

CORS Configuration Report

Target: https://juice-shop.herokuapp.com | **Generated:** 2025-09-09_00-52-21

Total findings: 3 (vulnerabilities: 3) | Elapsed: 3.92s

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