**Web Security**

***Resources you should be familiar with for this lab.***

1. WebGoat: <http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project>
2. Burp Suite: <http://portswigger.net/suite/>

***General Instructions:***

Complete the following exercises. You record your results on these sheets. Please ask questions during the lab if you need help or do not understand a instruction.

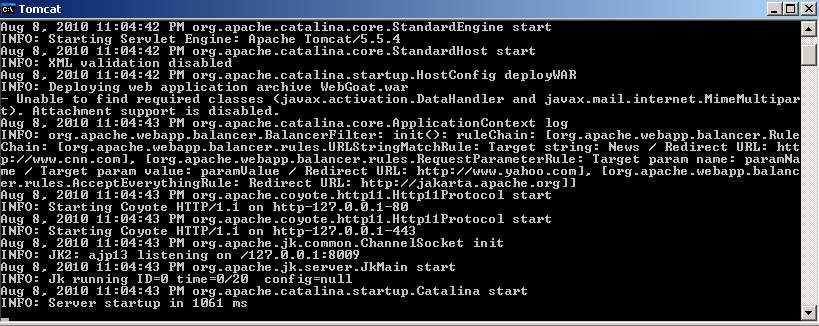
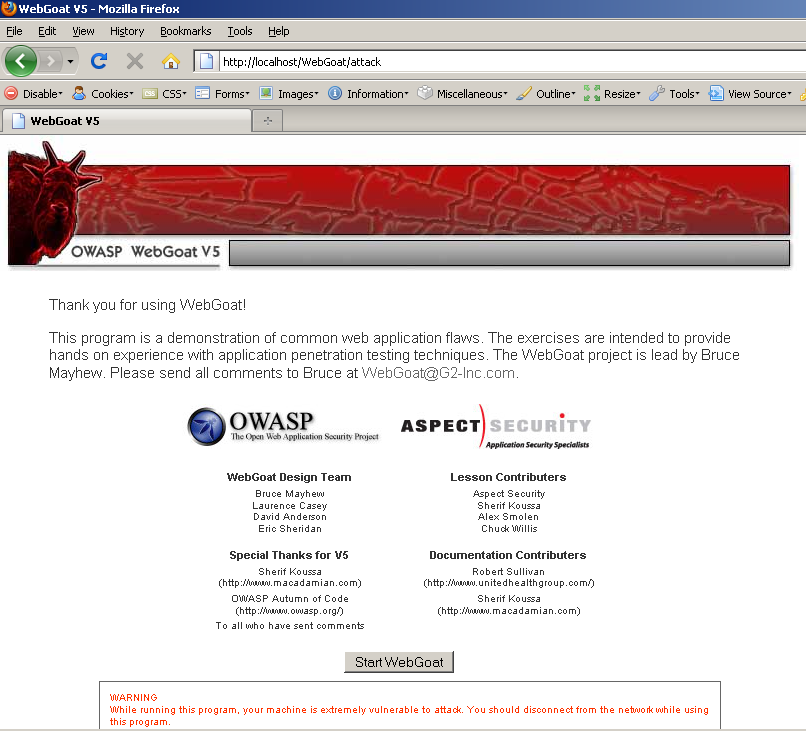
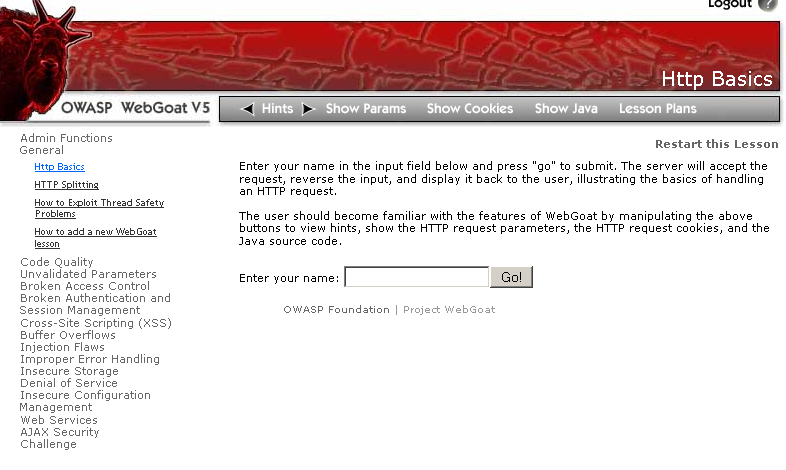
***Verify the Install and Configuration of the FireFox Browser***

1. Boot into Windows XP VM and open the Firefox browser.
2. Please don’t upgrade the browser when prompted to do so.
3. Verify the Web Developers Extensions addon for Firefox is installed. This addon gives is a must-have for any web application tester and provides features that help test security.
4. You should see the Web Developer tool bar within your browser. It should look something like:

******Note: If you don’t see the toolbar try right clicking in the Firefox toolbar frame and ensuring the “Web Developer Toolbar” is checked for visibility.

***WebGoat Web Security Training***

WebGoat is a full J2EE web application designed to teach web application security lessons. In each lesson, users must demonstrate their understanding by exploiting a real vulnerability on the local system. The system is even clever enough to provide hints and show the user cookies, parameters and the underlying Java code if they choose.

1. Copy the Windows\_WebGoat-5.0\_Release.zipfile to your desktop from C:\MIS501\lab5.
2. Unzip the Windows\_WebGoat-5.0\_Release.zip file to your working environment (accept defaults for directory).
3. To start Tomcat, browse to the WebGoat directory unzipped above and double click "webgoat". Do not close the console window and it should look like the following:  
     
   
4. Start your Firfox browser and browse to... *(Notice the capital 'W' and 'G')*   
     
   <http://localhost/WebGoat/attack>  
     
   Note: This address is also in your Bookmarks menu within Firefox for easy access. “WebGoat v5”.
5. Login in as: user = **guest**, password = **guest**
6. Select ‘Start WebGoat’ at the bottom of the introductory page. Start getting familiar with WebGoat by exploring.  
     
   
7. On the left side of the browser window are the various lessons included in WebGoat. Under the heading “General”, select HTTP Basics.  
     
   
8. The first thing you should do in all lessons is to click on the button “Show Lesson Plan”.
9. You should also take advantage of the “Hint” button, each lesson has several hints.
10. Skip down to the “**Code Quality**” heading and select “**How to discover clues in** **HTML Clues**”.
11. On your Web Developer Toolbar, select “***Miscellaneous***”, and select “***Show Comments***”.
12. Scroll to the bottom of the page. You should now see two orange boxes with a “!” in them. Click on the boxes to display developer comments that were not intended for you to find. Summarize what you found:  
      
    Two comments, one has a FIXME talking about the username and password. The other one says that you need to use Admin to regenerate a database.
13. Select “View Source” on your Web Developer toolbar and find the comments found in the step above. (Hint: Comments are highlighted in Green)
14. Did you find out the username and password? If Yes, record them below:

username: admin password: adminpw

1. In WebGoat **s**kip down to the “**Unvalidated Parameters”** heading and select **“How to exploit Hidden Fields”.**
2. On your Web Developer Toolbar, select “Forms” and “Display Form Details”. You may have to turn it on and off a couple times to notice, but you should be able to see a hidden field that contains a green box. Edit the value in the green box and then select “Purchase”. What happened?  
     
   The purchase was made with the price I input in the green box and the site also gave me a message saying that the purchase was successful.
3. “View Source” on your Web Developer toolbar and find the hidden field found in the step above.
4. To close WebGoat, exit the browser and close the Tomcat DOS window.
5. Feel free to try the other lessons if you finish early.

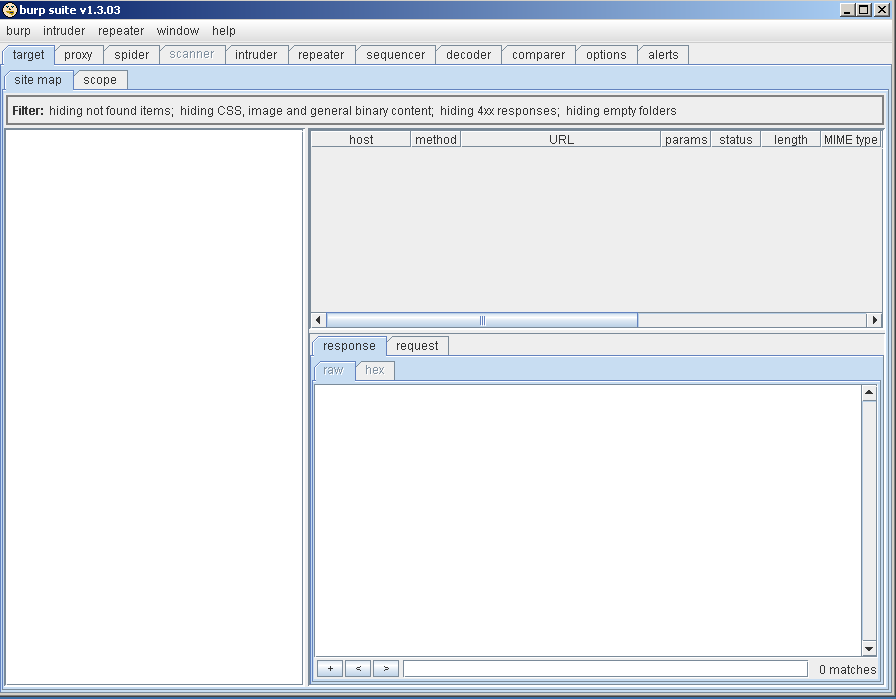
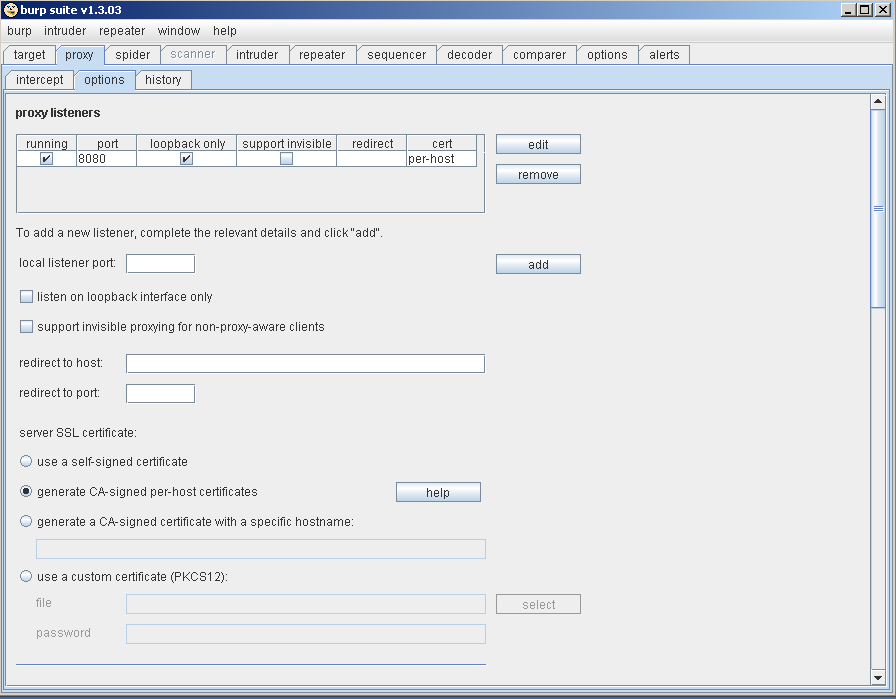
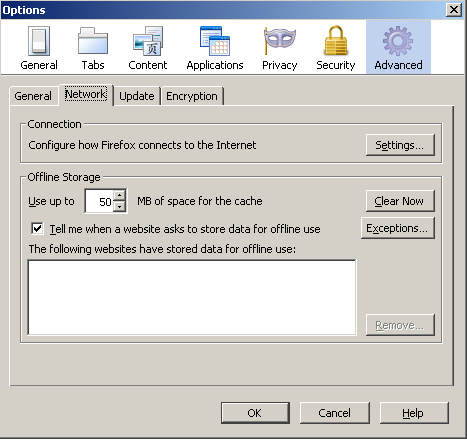
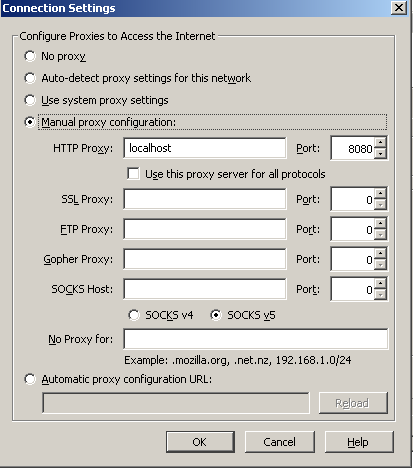
***Part IV - Burp Suite***

Burp Suite is an integrated platform for attacking web applications. It contains all of the Burp tools with numerous interfaces between them designed to facilitate and speed up the process of attacking an application. All tools share the same robust framework for handling HTTP requests, persistence, authentication, upstream proxies, logging, alerting and extensibility.

Burp Suite allows you to combine manual and automated techniques to enumerate, analyze, scan, attack and exploit web applications. The various Burp tools work together effectively to share information and allow findings identified within one tool to form the basis of an attack using another.

Key features unique to Burp Suite include:

* Detailed analysis and rendering of requests and responses.
* One-click transfer of interesting requests between tools.
* Site map showing information accumulated about target applications in tree and table form.
* Ability to "passively" spider an application in a non-intrusive manner, with all requests originating from the user's browser.
* Suite-level target scope configuration, driving numerous individual tool actions.
* Fully fledged web vulnerability scanner. [Pro version only]
* Ability to save and restore state. [Pro version only]
* FIPS-compliant statistical analysis of session token randomness.
* Utilities for decoding and comparing application data.
* A range of [engagement tools](http://portswigger.net/suite/help.html#engtools), to make your work faster and more effective. [Pro version only]
* Suite-wide search function. [Pro version only]
* Support for custom client and server SSL certificates.
* Extensibility via the [IBurpExtender](http://portswigger.net/suite/help.html#extensibility) interface.
* Centrally configured settings for upstream proxies, web and proxy authentication, and logging.
* Tools can run in a single tabbed window, or be detached in individual windows.
* Runs in both Linux and Windows.

1. Copy the burpsuite\_v1.3.03 file to your desktop from “C:\MIS501\lab5” on your virtual machine.
2. Unzip burpsuite\_v1.3.03.
3. Navigate to the burpsuite\_v1.3.03 directory and execute the suite file which should open the Burp Suite interface shown here:  
     
   
4. Click on the “proxy” tab and verify, “Intercept is on”.
5. Click the “options” tab to show the proxy settings shown here:  
     
   
6. Once you have verified the proxy listener settings look like the above image, select the intercept tab to return to the main proxy window.
7. Now you will need to configure your browser to use a proxy.
   1. In Firefox, select Tools, Options, Advanced (in the top menu bar) Network tab as shown here:  
        
      
   2. Select Settings for Configure how Firefox Connects to the Internet which should display the window below Select Manual Proxy Configuration.  
        
      
   3. Enter localhost and port 8080 (this must match the port in Burp Suite).
   4. Ensure there is no entry in “No proxy for:” box. You may have to delete out the contents within this textbox.
8. Restart the WebGoat server, as you did in the last lesson.
9. Verify the Burp Suite proxy is still in intercept mode.
10. Using the Firefox browser with the proxy configured, browse to the webgoat site:  
      
    http://localhost/WebGoat/attack   
      
    and login as guest guest.

In Burp Suite, you will need to “forward” each communication between the browser and server.

1. The proxy will intercept all web calls between Firefox and Web Goat. It will also intercept all web calls to any other site you visit.
2. Burp Suite also allows you to execute a Man-in-the-Middle attack. This means that now not only do you see all the transactions between web browser and web server, you can interact with them. Burp Suite will intercept each communication you select giving you the opportunity to change data between the browser and the server.
3. Navigate to Hidden Field Tampering in WebGoat. Remember it is under “Unvalidated Parameters”.
4. In Burp Suite, you will need to “forward” each communication between the browser and server.
5. In WebGoat, select purchase.
6. In Burp Suite, observe the information. Notice that once Burp Suite intercepted the web communications the following tabs can be navigated: raw, parms, header, hex.
7. Navigate to the “parms” tab and attempt to change the price and monitor both Burp Suite and WebGoat.
8. Now switch back to the “raw” tab and click the “forward” button to submit your changes. You will have to click the forward button approximately 6 times to fully submit the request.
9. Was it successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
10. Why would using Burp Suite be advantageous if the Price field wasn’t a hidden field but just a parameter being passed within the HTTP transaction?  
      
    You can modify the price with Burp Suite, unlike from a browser since there is no hidden field.
11. Turn intercept off in Burp Suite by clicking on the button “Intercept is on”.
12. Now navigate to the “Target” tab within Burp Suite and expand out the “localhost” choice to show its subcomponents.
13. Expand out the “Attack” section and notice that Burp Suite recorded your actions for everything you did. This allows you to generate fuzzing templates, automated attacks, and also document your findings for reporting at a later date.
14. Select your attack which should start with something like “QTY=” and record the following information from window on the top right of Burp Suite:  
    1. Method: POST
    2. Status: 200
    3. Length: 21735
    4. Mime Type: HTML
    5. Title: How to exploit hidden field
15. Exit Burp Suite and WebGoat. Delete directories created for Burp Suite and WebGoat and all associated zip files from your desktop.
16. Reset Firefox’s Proxy settings to disable the proxy.
17. Logout and shutdown your VM.