HRS Capture the Flag

Akhil Pullela & Max Calcoen

GitHub Repository

Scope & Purpose

This project aims to address the lack of awareness and understanding of cybersecurity among high school students. By creating a Capture The Flag (CTF) competition tailored for high schoolers, we aim to introduce them to cybersecurity fundamentals engagingly and interactively. The project seeks to demystify cybersecurity concepts and inspire interest in this crucial field.

Installation & Set Up

This project relies on several dependencies that are crucial to the program.

First, install Python using this website. We recommend version 3.11.3. Then, you must install a virtual environment and download the necessary modules that our project depends on:

1. Open the command line (Terminal / Command Prompt).
2. Navigate to the project folder using cd commands (i.e. cd path/to/the/folder). Here's a tutorial if you've never used cd commands before.
3. Type this into the command line and press enter: "python -m venv venv". This will create a virtual environment.
4. Run "source venv/bin/activate" to enter the virtual environment.
5. Run "pip install -r requirements.txt" to install the dependencies. Pip is a package manager that can be used to install dependencies, and it should have been installed with the virtual environment.

We also depend upon certain applications for our program to run.

- Redis: an in-memory store that handles user sessions.
- Docker: a platform to deploy "containers", which we use to create insecure servers that can be safely hacked without consequence to the host machine. We recommend Docker Desktop for easy use.

Next, you must install the docker images used.

1. Open the Docker Desktop app.
2. Currently, only problems 5 and 11 use containers. Repeat the following steps for both containers:
3. Open the command line.
4. Navigate to the project folder using cd commands.
5. Navigate to the "gym_resources" folder.
6. Navigate to the problem folder. Either "05_sql_injection" or "11_trace_the_dots"
7. Navigate to the container folder.

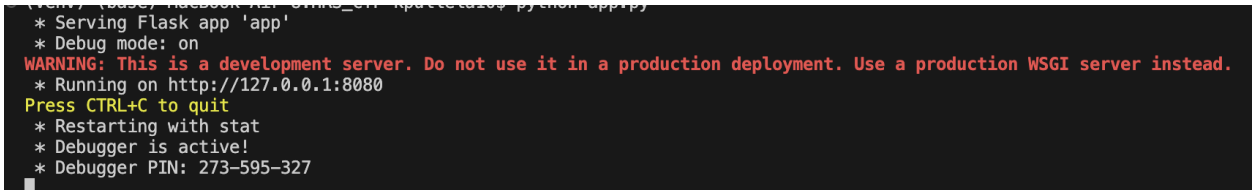
8. Run “docker-compose up --build” to build the image. This will also launch a container, so use ctrl-c to remove the container.
9. Remember to repeat for both problems!

Let’s make sure you’ve installed everything before we run the program!

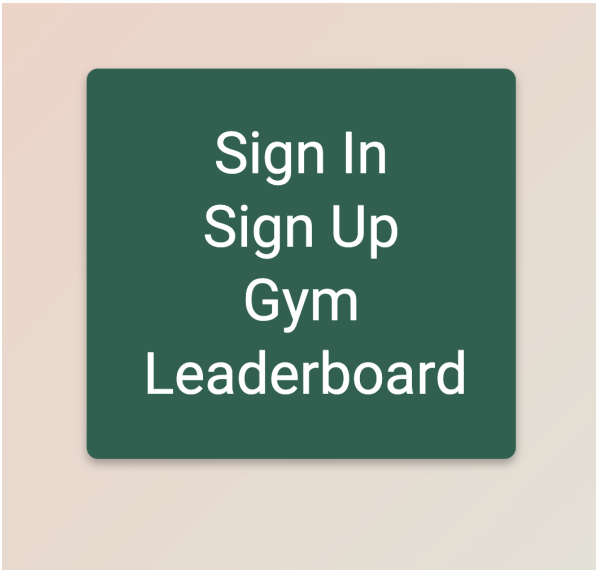
- ☐ Ensure redis is running by entering “redis-cli ping” in the command line. It should reply “PONG”. It’s managed by your system’s service manager to start automatically, but if it isn’t running, try restarting your machine. On Mac, you can try running “brew services restart redis”. On Windows, try “net stop Redis”, then “net start Redis”.
- ☐ Ensure the docker daemon is running by opening the Docker Desktop application.
- ☐ Ensure you’re in the virtual environment. You should see “(venv)”. If not, run “source venv/bin/activate”.
- ☐ Ensure you have all dependencies installed by running “pip freeze”. You should see all 30 dependencies in the form “name==version”

You can now run the program. cd into the project directory and run, “python app.py” or “python3 app.py”.

In the terminal, you should see something resembling the image below:



Simply cmd+click on http://127.0.0.1:8080; you’ll arrive at the site’s landing page below.

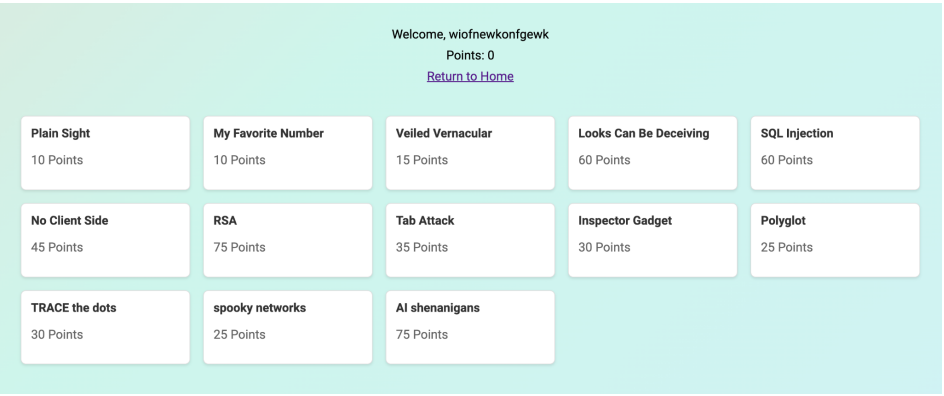


Your first step as a first-time user should be to create an account. You’ll see an option to “Sign Up”. Clicking on it will bring you to a sign-up page. Just enter a username and password, and you’ll have an account.

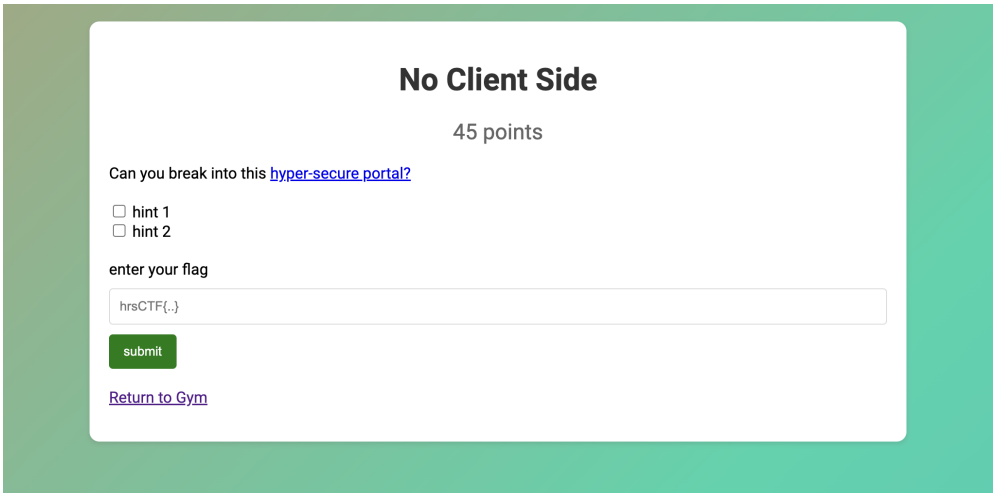
Navigating the Site

After creating an account, you'll be able to access the gym and leaderboard pages.

Gym



Let's take a look at the gym page first. Each box is an exercise. Exercises already completed turn green. Each problem has a name and the amount of points you'd receive for completing it—the harder the problem, the more points you'd receive. As a new user, none of the problems will be green, and the total amount of points you've accumulated, as seen at the top of the screen, will be 0.



To solve an exercise, simply click an exercise box. You'll arrive at a page similar to the one on the left.

Underneath the problem's point worth, there's a description, and either a link to download the exercises' files, or a button to launch a server that will be involved in the problem.

The objective of each exercise is to locate a flag—a phrase that looks like this: hrsCTF{*some keyword here*}. These flags are located within each exercise's associated files or servers, where

you'll need to use a variety of cybersecurity techniques to uncover them, like deciphering ciphers or exploiting server vulnerabilities.
Once you've found a flag, simply copy and paste it into the submission box, and hit submit. If you see confetti, congratulations! You've earned the problem's points. If not, keep looking.

If you get stuck, feel free to check the 'hints' boxes. Each one will reveal some important information, such as perhaps a recommended approach to a problem, without penalty.

Leaderboard
If you head to the Leaderboard page, you'll see a ranking of all players, sorted by the most amount of points. (**image**)

Signing Out
At any time, you may sign out of your account by returning to the home page and clicking sign out. Your progress will still be saved; you'll be able to log into your account on other devices without your point total being affected by clicking sign in, and entering your credentials.

Recommended Tools

Proxyman: Used to monitor and generate GET, POST, PUT, and other requests
Visual Studio Code: Highly recommended text editor; use it to solve CTF exercises