cross site request forgery(csrf):

cross site request forgery is also known as csrf, **one-click attack** or **session riding** ,here the attacker will tries make the victim to perform actions specified by attacker when the user is authenticated , the impact of csrf will depend on the access rights that the victim has which includes change password of victims, creating the new user accounts, the attacker can also take full control of application data and functionality if victim is privileged user

the cross site request forgery will be possible in the following cases if the application is using cookie based session handling, **unpredictable request parameters should not be there and there should be a relevant action for a request to generate forged request for example password update page,new user creation pages etc.**

A csrf attack works because session cookie, IP address, etc associated with the website will be automatically include in browsers request.so if user is authenticated the browser can not distinguish between the forged and legitimate request. csrf is serious vulnerability even though it is not included in owasp top 10.

the best mitigation for csrf token is using the csrf token which has to be validated in every request and also implementing the same site cookie.