Introduction To Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF)

- Cross-Site Request Forgery (CSRF) is a type of web security vulnerability that occurs when an attacker tricks a user into performing actions on a web application without their knowledge or consent.

- This attack takes advantage of the trust that a web application has in the user's browser.

- In the context of web application penetration testing, understanding CSRF is crucial for identifying and mitigating this security risk.

CSRF Attack Methodology

- In a CSRF attack, the attacker crafts a malicious request and tricks a user into unknowingly sending that request to a vulnerable web application.

- Web applications typically trust that requests coming from a user's browser are legitimate. However, CSRF exploits this trust.

- Most web applications use cookies for user authentication. When a user logs in, they receive a session cookie that identifies them during their session. This cookie is automatically sent with every request to the application.

CSRF Attack Methodology

- The attacker crafts a malicious request (e.g., changing the user's email address or password) and embeds it in a web page, email, or some other form of content.
- The attacker lures the victim into loading this content while the victim is authenticated in the target web application.
- The victim's browser automatically sends the malicious request, including the victim's authentication cookie.
- The web application, trusting the request due to the authentication cookie, processes it, causing the victim's account to be compromised or modified.

CSRF Impact

- CSRF attacks can have serious consequences:
  - Unauthorized changes to a user's account settings.
  - Fund transfers or actions on behalf of the user without their consent.
  - Malicious actions like changing passwords, email addresses, or profile information.

Advanced Electron Forum CSRF