Homework 2 – Using HTTP

# Lab Information

## Due Date:

Homework 2 Dropbox Deadline

## Objectives/Goal:

To understand the usage of popular HTTP design decisions by creating and using an HTTP user-agent.

Hooli Inc, is a reputable web application service provider. This semester you will be serving as Hooli’s Web Application Tester.

This week you have learned about various aspects of HTTP. Your goal is to design and use a custom made implementation of an HTTP user-agent. This user-agent will send requests and parse responses based on RFC 2616. As you develop your solutions you will be charged with undertaking certain common within Hooli’s webservice.

## Deliverables:

* An image or scan of the completed signoff sheet.
* A copy of your code

## Table of Contents:

[Lab Information 1](#_Toc460328030)

[Platform Choice: 2](#_Toc460328031)

[Vulnerability Scanning: 5](#_Toc460328032)

[Signoffs 6](#_Toc460328033)

# Activity 1: Initial Server Access:

Hooli Inc, has a simple registration portal for developers and security testers, like yourself. Follow the instructions to make your user account. During the course of this homework you MUST use sockets (this means no requests library or curl or anything like that).

## Step 1: Start your [coding] engines

The first thing that you’ll have to do is access the server. A simple valid HTTP 1.1 request is required here. The host you’ll be using for the rest of your requests is [http://54.209.150.110/](%20http://54.209.150.110/). You MUST receive the flag in order to get credit for this activity.

# Activity 2: Get your tokens

Of course there is security here. Hooli IS security. Before you can get your second flag, you must access get your security tokens. These tokens are UBER secure. They are time sensitive and linked to your IP address, you will be required to use them for all subsequent requests

## Step 1: Take a practice lap

Hooli will provide you a token by accessing /getSecure. Once you’ve gotten your token supply it as the ‘token’ parameter to /getFlag2. If you’ve done this correctly you’ll be given a flag. Simple, right?

# Activity 3: Let’s see some CAPTCHA

Hooli understands security, and they want only their engineers with their applications to be able to access the next flag. To that end they’ve put a little challenge in place that only their application can solve. Can you get by it and get to the third flag?

## Step 1: Avoid the pit stop

This flag requires you to get your security token and access / getFlag3Challenge providing your token (just as in the previous activity). This will return a CAPTCHA challenge. Solve the CAPTCHA and provide it back. The CAPTCHA solution should be provided as the ‘solution’ parameter of the / getFlag3Challengepage. Upon successfully doing this you will be greeted with Flag3.

# Activity 4: Register your account

Great! You should have everything you need to register for your account at Hooli. Now you need to just do it! But your Hooli overlords have thrown one more wrench in your path. They decided that NO hacker ever has used Internet Explorer, so they’ll only accept requests from IE. Show them who is boss!

## Step 1: Cross the Finish Line

To make you’re Hooli account send a request with a ‘username’ parameter and a token to /createAccount. Of course you can choose what your username is going to be. Hooli will provide you with a password. From there you should log in to test your account. You can login on the /login page. This page requires a token, username, and password

# BONUS Activity 5: Javascript’n

Hooli has put an additional security mechanism in place! It is meant to prevent automation, because you’ve thwarted them before. This security comes in the form of a snippet of javascript that must be run and the response sent to the server before the page will load using AJAX. If you interested in this ask your professor for more details.

Signoffs

## Activity 1 – Demonstrate that you have the first flag

Show your instructor your code for accessing the first flag. Inform your instructor what the minimum requirements of an HTTP/1.1 request are.

## Activity 2 – Demonstrate that you have the second flag

Show your instructor your code for accessing the second flag. Inform your instructor of the level of security that the token has and explain how you would verify that

## Activity 3 – Demonstrate that you have the third flag

Show your instructor your code for accessing the third flag. Inform your instructor why this CAPTCHA system is broken and how it could be improved.

## Activity 4 – Demonstrate that you have the fourth flag

Show your instructor your code for accessing the fourth flag. Inform your instructor what challenges you ran into and any security issues that Hooli has with their registration system.