- Cyber360
- CSRF (Cross Site Request Forgery)
  - whoami
    - HasanRhani
  - What is CSRF ?
    - CSRF used the browser default functionality of cookie where the attacker tricked the web application and the authentication user to carry out an unintended attack.
      - Means One domain is making/forgerying request to another domain in order to modify values.
  - Conditions
    - Relevant Action
      - An Action feature in the web application that attacker can do something like email change function.
    - Cookie Based Session
      - The web application should used cookie sessions for tracking sessions not any defence mechanism.
    - No unpredictable parameters
      - An Action feature which doesn't contain any unpredictable parameters which attacker can guess.
  - Blackbox
    - reviews the function of the application.
    - Condition should be there
    - Create POC
      - GET Request Mostly used <img> , <svg src , source>
      - POST request used iframe.
    - Tricks
      - Remove the CSRF token and see the web application accept it or not.
      - Change the HTTP requeste from GET to POST
      - Change the CSRF Token Value.
        - Check the CSRF token is blind to current user sessions By exchange the CSRF token value from another user.
      - CSRF Token and CSRF key
        - Check if CSRF token is blind to the CSRF key
        - Submit an invalid CSRF token And see if its accept
        - Submit an valid CSRF token from another user and see if it accept
        - Submit an valid CSRF token and Cookie (CSRF key) From another user
      - remove referrer header tags
        - <meta name="referrer" content="no-referrer">
  - Defense Against CSRF
    - CSRF Token
      - A CSRF Token is random generated value by server which is shared with client when the client attempt some relevant actions. The token is valid till the user is active.
        - unpredictable session token
        - blind with session cookie so that attacker can't use its own cookie
        - Validate the User before relevants actions.
    - Same Site
      - Its a browser feature which check cookie are present there when request comes from another domain
        - Types
          - NONE
            - NONE will allows another domain websites.
          - LAX
            - Its will allow another domain website request when the request is from TOP Level Navigation (Manually Clicked by User) and has to be GET Request.
          - Strict
            - It will allow when the request is from current domain.
    - Referrer Header
      - Check and allow current domain request and check for the cookie if not then its include cookie.
  - Break the defense
    - CSRF Token
      - Remove the token and check if the application accept it
      - change the request from POST to GET
      - Check if the token is blinded with user
      - Check if the token is blinded with the CSRF key
        - Submit an invalid token.
        - Submit an valid token of another user.
  - THANK YOU :)