**CS763 Lab 4 Web Security**

Yourname

**Instructions**

* Please document how you implement these requirements by showing your source code snippets and the screenshot(s) of the execution result in the lab report.
* Please name your report as CS683\_<Last Name><First Name>\_Lab4. It can be either a PDF or Word document.
* Please provide your feedback in the “Add comments” section when submitting your lab report. Thanks!

## **Brief description (purpose and overview)**

CSS (Cross Site Script) is one of the top vulnerabilities in web applications. In this lab, you will gain further understanding of the CSS vulnerability by conducting attacks. We will use a well designed lab developed by Prof. Wenliang Du from Syracuse University.

## **Learning Objectives**

After finishing this lab, students shall be able to:

1. Understand basic concepts about CSS.
2. Use burp suite to monitor web traffic.
3. Write basic exploit code and perform attacks.

## **Prerequisite knowledge**

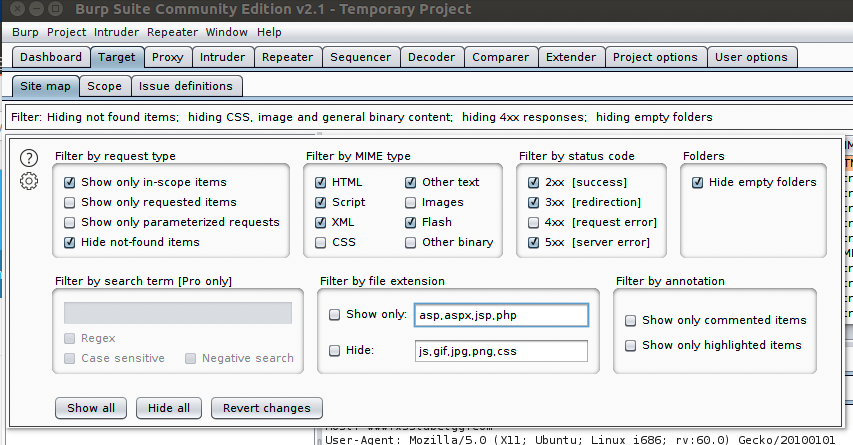
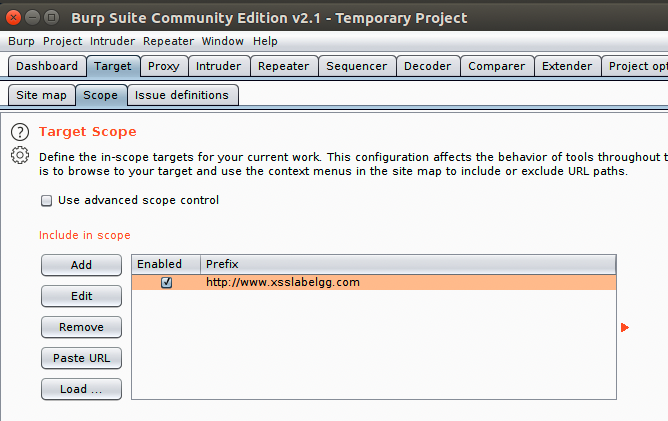
* Have very basic knowledge of web security
* Have installed prebuilt ubuntu 16.04 VM from the SEED website (<http://www.cis.syr.edu/~wedu/seed/labs.html> ) (This should be done in Lab2)

## **Lab Setup Requirements**

* Download Burp Suite Community Version (<https://portswigger.net/burp> )

## **Detailed instructions**

1. Download, install and set up Burp suite in the Ubuntu VM.
   1. First, you will need to download the Burp Suite Community version and install it into the Ubuntu VM (<https://portswigger.net/burp/releases?initialTab=community#community> ). The latest version cannot run on this old ubuntu machine. Instead, we will use an older version Community 2.1. You should download the plain Jar file, instead of the Linux 64 bit version, since the Ubuntu VM is 32bits. (The community version has limited functionalities. You can also request a free trial licence for the enterprise version if you want to use on your own computer. )  
      
   2. Follow step by step instructions on the Burp Suite support page (<https://support.portswigger.net/customer/portal/articles/1816883-getting-started-with-burp-suite>) to set up Burp suite.
      1. Start Burp Suite using the command: java -jar -Xmx2G /path/to/burp.jar or just java -jar /path/to/burp.jar. The default download path is ~/Downloads/. You can just use the default configuration and create a temporary project.
      2. Configure Firefox to work with Burp (<https://portswigger.net/burp/documentation/desktop/getting-started/proxy-setup/browser/firefox> ). Mainly you need to set up the proxy to use Burp to intercept the traffic.
      3. Install Burp’s CA certificate into Firefox in the ubuntu VM. Burp also intercepts https traffic. It uses its own CA certificate. Downloading and importing that into Firebox can make Burp work with https traffic without any issues. Make sure the burp is running and the firefox browser is configured to work with Burp in the previous step. Then follow the instructions on this page <https://support.portswigger.net/customer/portal/articles/1783087-Installing_Installing%20CA%20Certificate%20-%20FF.html>. If the interception is working, but “<http://burpsuite/>” doesn’t work, try to use “<http://localhost:8080>”. The CA certificate should be downloaded (cacert.der) in the ~/Downloads folder. Import that into the firefox and restart the firefox.
   3. A good tutorial about Burp can be found at: <https://www.youtube.com/watch?v=dwtUn3giwTk&list=PLv95pq8fEyuivHeZB2jeC435tU3_1YGzV> (There are 12 short videos available on youtube that explain some basic functionalities of Burp. You can take a look at the first several videos to get to know the basics about Burp.)
2. We will use the CSS attacks lab provided on the seed lab page as the base <https://seedsecuritylabs.org/Labs_16.04/Web/Web_XSS_Elgg/> . In this lab, a sample vulnerabile website xsslabelgg is hosted on the ubuntu VM. You need to start an apache server if it is not started, then you can access those websites in the browser. Instead of using HTTP header Live extension tool, we will use Burp Suite to observe http traffic, and perform various tasks. You can log into the elgg website as Samy. The credentials are given in the lab description.
3. Add <http://www.xsslabelgg.com> into the target scope in the Burp Suite since we are only interested in the traffic to this server. Use Spider in the Burp Suite to build the site map of this website. Explore the site and highlight the path for the add-friend action and edit-profile service. Use Proxy/HTTP history to observe the request and response detail of the http requests. You can use Repeater to send requests with different parameters.



1. Follow the instructions provided in the lab description, and try to complete all 7 tasks.

## **Questions**

Describe what you have done and what you have observed for each task listed in the lab instructions. You also need to provide explanations to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation.

## **Deliverables**

Please submit the lab report in a single document named *CS763\_yourusername\_Lab4*. Please submit a word or PDF document. The lab report should include:

1. Title, author
2. Table of Contents
3. The detailed steps and results using text descriptions and screenshots that answer the above questions and demonstrate your lab progress.
4. A summary of your own reflection on the lab exercise, such as:
   1. What is the purpose of the lab in your own words?
   2. What did you learn? Did you achieve the objectives?
   3. Was this lab hard or easy? Are the lab instructions clear?
   4. What do you think about the tools used? What worked? What didn’t? Are there other better alternatives?
   5. Any other feedback?