Session Hijacking & Session Fixation

Session Hijacking

- Session hijacking, also known as session theft, is a security attack where an attacker illegitimately takes over a user's active session on a web application.
- In this type of attack, the attacker gains unauthorized access to the user's session token or identifier, allowing them to impersonate the victim and perform actions on their behalf.
- Session hijacking is a severe security threat because it can lead to unauthorized access to user accounts, sensitive data, and potential misuse of the hijacked session.

Session Hijacking - Token Acquisition

- Session Prediction: Predicting or guessing the session token, especially if it's predictable or lacks sufficient randomness.

- Session Sniffing: Intercepting the session token as it's transmitted over an unsecured network, such as an open Wi-Fi hotspot.

- Cross-Site Scripting (XSS): Exploiting a vulnerability in the web application to inject malicious JavaScript into a victim's browser, which can steal the session token.

Session Hijacking - Impersonation

- Once the attacker has the session token, they can impersonate the victim by presenting this token during requests to the web application.

- The application, unaware of the hijacking, treats the attacker as the authenticated user.

Session Hijacking - Impact

- Data Theft: Access and steal the victim's sensitive data, such as personal information, financial details, or confidential documents.
- Account Takeover: Change the victim's account settings, passwords, or email addresses, effectively locking the victim out of their account.
- Malicious Transactions: Conduct unauthorized transactions, make purchases, or manipulate the victim's data.
- Data Manipulation: Modify or delete the victim's data or settings.

Session Fixation

- Session fixation is a web application security attack where an attacker sets or fixes a user's session identifier (session token) to a known value of the attacker's choice.

- Subsequently, the attacker tricks the victim into using this fixed session identifier to log in, thereby granting the attacker unauthorized access to the victim's session.

Session Fixation - Token Acquisition

- The attacker obtains a session token issued by the target web application. This can be done in several ways, such as:
- Predicting or guessing the session token: Some web applications generate session tokens that are easy to predict or lack sufficient randomness.
- Intercepting the session token: If the application doesn't use secure channels (e.g., HTTPS) to transmit session tokens, an attacker may intercept them as they travel over an insecure network, such as an open Wi-Fi hotspot.

Session Fixation - Impersonation

- With a session token in hand, the attacker sets or fixes the victim's session token to a known value that the attacker controls. This value could be one generated by the attacker or an existing valid session token.

- The attacker lures the victim into using the fixed session token to log in to the web application. This can be accomplished through various means:
    - Sending the victim a link that includes the fixed session token.
    - Manipulating the victim into clicking on a specially crafted URL.
    - Social engineering tactics to convince the victim to log in under specific circumstances.

Session Fixation - Hijacking

- Once the victim logs in with the fixed session token, the attacker can now hijack the victim's session.

- The web application recognizes the attacker as the legitimate user since the session token matches what is expected.

Session Hijacking Via Cookie Tampering

Demo: Session Hijacking Via Cookie Tampering