

# Security Assessment Report - index

Security Assessment Report Comprehensive Web Application Security Analysis for index

## Security Assessment Report

Comprehensive Web Application Security Analysis for index

**Executive Summary** This report summarizes the security assessment of the target application. The scan identified a MEDIUM overall risk level, with a total of 11 vulnerabilities detected. Key findings include HIGH-risk SQL Injection vulnerabilities and MEDIUM-risk CORS issues. Immediate attention is recommended to address these critical vulnerabilities and improve the application's overall security posture. The report also provides actionable recommendations for remediation.

### Executive Summary

This report summarizes the security assessment of the target application. The scan identified a MEDIUM overall risk level, with a total of 11 vulnerabilities detected. Key findings include HIGH-risk SQL Injection vulnerabilities and MEDIUM-risk CORS issues. Immediate attention is recommended to address these critical vulnerabilities and improve the application's overall security posture. The report also provides actionable recommendations for remediation.

Scan Details Target URL: <https://juice-shop.herokuapp.com/#> Scan Date: 2025-09-08 00:21:14  
Total Duration: 0.0 seconds Scanners Used: 6 modules

### Scan Details

Target URL: <https://juice-shop.herokuapp.com/#> Scan Date: 2025-09-08 00:21:14 Total Duration: 0.0 seconds Scanners Used: 6 modules

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

Scan Date: 2025-09-08 00:21:14

Total Duration: 0.0 seconds

Scanners Used: 6 modules

Security Overview Overall Risk: MEDIUM 11 Total Vulnerabilities 2 Secure Components 5 Links Analyzed 0 Forms Tested

### Security Overview

Overall Risk: MEDIUM

Overall Risk: MEDIUM

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

11 Total Vulnerabilities

11

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. CSRF Protection LOW RISK Validates Cross-Site Request  
Forgery prevention mechanisms Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time:  
31.0s Found 1 minor issue. Consider reviewing for improvements. SQL Injection HIGH RISK  
Examines database security against injection attacks Vulnerabilities: 6 Links Crawled: 1 Forms  
Found: 0 Scan Time: 35.0s Critical: 6 significant vulnerabilities found. Immediate action required.  
XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities  
Vulnerabilities: 0 Links Crawled: 2 Forms Found: 0 Scan Time: 27.0s No vulnerabilities detected.  
Security measures appear effective. Cors MEDIUM RISK cors security assessment Vulnerabilities:  
3 Links Crawled: 1 Forms Found: 0 Scan Time: 43.0s Identified 3 vulnerabilities requiring attention.  
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.

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.

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.

No vulnerabilities detected. Security measures appear effective.

CSRF Protection LOW RISK Validates Cross-Site Request Forgery prevention mechanisms  
Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 31.0s Found 1 minor issue.  
Consider reviewing for improvements.

CSRF Protection LOW RISK Validates Cross-Site Request Forgery prevention mechanisms  
Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 31.0s

CSRF Protection LOW RISK

Validates Cross-Site Request Forgery prevention mechanisms

Vulnerabilities: 1 Links Crawled: 1 Forms Found: 0 Scan Time: 31.0s

Vulnerabilities: 1

Links Crawled: 1

Forms Found: 0

Scan Time: 31.0s

Found 1 minor issue. Consider reviewing for improvements.

Found 1 minor issue. Consider reviewing for improvements.

SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6  
Links Crawled: 1 Forms Found: 0 Scan Time: 35.0s Critical: 6 significant vulnerabilities found.  
Immediate action required.

SQL Injection HIGH RISK Examines database security against injection attacks Vulnerabilities: 6  
Links Crawled: 1 Forms Found: 0 Scan Time: 35.0s

SQL Injection HIGH RISK

Examines database security against injection attacks

Vulnerabilities: 6 Links Crawled: 1 Forms Found: 0 Scan Time: 35.0s

Vulnerabilities: 6

Links Crawled: 1

Forms Found: 0

Scan Time: 35.0s

Critical: 6 significant vulnerabilities found. Immediate action required.

Critical: 6 significant vulnerabilities found. Immediate action required.

XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities  
Vulnerabilities: 0 Links Crawled: 2 Forms Found: 0 Scan Time: 27.0s No vulnerabilities detected.  
Security measures appear effective.

XSS Prevention SECURE Tests protection against Cross-Site Scripting vulnerabilities  
Vulnerabilities: 0 Links Crawled: 2 Forms Found: 0 Scan Time: 27.0s

XSS Prevention SECURE

Tests protection against Cross-Site Scripting vulnerabilities

Vulnerabilities: 0 Links Crawled: 2 Forms Found: 0 Scan Time: 27.0s

Vulnerabilities: 0

Links Crawled: 2

Forms Found: 0

Scan Time: 27.0s

No vulnerabilities detected. Security measures appear effective.

No vulnerabilities detected. Security measures appear effective.

Cors MEDIUM RISK cors security assessment Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0  
Scan Time: 43.0s Identified 3 vulnerabilities requiring attention.

Cors MEDIUM RISK cors security assessment Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0  
Scan Time: 43.0s

Cors MEDIUM RISK

cors security assessment

Vulnerabilities: 3 Links Crawled: 1 Forms Found: 0 Scan Time: 43.0s

Vulnerabilities: 3

Links Crawled: 1

Forms Found: 0

Scan Time: 43.0s

Identified 3 vulnerabilities requiring attention.

Identified 3 vulnerabilities requiring attention.

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.

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.

Found 1 minor issue. Consider reviewing for improvements.

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\_00-21-14 This automated security assessment should be complemented with manual security testing.

■ Generated by Advanced Security Scanner | Report ID: 2025-09-08\_00-21-14

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