REVIEW

The design and structure are okey. The documentation tells us how to get the app running and what you can do. The source code has a lot of comments explaining functions. There are a lot of unused imports and some code. The source code consists of functions that initialize the other scripts in the project, and is used to declare and link the attributes in the server together creating a good enough backend structure for the app.

I don't know if you want me to provide a full description of the source code, so i'll wait with it and do it if i have enough time.

design / coding style improvement
I would try to group each aspect of the code in a better way, and make the code style clearer so that it's easier to spot bugs in the program. I think i would make the login and logout handling more related to each other and then make it easier by just importing the code needed into the source code. I would structure the code better to make sure that unused imports and code will not be a problem, and also make sure the different parts of the project is not alway opened unless it's called. This is to prevent attackers from taking advantege of the unused functions that may not be security checked or are weak. Also handle the connection to the database only callable where it's needed. Generally speaking:

- Make the code cleaner to spot bugs
- Group functions into categories so that they are called only when needed and not being run in the background when they are not needed.

Threat model
I realise now that i'm dumb and didn't know that if you did not complete obligatory 2 you needed to analyze someone else's code. I did actually start task 2, but i had issues connecting all the aspects of the problem and i even had to switch computers before getting it to work, So my answer is based on what i learned from this. I did add a logout route for the project, but that's about it. This means that the security issues from obligatory 2. are still there. I'm just going to explain these and if i have some time i could try to improve the code a bit. (I don't know if this gives me any points but i'll do it anyways if i have time)

Security issues:
I was able to preforme a cross-site scripting attack. I'll include som pictures. I basically played around a bit with the input fields to see if i could do something. Using the message box i was able to insert a script which made an alert pop up in the search site. I don't know if the app is protected against this, but i think it's hidden, but i tried to insert <script>alert(document.cookie)</script>. This is a normal way for attackers to get ahold of cookie session id's

I used Zap to discover vulnerabilities in the program:
It gave me alerts. (I only ran the scan to 43%)

- SQL injections
- CSP header not set
- Cookie without sameSite attribute
- Server leaks version information via "server"

- X-content type option header missing.

I didn’t realize until too late what project i was supposed to analyze my bad :(So i’m just handing in this.