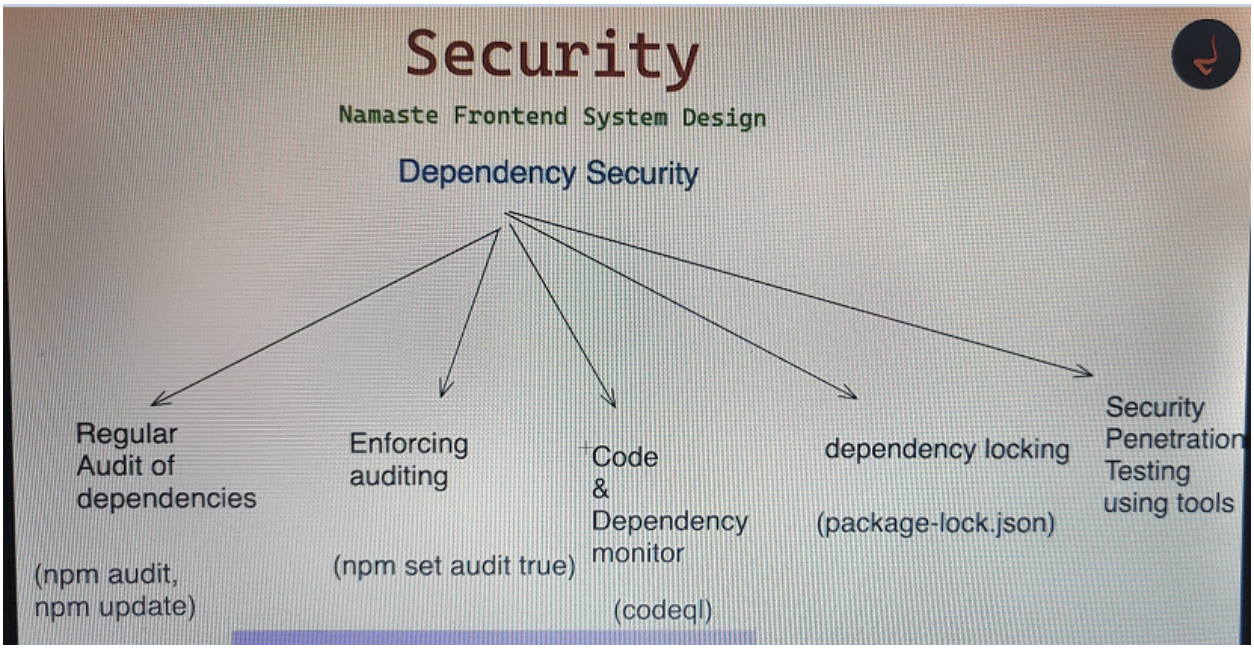
Dependency security



Regular audit of dependencies

npm audit

npm update

npm audit report - generates detailed report

Enforcing auditing

In your package itself - npm set audit true

Everytime during npm install/update it will automatically be execute and highlight vulnerabilities

Code & Dependency monitor

Sometimes in some projects we don’t run them daily but we want them to be proper with dependencies and all

In such cases, we can use

dependabot - for dependency monitoring

dependabot.yml(github) file is created and code id written to monitor dependencies in some time interval

codeql - it goes one step ahead and does code as well as dependency monitoring

codeql-analysis.yml file(github)

Dependency locking

Generally we have pipelines set up which runs when we merge a code. In such case, you want to avoid a frequent dependency errors.

Therefore we set up package-lock.json

It locks the version of direct and indirect dependencies in your project so that it is not going to change everytime you run npm install.

We update dependencies only when needed

To achieve reproducible builds, it is necessary to *lock* versions of dependencies and transitive dependencies such that a build with the same inputs will always resolve the same module versions. This is called *dependency locking*.

Security penetration testing using tools

Even if we take care of above things, still there are lot of things on which we need help from tools

https://owasp.org/www-community/Vulnerability_Scanning_Tools

App scanner, burp suite, zed attack proxy - famous tools