What is CSRF?

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.

[www.xyzbank.com](http://www.xyzbank.com)

[www.xyzbank.com/b\_acno=”accountno”+amt=”amount\_in\_rs”token=”541658765498654546546454545465465454654654](http://www.xyzbank.com/b_acno=”accountno”+amt=”amount_in_rs”token=”541658765498654546546454545465465454654654)”

abc movie

qwertymovies.com

[www.xyzbank.com/b\_acno=”123456789”+amt=”10000](http://www.xyzbank.com/b_acno=”123456789”+amt=”10000)”

Cross-Site Request Forgery (CSRF) in simple words

* Assume you are currently logged into your online banking at [www.mybank.com](http://www.mybank.com)
* Assume a money transfer from mybank.com will result in a request of (conceptually) the form http://www.mybank.com/transfer?to=<SomeAccountnumber>;amount=<SomeAmount>. (Your account number is not needed, because it is implied by your login.)
* You visit www.random.org, not knowing that it is a malicious site.
* If the owner of that site knows the form of the above request (easy!) and correctly guesses you are logged into mybank.com (requires some luck!), they could include on their page a request like http://www.mybank.com/transfer?to=123456;amount=10000 (where 123456 is the number of their xyz and 10000 is an amount that you previously thought you were *glad* to possess).
* *You* retrieved that www.random.org page, so *your* browser will make that request.
* Your bank cannot recognize this origin of the request: Your web browser will send the request along with your www.mybank.com cookie and it will look perfectly legitimate. There goes your money!

This is the world **without CSRF tokens**.

Now for the better one ***with* CSRF tokens**:

* The transfer request is extended with a third argument: http://www.mybank.com/transfer?to=123456;amount=10000;token=31415926535897932384626433832795028841971.
* That token is a huge, impossible-to-guess random number that mybank.com will include on their own web page when they serve it to you. It is *different* each time they serve any page to anybody.
* The attacker is not able to guess the token, is not able to convince your web browser to surrender it (if the browser works correctly...), and so the attacker will *not* be able to create a valid request, because requests with the wrong token (or no token) will be refused by www.mybank.com.