CSRF

Saturday, February 8, 2020 10:34 PM

CONDITIONS

1.The parameter whose value is not predefined or user pre register details . ex=>password change =no (existing password required)
mail change=yes(only new mail required)

2.No CSRF tokens.

3.work in "cookie based" session hendling.

Bypassing of CSRF tokens

1.Change the request method. many application do not impose security on Get parameter.

2.Remove the csrf parameter and try to execute it.

3.Obtain a new csrf token using another account and use it. many times application does not check weather a token is associated with account or not.

4.If csrf has its own cookie then test it. Copy both csrf cookie and csrf token and insert in request and check. Many times csrf cookie and csrf token are checked but they did not check the if session cookie is associate or not.

5.Before directly appling payload just check the manual result of the request. many times csrf cookie value and csrf parameter value are same so you only need to set both values same and in same format.

REFERER BASED ATTACKS

1.Many times it check the refere hadder and if no referer is given then it just allow the request but referer hadder must not be empty.so for this we use to bypass it.

"<meta name="referrer" content="never">"

2.many times referer works fine so to bypass it use burp payload and use this "**history.pushState("", "", "/?$original-domain")** "
To bypass it.