Web Security

1. Web Security Considerations

Web security aims to protect data transmitted over the internet and prevent malicious activities such as hacking, phishing, and data breaches.

Key considerations include:

- **Confidentiality:** Protect sensitive information from unauthorized access.
- **Integrity:** Ensure that data is not altered during transmission.
- **Authentication:** Verify the identities of users and servers.
- **Authorization:** Grant access rights based on user identity.
- **Availability:** Ensure that services are available when needed (protect against Denial of Service attacks).

Common Threats:

- **Man-in-the-Middle (MITM) Attacks**
- **Phishing and Social Engineering**
- **Cross-Site Scripting (XSS)**
- **Cross-Site Request Forgery (CSRF)**
- **SQL Injection**
- **Session Hijacking**

Security Best Practices:

- Use HTTPS instead of HTTP.
- Implement strong password policies.
- Validate and sanitize all user inputs.
- Regularly update and patch systems.
- Use firewalls, intrusion detection/prevention systems.

---

2. Secure Socket Layer (SSL)

SSL is a cryptographic protocol designed to provide secure communication over a network.

Key Features:

- **Encryption:** Encrypts the data transmitted between a user and a web server.
- **Authentication:** Uses certificates (issued by Certificate Authorities) to verify server identity.
- **Data Integrity:** Ensures that data is not tampered with during transmission.

SSL Handshake Process:

1. **Client Hello:** The client sends a hello message with SSL version, supported cipher suites, and a random number.
2. **Server Hello:** The server responds with its own random number, chosen cipher suite, and its digital certificate.

3. **Certificate Verification:** The client verifies the server's certificate.
4. **Key Exchange:** The client and server exchange keys to establish a shared secret.
5. **Session Keys:** Both parties generate session keys from the shared secret.
6. **Secure Communication:** All subsequent communication is encrypted using these keys.

Important:

- SSL 2.0 and SSL 3.0 are considered insecure and deprecated.

---

3. Transport Layer Security (TLS)

TLS is the successor to SSL. It provides better security and performance.

Key Features:

- Stronger encryption algorithms than SSL.
- Improved handshake process to prevent downgrade attacks.
- Support for Forward Secrecy (keys are not reused).
- Protection against many modern vulnerabilities.

TLS Versions:

- **TLS 1.0:** Introduced in 1999; now deprecated.
- **TLS 1.1:** Also deprecated.
- **TLS 1.2:** Widely used; strong and secure.
- **TLS 1.3:** Released in 2018; faster and even more secure (removes outdated cryptographic algorithms).

TLS Handshake (Simplified):

1. **Negotiation:** Client and server agree on TLS version and cipher suite.
2. **Authentication:** Server sends its certificate; optionally, the client does too.
3. **Key Exchange:** A shared secret is established securely.
4. **Secure Session:** Encryption keys derived and used for encrypted communication.

Differences Between SSL and TLS:

Aspect	SSL	TLS
Security	Less secure	More secure
Versioning	SSL 2.0, 3.0	TLS 1.0, 1.1, 1.2, 1.3
Speed	Slower	Faster
Usage Today	Obsolete	Actively used (TLS 1.2, 1.3)

Summary

- **Web Security** protects web applications from attacks.
- **SSL** was the original protocol for securing web communications.
- **TLS** replaced SSL and is now the standard for web security.
- Modern websites should use **TLS 1.2** or **TLS 1.3** with strong cipher suites.