Security

1. Authentication vs. authorization
   1. Authentication – The process of checking validity of a user or request. To verify who you are.
      1. Username + password
   2. Authorization – To give someone the permission to do some actions. After authentication, you automatically have authorization.
      1. A role, ex: admin user
      2. A token
2. Security
   1. Data at rest
   2. Date in transit
3. Encryption
   1. Symmetric – 123 -> key -> &\*%^&% -> key -> 123
      1. For data
   2. Asymmetric – 123 -> key1 -> &\*%^&% -> key2 -> 123
      1. For signature, authentication
4. Hashing – used to verify
   1. Same text, same hex code
   2. Ex: used to save user password, and hash the user input each time to compare
   3. 123 -> md5/SHA (algorithm) -> 128 bits (hex)
5. Encoding
   1. URL encoding
      1. Convert ex the Chinese character into a format that can be transmitted over the internet
      2. 123a-z中文 -> 123a-z
   2. File encoding
      1. Binary -> characters
      2. Ex: Base64
6. SSH (user -> Linux)
   1. Server (has public key of a user) <- SSH (private)
      1. Server encrypt with public key “hello”
      2. SSH decrypt with private key
      3. Server verify your role
7. API (?) – we protect the server

GET /api/user

GET /api/user?pageNo=100

POST /api/user {username, password, tel…}

PUT

DELETE

POST /api/login {username;passname} -> token

* 1. Validate input controller – ex: SQL injection (drop user, truncate admin, or 1==1 -- ; , () potential special characters to hack), XSS attack
  2. HTTP + Security (TLS > SSL)
     1. TLS handshakes
  3. Token -> JWT (Jason Web Token)

1. Oauth2
   1. Flow
2. CORS (cross origin resource sharing) \*\* RESTful + SPA(angular react)
3. SSO (Single Sign On) -> login once, login everything
4. LDAP, Active Directory (AD) -> Directory DB.