The assignment is centered around Condution, an open-source task management platform. Data processing and querying is done on-device, but raw user tables and data is stored in a remote PosgreSQL server that's either officially hosted and supported or optionally on-prem hosted by the user.

1 | **What are we protecting?**

Because of the open-source nature of Condution, and the fact that all data processing code is done with the client application, the most important asset to actually protect is any user's data (tasks, perspectives, due dates, etc.).

This means creating a secure pipeline between our servers and that of the clients, that from self-hosted servers and that of their clients, and finally the clients themselves.

The scope of Condution is has too narrow scope to protect anyone but direct Condution user's data, including misuses of the client app or API but not including users of a third-party services with indirect API interfaces to Condution.

2 | **Who are we protecting it from, and what are their motivations?**

2.1 | **Protecting from...**

- Advertisers who may want to advertise based on notes of users
- Foreign companies and groups who are attempting to access privileged information
- Bad actors looking to leverage a ”weak-point” in a user's security profile
- Well-meaning but security-unconscious users

2.2 | **Not Protecting from...**

- Organized, state-supported exploits
- Third party authorization and our hosting partners (AWS S3)
- Intentional, non-data leaking misuses (DDOS; creating fake accounts, etc.)

3 | **What methods of attacks do we prevent?**

3.1 | **Software Attacks**

- Auth pipeline password cracking
- Cross-site cookie sniffing
- UI design

3.2 | **Pipeline Attacks**

- Breaching of PAM on our pipeline (once it gets to AWS IAM, its their problem)
- Breaching keys and cookies for our deployment system
- Leaking signing keys

3.3 | **Social Attacks**

- Security misinformation (like self XSS via the JavaScript Console)

- Weak passwords
-