Offensive Approach to Hunt Bugs

Insecure CORS through Request Header

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

Targets

- hackersera.in
- www.invisionapp.com
- drift.eur.nl

Server May Respond with

- 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