Offensive Approach to Hunt Bugs

Insecure CORS

Background Concept about Insecure CORS Configuration

- Wikipedia defines Cross-origin resource sharing (CORS) as « a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. ». So, CORS came essentially to eliminate some restrictions imposed by the Same-origin policy which would block a AJAX requests from accessing data on a web page unless it is coming from the same origin.

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: *

  Access-Control-Allow-Origin: *
- Request Blocked