

Security Assessment Report - index

Security Assessment Report Comprehensive Web Application Security Analysis - index Executive Summary This report summarizes the security assessment conducted on <https://juice-shop.herokuapp.com> on 2025-09-09. The overall risk level is rated as MEDIUM, with a total of 10 vulnerabilities identified. Key findings include HIGH-risk SQL Injection vulnerabilities requiring immediate attention and MEDIUM-risk CORS vulnerabilities that should be addressed. The report provides detailed findings from each security scanner module and offers recommendations to improve the application's security posture. It is imperative to review the detailed reports for each vulnerability and implement the suggested remediations promptly. Scan Details Target URL: <https://juice-shop.herokuapp.com> Scan Date: 2025-09-09 00:59:20 Total Duration: 0.0 seconds Scanners Used: 6 modules Security Overview Overall Risk: MEDIUM 10 Total Vulnerabilities 3 Secure Components 3 Links Analyzed 0 Forms Tested Access Control SECURE Tests for unauthorized access to restricted resources and functionalities Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s No vulnerabilities detected. Security measures appear effective. View Detailed Report CSRF Protection SECURE Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 20.0s No vulnerabilities detected. Security measures appear effective. SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 20.0s Critical: 6 significant vulnerabilities found. Immediate action required. View Detailed Report XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities Vulnerabilities: 0 Links Crawled: 1 Forms Found: 0 Scan Time: 25.0s No vulnerabilities detected. Security measures appear effective. View Detailed Report Cors MEDIUM RISK cors security assessment Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0 Scan Time: 23.0s Identified 3 vulnerabilities requiring attention. View Detailed Report Ssl Tls LOW RISK ssl_tls security assessment Vulnerabilities: 1 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s Found 1 minor issue. Consider reviewing for improvements. View Detailed Report Security Recommendations Secure Database Interactions Use parameterized queries or prepared statements, implement input validation, and apply the principle of least privilege for database accounts. Regular Security Testing Schedule regular security assessments, implement automated security testing in your CI/CD pipeline, and stay updated with latest security best practices. Security Headers Implement security headers like HSTS, X-Frame-Options, X-Content-Type-Options, and Content Security Policy to enhance overall security posture. Generated by Advanced Security Scanner | Report ID: 2025-09-09_00-59-20 This automated security assessment should be complemented with manual security testing.

Security Assessment Report Comprehensive Web Application Security Analysis - index

Security Assessment Report

Comprehensive Web Application Security Analysis - index

Executive Summary This report summarizes the security assessment conducted on <https://juice-shop.herokuapp.com> on 2025-09-09. The overall risk level is rated as MEDIUM, with a total of 10 vulnerabilities identified. Key findings include HIGH-risk SQL Injection vulnerabilities requiring immediate attention and MEDIUM-risk CORS vulnerabilities that should be addressed. The report provides detailed findings from each security scanner module and offers recommendations to improve the application's security posture. It is imperative to review the detailed reports for each vulnerability and implement the suggested remediations promptly.

Executive Summary

This report summarizes the security assessment conducted on <https://juice-shop.herokuapp.com> on 2025-09-09. The overall risk level is rated as MEDIUM, with a total of 10 vulnerabilities identified. Key findings include HIGH-risk SQL Injection vulnerabilities requiring immediate attention and MEDIUM-risk CORS vulnerabilities that should be addressed. The report provides detailed findings from each security scanner module and offers recommendations to improve the application's security posture. It is imperative to review the detailed reports for each vulnerability and implement the suggested remediations promptly.

Scan Details Target URL: <https://juice-shop.herokuapp.com> Scan Date: 2025-09-09 00:59:20 Total Duration: 0.0 seconds Scanners Used: 6 modules

Scan Details

Target URL: <https://juice-shop.herokuapp.com> Scan Date: 2025-09-09 00:59:20 Total Duration: 0.0 seconds Scanners Used: 6 modules

Target URL: <https://juice-shop.herokuapp.com>

Scan Date: 2025-09-09 00:59:20

Total Duration: 0.0 seconds

Scanners Used: 6 modules

Security Overview Overall Risk: MEDIUM 10 Total Vulnerabilities 3 Secure Components 3 Links Analyzed 0 Forms Tested

Security Overview

Overall Risk: MEDIUM

Overall Risk: MEDIUM

10 Total Vulnerabilities 3 Secure Components 3 Links Analyzed 0 Forms Tested

10 Total Vulnerabilities

10

Total Vulnerabilities

3 Secure Components

3

Secure Components

3 Links Analyzed

3

Links Analyzed

0 Forms Tested

0

Forms Tested

Access Control SECURE Tests for unauthorized access to restricted resources and functionalities Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s No vulnerabilities detected. Security measures appear effective. View Detailed Report CSRF Protection SECURE Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 20.0s No vulnerabilities detected. Security measures appear effective. SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6 Links

Crawled: 1 Forms Found: 0 Scan Time: 20.0s Critical: 6 significant vulnerabilities found. Immediate action required. View Detailed Report XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities Vulnerabilities: 0 Links Crawled: 1 Forms Found: 0 Scan Time: 25.0s No vulnerabilities detected. Security measures appear effective. View Detailed Report Cors MEDIUM RISK cors security assessment Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0 Scan Time: 23.0s Identified 3 vulnerabilities requiring attention. View Detailed Report Ssl Tls LOW RISK ssl_tls security assessment Vulnerabilities: 1 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s Found 1 minor issue. Consider reviewing for improvements. View Detailed Report

Access Control SECURE Tests for unauthorized access to restricted resources and functionalities Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s No vulnerabilities detected. Security measures appear effective. View Detailed Report

Access Control SECURE Tests for unauthorized access to restricted resources and functionalities Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s

Access Control SECURE

Tests for unauthorized access to restricted resources and functionalities

Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s

Vulnerabilities: 0

Links Crawled: 0

Forms Found: 0

Scan Time: 0.0s

No vulnerabilities detected. Security measures appear effective. View Detailed Report

No vulnerabilities detected. Security measures appear effective.

View Detailed Report

CSRF Protection SECURE Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 20.0s No vulnerabilities detected. Security measures appear effective.

CSRF Protection SECURE Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 20.0s

CSRF Protection SECURE

Validates Cross-Site Request Forgery prevention mechanisms

Vulnerabilities: 0 Links Crawled: 0 Forms Found: 0 Scan Time: 20.0s

Vulnerabilities: 0

Links Crawled: 0

Forms Found: 0

Scan Time: 20.0s

No vulnerabilities detected. Security measures appear effective.

No vulnerabilities detected. Security measures appear effective.

SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 20.0s Critical: 6 significant vulnerabilities found. Immediate action required. View Detailed Report

SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 20.0s

SQL Injection HIGH RISK

Examines database security against injection attacks

Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 20.0s

Vulnerabilities: 6

Links Crawled: 1

Forms Found: 0

Scan Time: 20.0s

Critical: 6 significant vulnerabilities found. Immediate action required. [View Detailed Report](#)

Critical: 6 significant vulnerabilities found. Immediate action required.

[View Detailed Report](#)

XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities

Vulnerabilities: 0 Links Crawled: 1 Forms Found: 0 Scan Time: 25.0s No vulnerabilities detected.

Security measures appear effective. [View Detailed Report](#)

XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities

Vulnerabilities: 0 Links Crawled: 1 Forms Found: 0 Scan Time: 25.0s

XSS Prevention SECURE

Tests protection against Cross-Site Scripting vulnerabilities

Vulnerabilities: 0 Links Crawled: 1 Forms Found: 0 Scan Time: 25.0s

Vulnerabilities: 0

Links Crawled: 1

Forms Found: 0

Scan Time: 25.0s

No vulnerabilities detected. Security measures appear effective. [View Detailed Report](#)

No vulnerabilities detected. Security measures appear effective.

[View Detailed Report](#)

Cors MEDIUM RISK cors security assessment Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0
Scan Time: 23.0s Identified 3 vulnerabilities requiring attention. [View Detailed Report](#)

Cors MEDIUM RISK cors security assessment Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0
Scan Time: 23.0s

Cors MEDIUM RISK

cors security assessment

Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0 Scan Time: 23.0s

Vulnerabilities: 3

Links Crawled: 1

Forms Found: 0

Scan Time: 23.0s

Identified 3 vulnerabilities requiring attention. [View Detailed Report](#)

Identified 3 vulnerabilities requiring attention.

[View Detailed Report](#)

Ssl Tls LOW RISK ssl_tls security assessment Vulnerabilities: 1 Links Crawled: 0 Forms Found: 0
Scan Time: 0.0s Found 1 minor issue. Consider reviewing for improvements. [View Detailed Report](#)

Ssl Tls LOW RISK ssl_tls security assessment Vulnerabilities: 1 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s

Ssl Tls LOW RISK

ssl_tls security assessment

Vulnerabilities: 1 Links Crawled: 0 Forms Found: 0 Scan Time: 0.0s

Vulnerabilities: 1

Links Crawled: 0

Forms Found: 0

Scan Time: 0.0s

Found 1 minor issue. Consider reviewing for improvements. [View Detailed Report](#)

Found 1 minor issue. Consider reviewing for improvements.

[View Detailed Report](#)

Security Recommendations Secure Database Interactions Use parameterized queries or prepared statements, implement input validation, and apply the principle of least privilege for database accounts. Regular Security Testing Schedule regular security assessments, implement automated security testing in your CI/CD pipeline, and stay updated with latest security best practices. Security Headers Implement security headers like HSTS, X-Frame-Options, X-Content-Type-Options, and Content Security Policy to enhance overall security posture.

Security Recommendations

Secure Database Interactions Use parameterized queries or prepared statements, implement input validation, and apply the principle of least privilege for database accounts.

Secure Database Interactions

Use parameterized queries or prepared statements, implement input validation, and apply the principle of least privilege for database accounts.

Regular Security Testing Schedule regular security assessments, implement automated security testing in your CI/CD pipeline, and stay updated with latest security best practices.

Regular Security Testing

Schedule regular security assessments, implement automated security testing in your CI/CD pipeline, and stay updated with latest security best practices.

Security Headers Implement security headers like HSTS, X-Frame-Options, X-Content-Type-Options, and Content Security Policy to enhance overall security posture.

Security Headers

Implement security headers like HSTS, X-Frame-Options, X-Content-Type-Options, and Content Security Policy to enhance overall security posture.

Generated by Advanced Security Scanner | Report ID: 2025-09-09_00-59-20 This automated security assessment should be complemented with manual security testing.

Generated by Advanced Security Scanner | Report ID: 2025-09-09_00-59-20

This automated security assessment should be complemented with manual security testing.

