A8 – Cross-Site Request Forgery (CSRF)

- **Velmi jednoduchým příkladem může být ukázka GET CSRF v DVWA:**
- http://localhost/dvwa/ admin / password
- CSRF
- zadejte nové heslo (v polích "New password:" a "Confirm new password:")
- Change
- všimněte si, že se změnila URL adresa na http://localhost/dvwa/vulnerabilities/csrf/?password_new=heslo&password_conf=heslo&Change=Change#
- Když útočník ví, jakou podobu taková URL má, muže se pokusit vám podvrhnout požadavek na změnu hesla. Například vám pošle e-mailovou zprávu s odkazem, který bude obsahovat zcela jiné heslo: http://localhost/dvwa/vulnerabilities/csrf/?password_new=utocnikovoheslo&password_conf=utocnikovoheslo&Change=Change
- Ale v e-mailové zprávě si něco takového může oběť všimnout. Proto útočník svůj útok zamaskuje a požádá vás, abyste kliknuli na jinou adresu, např. https://www.silenceplease.cz/soutez.php ve které je schován kód *<img src="http://localhost/dvwa/vulnerabilities/csrf/?password_new=utocnikovoheslo&password_conf=utocnikovoheslo&Change=Change" width="0" height="0" border="0">*
- Když se odhlásíte a pokusíte se znovu přihlásit, zjistíte, že původní heslo nemůžete použít.
- Můžete použít útočníkovo heslo.
- V tomto případě se jednalo o podvržení GET požadavku. Byť je to o trošičku složitější, lze podvrhnou také POST požadavky.