Complete Security Report

Generated from index_full.html

Complete Security Report

Executive Summary

Automated scan completed. Review module reports for details.

• Prioritize remediation of High and Medium risk findings.
• Implement input validation, output encoding, and least privilege.
• Broken Access
• Csrf
• Sqli
• Xss
• Cors
• Ssl Tls

Broken Access

Broken Access Control Report

Findings

|| Issue / Type || Location || Param || Payload / Vector || Status || Risk || Evidence / Details || Mitigation | 1 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/admin || - || - || Vulnerable || High || - || General best practices | 2 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/admin/login || - || - || Vulnerable || High || - || General best practices | 3 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/admin/panel || - || - || Vulnerable || High || - || General best practices | 4 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/dashboard || - || - || OK || Low || - || General best practices | 5 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/config || - || - || Vulnerable || High || - || General best practices | 6 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/debug || - || - || Vulnerable || High || - || General best practices | 7 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/manage || - || - || Vulnerable || High || - || General best practices | 8 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/management || - || - || Vulnerable || High || - || General best practices | 9 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/control || - || - || OK || Low || - || General best practices | 10 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/settings || - || - || OK || Low || - || General best practices | 11 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/user/admin || - || - || Vulnerable || High || - || General best practices | 12 || Force Browsing (Quick) || https://juice-shop.herokuapp.com/users/admin || - || - || Vulnerable || High || - || General best practices | 13 || Directory Traversal (Quick) || https://juice-shop.herokuapp.com/../../etc/passwd || - || /../../etc/passwd || OK || Low || - || General best practices | 14 || Directory Traversal (Quick) || https://juice-shop.herokuapp.com/..%2f..%2fetc/passwd || - || /..%2f..%2fetc/passwd || OK || Low || - || General best practices | 15 || Directory Traversal (Quick) || https://juice-shop.herokuapp.com/..%2F..%2Fwindows/win.ini || - || /..%2F..%2Fwindows/win.ini || OK || Low || - || General best practices

Csrf

CSRF Report

Findings

No findings recorded.

Sqli

SQL Injection Report

Findings

|| Issue / Type || Location || Param || Payload / Vector || Status || Risk || Evidence / Details || Mitigation | 1 || error_based || https://juice-shop.herokuapp.com?id=' || id || ' || OK || Low || - || - | 2 || error_based || https://juice-shop.herokuapp.com?id=" || id || " || OK || Low || - || - | 3 || error_based || https://juice-shop.herokuapp.com?id=' OR 1=1-- || id || ' OR 1=1-- || OK || Low || - || - | 4 || error_based || https://juice-shop.herokuapp.com?id=" OR "1"="1 || id || " OR "1"="1 || OK || Low || - || - | 5 || error_based || https://juice-shop.herokuapp.com?id=' UNION SELECT null-- || id || UNION SELECT null-- || OK || Low || - || - | 6 || error_based || https://juice-shop.herokuapp.com?id=') OR ('1'='1 || id || ') OR ('1'='1 || OK || Low || - || -

Xss

XSS Report

Findings

No findings recorded.

Visited URLs

• https://juice-shop.herokuapp.com

`https://juice-shop.herokuapp.com`

• https://juice-shop.herokuapp.com/#/

`https://juice-shop.herokuapp.com/#/`

Cors

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://fduhdlxy.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.

Ssl Tls

SSL/TLS Report

Findings

|| Issue / Type || Location || Param || Payload / Vector || Status || Risk || Evidence / Details || Mitigation | 1 || Self-Signed Certificate || - || - || - || Vulnerable || High || Issuer matches subject || Use a publicly trusted CA-signed certificate (Let's Encrypt or commercial CA). | 2 || Hostname Mismatch || - || - || - || Vulnerable || High || Host juice-shop.herokuapp.com not in SAN/CN || Serve a certificate whose SAN/CN matches the requested hostname.

TLS Protocol Support

Protocol || Supported | TLSv1.0 || ■ | TLSv1.1 || ■ | TLSv1.2 || ■ | TLSv1.3 || ■

Certificate

Subject / CN || {} | Issuer || {} | Valid From || None | Valid To || None | Days Until Expiry || None | Wildcard || No | Self-Signed || Yes