Cheatography

Cross-origin Resource Sharing (CORS) Cheat Sheet

by Frank Leitner (fleitner) via cheatography.com/148203/cs/32307/

H CORS headers

Access-Control--Allow-Origin	Instructs the browser which origin may process the response
Access-Control--Allow-Credentials	Instructs the browser whether responses to credentialed requests may be processed

Check for reflected origin

Usage

Origin: xzy.com

TODO: Explain

Check for null origin

Usage

Origin: null

TODO: Explain

Check for target as subdomain of malicious domain

Usage

Origin: target.com.malicious.com

TODO: Explain

Check for a random subdomain of target

Usage

Origin: xyz.target.com

TODO: Explain

Values for Access-Control-Allow-Origin

<domain>	Allow a single domain origin
*	Allow any domain origin Allow-Credentials is forbidden
null	Allow the null origin

Values of Access-Control-Allow-Credentials

true is the only permitted value of the header. If it is missing, the browser will prohibit processing responses for credentialed requests. This header is forbidden if the wildcard origin (*) is used.

Mitigation

TODO: List mitigation against the vulnerability

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com