Summary of CSRF, OAuth 2.0, OpenID Connect, and Session Management

CSRF (Cross-Site Request Forgery): CSRF is a type of attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. By leveraging the authenticated user's session, an attacker can make unauthorized requests without the user's knowledge. These attacks can be mitigated by using techniques such as CSRF tokens, SameSite cookies, and verifying the origin of requests.

OAuth 2.0: OAuth 2.0 is an open standard for access delegation commonly used as a way to grant websites or applications limited access to a user's information without exposing their passwords. It works through a series of steps, involving an authorization server, a resource owner, and a client. The client requests access to a resource, the user grants permission, and the client receives a token to access the resource without needing the user's credentials.

OpenID Connect: OpenID Connect is an authentication layer built on top of OAuth 2.0. It allows clients to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the user. It provides a simple identity layer that can be used by web-based applications, mobile apps, and other systems to handle user authentication securely.

Session Management: Session management refers to the practice of managing the session state between a user's device and a web application. Proper session management ensures that users remain authenticated as they navigate a web application while maintaining security against attacks like session hijacking. Common practices include the use of secure session cookies, session expiration, and regenerating session identifiers upon login to prevent attacks