Session 3 Task

1. What Hashing Passwords?

   Hashing is the foundation of secure password storage, Password hashing is defined as putting a password through a hashing algorithm to turn password into an unintelligible series of numbers and letters. This is important for security because, in the event of a security breach, any compromised hashed passwords are unintelligible to the bad actor. As a result, the theft of this information is considerably more difficult.

2. How Salt can improve Hashing?

   In order to add an additional layer of security, randomness needs to be added to the original plaintext value before hashing so that it will not generate the same hashed value each time (to ignore collision), Randomizing these hashes by appending or prepending a random string, known as a salt.

3. What is SSL?

   An acronym of Secure Sockets Layer, SSL is a type of digital certificate that you can install on your server to enable a secure, encrypted connection for users accessing your website or application, SSL encrypts data that is transmitted across the web, SSL make handshake process between two communicating devices to ensure that both devices are really who they claim to be. So data on the Web when transmitted not can anyone read it.