Security Assessment Report - index

Security Assessment Report - index Comprehensive Web Application Security Analysis Executive Summary This report summarizes the security assessment conducted on https://juice-shop.herokuapp.com/# on 2025-09-08. The overall risk level is rated as MEDIUM. Key findings include multiple SQL Injection vulnerabilities requiring immediate attention, several CORS issues, and one instance of a potential CSRF vulnerability. The application demonstrated adequate XSS and Access Control protections. Recommendations are provided to address identified vulnerabilities and improve the application's security posture. Scan Details Target URL: https://juice-shop.herokuapp.com/# Scan Date: 2025-09-08 00:15:10 Total Duration: 0.0 seconds Scanners Used: 5 modules Security Overview Overall Risk: MEDIUM 10 Total Vulnerabilities 2 Secure Components 5 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 LOW RISK Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 22.0s Found 1 minor issue. Consider reviewing for improvements. View Detailed Report SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 24.0s 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: 2 Forms Found: 0 Scan Time: 41.0s 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: 29.0s Identified 3 vulnerabilities requiring attention. View Detailed Report Security Recommendations Implement CSRF Protection Add CSRF tokens to all state-changing operations, implement SameSite cookie attributes, and validate origin headers. 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: 2025-09-08_00-15-10 This automated security assessment should be complemented with manual security testing.

Security Assessment Report - index Comprehensive Web Application Security Analysis

Security Assessment Report - index

Comprehensive Web Application Security Analysis

Executive Summary This report summarizes the security assessment conducted on https://juice-shop.herokuapp.com/# on 2025-09-08. The overall risk level is rated as MEDIUM. Key findings include multiple SQL Injection vulnerabilities requiring immediate attention, several CORS issues, and one instance of a potential CSRF vulnerability. The application demonstrated adequate XSS and Access Control protections. Recommendations are provided to address identified vulnerabilities and improve the application's security posture.

Executive Summary

This report summarizes the security assessment conducted on https://juice-shop.herokuapp.com/# on 2025-09-08. The overall risk level is rated as MEDIUM. Key findings include multiple SQL Injection vulnerabilities requiring immediate attention, several CORS issues, and one instance of a potential CSRF vulnerability. The application demonstrated adequate XSS and Access Control protections. Recommendations are provided to address identified vulnerabilities and improve the application's security posture.

Scan Details Target URL: https://juice-shop.herokuapp.com/# Scan Date: 2025-09-08 00:15:10 Total Duration: 0.0 seconds Scanners Used: 5 modules

Scan Details

Target URL: https://juice-shop.herokuapp.com/# Scan Date: 2025-09-08 00:15:10 Total Duration: 0.0 seconds Scanners Used: 5 modules

Target URL: https://juice-shop.herokuapp.com/#

Scan Date: 2025-09-08 00:15:10

Total Duration: 0.0 seconds

Scanners Used: 5 modules

Security Overview Overall Risk: MEDIUM 10 Total Vulnerabilities 2 Secure Components 5 Links Analyzed 0 Forms Tested

Security Overview

Overall Risk: MEDIUM

Overall Risk: MEDIUM

10 Total Vulnerabilities 2 Secure Components 5 Links Analyzed 0 Forms Tested

10 Total Vulnerabilities

10

Total Vulnerabilities

2 Secure Components

2

Secure Components

5 Links Analyzed

5

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 LOW RISK Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 22.0s Found 1 minor issue. Consider reviewing for improvements. View Detailed Report SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 24.0s 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: 2 Forms Found: 0 Scan Time: 41.0s 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: 29.0s Identified 3 vulnerabilities requiring attention. 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 LOW RISK Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 22.0s Found 1 minor issue. Consider reviewing for improvements. View Detailed Report

CSRF Protection LOW RISK Validates Cross-Site Request Forgery prevention mechanisms Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 22.0s

CSRF Protection LOW RISK

Validates Cross-Site Request Forgery prevention mechanisms

Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 22.0s

Vulnerabilities: 1

Links Crawled: 1

Forms Found: 0

Scan Time: 22.0s

Found 1 minor issue. Consider reviewing for improvements. View Detailed Report

Found 1 minor issue. Consider reviewing for improvements.

View Detailed Report

SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 24.0s 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: 24.0s

SQL Injection HIGH RISK

Examines database security against injection attacks

Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 24.0s

Vulnerabilities: 6

Links Crawled: 1

Forms Found: 0

Scan Time: 24.0s

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: 2 Forms Found: 0 Scan Time: 41.0s No vulnerabilities detected. Security measures appear effective. View Detailed Report

XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities Vulnerabilities: 0 Links Crawled: 2 Forms Found: 0 Scan Time: 41.0s

XSS Prevention SECURE

Tests protection against Cross-Site Scripting vulnerabilities

Vulnerabilities: 0 Links Crawled: 2 Forms Found: 0 Scan Time: 41.0s

Vulnerabilities: 0

Links Crawled: 2

Forms Found: 0

Scan Time: 41.0s

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: 29.0s Identified 3 vulnerabilities requiring attention. View Detailed Report

Cors MEDIUM RISK cors security assessment Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0 Scan Time: 29.0s

Cors MEDIUM RISK

cors security assessment

Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0 Scan Time: 29.0s

Vulnerabilities: 3

Links Crawled: 1

Forms Found: 0

Scan Time: 29.0s

Identified 3 vulnerabilities requiring attention. View Detailed Report

Identified 3 vulnerabilities requiring attention.

View Detailed Report

Security Recommendations Implement CSRF Protection Add CSRF tokens to all state-changing operations, implement SameSite cookie attributes, and validate origin headers. 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

Implement CSRF Protection Add CSRF tokens to all state-changing operations, implement SameSite cookie attributes, and validate origin headers.

Implement CSRF Protection

Add CSRF tokens to all state-changing operations, implement SameSite cookie attributes, and validate origin headers.

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: 2025-09-08_00-15-10 This automated security assessment should be complemented with manual security testing.

Generated by Advanced Security Scanner | Report ID: 2025-09-08_00-15-10

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