Vulnerabilities

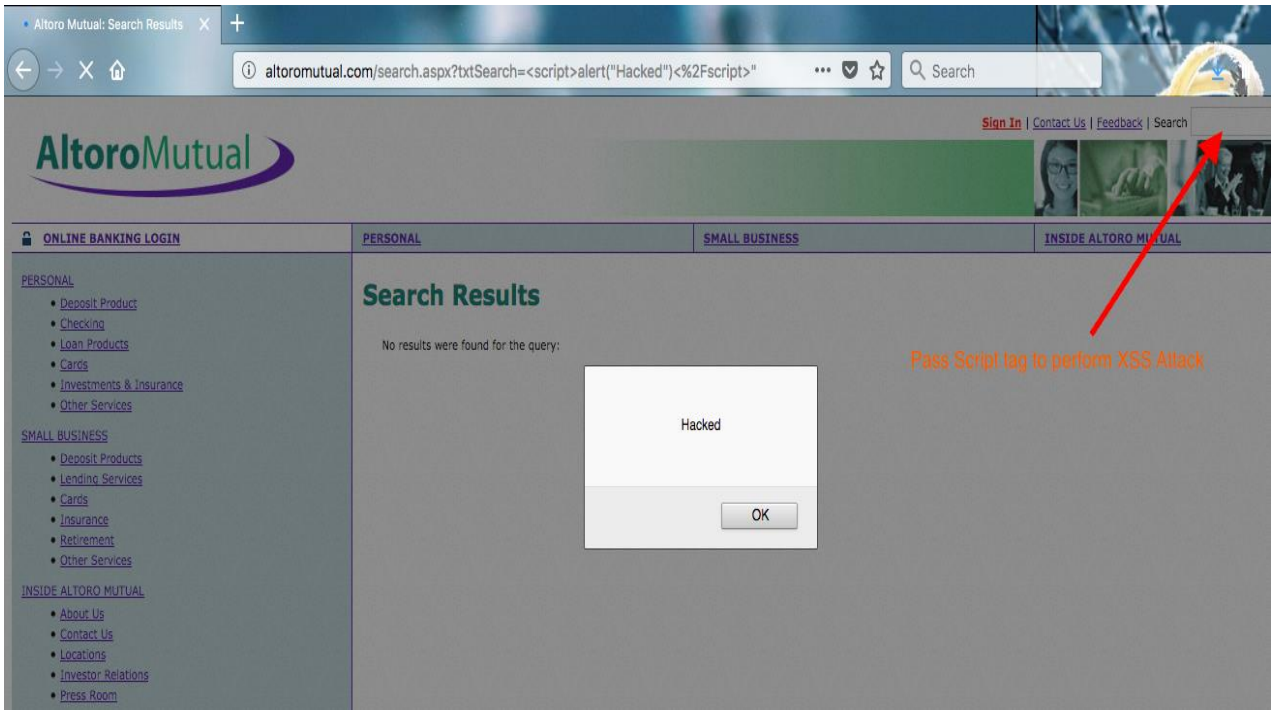
Issue: 1

Cross-Site Scripting	
URL:	http://www.altoromutual.com/
Entity:	Search filter
Risk:	XSS Attack
Cause:	Improper Input Validations

Steps:

1. Go to the URL
2. Enter the script tag i.e *<script>alert("hacked")</script>*
3. Click on Go button
4. You will observe the alert popup

ScreenShot



Issue: 2

Cross-Site Scripting	
URL:	http://www.altoromutual.com/comment.aspx
Entity:	Feeback form
Risk:	XSS Attack
Cause:	Improper Input Validations

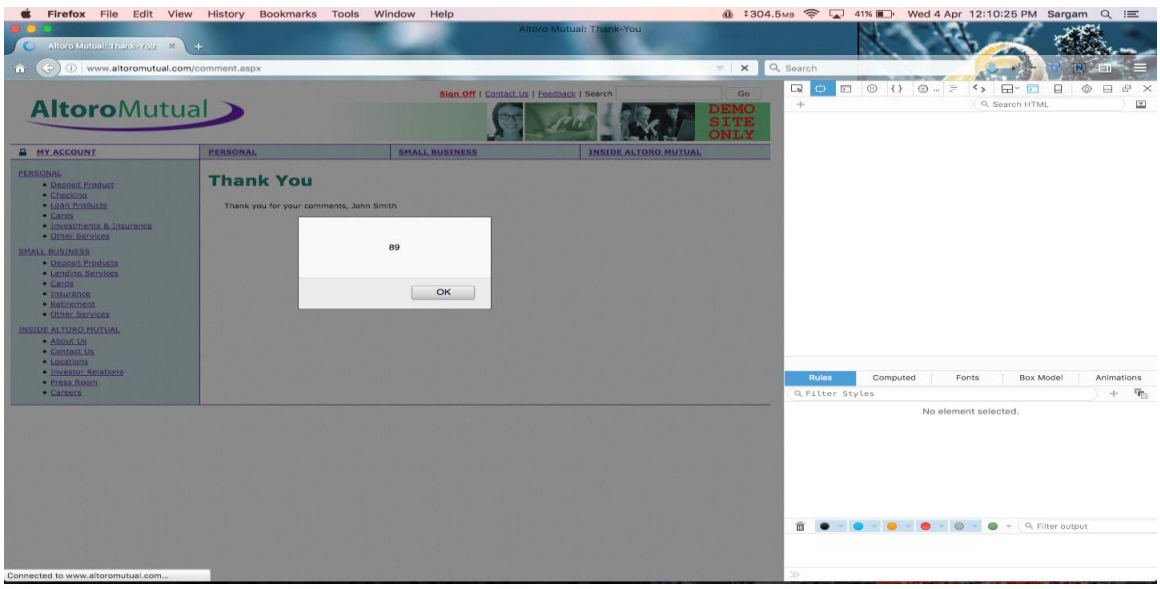
Steps:

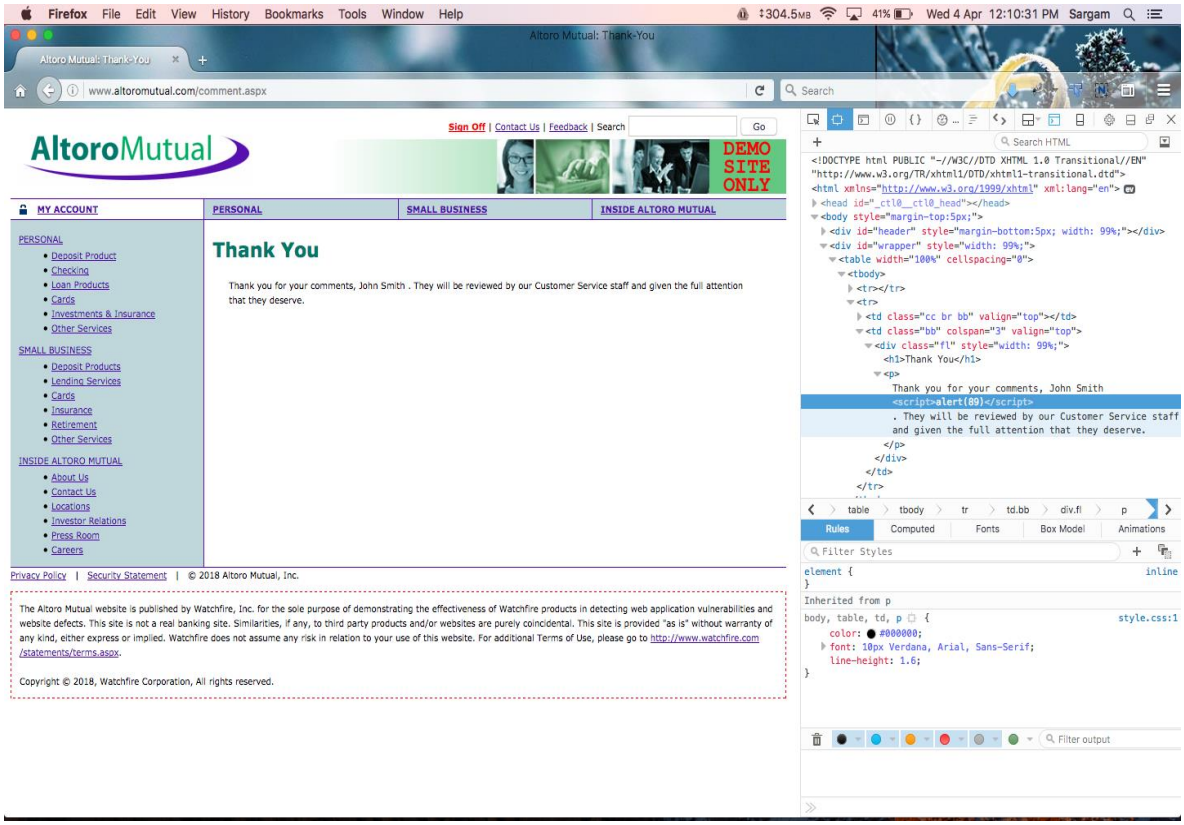
1. Login with valid credentials
    a. Username: jsmith
    b. Password: Demo1234
2. Go to Feedback form
3. Enter script tag in “Your Name” field
    a. John Smith 1234 <script>alert(89)</script>
4. Fill other field and click on submit button
5. Observe the alert popup

Response (via inspect element):

* Thank you for your comments, a. John Smith 1234 <script>alert(89)</script>. They will be reviewed by our Customer Service staff and given the full attention that they deserve. *

ScreenShot





Issue: 3

Cross-Site Scripting	
URL:	http://www.altoromutual.com/comment.aspx
Entity:	Feeback form
Risk:	XSS Attack
Cause:	Improper Input Validations

Steps:

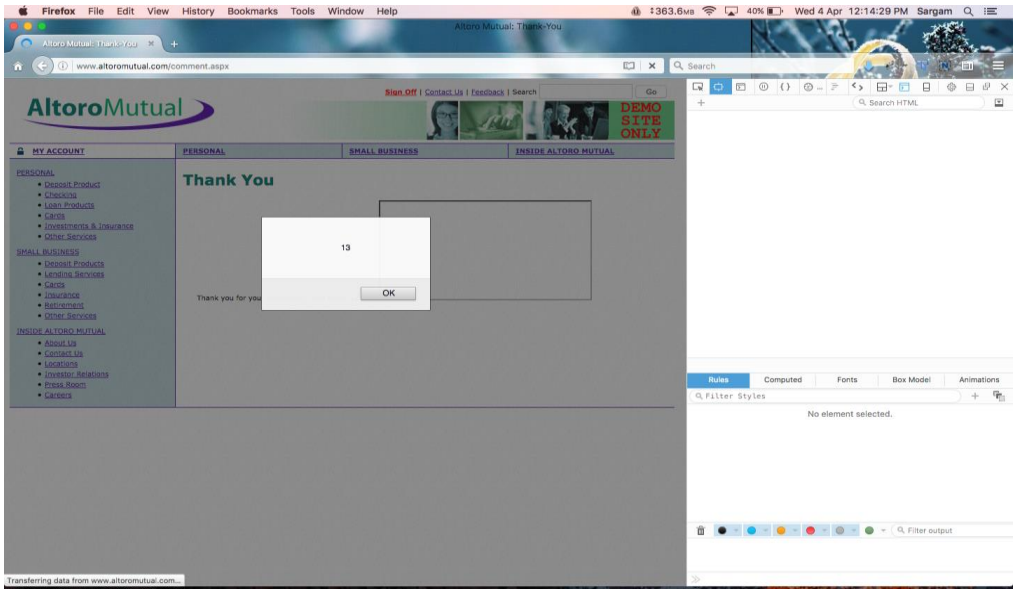
1. Login with valid credentials
    a. Username: jsmith
    b. Password: Demo1234
2. Go to Feedback form
3. Enter script tag in “Your Name” field
    a. John Smith 1234 <iframe src="javascript:alert(13)">
4. Fill other field and click on submit button
5. Observe the alert popup

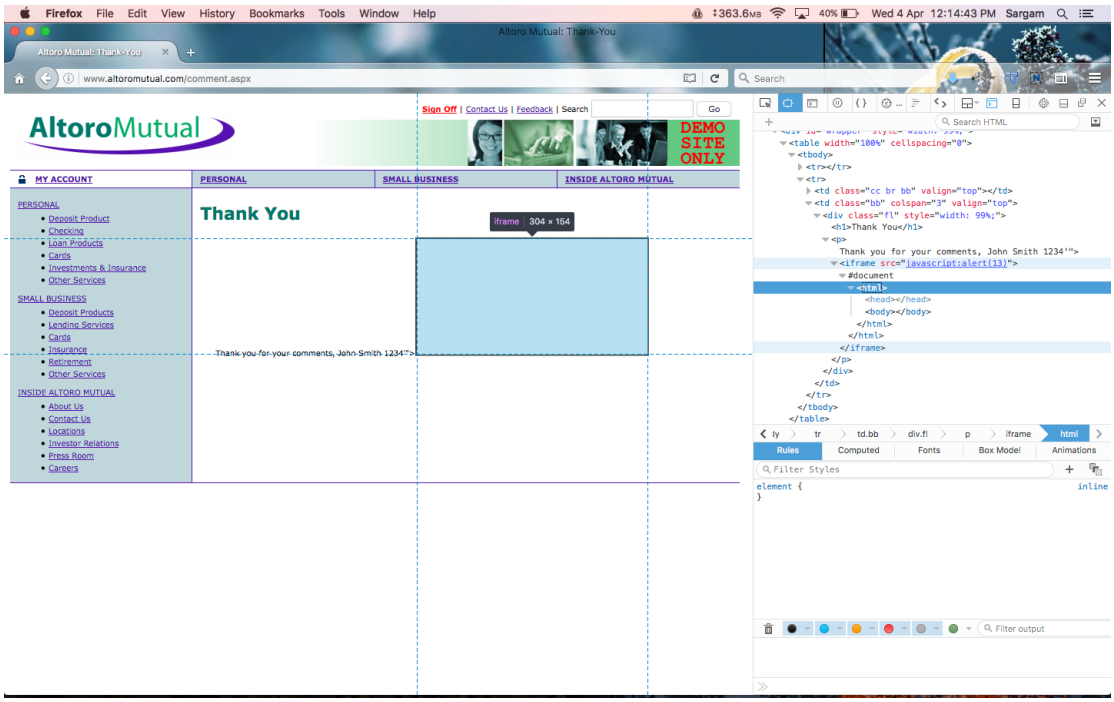
Response (via inspect element):

<p>Thank you for your comments, John Smith 1234"'><iframe src="javascript:alert(13)">. They will be reviewed by our Customer Service staff and

given the full attention that they deserve.</p>

ScreenShot





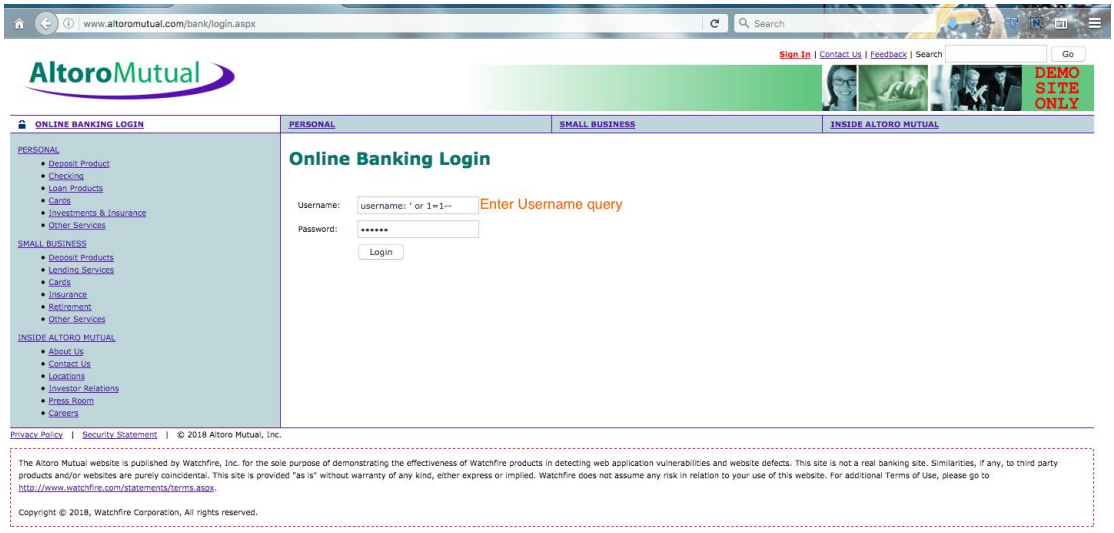
Issue: 4

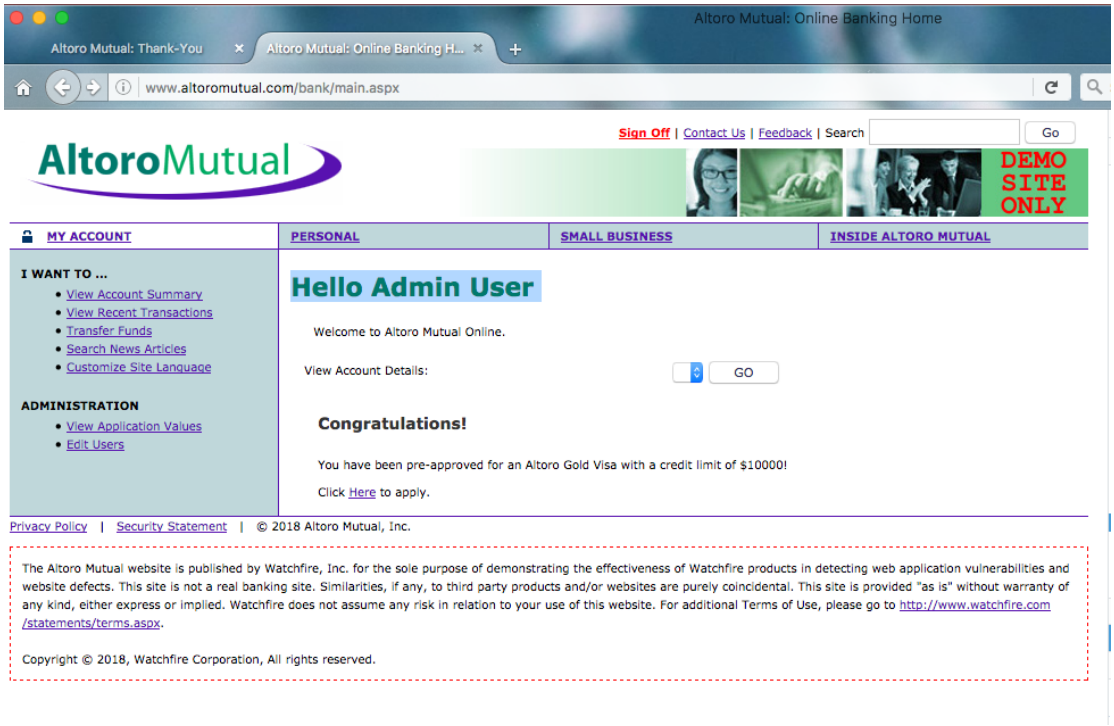
SQL Injection	
URL:	http://www.altoromutual.com/bank/login.aspx
Entity:	Login Form
Risk:	Can by pass authentication mechanism
Cause:	Sanitization of input fields are not properly done
Tool(if any):	NA

Steps:

1. Go to Url
2. Click on sign in Link
3. Enter either of the below details:
    - Enter *username:->* username: ' or 1=1-- AND enter any password. Press Enter
    - OR Enter any username AND *password:->* password: ' or 1=1--
4. You will observe that you are logged in as a authorized user.

ScreenShot

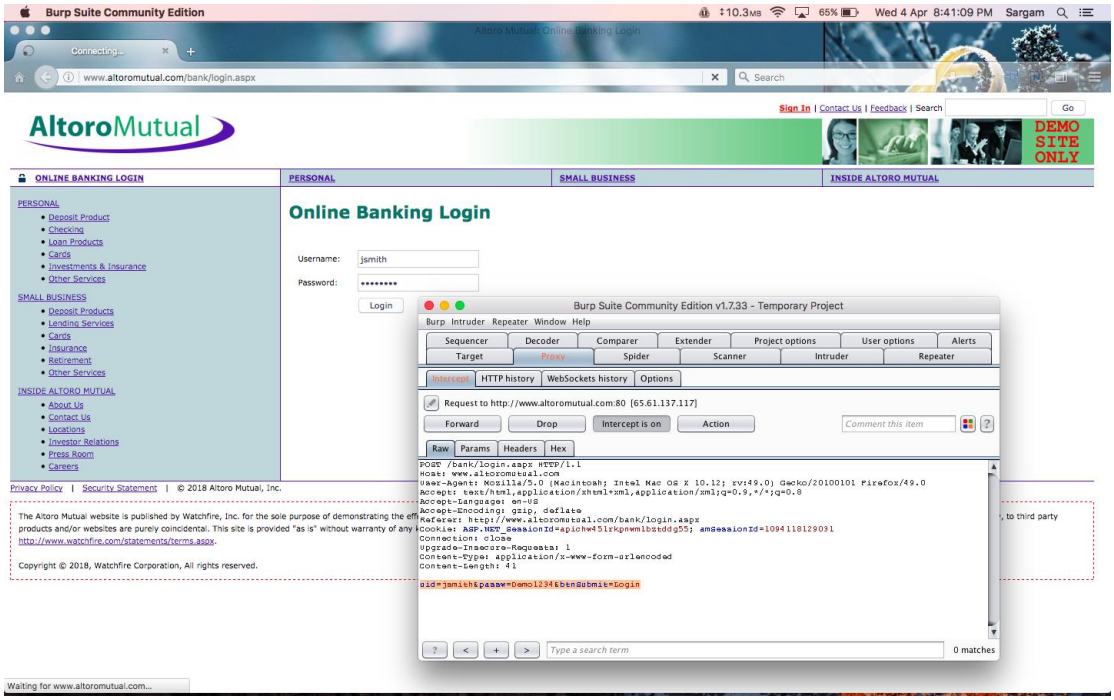




Issue: 5

Sensitive Data Exposure	
URL:	http://www.altoromutual.com/bank/login.aspx
Entity:	Login Form
Risk:	Easy to seal sensitive information such as username, password
Cause:	Sensitive information is sent over unencrypted (Not sent over ssl)
Tool(if any):	Burp Suite

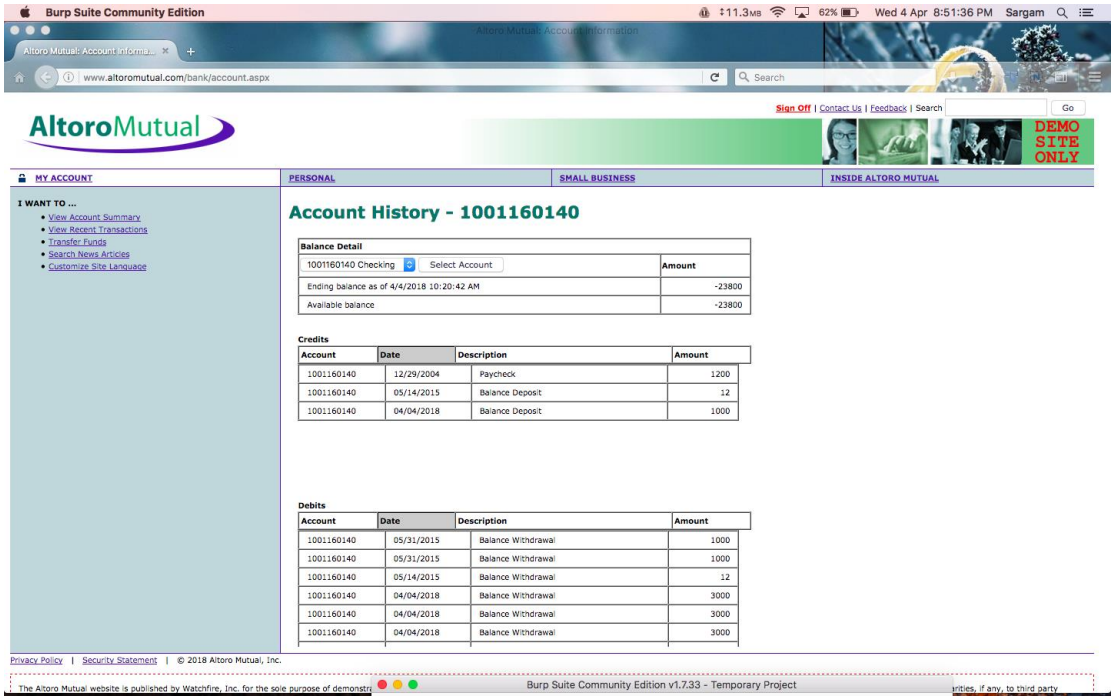
ScreenShot

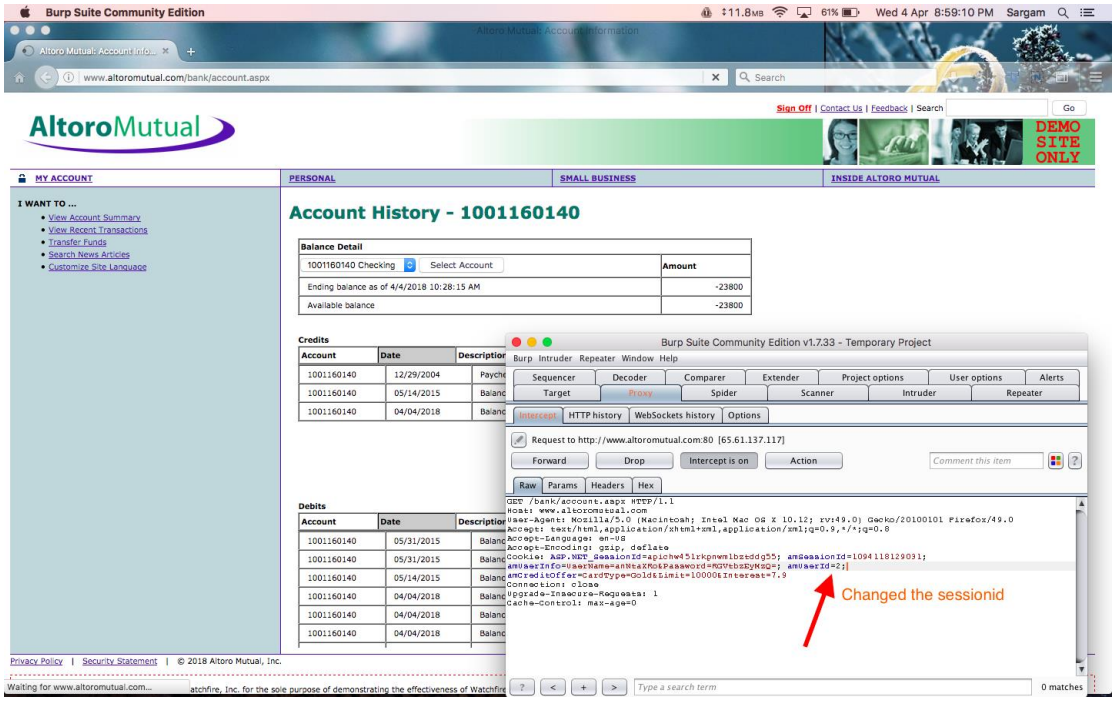


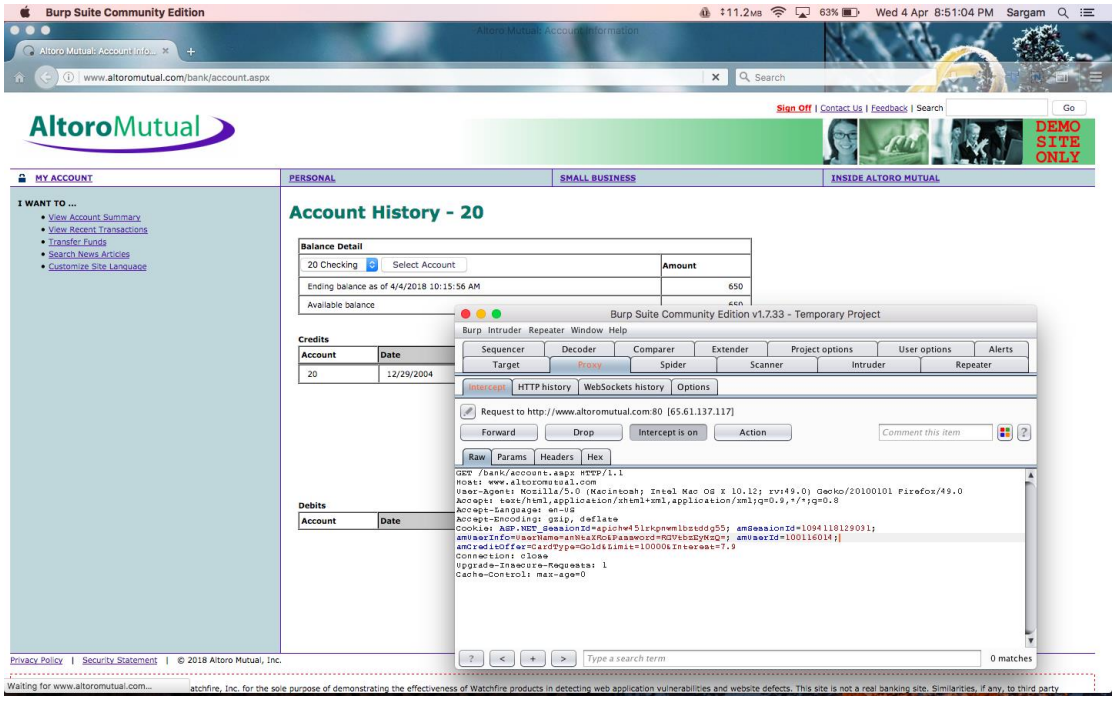
Issue: 6

Broken Authentication	
URL:	http://www.altoromutual.com/bank/account.aspx
Entity:	Account Number
Risk:	Can view other user's account details
Cause:	Session id is not protected and can be alter via interception.
Tool(if any):	Burp Suite

ScreenShot


Burp Suite Community Edition
Wed 4 Apr 8:51:36 PM Sargam
www.altoromutual.com/bank/account.aspx
AltoroMutual
Sign Off | Contact Us | Feedback | Search
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Account History - 1001160140
Balance Detail
1001160140 Checking
Select Account
Amount
Ending balance as of 4/4/2018 10:20:42 AM
-23800
Available balance
-23800
Credits
Account
Date
Description
Amount
1001160140 12/29/2004 Paycheck 1200
1001160140 05/14/2015 Balance Deposit 12
1001160140 04/04/2018 Balance Deposit 1000
Debits
1001160140 05/31/2015 Balance Withdrawal 1000
1001160140 05/31/2015 Balance Withdrawal 1000
1001160140 05/14/2015 Balance Withdrawal 12
1001160140 04/04/2018 Balance Withdrawal 3000
1001160140 04/04/2018 Balance Withdrawal 3000
1001160140 04/04/2018 Balance Withdrawal 3000
Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstr
Burp Suite Community Edition v1.7.33 - Temporary Project


Burp Suite Community Edition
Wed 4 Apr 8:59:10 PM Sargam
www.altoromutual.com/bank/account.aspx
AltoroMutual
Sign Off | Contact Us | Feedback | Search
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Account History - 1001160140
Balance Detail
1001160140 Checking
Select Account
Amount
Ending balance as of 4/4/2018 10:28:15 AM
-23800
Available balance
-23800
Credits
Debits
Burp Suite Community Edition v1.7.33 - Temporary Project
Burp Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater
Intercept HTTP history WebSockets history Options
Request to http://www.altoromutual.com:80 [65.61.137.117]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
GET /bank/account.aspx HTTP/1.1
Host: www.altoromutual.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Cookie: ASP.NET_SessionId=apichw451rkpnwmlbzeddg55; amSessionId=1094118129031;
amUserInfo=UserName=anNtaXM6&Password=MGVtbzEyMzQ=; amUserId=2;
amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Changed the sessionid
Type a search term
0 matches
Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.
Waiting for www.altoromutual.com...



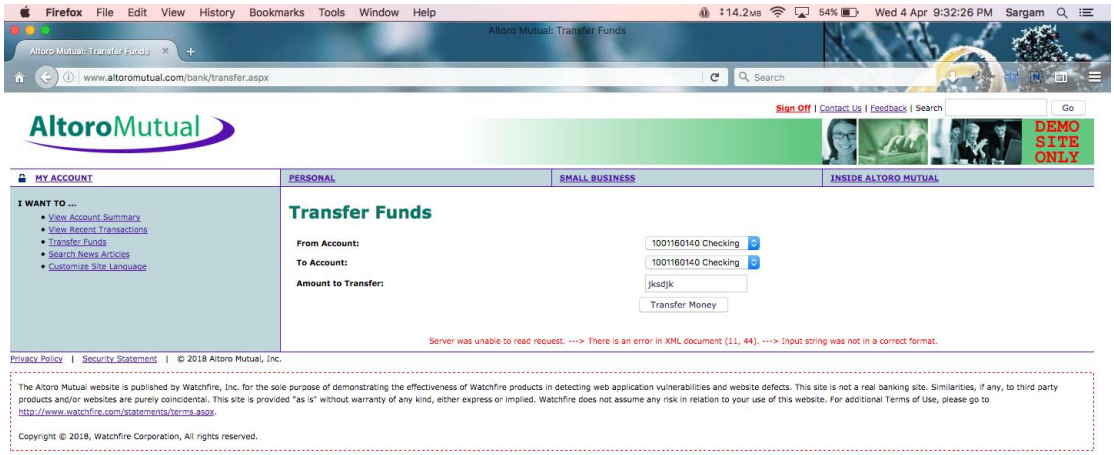
Issue: 7

Security Misconfiguration	
URL:	http://www.altoromutual.com/bank/transfer.aspx
Entity:	Amount to be transfer
Risk:	Error message Containing Sensitive Information
Cause:	Improper handling of Validations messages

Steps:

1. Go to the URL
2. Enter any characters
3. Click on transfer button
4. You will observe the error message

ScreenShot



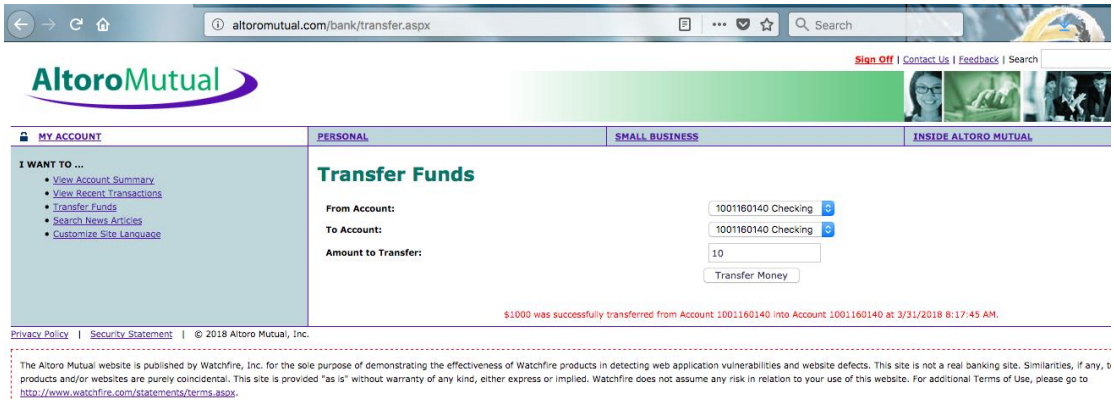
Issue: 8

Sensitive Data Exposure	
URL:	http://www.altoromutual.com/bank/transfer.aspx
Entity:	Amount to be transfer
Risk:	Amount can be alter
Cause:	Improper handling of Sensitive Data

Steps:

1. Go to the URL
2. Enter amount
3. Start Burp Suite: Interception ->ON
4. Click on transfer button
5. Alter the amount via Burp Suite
6. Forward the request from Burp Suite
7. You will see the message that altered amount has been transferred.

ScreenShot


altoromutual.com/bank/transfer.aspx
Search
Sign Off | Contact Us | Feedback | Search
AltoroMutual
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Transfer Funds
From Account:
1001160140 Checking
To Account:
1001160140 Checking
Amount to Transfer:
10
Transfer Money
$1000 was successfully transferred from Account 1001160140 into Account 1001160140 at 3/31/2018 8:17:45 AM.
Privacy Policy | Security Statement | © 2018 Altoro Mutual, Inc.
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,
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
http://www.watchfire.com/statements/terms.aspx.