Homework 4 – Client Side attacks

# Lab Information

## Due Date:

Homework 4 Dropbox Deadline

## Objectives/Goal:

In this homework we will be investigating part one of client side attacks. While you are free to experiment however you’d like – note that this lab is not intended to be completed by leveraging XSS. The environment which you are entering is also hostile so be aware and use private browsing as needed.

## Deliverables:

* An image or scan of the completed signoff sheet.
* You code

## Table of Contents:

[Lab Information 1](#_Toc465113803)

[Activity 1: Know Thy Enemy 2](#_Toc465113804)

[Activity 2: Attack Thy Enemy 2](#_Toc465113805)

[Activity 3: Rebuff Thy Enemy 2](#_Toc465113806)

# Activity 1: Know Thy Enemy

## On the backend we have setup a Selenium script to represent our vulnerable client. This script will click any link that you post to the following message board (<http://52.54.91.74:5000/>). Your first goal is to demonstrate that this client is functioning.

## Step 1: Setup a server

Setup a publicly facing webpage. This may be on EC2 or it may be on a RIT wireless, you just need a publicly routable external IP. Don't forget to disable your firewall as needed. Send our client a message with the link to your page. Use your access logs to verify that the client has connected to your site. Show this to your professor for a signoff

## Step 2: Find out about the client

After you have proved that the client will access your page, modify your site to gather some information about the client. You should gather the referer, IP, User-Agent, and inject JavaScript to determine what plugins are running. Once you have gathered the information show this to your professor for a signoff.

# Activity 2: Attack Thy Enemy

Our first encounter with our enemy allowed us to get a better understanding of where the enemy’s weaknesses may lie. This was our first foray into attacking a client. Now we will leverage some aspects of their environment to our benefit.

## Step 1: Cross that client

Now we’re going to use a weakness of the client (Jon Doe) against them. We know our client LOVES Armbook, he’s ALWAYS online (<http://54.84.187.188/armbook/>) and he’ll also click on links. Make an account and figure out a way to get him to friend you. Do not use Cross-Site-Scripting.

## Step 2: Fix an Agent

The source code for the current version of Armbook is available online. Fix all variants of the underlying issue that you have encountered and get a signoff from your professor that the issue is fixed. Make sure to post your code in the dropbox.

# Activity 3: Rebuff Thy Enemy

## Step 1: A Jack of all attacks

Your attacker has implemented the changes you suggested, but you still want to attack him. Using a different attack method, generate a page that if visited and interacted with would result in him becoming your friend once again (This is not the same attack as in the previous activity). Create such a demonstration page and show this to your professor for the sign off.

## Step 2: A fix for the itch

Describe to your professor how you would go about fixing this issue.

Signoffs

## Activity 1.1 – You have forced the client to connect back

## Activity 1.2 – You are able to undertake client attribution

## Activity 2.1 – Show that you were able to get our client to friend you and describe how

## Activity 2.2 – Show that your countermeasures are successful at preventing this

## Activity 3.1 – Show a demonstration of how you would get the client to friend you, with minimal client interaction and describe how

## Activity 3.2 – Describe the fix for 3.1