Homework 7 – Session Security

# Lab Information

## Due Date:

Homework 5 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](#_Toc465949991)

[Activity 1: A Fixation on Security 2](#_Toc465949992)

[Activity 2: I Predict Weak Security in Your Future 2](#_Toc465949993)

[Activity 3: Session Hijacking 2](#_Toc465949994)

[Activity 4: Authentication Brute Force 3](#_Toc465949995)

# Activity 1: A Fixation on Security

## We are going to retarget our vulnerable client again on the backend. This script will click any link that you post to the following message board (<http://52.54.91.74:1237/>). He also really likes Armbook and will check it whenever given the opportunity to do so.

## Step 1: Send that Session ID

As we learned in class it is often possible to provide a user with a session. Of course we demonstrated using a GET parameter, but this is unrealistic as we know that no one would DREAM of sending session ID’s or other sensitive information via GET. Take a look at the NEW ARMBOOK (<http://52.90.2.57/>). Investigate how it stores sessions.

## Step 2: Find out about the client

Once you’ve figured out the session management, you need to trick the client such that you’ll be able to get access.

## Step 3: Fix the client

Now take the code for the new Armbook and fix the session management such that this problem doesn’t occur again. You may not use PHP sessions. You should rearchitect the application to prevent this issue, not merely make it more difficult to exploit.

# Activity 2: I Predict Weak Security in Your Future

Alright you have recommended a fix for the previous session issue, great job, but there are other problems with our sessions. Someone has breached even the fixed version of Armbook and it is your job to figure out how they did that!

## Step 1: Testing for fitness

Both Burp and ZAP have some capabilities to analyze session information. Use either Burp or ZAP to collect and analyze the security of the session ID generated by the new Armbook. Figure out how they snuck through by demonstrating it.

## Step 2: Recommended changes

Rather than fixing it in the code, the developers wanted to take a crack at fixing this one themselves, explain what went wrong and how they would fix it. Make a mini presentation for them highlighting the areas in the code that are the problem and the right way to go about fixing it in their language.

# Activity 3: Caffeine Hi for Jack.

Man there is nothing our Hooli employee loves more than Coffee in the morning. You might find that there is a Starbucks Coffee nearby, that’s probably where he went. It is pretty likely that our Hooli employee will login and browse Armbook every so often over this connection.

## Step 1: Punish Him!

Leverage our Hooli employees need for caffeine to gain access to his account. Demonstrate that this attack is functional using the HTTP generation took that you made in the previous labs.

# Activity 4: Take a Sip of This Brute

If all else fails you can always go for broke. In most cases this is some sort of Brute Force attack. It is important to note that while many authentication systems have limits, often alternative login methods like mobile API’s will not.

## Step 1: Finish Him!

Use Burp or ZAP in order to brute force the login credentials. Note, while we have demonstrated Burp in class, it will be throttled in its demo version. Demonstrate that you now know at least two (non-student) user account passwords

Signoffs

## Activity 1.1 – Demonstrate that you can trick the client and log in as them.

## Activity 1.2 – Show how the code was fixed and demonstrate that your attack no longer works.

## Activity 2.1 – Show that you are able to log in as the client again.

## Activity 2.2 – Give your demonstration on how to fix the project.

## Activity 3.1 – Show that you were able still able to get our client to friend you and describe how

## Activity 3.2 – Describe the fix for 3.1

## Activity 4 – Show that you can brute force the password