Homework 5: HTTPS

Application Objective: HTTPS and Nginx

Setup your app to listen for HTTPS requests on port 443 using a self-signed certificate and nginx running in a separate docker container. The app must function properly. More specifically:

- If you receive an HTTP request over port 80, it should be redirected to HTTPS over port 443
- The app should be set up to use WebSockets for the chat feature. The WebSockets should be encrypted using WSS
- Add the secure directive to your auth token cookies

Testing Procedure

1. Start your server with docker compose up
2. Open a browser and, with the network tab open, navigate to http://localhost
    a. Accept any warning about a self-signed certificate
    b. Verify that the home page loads
    c. Check the network tab to verify that you received a redirect to https://localhost and that the page loaded properly over HTTPS
3. Verify that WebSocket connection was made using the WSS protocol
4. Register and login
5. Send a message in chat and verify that the feature still works (Displays your username) over WSS
6. Check the auth token cookie and verify that the secure directive was set

Submission

Submit all files for your server to AutoLab in a .**zip** file (A .rar or .tar file is not a .zip file!). Be sure to include:

- A docker-compose file in the root directory that exposes your app on port 8080
- All of the static files you need to serve (HTML/CSS/JavaScript/images)

It is **strongly** recommended that you download and test your submission after submitting. To do this, download your zip file into a new directory, unzip your zip file, enter the directory where the files were unzipped, run docker compose up, then navigate to localhost:8080 in your browser. This simulates exactly what the TAs will do during grading.

If you have any Docker or docker compose issues during grading, your grade for each objective may be limited to a 1/3.

Grading

Each objective will be scored on a 0-3 scale as follows:

3 (Complete)	Clearly correct. Following the testing procedure results in all expected behavior

2 (Complete)	Mostly correct, but with some minor issues. Following the testing procedure does not give the *exact* expected results, but all features are functional
1 (Incomplete)	Not all features outlined in this document are functional, but an honest attempt was made to complete the objective. Following the testing procedure gives an incorrect result, or no results at all, during any step. This includes issues running Docker or docker-compose even if the code for the objective is correct
0.3 (Incomplete)	The objective would earn a 3, but a **security** risk was found while testing
0.2 (Incomplete)	The objective would earn a 2, but a **security** risk was found while testing
0.1 (Incomplete)	The objective would earn a 1, but a **security** risk was found while testing
0 (Incomplete)	No attempt to complete the objective or violation of the assignment (Ex. Using an HTTP library)

Note that for your final grade there is no difference between a 2 and 3, or a 0 and a 1. The numeric score is meant to give you more feedback on your work.

3	Objective Complete
2	Objective Complete
1	Objective Not Complete
0	Objective Not Complete

Autograded objectives are graded on a pass/fail basis with grades of 3.0 or 0.0.

Security Essay

For each objective for which you earned a 0.3 or 0.2, you will still have an opportunity to earn credit for the objective by submitting an essay about the security issue you exposed. These essays must:

- Be at least 1000 words in length
- Explain the security issue from your submission with specific details about your code
- Describe how you fixed the issue in your submission with specific details about the code you changed
- Explain why this security issue is a concern and the damage that could be done if you exposed this issue in production code with live users

Any submission that does not meet all these criteria will be rejected and your objective will remain incomplete.

Due Date: Security essays are due 1-week after grades are released.

Any essay may be subject to an interview with the course staff to verify that you understand the importance of the security issue that you exposed. If an interview is required, you will be contacted by the course staff for scheduling. Decisions of whether or not an interview is required will be made at the discretion of the course staff.

When you don't have to write an essay:

- If you never submit a security violation, you never have to write an essay for this course. Be safe. Be secure

- If you earn a 0.1, there's no need to write an essay since you would not complete the objective anyway
- If you earn a 0.3 or 0.2 for a learning objective after the expected deadline, you may fix the issue and resubmit for the final deadline instead of writing an essay (Or you can write the essay so you don't have to sweat the final deadline)