Cross Site Request Forgery(CSRF):

cross-site request forgery is also known as csrf,**one-click attack** or **session riding**, here the attacker will try to send the forged request and makes the victim to submit the request on behalf of him the csrf will be possible if the user is logged in the same browser where he is submitting the request. 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 the victim is a 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 the forged request, for example, password update page, new user creation pages, etc.in general, the cookies related to the particular web site will be included in the request of browser from other domain if a user is authenticated because the browser can not distinguish between the forged and legitimate request so csrf is possible and it 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.