When creating an email site, it is important to keep email credentials extremely secure. This is because oftentimes when signing up for a website, an email is required as a form of authentication and many services send “forgot password” prompts through the email. A breach in email security would compromise every single account the user has linked to the email. A best case scenario would be that a video game account is hacked. Worst case scenario would be a bank account is compromised. This is especially true for our group project. Our group project utilizes Google Cloud Developer tools. This would allow us to access all of our client’s emails, calendar events, chat logs, tasks, etc. If our database were to be compromised, all users' gmail accounts could be scraped for sensitive information, used as zombies for malicious email spam, and various other schemes. For this main reason, we will not be pushing our database up to the repo when we actually include our google token as a part of the user data.