Cross Site request Forgery

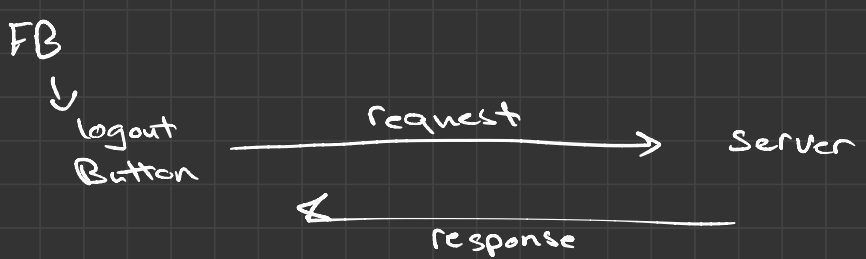
It can be anywhere

* CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.

* CSRF can be just a GET or POST Based but not header Based and not cookie Based, because cookie based does not have access of cookie.

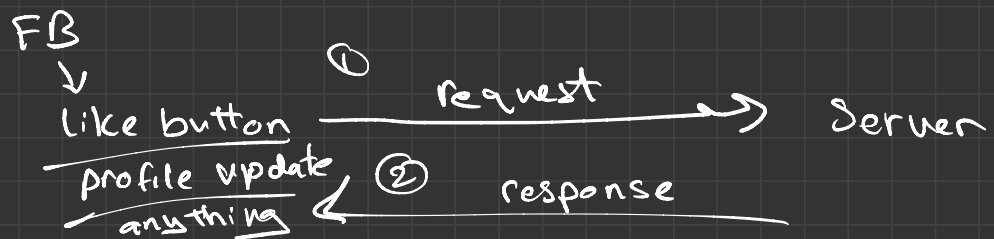
* CSRF through login or anything just do following:
  - login into a page & intercept it before login.
  - burpsuit intercept the request -> Click right -> Engagement tools -> Generate CSRF Poc -> Copy it and save it as a .html, send it to anyone and it will login automatically.

CSRF



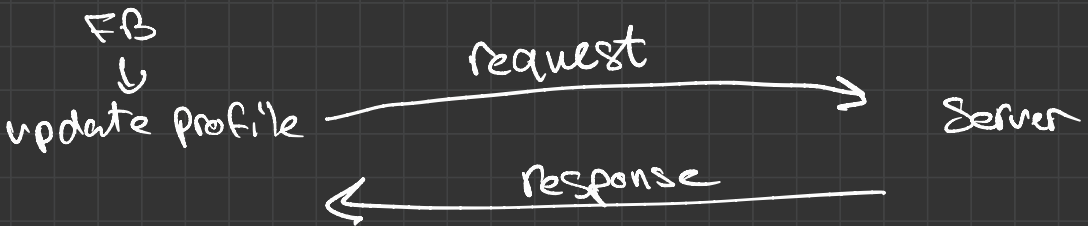
Attacker will capture the request an convert it to an HTML form. Send it to another user and PC will perform the request. Server will interact with the request and user will be loged out.

another example :



a hacker will capture the request and do like above
< the user must be authenticated. >

another example



Attacker will capture request and convert it to html and edit informations. like put fake email. Now account has my email and I can login with it.
forget password will send email to my fake email.

you can try it on any request sent to server.

Steps:

① go to any website
② update your profile or anything.
③ intercept the request & edit infos
④ change the request to an HTML and save it as .html
⑤ upload it to any server and send it to any victim.

* CSRF - Same Site bypass

lab OWASP S.K.F

Same site attribute used to defense in depth mechanism against CSRF type of attack. And it has 3 values.

Strict: cookie will be only sent with same site requests (for secure)
Lax: cookie will be sent with same site requests and, also with CSRF generated after top level navigation that are not prone to CSRF.
None: Cookie will always be sent with cross site request

→ Lax Mode also block cross site post request

Notes: if Same-Site will be set as a lax, GET query string parameter you can use.