**Significant Security Risks/Assumptions**

Fast API has built-in data validation, makes it an ideal candidate for the backend side of our web application. Fast API validates the developer’s data type even in deeply nested JSON requests

Fast API is built on standards like JSON Schema (a tool used for validating the structure of JSON data), OAuth 2.0 (it’s the industry-standard protocol for authorization), and OpenAPI (which is a publicly available application programming interface). OpenAPI has a way to define multiple security "schemes".

OpenAPI defines the following security schemes:

* **apiKey:** an application specific key that can come from:
  + A query parameter.
  + A header.
  + A cookie.
* **http:** standard HTTP authentication systems, including:
  + bearer: a header Authorization with a value of Bearer plus a token. This is inherited from OAuth2.
  + HTTP Basic authentication.
  + HTTP Digest, etc.
* **oauth2:** all the OAuth2 ways to handle security (called "flows").
* **openIdConnect:** has a way to define how to discover OAuth2 authentication data automatically.

FastAPI provides several tools for each of these security schemes in the fastapi. Security module that simplify using these security mechanisms.