# CYBR430, Penetration Testing and Incident Response Week 8 Lab – Web Attacks and Accessing Shares

Your lab this week has two parts. In part one you will demonstrate a simple SQL injection attack and a XSS attack on a publicly available website developed for this type of training. In Part two you will explore the HAL network shares.

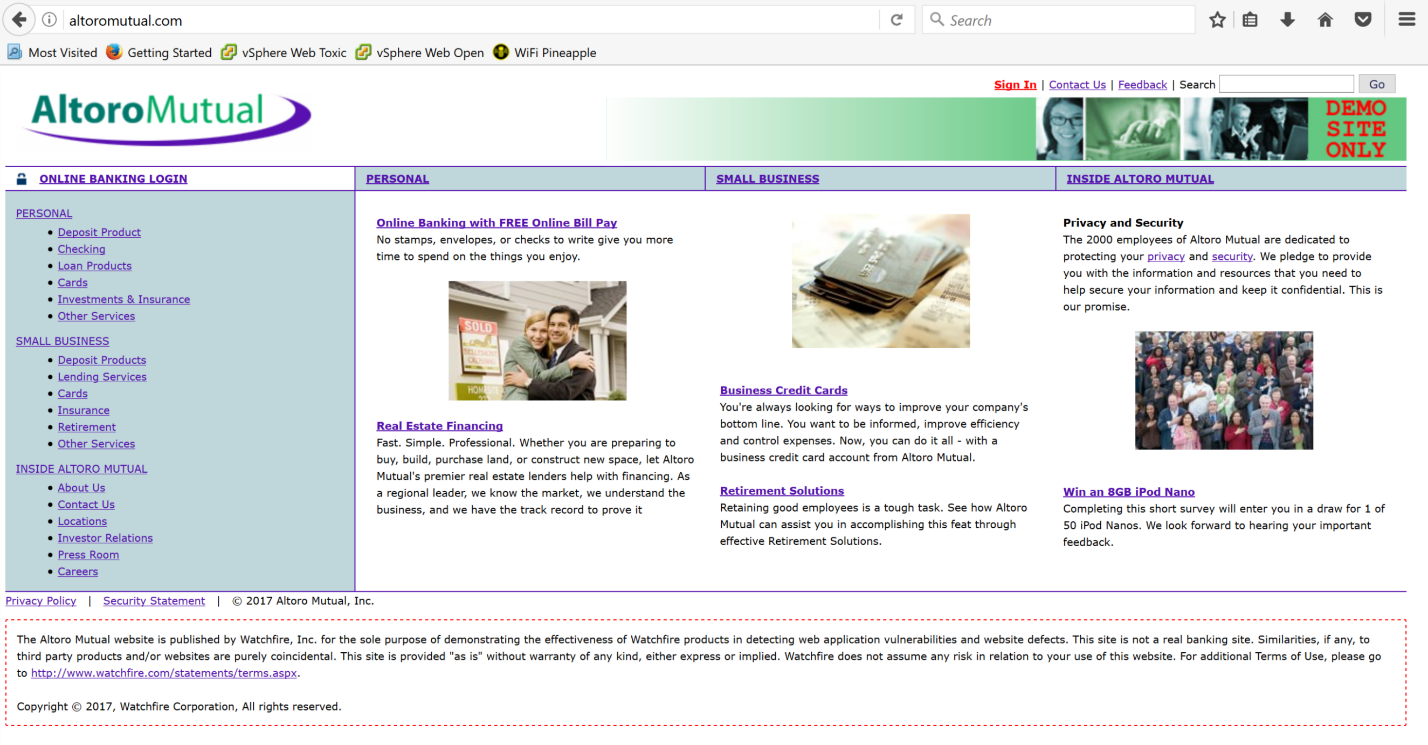
**Part 1: SQL Injection and XSS Attacks**

Part 1 of this lab will be done from your test lab or other internet connected computer.

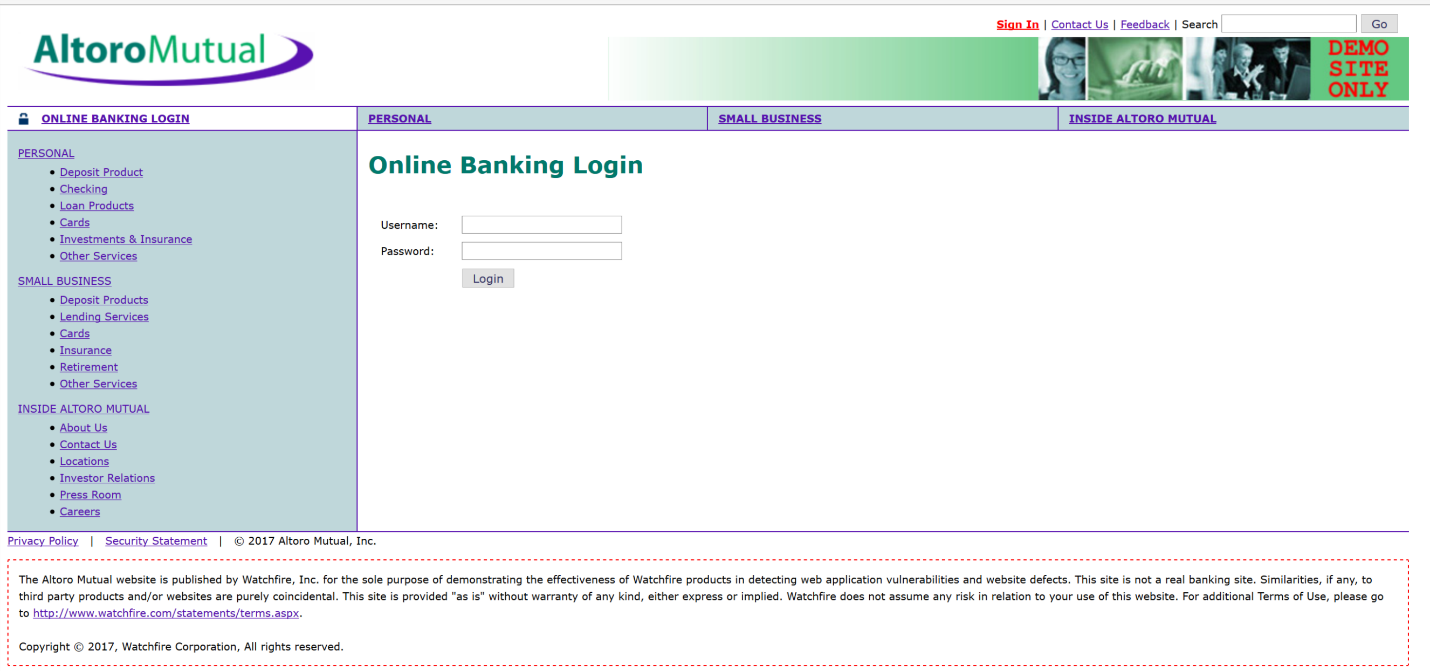
The web site we will use for part 1 of the lab is **altoromutual.com**. You can also access the site at **demo.testfire.net**. This website has been made available for training and testing various product’s effectiveness at identifying and defending against web attacks. You should be sure you have read and understood the sections of your readings listed in Blackboard this week.

**SQL Injection**

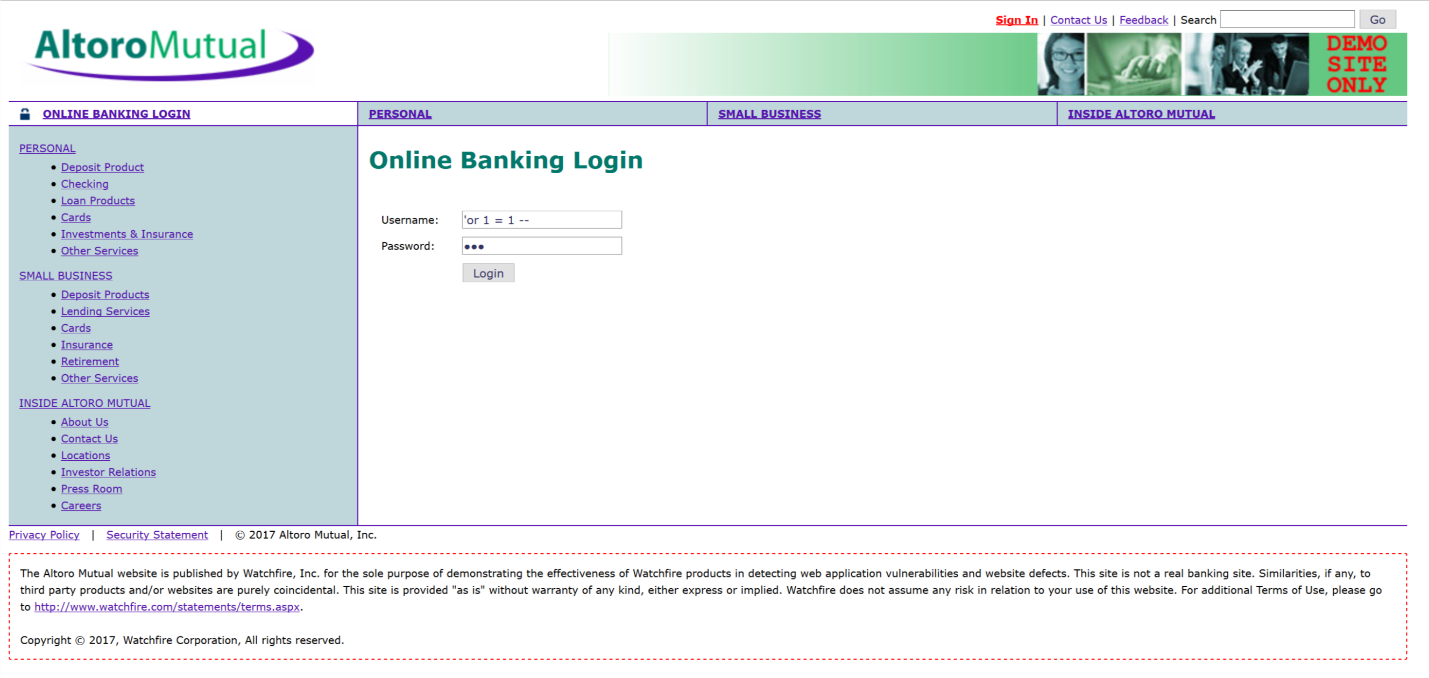
If you recall from your reading a SQL injection attack takes advantage of an input field not doing input validation. The entry made by the user is constructed in such a way so it is interpreted as SQL and produces results other than what the developer intended. To demonstrate a SQL injection attack we are going to attempt to bypass a login dialog and gain administrator access to a banking website, altoromutual.com. Go to the website altoromutual.com in an internet connected web browser.



Click the **sign in** link on the upper right.



We are going to use a SQL injection to bypass the need to enter a valid password in the dialog box. The SQL code we are going to use is **‘ or 1 = 1 --**



This code, when entered into the username field will generally result in the system selecting the first username in its list, usually admin, and then ignoring the requirement for a password. Remember **or 1=1** is SQL code which evaluates to ‘or true’ which makes all statements true. You will still have to enter a password in the field but as it never gets checked. Remember, the -- is a comment identifier so everything after is ignored, to include the password check.

**Provide a screenshot of the login confirmation displayed after your successful SQL injection attack (5 pts).Graphical user interface, text

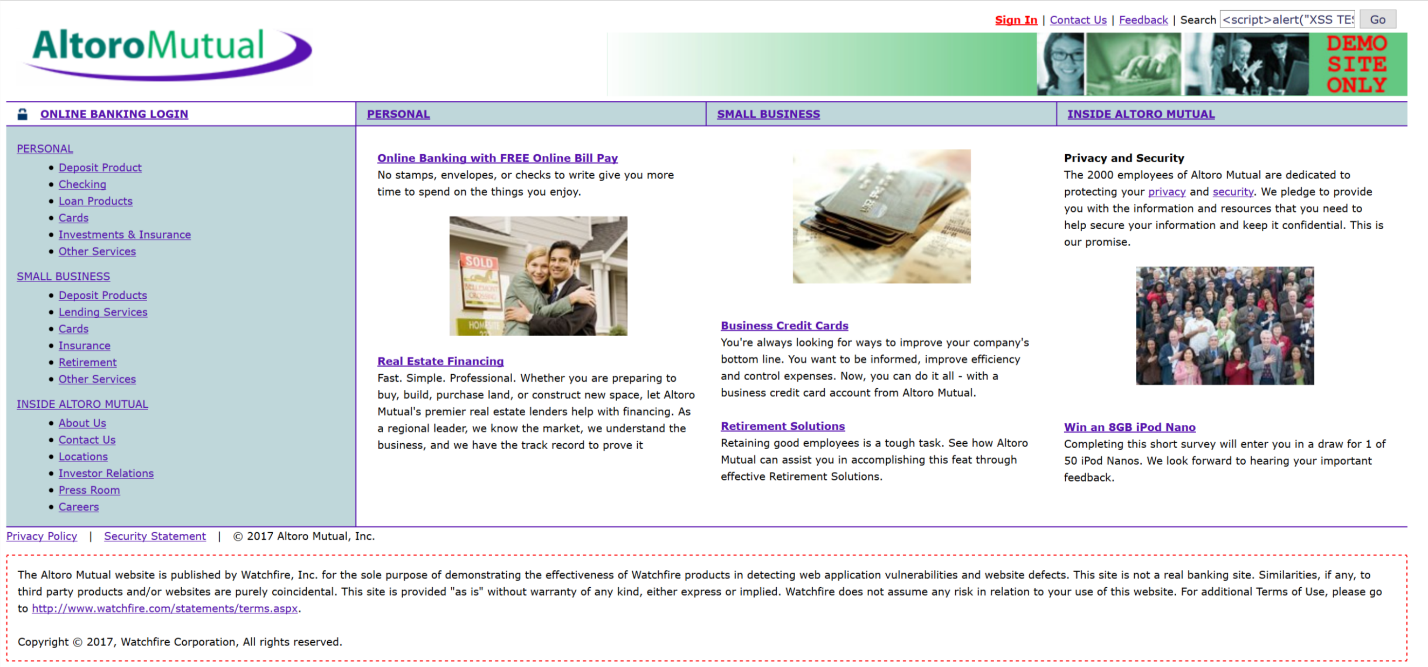
Description automatically generated**

**XSS Attack**

Recall that a cross-site scripting or XSS attack is one in which code, other than which the developer intended, is sent to a web browser. The browser executes the code as if it were part of the intended web session. Instead of taking an action the user desires however it will capture information, launch an exploit, or take any other action the hacker desires. For this demonstration we will tell the browser to display a simple alert box on the screen. Take note that several browsers are getting better at blocking XSS attacks so depending on what protections you have running on your system you may receive a warning when executing this attack. If this occurs you may need to try a different browser or as this attack uses javascript you may need to enable javascript. The firefox browser with a default install generally works for this lab.

Go to the home page for **altoromutual.com** and locate the search box in the upper left corner of the screen. In that box enter the following all in one line

**<script>alert(“XSS test”)</script>**

****

**Provide a screen shot of the alert dialog box generated from your XSS attack (5pts).Graphical user interface

Description automatically generated with medium confidence**

Feel free to try other attacks on the website. Don’t ignore error messages, in pentesting (as in hacking) they often give up very useful information.

**Part 2: Accessing HAL shares**

Part 2 of this lab will be done in the University’s virtual labs.

Now that you have successfully mapped several file shares at Happy Accident Labs and harvested some user credentials you are ready to start accessing the client and server shares to see if there is any valuable data which could be accessible to hackers. Your goal is to identify where valuable data is, what the data is, and which credentials you need to use to access them. The pentest report you will submit at the end of the term should detail this information so take good notes. Let’s begin by reviewing how you access file shares from Linux.

**Accessing Samba and Windows file shares from Linux**

Samba is a Linux file sharing protocol that allows file transfer between Linux and Windows computers on the same local area network. One way to access shared directories and files is through the Kali Linux the command prompt.

**Using the command line**

You have already done several scans of SMB in previous labs so you already know some of the available machines and shares. A valuable command in the SMB toolset is smbtree. Depending on your permissions when you type ‘smbtree’ at a command prompt you will receive a list such as the below showing you system names and shared devices, folders, and services.

Text

Description automatically generated

Note, the above is an example only, try smbtree on your Kali system to see what is available on the HAL network. You can always do a ‘man smbtree’ from a command prompt to see the various command parameters you can use.

You can access shares through the command line using the **smbclient** program. This program is installed by default on Kali. You may have to install it prior to use on other Linux distributions.

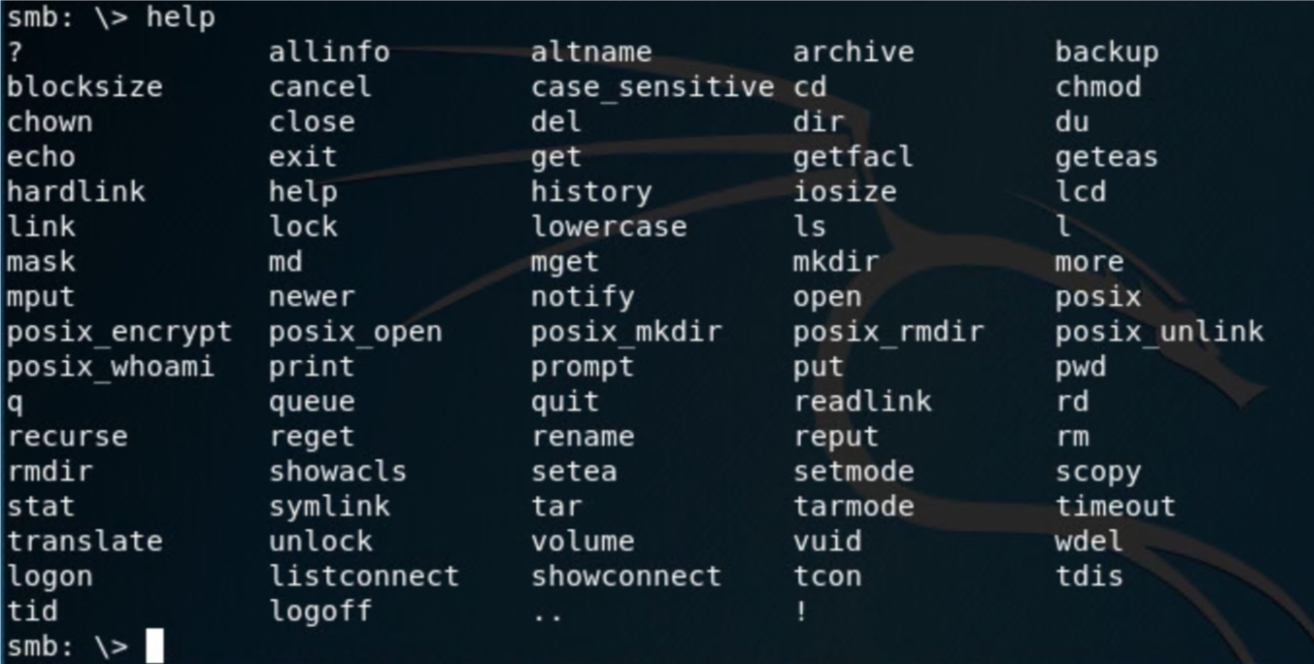
The command format is **smbclient //computer-name/share-name –U username**

For example if you wanted to access a share called “good-stuff” on the computer “shared-use” as user “jimb” the command would be



You would find the computer and share name from your earlier scans. If you don’t enter a user name the user root is assumed as the default. Once you enter this command you will be asked for a password if needed. You will use the same format whether you are accessing a share on a Linux or Windows machine.

If you successfully access the share you will receive a **smb>** prompt. The command **help** will list the available commands.



Some useful commands are **get** to get a file. The file is downloaded into your current Linux directory. The command **cd** will allow you to change directories. The command **quit** will log you off the connected share and return you to your Linux prompt. Be advised that you will often find filenames with spaces in them, especially on windows machines where GUI interfaces tend to be the default for use. Since spaces are delimiters between commands on the Linux command line having spaces in a file name will not work. In that case you must enter the entire path and file name in quotes. For example to access the file **cool stuff** you would need to use **“cool stuff”**. Through your scans you know several machine names that are on the network as well as some potential file shares. You also have some user credentials harvested in the lab last week.

**Use your access to the HAL network to find accessible shares on the client systems. This may take some time as you try different shares with different user credentials. What information did you find where? Document below what information was found, the client and share you found it on, and which credentials you used. You have appropriate file viewers on your Kali VM to view the HAL files (40 pts).**

Note: You should not access the other students systems but only those you conducted initial scans on (10.19.99.1 – 10.19.99.100) or the HAL client machine you were assigned last week which is a duplicate of 10.19.99.10.

Text

Description automatically generated

Text

Description automatically generated

**Graphical user interface, text

Description automatically generated**

Graphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated