**Notes**

* Discussed having a food blog, maybe posting recipes and having comments
* Ability to edit, delete posts and change publicity.
* Account enumeration – remove multiple attempts, never verify an account exists when the user is not logged in. CAPTCHA helps mitigate the multiple attempts and stops usage by bots. Do not add any user details that you can use to login when seeing which user posted the blog.
* Session hijacking – Using HTTPS
* Cross-site scripting – Encryption and decryption system using PGP.
* Suggested using postgres for data
* Best to use mongoose db to avoid SQL injection
* Use bcrypt library for encryption
* Express to update webpages
* Use JSON tokens to store usernames and passwords to avoid account enumeration