CSCI 4178 CYBER SECURITY AND DEFENSE

Capture the Flag 2

Prof. Rafael Copstein

Objectives

- Apply the techniques learned in class to invade a real system
- Identify possible points of attack and their vulnerabilities
- Perform the right technique to exploit each vulnerability

*You have come across an unreleased system management software provided by **LiSQ**, as they continue to pursue new ideas after a recent fiasco with their chat app. It is your job as a security professional to find and report any new vulnerabilities you can find on this software. Are you up to the challenge?*

Capture the flag

A *Capture the flag* (CTF) is an exercise where a vulnerable system is made available to the participants and their objective is to find all such vulnerabilities. To prove that you have found the vulnerability, you must submit a *flag*, that is, a string composed of random characters prefixed by "**FLAG_**". Once a flag has been found, the participant submits it to the competition, which awards them points.

In this assignment, you must enter the website for the *Uploader* and find all 5 vulnerabilities hidden within. Each vulnerability will provide you a flag that you must later attach to your submission. For each vulnerability that you find, you must also be able to describe the steps taken to exploit it.

How to play

Using the *docker-compose.yml* file available on Brightspace, fire up the containers that compose the system. You'll then access the main page of the website via the URL http://localhost:80/. If port 80 is taken on your system, you are allowed to change the *docker-compose.yml* file to map another local port to the container. **You are not allowed to make any other changes to the Docker Compose file**.

During your analysis of the system, keep in mind that you will **not** be required to perform any form of large-scale attack (such as DDoS), or any form of social engineering against the instructor, TA, or other faculty members/students. All the information you require is available on the system at hand. You are also **not** allowed to tamper with the Docker containers, that is, you must not edit their contents or access them directly. All the interaction required must be done through the deployed website or via SSH. You **are** allowed to use external tools/scripts as long as they target the system, not the underlying container.

Submission

Your submission consists of a report containing 5 sections (one for each vulnerability), with the following:

- What the vulnerability is
- How the vulnerability was exploited
- What was the flag found
- A screenshot of the system with the flag visible

It's important to keep in mind that, in your report, you must be able to explain **why** the actions you performed are a vulnerability. If, by any chance, you stumble upon a flag but are not able to explain what the vulnerability is or how to consistently find that vulnerability, you will not be awarded the points for that challenge.

Each student must submit their own report on Brightspace, this is **not** a group assignment. Include your name and B00 number on the report itself and name the file **B00XXXXXX_YourNameLastName_CTF2.pdf**.