**Cross Site Request Forgery**

**Description 1**

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application. [1]

**Description 2**

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. Unlike cross-site scripting (XSS), which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser. [2]

**Description 3**

cross-site request forgery is an attack vector that enables an attacker to send arbitrary HTTP requests from a victim user. The typical scenario involves a victim that has an established level of privilege with the target site, and this allows an attacker to initiate unauthorized actions. ( sample application and example exploit can be found in [3] )

**REFERENCES:**

**[1]** [**https://www.owasp.org/index.php/Cross-Site\_Request\_Forgery\_(CSRF)**](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))

**[2]** [**https://en.wikipedia.org/wiki/Cross-site\_request\_forgery**](https://en.wikipedia.org/wiki/Cross-site_request_forgery)

**[3]** [**http://shiflett.org/articles/cross-site-request-forgeries**](http://shiflett.org/articles/cross-site-request-forgeries)