CORS Report - https://juice-shop.herokuapp.com/#

Generated from juice-shop.herokuapp.com_#_cors_2025-09-09_00-42-59.html

Vulnerability Summary

[CVSS 5.3] MEDIUM - Wildcard Access-Control-Allow-Origin

[CVSS 5.3] MEDIUM - Overly permissive methods

[CVSS 5.3] MEDIUM - Sensitive headers exposed

Details

CORS Report

Findings

|| Issue / Type || Location || Param || Payload / Vector || Status || Risk || Evidence / Details ||
Mitigation | 1 || Wildcard Access-Control-Allow-Origin || - || - || - || Vulnerable || Medium || ACAO: *
(random origin http://pxcnufuh.attacker.site) || Avoid wildcard; list only trusted origins. | 2 ||
Overly permissive methods || - || - || - || Vulnerable || Medium || ACAM includes:
GET,HEAD,PUT,PATCH,POST,DELETE || Restrict Access-Control-Allow-Methods to only required methods. | 3 ||
Sensitive headers exposed || - || - || - || Vulnerable || Medium || ACAH includes: Authorization,
X-Api-Key || Do not expose Authorization or sensitive headers via Access-Control-Allow-Headers.