R·I·T

Rochester Institute of Technology
Golisano College of Computing and Information Sciences
Department of Computing Security

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 security 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 solution you will be charged with undertaking certain common tasks using Hooli’s web service.

Fun fact, each of the activities in this assignment is representative of an issue identified on real customer assessments at one point or another in my career. The web is a crazy place and you should always expect the unexpected.

Deliverables

- All flags must be submitted **via course portal** at https://csec380-core.csec.rit.edu.
- A copy of your code to the Dropbox.

Table of Contents:

Activity 1: Initial Server Access:

Hooli Inc, has a simple registration portal for developers and security testers, like yourself. Follow the instructions to use their API. During the course of this homework, **you MUST use sockets** (this means no requests library or curl or anything like that). **The flags you receive are CUSTOM for your user. Make sure to submit a parameter called 'user' with the value of your RIT username.** This parameter can be submitted as a POST or GET parameter and is required for all activities (even the one where you specify a username parameter)

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://csec380-core.csec.rit.edu:82/. You MUST receive the flag in order to get credit for this activity.

Hint: Check your HTTP return code, if it's 200, it means the webserver received a valid HTTP request. If you're not getting the answer you need, perhaps you need to be more creative.

Activity 2: Get your tokens

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

Note: These tokens expire after 2 seconds, you'll need to automate the tasks to complete the remainder of the homework (this is not a challenge).

Step 1: Take a practice lap

Hooli will provide you a token by accessing /getSecure. Once you've received your token, supply it as the value to the 'token' parameter on /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 to access their service. They've put a CAPTCHA in place to prevent you from accessing the next flag. The CAPTCHA is a little challenge that only a Hooli employee can solve. Can you solve 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 /getFlag3Challenge page. 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 your Hooli account send a request with a ‘username’ parameter and a token to /createAccount. You can choose what your username is going to be (it may be different from the ‘user’ parameter). 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 the automation they’ve detected you. 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’re up to the challenge head to /getFlag5. This type of model is a mix of JavaScript challenge and a technique that is occasionally used with native thick clients. Good luck!

Submissions:

Activity 1 - Submit flag one (20%)

Activity 2 - Submit flag two (20%)

Activity 3 - Submit flag three (20%)

Activity 4 - Submit flag four (20%)

Code submitted to MyCourses (20%)

Bonus [Optional] - Submit flag five (20%)