Venus, Kristofersen Marley A. BIT43

1.) What is SSL?

SSL (Secure Sockets Layer) is a cryptographic protocol designed to provide secure communication over a computer network. It was originally developed to ensure the privacy and integrity of data exchanged between web browsers and servers. SSL uses encryption to protect sensitive information, such as credit card details and login credentials, from being intercepted by unauthorized parties. When SSL is used, websites display a padlock icon in the browser address bar, signaling that the connection is secure.

2.) What is the importance of SSL?

SSL (Secure Sockets Layer) is critically important because it ensures the security and privacy of data transmitted over the internet. By encrypting communication between a web server and a client (such as a web browser), SSL protects sensitive information, such as login credentials, payment details, and personal data, from being intercepted by malicious actors. Without SSL, data sent over the internet is vulnerable to eavesdropping, tampering, and theft. In addition to encryption, SSL also provides authentication, helping users verify that the website they are communicating with is legitimate and not an imposter. This is crucial for building trust, especially for e-commerce and financial transactions.

3.) How do we configure SSL?

Configuring SSL involves several key steps to ensure secure communication between a web server and clients. The process begins with obtaining an SSL certificate, which can be purchased from a trusted Certificate Authority (CA) or obtained for free from services like Let's Encrypt. To obtain the certificate, you first generate a Certificate Signing Request (CSR) on your server, which includes details about your domain and server. After submitting the CSR, the CA will validate your domain ownership and, once confirmed, issue the SSL certificate. Next, the SSL certificate needs to be installed on the web server, a process that differs based on the server software being used, such as Apache, Nginx, or IIS. This typically involves uploading the certificate files and configuring the server to use the correct paths for the certificate and private key. Additionally, you must configure the web server to handle HTTPS requests, enabling the SSL module and adjusting the server settings to securely serve traffic on port 443. To ensure all traffic is encrypted, you should set up redirects from HTTP to HTTPS. After installation and configuration, it's important to test the SSL setup using tools like SSL Labs' SSL Test, which ensures that the certificate is properly installed and configured. Finally, you should update any internal links to use HTTPS and monitor the certificate's expiration date, renewing it before it lapses to maintain security.