Web Security Concepts

CSRF (Cross-Site Request Forgery)

CSRF is a type of attack that tricks the user into executing unwanted actions on a web application in which they are authenticated. The attacker does this by injecting malicious code or exploiting existing code to send unauthorized commands. Protection against CSRF typically involves using tokens that are associated with each session or form submission, ensuring that the request comes from a legitimate source.

OAuth 2.0

OAuth 2.0 is an authorization framework that enables third-party applications to obtain limited access to a user's resources without exposing the user's credentials. It works by using access tokens that represent the user's authorization. OAuth 2.0 supports various grant types, including Authorization Code, Implicit, Resource Owner Password Credentials, and Client Credentials. It is commonly used for providing secure access to APIs.

OpenID Connect

OpenID Connect is an authentication layer built on top of OAuth 2.0. It allows clients to verify the identity of the user based on the authentication performed by an authorization server. OpenID Connect provides user identity information in a secure, standardized manner using ID tokens. It is widely used for single sign-on (SSO) across different applications.

Session Management

Session management refers to the handling of user sessions in a web application. A session is a series of interactions between a user and a web application that take place during a time frame. Proper session management involves securely creating, maintaining, and destroying sessions. This includes the use of session IDs, secure cookies, and measures to prevent session hijacking and fixation attacks.