Complete Security Report

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

• 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=' OR 1=1-- || id || ' OR 1=1-- || 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=' UNION SELECT null-- || id || ' UNION SELECT null-- || OK || Low || - || - | 5 || 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/#/

Ssl Tls

SSL/TLS Report

Findings

|| Issue / Type || Location || Param || Payload / Vector || Status || Risk || Evidence / Details || Mitigation | 1 || Broad Wildcard Certificate || - || - || - || OK || Low || Wildcard used with minimal SAN entries || Limit wildcard certificates; prefer SAN certificates scoped to required hosts only.

TLS Protocol Support

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

Certificate

Subject / CN || *.herokuapp.com | Issuer || Amazon RSA 2048 M02 | Valid From || Jan 31 00:00:00 2025 GMT | Valid To || Mar 1 23:59:59 2026 GMT | Days Until Expiry || 173 | Wildcard || Yes | Self-Signed || No