# CIT 448 Challenge Lab Setup & Solution

## Setup

The grade server is a Python application. The application requires [Flask](http://flask.pocoo.org/), a web development microframework. You will need [pip](http://www.pip-installer.org/en/latest/), a Python package manager, to install Flask. Once pip is installed, download Flask by executing:

$ pip install flask

Once Flask has been installed the server can be run by executing the following command:

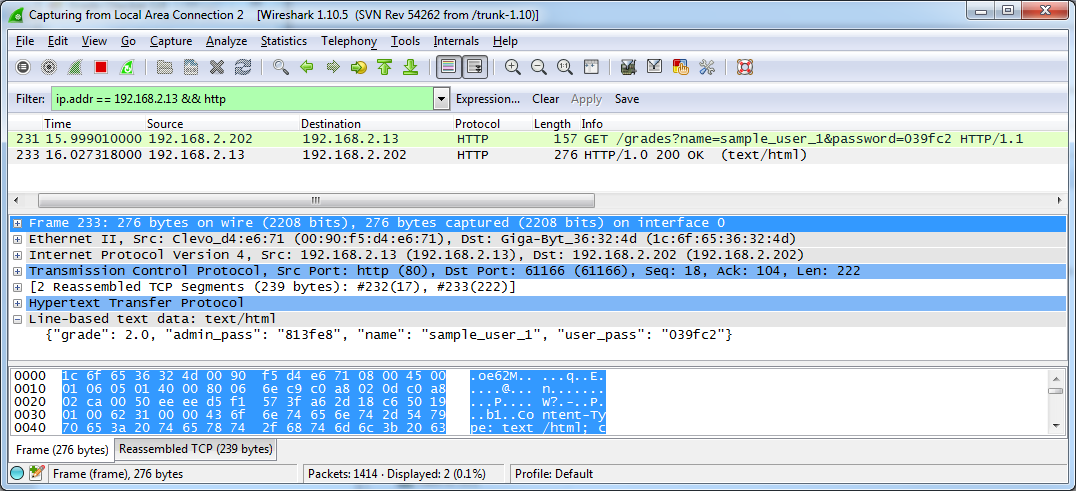
$ python webserver/cit448-finallab-webserver.py

The server will listen on port 80. The server hosts a RESTful API used by the Grade Checker app to return and update grades. It also has two pages that show the current values for the different users. Going to /status will give a list of all users and their current grade. Going to /status-full will show all users and the grade, as well as their regular password and admin password. Each student should be given their username and regular password. They should also be given the username only of an “adversary”. Their goal is to change their own grade (presumably to a 4.0). Bonus points should be awarded to the team that can also change the adversary’s grade to a 0.0.

The Grade Checker app requires .NET 3.5 (which should be installed by default on Windows 7 and up). Provide the IP address of the server to each student; this will be needed to log into the app. If your server’s IP address is 1.2.3.4 then students should put “1.2.3.4” into the server address box in the app.

## Solution

The grade checker app connects to the webserver and uses a [RESTful](http://en.wikipedia.org/wiki/Representational_state_transfer) API to retrieve grades. Because this occurs over unsecured HTTP, the resulting communications can be sniffed using [Wireshark](http://www.wireshark.org/). The key vulnerability is that the admin password for the user is sent in the RESTful response to a GET to /grades by the app.



The data is returned as a JSON object. Clearly, the “admin\_pass” member should not have been included by the server! By re-logging in with the admin password, the student will be presented with a text box to change their grade.

The extra credit solution involves recognizing that both the regular and admin passwords are derived from the MD5 sum of the username. For example the MD5 of “sample\_user\_1” is 039fc25e9c5100fea67c27c8d8813fe8. We can see that for a given user, their regular password is the first six digits of the MD5 sum; the admin password is the last 5 digits. If the students recognize this then they can calculate the MD5 of the adversary username, log in with their admin password, and change their grade as well.