Offensive Approach to Hunt Bugs

Exploitation of Insecure CORS

Exploitation of Insecure CORS

- POORLY IMPLEMENTED, BEST CASE FOR ATTACK:

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

  Access-Control-Allow-Credentials: true

Exploitation of Insecure CORS

- POORLY IMPLEMENTED, EXPLOITABLE:

  Access-Control-Allow-Origin: null

  Access-Control-Allow-Credentials: true

Another way to check Insecure CORS Vulnerability

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

Targets

- www.invisionapp.com
- Hackersera.in
- Foundation.eccouncil.org

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