Alex Hamilton

CS-499: Computer Science Capstone

Southern New Hampshire University

August 2, 2020

Narrative: Databases

1. This artifact is from the Client/Server development course at SNHU. It uses a RESTful API with Bottle to allow a user to send HTTP requests to make CRUD changes to a Mongo database.
2. This artifact uses python to directly manipulate a MongoDB, and it is the only project I have that works with databases in some way. The pymongo commands show that I understand database CRUD functions and the MongoDB collections system. The endpoints show that I understand the concept of a RESTful API and cURL HTTP requests. Lastly, the program itself shows understanding of python and how it is used in web programming. For this artifact, I added a delete\_one endpoint as chosen in the outline and tested it to make sure it behaved differently than the original delete function that used delete\_many (see screenshot). I also added a very basic password system.
3. This artifact covers the security mindset course outcome, though I had hoped to add authentication for the client side as well. I couldn’t really figure out how to do login with redirects for a CLI application; I don’t think it’s reasonable. However, I think the error handling also fulfills this objective and shows that I understand how try/catch loops are used to prevent vulnerabilities and improve the user experience by preventing crashes.
4. Out of all the artifacts, this one required the most re-learning and environment set-up with the client and server sides along with the database and the python application. It also required the most research. I think RESTful APIs are a complicated topic, especially seeing how it took the full course to make the application originally. In my research, I learned about the different API frameworks such as Flash and Django and realized that they have a lot more functionality than Bottle. I also learned that securing the user is a sort of rabbit hole and the developer needs to decide where to stop. For example, it starts with implementing user authentication, then realizing that the password needs to be secured, then that the database needs to be secured etc. I think a lot of companies that have data breaches stopped in this process before they should have.