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

Generated from juice-shop.herokuapp.com_cors_2025-09-09_00-15-59.html

## 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://fovhafqy.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.*