Cross-Site Request Forgery (CSRF)

A type of attack where a malicious user is able to trick a victim into performing actions on a website without their consent.

Victim is logged into their bank or similar account, and the session is authenticated (using cookies).

Attacker creates an impersonating or fake webpage similar to the authentic one and with malicious code as below,

<img src="http://service.com/transfer?acc=347892 & amount = 1250 & currency = INR "style = "display:none;">

Mitigation:

- Set CSRF tokens on web forms

<form------>

<input type="hidden" name = "CSRF_Token" value = "XD89746E54">

</form>

Set cookie: `Session ID: 17832; SameSite=Strict; Secure=https`

- Checking CSRF tokens from server and checking the origin or Referrer.