Ibrokhim Mirzakhonov

Senior Project

Use Case 4

Security is one of the most important part of a system when making an application, therefore it is something that requires a lot of attention even after the application is complete.

After doing some research I came across some ways to protect the software.

* Protect your database from SQL injection
  + Most common attacks on web apps is apparently SQL Injection. Attackers insert malicious SQL into a dynamic SQL statement
* Protect from JavaScript injection
* Validate input data before storing it
  + It doesn’t matter if the client or the other system validated the data
* Test with different tools that run through paths in the code and identify when you are referencing data that has not been validated

Protecting personal data and privacy is very important. It is about access control, auditing, encryption. For web apps and mobile apps. Make sure that SSL is setup correctly. Avoid forgetting to encrypt data, trying to roll your own encryption algorithms, mishandling keys or other setup steps. HTTPS is used for secure communication over a computer network and is used on Internet. I think we need to identify our most valuable data, encrypt it and then manage the keys to protect access to the information. In our case, this can be the logins for the admins, linen requesting and anything that requires some kind of protection.