Insecure CORS configuration

Background Concept about Insecure CORS Configuration

- In simple words, Imaging the microsoft.com wants to access some data on another website, suppose site.com. This type of request traditionally wouldn't be allowed under the browser's Same Origin Policy. However, by supporting CORS requests, site.com can add a few special response headers that allows example.com to access the data.

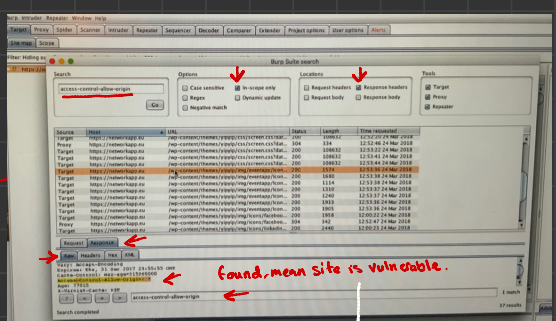
Server Response Header Concept

- Access-Control-Allow-Origin: http://www.evil.com
  Access-Control-Allow-Origin: http://www.evil.com
- Access-Control-Allow-Origin: * } vulnerable
  Access-Control-Allow-Origin: * } not vulnerable
- Request Blocked

Insecure CORS by Checking Response Header

- Look for Access-Control-Allow-Origin: http://any.com
- Or Look for Access-Control-Allow-Origin: *

* How to hunt
- spider the target website
- burp -> search -> following



ther is insecure CORS
So send link to repeater and see result.

Insecure CORS through Request Header

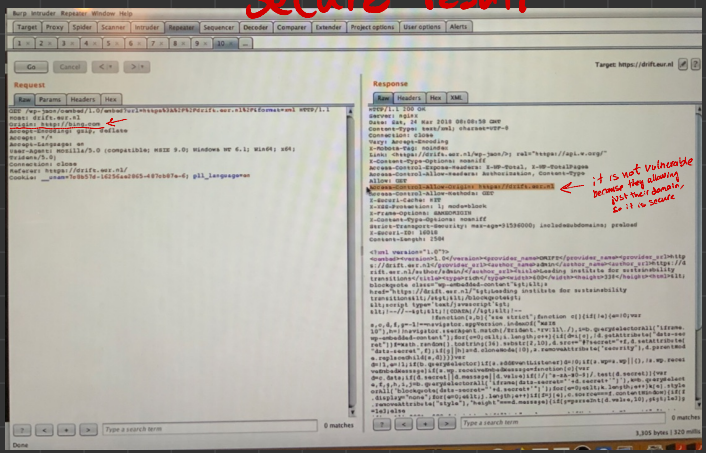
You can use burpsuite to check if the website has CORS enabled or not. You can simply add new header in request body i.e Origin: http://evil.com | null |

If you find Access-control-allow-origin: evil.com| * |null

Then domain is vulnerable

+ Spider the website
+ Search for embed? in url (not necessary)
+ do this

Secure result



* three condition for exploit

0

Exploitation of Insecure CORS

- POORLY IMPLEMENTED, BEST CASE FOR ATTACK:

  Access-Control-Allow-Origin: https://attacker.com

  Access-Control-Allow-Credentials: true

2

Exploitation of Insecure CORS

- POORLY IMPLEMENTED, EXPLOITABLE:

  Access-Control-Allow-Origin: null

  Access-Control-Allow-Credentials: true

3

Exploitation of Insecure CORS

- POORLY IMPLEMENTED, EXPLOITABLE:

  Access-Control-Allow-Origin: *

  Access-Control-Allow-Credentials: true

X if you see something like forbidden, deny, request block it means the site is secure.

*

Another way to check Insecure CORS Vulnerability

- curl http://any.com -H “Origin: http://hackersera.com” -I

* use the html code to exploit.