Same Origin policy (SOP)

Ebrahim Elhegazy

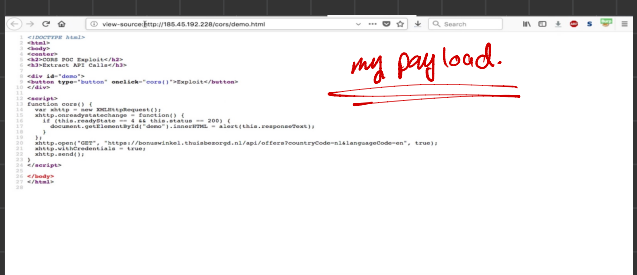
* X sit can't get request from y site because of SOP but if x site has completed 3 conditions
  1. Same protocol http or https etc.
  2. Same domain name
  3. Same port -> http:80 , https:443

-> if the three conditions are not Seccussfully completed, it will show us an error called: cross origin request blocked. and the site will not be able to read the response.

* but Cross Origin Resource Sharing (CORS) is a response header that allow cross origin request: Access-Control-Allow-Origin: * -> allow all requests.
  Access-Control-Allow-Credentials: true

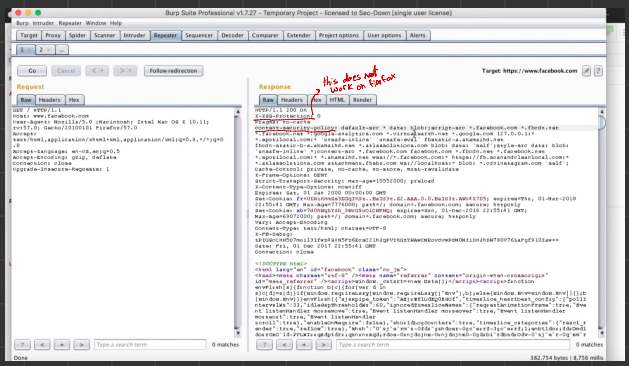
* How to hunt:
  -> in request header add Origin: any.com
  -> if you get a response header contains Access-Control-Allow-Origin: any.com &
  Access-Control-Allow-Credentials: true

  then the site is vulnerable.



Content security policy (CSP)

* If is header that gives permition to who can execute javascript code on my website.



* How to hunt.

same as CORS. try also ayklam.targetdomain.com

it may works sometimes.