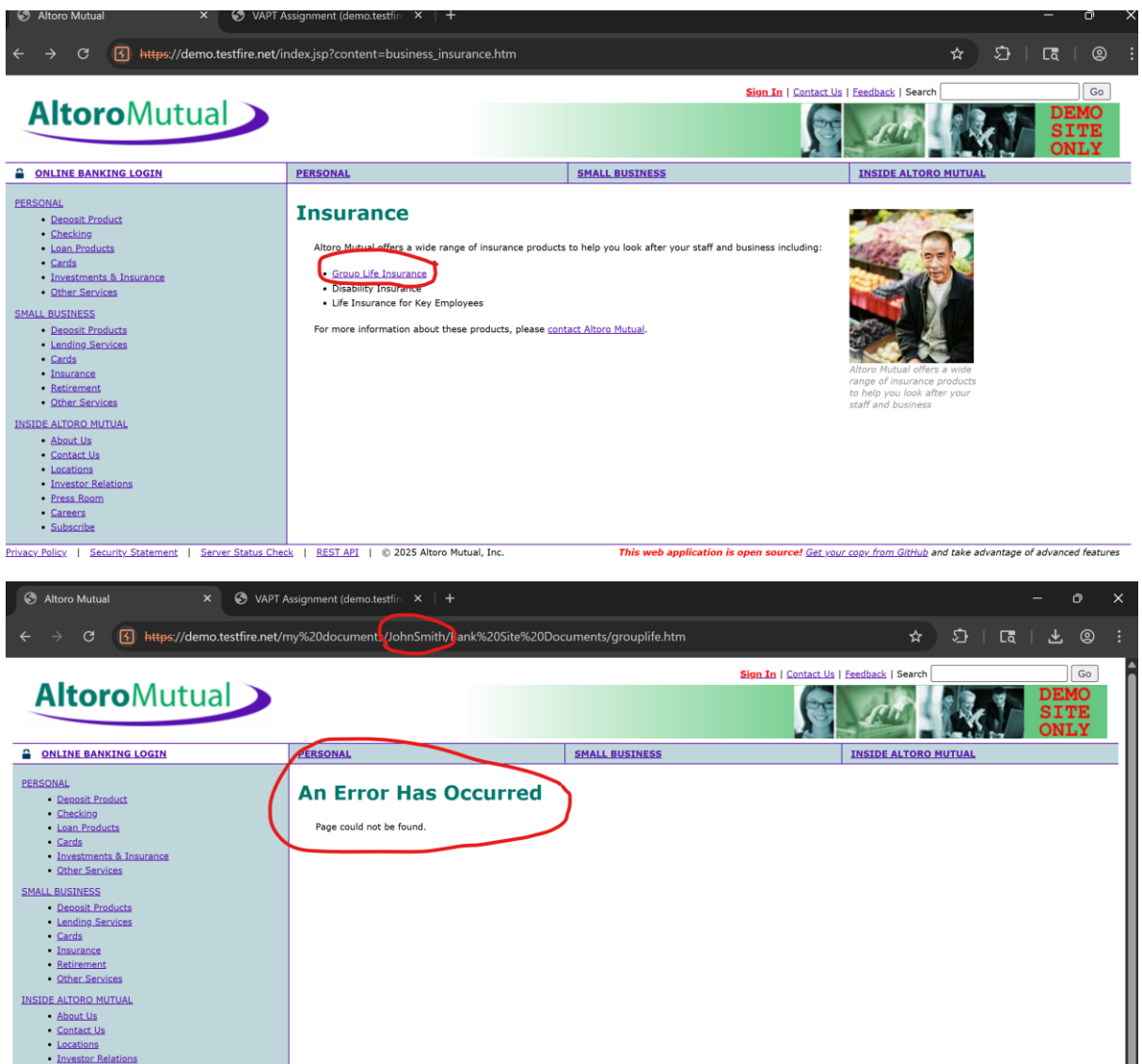
This page was found:

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:



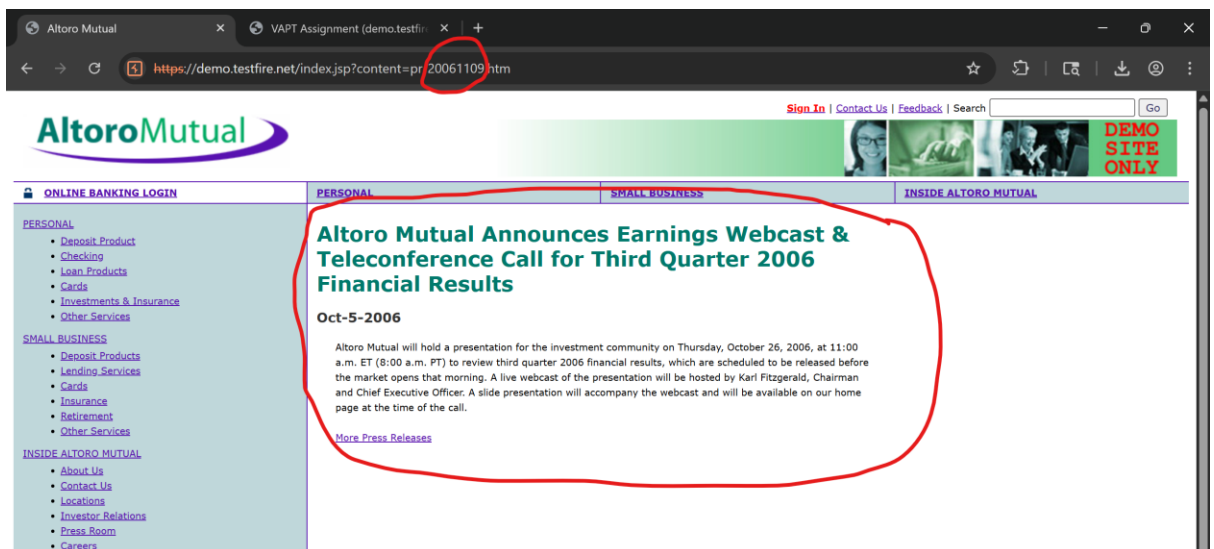
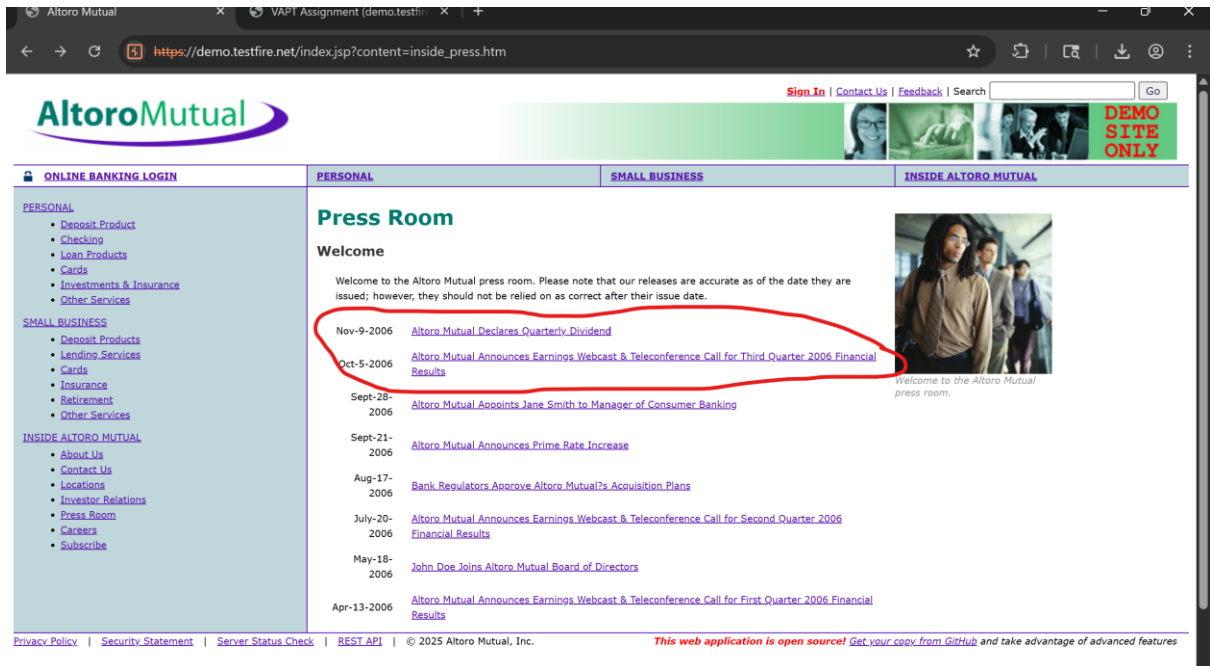
14. Incorrect Backend Mapping:-

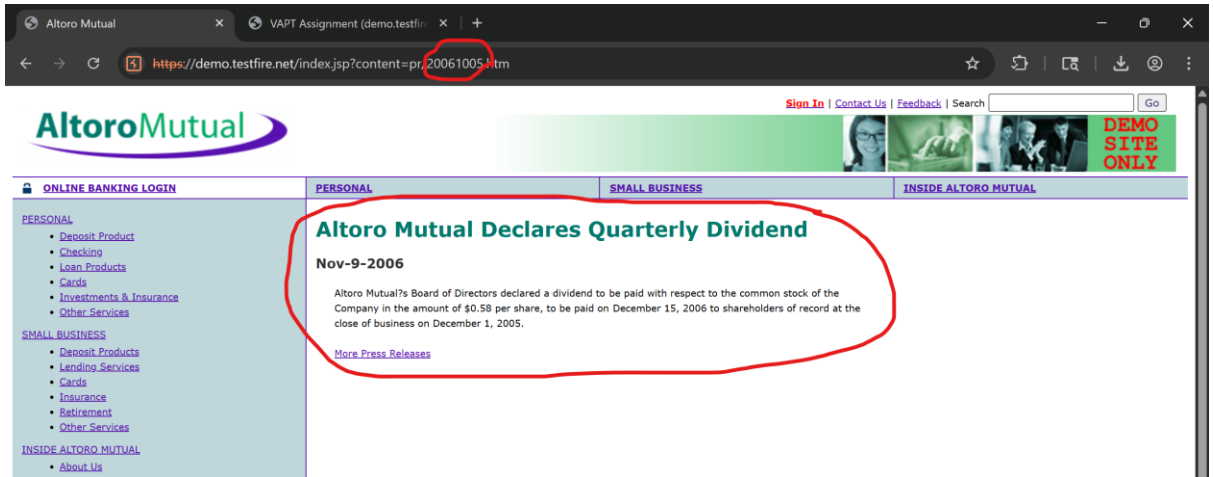
In the **Press Room** section on the link https://demo.testfire.net/index.jsp?content=inside_press.htm, the first two press release links behave inconsistently compared to the rest:

- 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: -

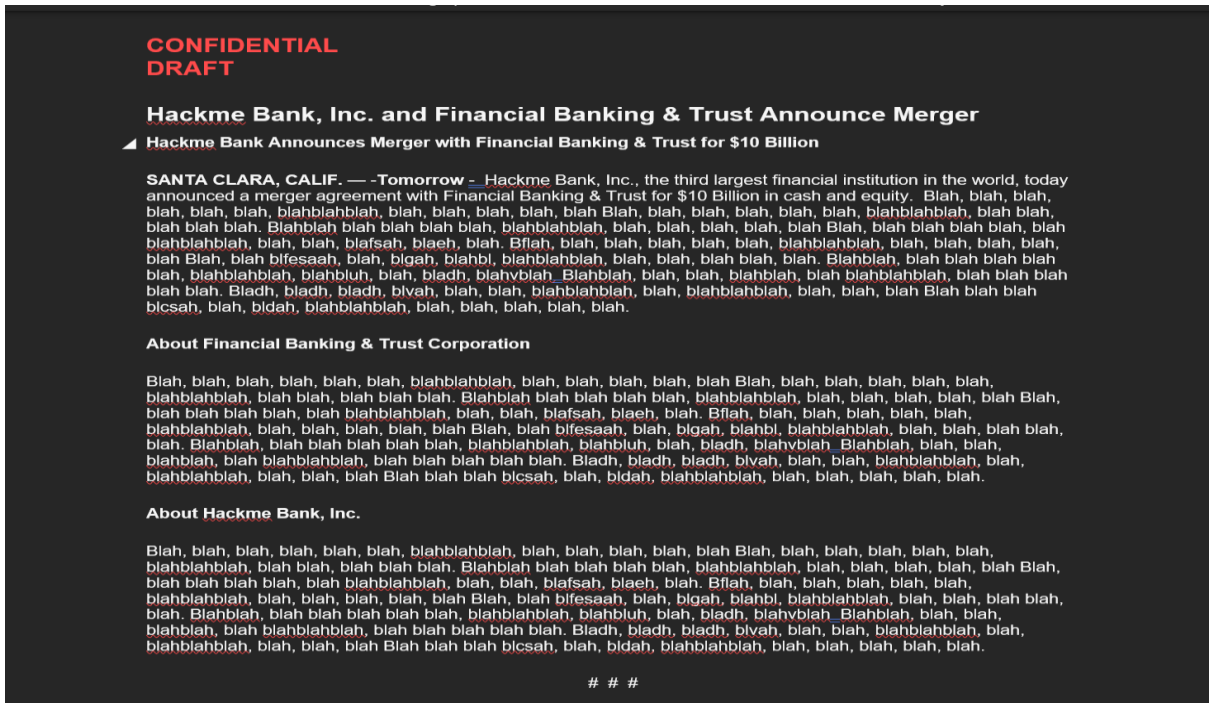
Directory listing was not disabled on this link:

<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:



Not For Immediate Release
Contact:

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

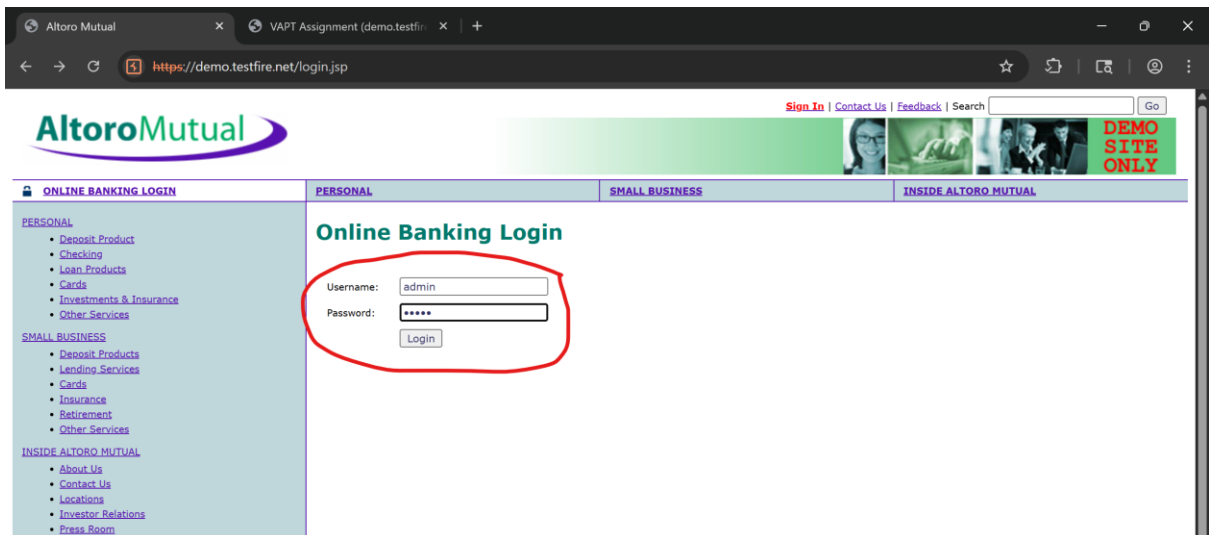
Jean Enerson
PR Communications, Inc.
(415) 123-4567
[Hackme Bank@prcommunications.com](mailto:HackmeBank@prcommunications.com)

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**.



The screenshot shows the AltoroMutual website interface. At the top right, there are links for 'Sign Off', 'Contact Us', and 'Feedback', along with a search bar and a 'Go' button. Below this is a navigation bar with 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL' tabs. The main content area displays 'Hello Admin User' with a welcome message and account details for '800000 Corporate'. A 'Congratulations!' message states the user is pre-approved for an Altoro Gold Visa with a credit limit of \$10000. A sidebar on the left contains navigation links under 'I WANT TO ...' and 'ADMINISTRATION'. The footer includes a privacy policy, security statement, server status check, REST API, and copyright information for 2025 Altoro Mutual, Inc.

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/aposcan/>.

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.

The screenshot shows the AltoroMutual website's 'Online Banking Login' page. The URL in the browser is 'https://demo.testfire.net/login.jsp'. The page features the AltoroMutual logo and navigation tabs for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The main content area is titled 'Online Banking Login' and contains a form with 'Username:' and 'Password:' fields, both of which are circled in red. The 'Username' field contains the text 'OR 1=1--' and the 'Password' field contains '****'. A 'Login' button is positioned below the password field. The sidebar on the left lists various services under 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The footer includes a privacy policy, security statement, server status check, REST API, and copyright information for 2025 Altoro Mutual, Inc.

This screenshot is identical to the one at the top of the page, showing the AltoroMutual website with a user logged in as 'Admin User'. It displays the same navigation, account details, and 'Congratulations!' message as the first screenshot.

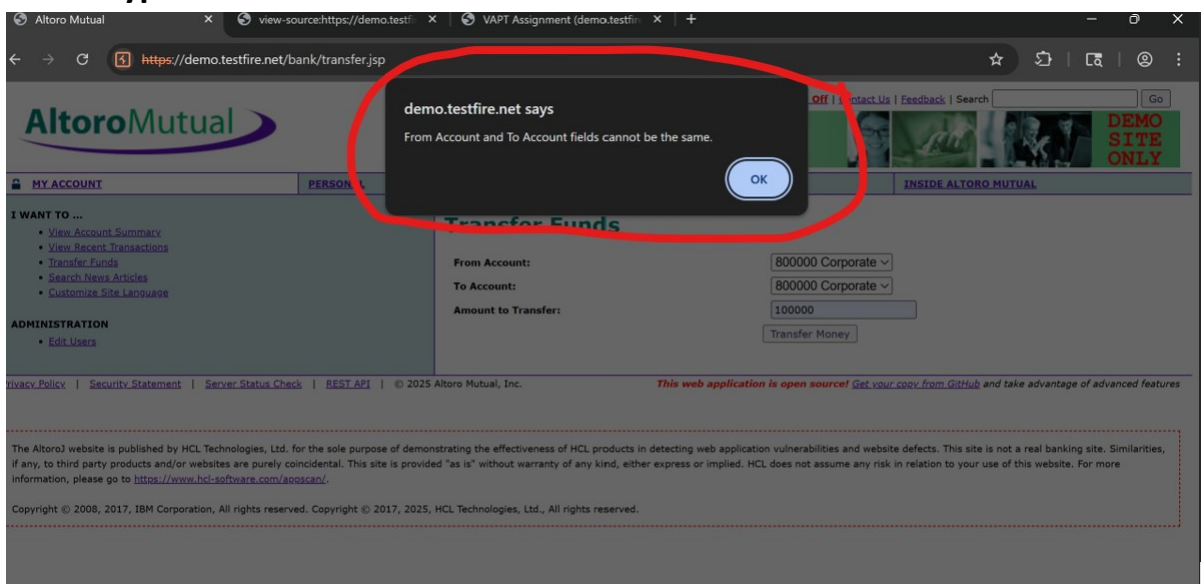
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/aposcan/>.

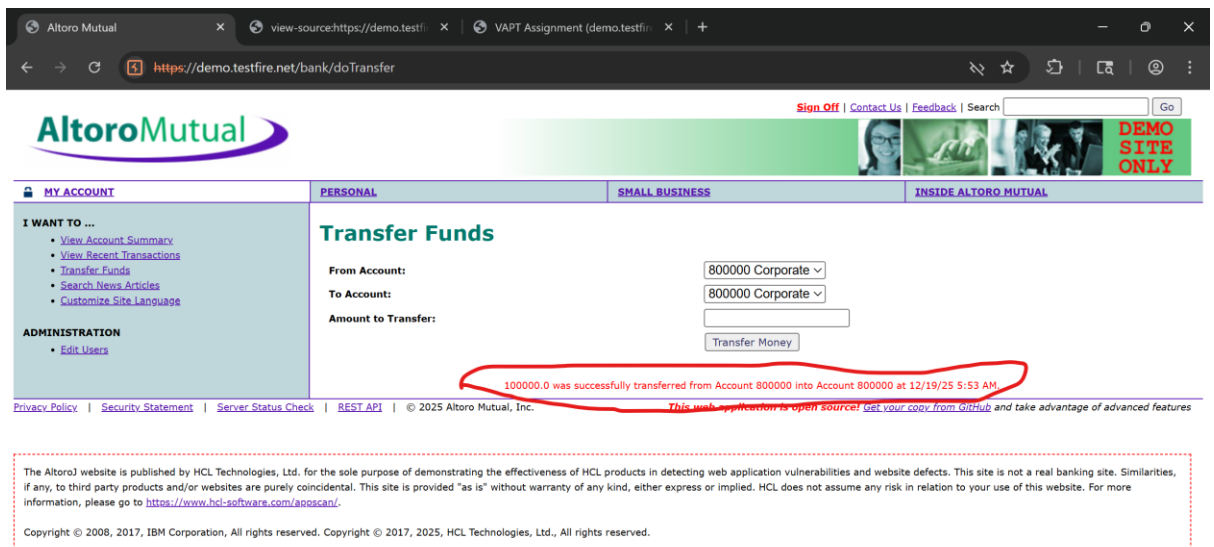
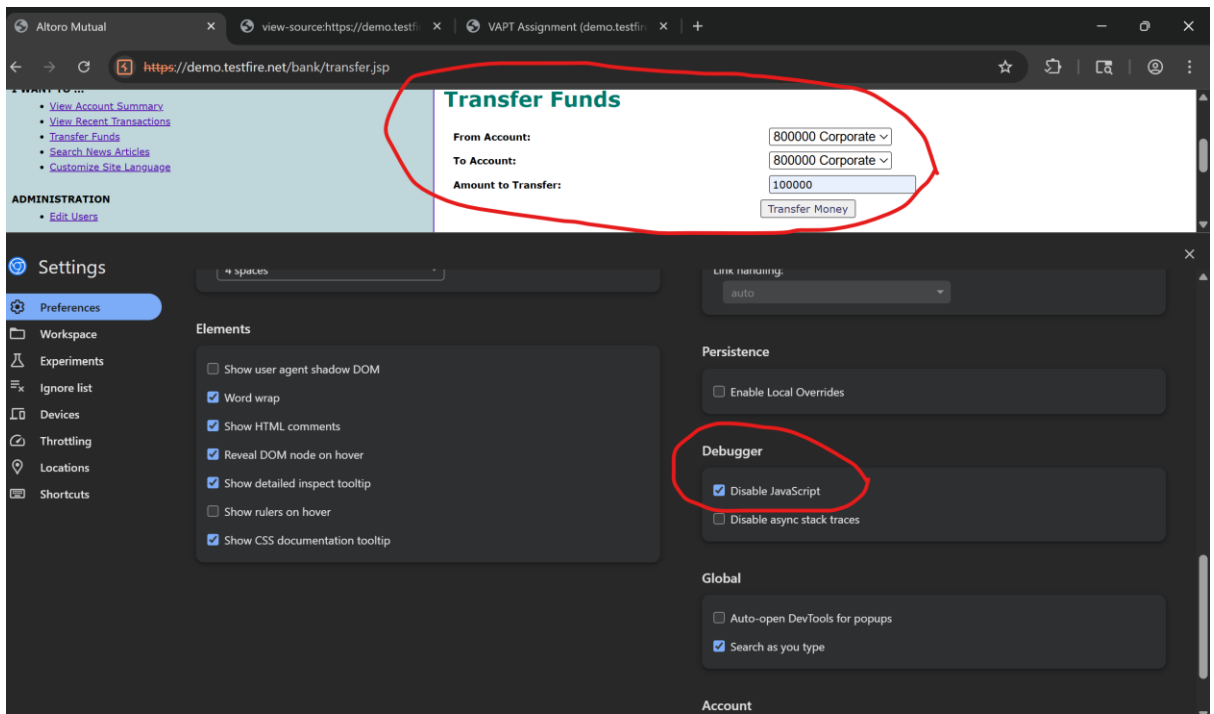
18. Clipboard Data Exposure:-

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:**





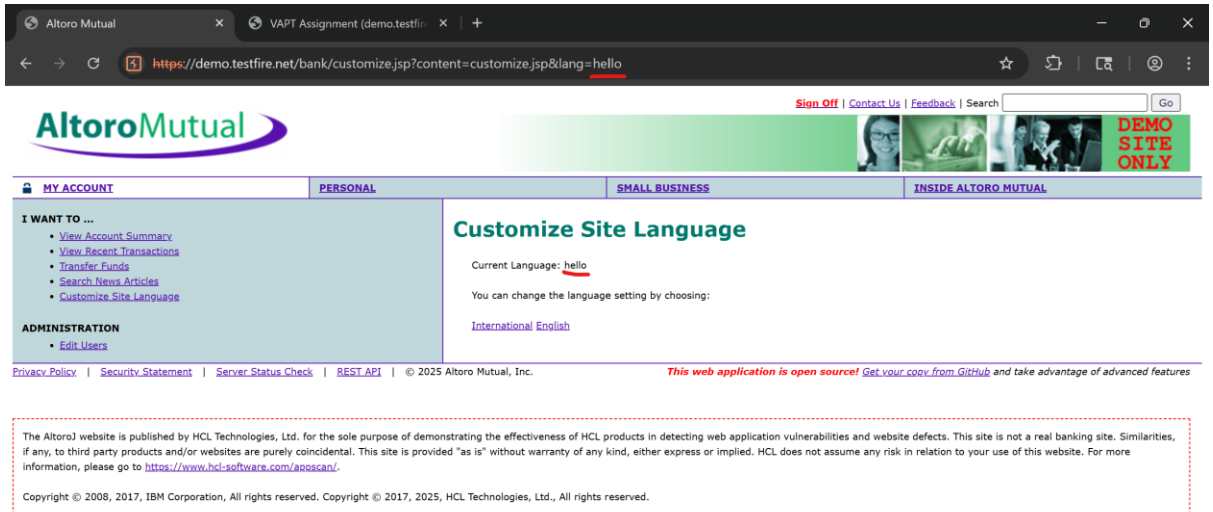
20. Improper Input Validation:-

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:

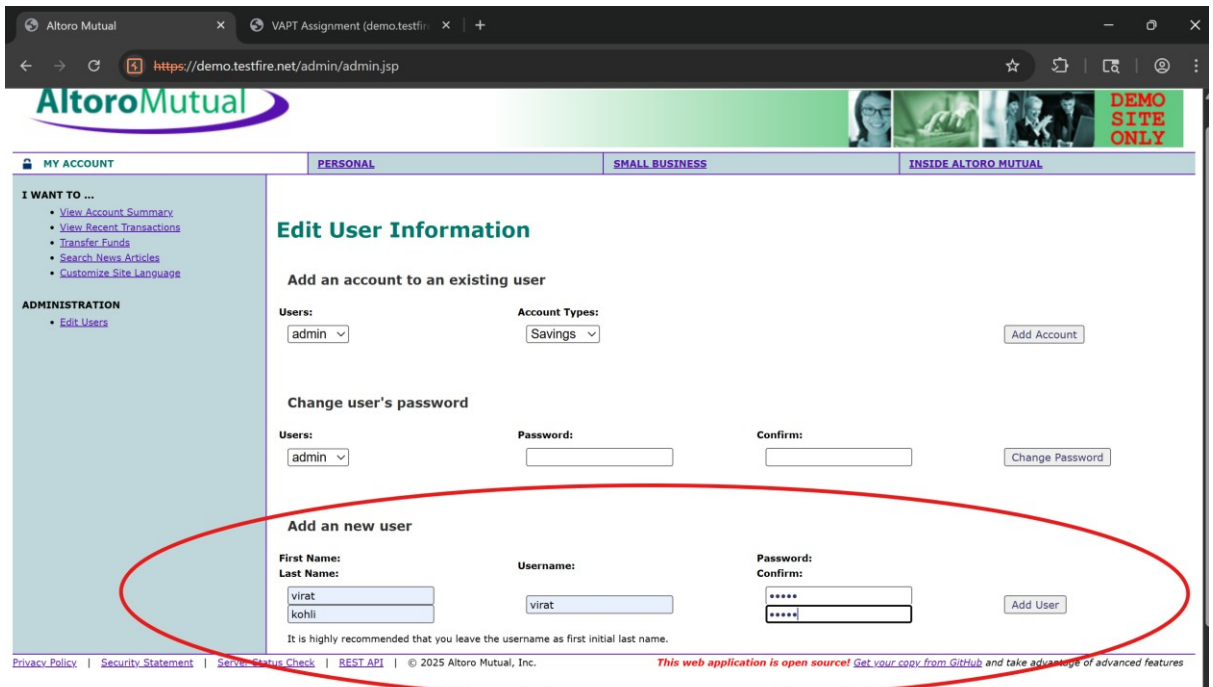
The screenshot shows a web browser window with the URL <https://demo.testfire.net/bank/customize.jsp>. The page features the AltoroMutual logo and navigation tabs for 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is active, and the 'Customize Site Language' page is displayed. The page content includes a sidebar with links like 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. The main content area shows 'Current Language: International English' and a link to 'International English'. A red circle highlights the 'Customize Site Language' section. The footer contains a disclaimer and copyright information.

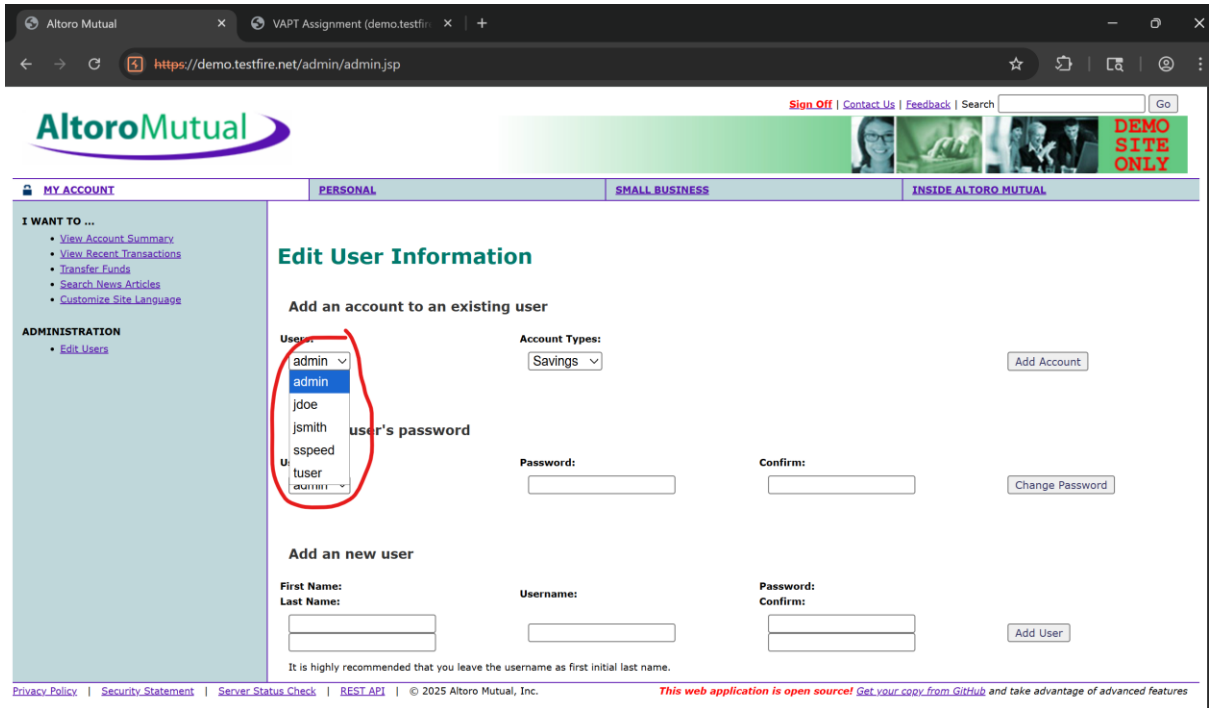
The screenshot shows a web browser window with the URL <https://demo.testfire.net/bank/customize.jsp?content=customize.jsp&lang=international>. The page features the AltoroMutual logo and navigation tabs for 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is active, and the 'Customize Site Language' page is displayed. The page content includes a sidebar with links like 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. The main content area shows 'Current Language: international' and a link to 'International English'. The 'International English' link is highlighted. The footer contains a disclaimer and copyright information.



21. Broken Functionality:-

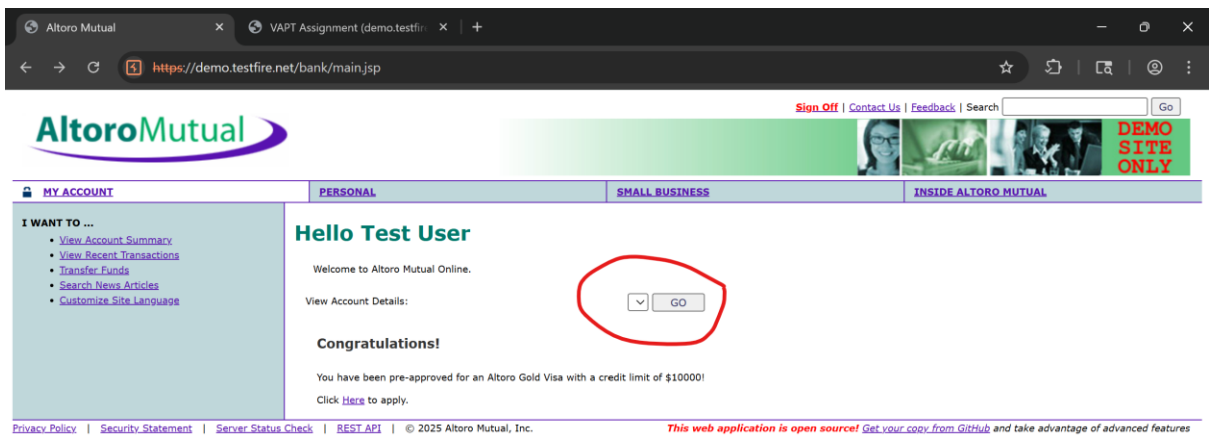
The **Edit Users** page is on <https://demo.testfire.net/admin/admin.jsp>. Even with admin rights one can't add a new user or add an account to an existing user. After submitting the details the user is not added in the drop down menu of "Users":





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>:

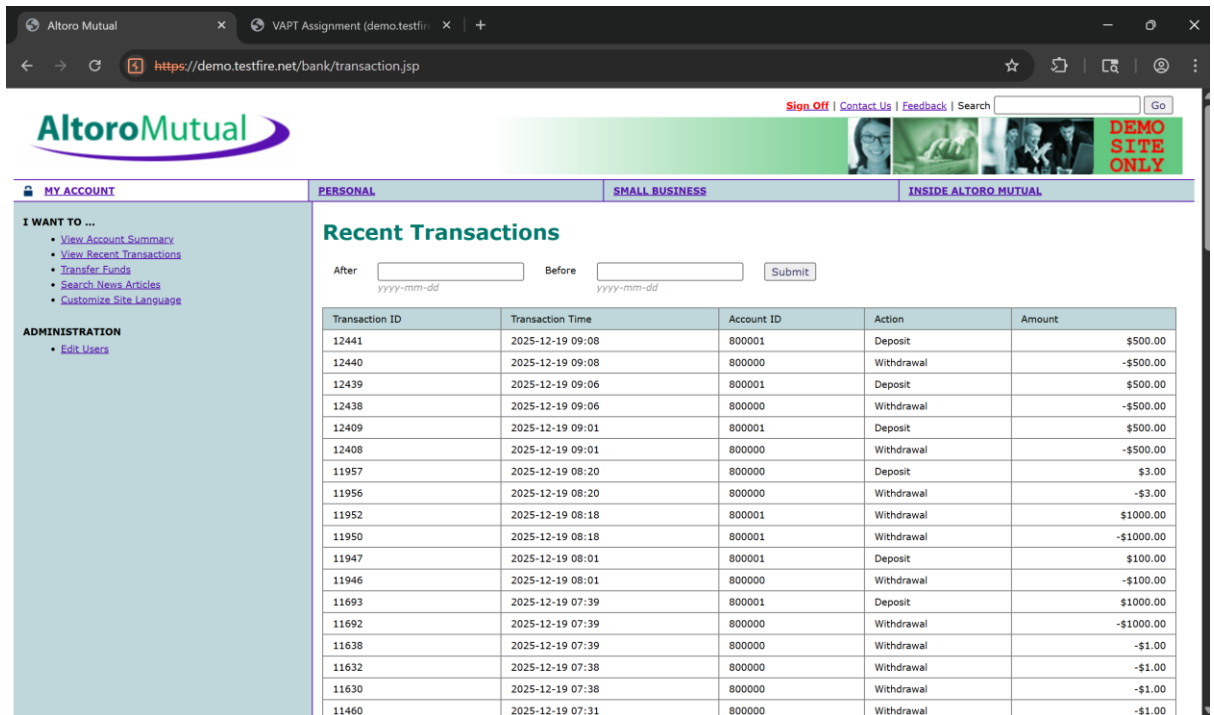


23. Authorization Handling Bug:-

The **View Recent Transactions** page on

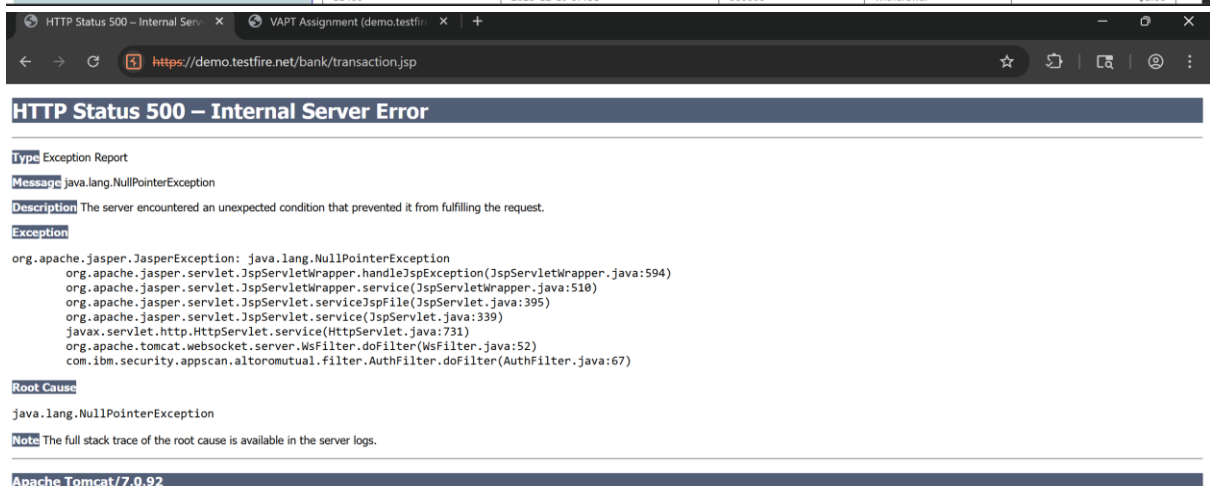
<https://demo.testfire.net/bank/transaction.jsp> can be accessed by

'admin' but gives an error for other users:



The screenshot shows the Altoro Mutual website interface. The main content area is titled "Recent Transactions" and features a table with the following data:

Transaction ID	Transaction Time	Account ID	Action	Amount
12441	2025-12-19 09:08	800001	Deposit	\$500.00
12440	2025-12-19 09:08	800000	Withdrawal	-\$500.00
12439	2025-12-19 09:06	800001	Deposit	\$500.00
12438	2025-12-19 09:06	800000	Withdrawal	-\$500.00
12409	2025-12-19 09:01	800001	Deposit	\$500.00
12408	2025-12-19 09:01	800000	Withdrawal	-\$500.00
11957	2025-12-19 08:20	800000	Deposit	\$3.00
11956	2025-12-19 08:20	800000	Withdrawal	-\$3.00
11952	2025-12-19 08:18	800001	Withdrawal	\$1000.00
11950	2025-12-19 08:18	800001	Withdrawal	-\$1000.00
11947	2025-12-19 08:01	800001	Deposit	\$100.00
11946	2025-12-19 08:01	800000	Withdrawal	-\$100.00
11693	2025-12-19 07:39	800001	Deposit	\$1000.00
11692	2025-12-19 07:39	800000	Withdrawal	-\$1000.00
11638	2025-12-19 07:39	800000	Withdrawal	-\$1.00
11632	2025-12-19 07:38	800000	Withdrawal	-\$1.00
11630	2025-12-19 07:38	800000	Withdrawal	-\$1.00
11460	2025-12-19 07:31	800000	Withdrawal	-\$1.00



The screenshot shows an "HTTP Status 500 - Internal Server Error" page. The error details are as follows:

- Type:** Exception Report
- Message:** java.lang.NullPointerException
- Description:** The server encountered an unexpected condition that prevented it from fulfilling the request.
- Exception:**

```
org.apache.jasper.JasperException: java.lang.NullPointerException
  org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:594)
  org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:510)
  org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:395)
  org.apache.jasper.servlet.JspServlet.service(JspServlet.java:339)
  javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
  org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
  com.ibm.security.appscan.altoromutual.filter.AuthFilter.doFilter(AuthFilter.java:67)
```
- Root Cause:** java.lang.NullPointerException
- Note:** The full stack trace of the root cause is available in the server logs.

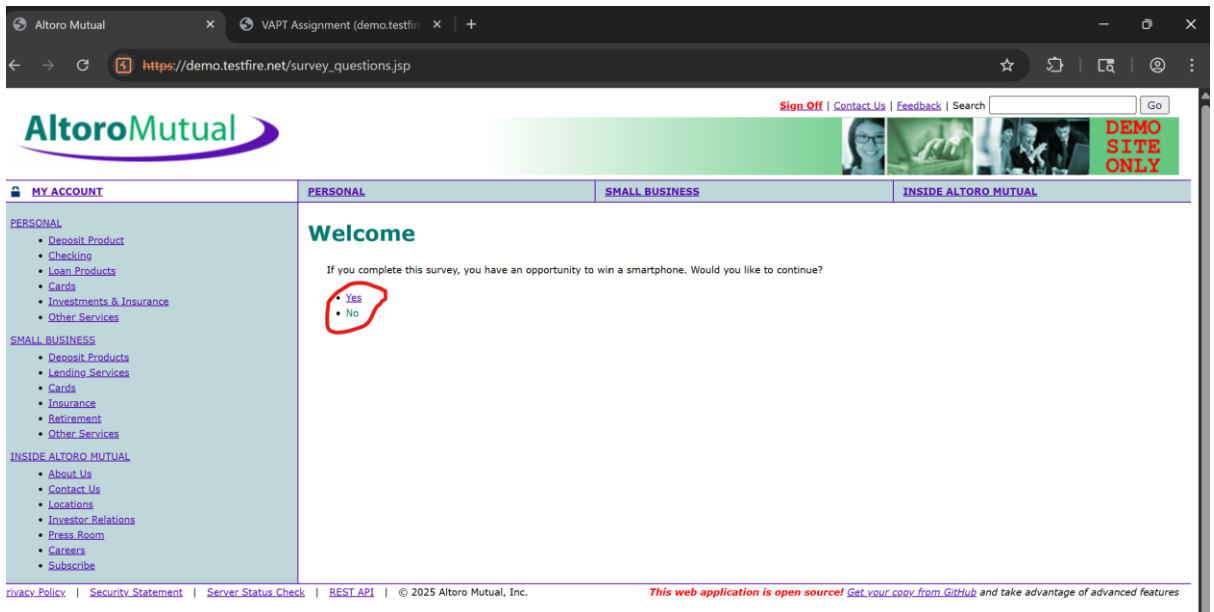
Apache Tomcat/7.0.92

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>
```

