Alex Miller
Jordan Latimer

Senior Project Proposal

Capture The Flag - Cybersecurity

Background

CTF (Capture The Flag) is a popular type of competition used for cybersecurity. It involves users using their cybersecurity knowledge to find a hash on a system that's known as a flag. CTF's are typically used to gain a better understanding not only of the cybersecurity realm but of terminal commands. Flags could be found inside of hidden files as well as a cipher for example. This project started last semester, for CS495, in a hope to provide the cybersecurity department an alternative web app to use for their CTF events. Dr. Marquardson of the cybersecurity department was a great help in sharing his vision of his ideal CTF web app. By semester's end, we were able to provide a prototype that included many of the desired features, but we felt there was still so much that could be done. This will be a continuation of that prototype that we can hopefully distribute and help students learn more about cybersecurity.

Project Details and Technologies Used

The project's bulk is a website using HTML and CSS. JavaScript will be used as client and server side programming. There are library modules in JS that let us connect to Docker Desktop that we will use for instances of the flags. Docker is a program that allows users to create environments called containers that can be manipulated. We can set up a container based on what the admin wants including the OS and where the flag is placed. Then we can use that container's terminal and use Xterm.js to view that terminal and be able to interact with it on our website. A SQLite database will be used to store all sorts of information such as the users, emails, passwords, flags, etc. We will be using GITea as a form of source control, to share code amongst one another. Since we didn't add everything we wanted to last semester, we figured we could add some more features which include: code injection via a Python script, to plant the flag, and the possibility of the admin to create a file system tree which is then used to create a dockerfile for the users to use in their virtual environment. Although we did do a lot of work last semester, most of which will be scrapped and/or restructured to make everything run more smoothly and efficiently as well as for scalability.

Learning Outcomes

With this project we hope to learn more about taking our idea and project to the next level by creating a product that can be used by actual users and potentially universities. This will require us to overhaul the design of our web app and make it suitable for scalability. By taking this next step, it will show us what we can expect from real world projects post graduation. We will also learn more insight into the cybersecurity world of computer science which gives us an extra tool in our toolbox for real world situations. Because we will be working in a group, this

will give us more experience with source control, sharing and revising code between the two of us. This project encompasses what is usually done when in software development.

Below, is a rough outline of who will be responsible for what throughout the project:

Alex:

- Tighter container creation/deletion
- Python code injection
- System stats for admin
- Security Concerns
    - Secure login system
    - Encryption for DB
    - Malicious/broken python code handling
    - HTTP → HTTPS

Jordan:

- Real time progress tracking of the users in the contest
- System logs for milestones reached “John Doe has collected half of the flags!”
- Database creation/deletion and DB scalability
- A way for users to go back to previous contests/environments and practice old flags, will not count towards their stats.
- Randomly generated names for the leaderboard, only the admin can see the actual email behind the name.

Both:

- File system tree to dockerfile/image
- Restructuring/optimization of old code for simplicity and scalability.