Creating a CSRF attack

CSRF stands for cross-site request forgery, and refers to the scenario where a request is constructed for users to unknowingly carry out. Users are typically tricked into clicking on a malicious link, which then performs some unwanted action on their computer, like transferring money or changing passwords.

Prerequisites for CSRF attacks

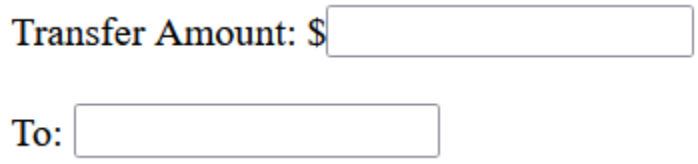
CSRF attacks can only happen when certain conditions are met in the underlying website or application which is targeted. Typically, this means that the website or form does not use CSRF tokens, which are random sequences of characters given to the user by the web server and used to confirm that the person who sent the request is the user.

An example

Let's say there's an insecure website www.bank.com with a funds transfer form at www.bank.com/transfer. The form sends a GET request to a web server.

Bob wants to make Alice transfer $200 to him by clicking on a link while she's logged in. What might that look like?

The form looks something like:



The request sends 2 pieces of information:

1. How much to transfer
2. Who to transfer to

In the URL, those pieces of information are sent as parameters, which look like transfer=200 or to=Bob. Then, Bob might trick Alice into clicking on a link like www.example.com/login/?transfer=200&to=Bob

Resources

https://owasp.org/www-community/attacks/csrf
https://brightsec.com/blog/cross-site-request-forgery-csrf/