**These are copied directly from my notes.**

**These are in no way “complete” and are probably a mess.**

# Some Points About Web Dev.

## Client Side

\* CSS Grids

\* Helps with layout and responsiveness

\* Use a CSS Framework if you don't have a specific plan for a style in mind

\* Bootstrap

\* Foundation

\* JavaScript

\* Keep JavaScript in separate file as much as possible for easier debugging.

\* Browser Dev Tools exist, use them!

\* CDNs

\* Help with client-side caching

\* Have a self-hosted fallback if practical

\* Front-End Javascript Framework?

\* You might want one if you are doing a lot client-side

\* What not to do client-side

\* Send as little sensitive information to the client-side as possible.

\* Assume all code and data in the client-side is visible to the user

## Server-Side

\* Don't trust the client-side

\* Validate data coming in from client-side

\* Cache-Busting

\* Find a way to automate this if you are doing more than a simple web page.

\* Prevent SQL Injection

\* Sanitize database queries properly or use an ORM

\* CSRF Protection

\* Tokens

\* Be sure to also use the tokens for AJAX requests

\* Database

\* Database Connections

\* Encrypt your connection if database is on a separate server

\* Database Migrations

\* Databases don't move the same way code does, they only like going forward.

\* Have some way to handle database changes going from dev to production.

\* Enforce Constraints

\* "Normalize until it hurts, denormalize until it works"

\* Handle user uploads and data separately from code.

\* Auth

\* Avoid rolling your own

\* Hash your passwords

\* Let users set their own passwords

\* If you can send users their passwords you're doing it wrong

\* Sensitive Credentials and Settings

\* Should be stored in configuration/settings file or as environment variables

\* Should only stay on the production server and secure storage

\* DO NOT commit into source control

## Server and Network

\* Web Server

\* Be Careful What You Are Serving

\* Know how your config works

\* Don't put anything in Document Root that you don't intend to serve as-is.

\* TLS/SSL

\* Let's Encrypt is easy

\* Check your ports

\* Know what ports are open

\* Use a firewall if it makes things easier

\* Scan the ports if you have to

\* Nmap can be used to scan ports

\* Permissions

\* Only give your web server what it needs

\* Treat user files with suspicion

## Other

\* Dependencies

\* Document your dependencies

\* Know when to refactor and replace dependencies

\* Keep offline backups of your dependencies!

\* User Data

\* Keep data separate from code whenever possible

\* DO NOT dev with production data