

# VULNERABILITY ASSESSMENT AND PENETRATION TESTING REPORT

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

Report Date: September 17, 2025

Assessment Period: September 2025

## **Prepared by:**

Cybrty Security Services  
Cybersecurity Excellence Division

## **Contact Information:**

Email: [security@cybrty.com](mailto:security@cybrty.com)  
Phone: +1 (555) 123-4567  
Web: <https://cybrty.com>

# DOCUMENT CONTROL

Document Title	VAPT Report - <a href="https://juice-shop.herokuapp.com">https://juice-shop.herokuapp.com</a>
Version	1.0
Date	September 17, 2025
Prepared by	Cybrty Security Team
Reviewed by	Senior Security Analyst
Approved by	Chief Security Officer
Classification	CONFIDENTIAL
Distribution	Client Management Team

# EXECUTIVE SUMMARY

Cybrty Security Services conducted a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) engagement against <https://juice-shop.herokuapp.com> during September 2025.

**Assessment Overview:** This security assessment identified 1 security finding requiring attention across various severity levels. The evaluation encompassed automated vulnerability scanning, manual penetration testing, and security configuration reviews. **Findings Summary:** • Medium: 1 finding **Overall Risk Assessment:** • Risk Rating: Medium • Risk Score: 5.0/10.0 • Total Security Findings: 1

**Business Impact:** The identified vulnerabilities present varying levels of risk to business operations. Critical and high-severity findings could potentially lead to data breaches, service disruptions, or unauthorized system access if left unaddressed. **Strategic**

**Recommendations:** • Prioritize remediation of critical and high-severity vulnerabilities • Implement defense-in-depth security controls • Establish continuous security monitoring capabilities • Develop incident response and recovery procedures

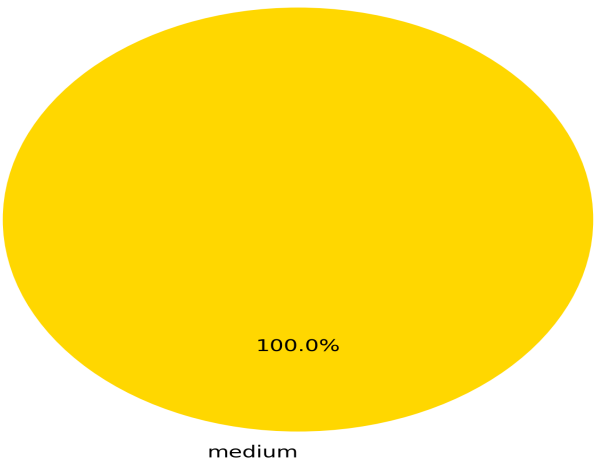
## Risk Assessment Summary

Metric	Value	Rating
Overall Risk Score	5.0/10.0	Medium
Total Findings	1	Various
Critical/High Priority	0	Immediate Action
Assessment Date	September 17, 2025	Current

# SUMMARY OF FINDINGS

## Vulnerability Distribution by Severity

Vulnerability Distribution by Severity



Severity Level	Count	Percentage
Critical	0	0.0%
High	0	0.0%
Medium	1	100.0%
Low	0	0.0%
Info	0	0.0%

# DETAILED FINDINGS

## Finding 1: Test Finding

Vulnerability ID	CYB-MEDI-001
Severity	MEDIUM
CVSS Score	N/A
Affected System	https://juice-shop.herokuapp.com
Discovery Tool	Manual Review

### Description:

Test

### Impact:

Medium

### Recommendation:

Fix it

## RECOMMENDATIONS & REMEDIATION

Based on the security assessment findings, we recommend implementing the following remediation measures in order of priority: **Immediate Actions (Critical/High Risk):** • Address all critical and high-severity vulnerabilities within 24-48 hours • Implement emergency security patches for identified vulnerabilities • Review and strengthen access controls **Short-term Actions (1-4 weeks):** • Remediate medium-severity vulnerabilities • Implement additional security monitoring • Update security policies and procedures **Long-term Actions (1-3 months):** • Address low-severity and informational findings • Implement security awareness training • Establish regular security assessment schedule **Ongoing Security Practices:** • Regular vulnerability scanning • Security patch management • Incident response planning • Continuous security monitoring

## CONCLUSION & NEXT STEPS

This VAPT assessment of <https://juice-shop.herokuapp.com> has identified 1 security findings that require attention. The assessment provides a comprehensive view of the current security posture and offers actionable recommendations for improvement. **Key Takeaways:** • Total findings identified: 1 • Critical/High priority items: 0 • Assessment date: September 17, 2025 **Next Steps:** 1. Review and prioritize remediation activities based on risk severity 2. Develop an implementation timeline for recommended security controls 3. Schedule follow-up assessment to validate remediation efforts 4. Establish ongoing security monitoring and assessment procedures Cybrty Security Services recommends addressing critical and high-severity findings immediately, followed by systematic remediation of medium and low-severity issues. We appreciate the opportunity to conduct this security assessment and remain available to assist with remediation planning and implementation.

# APPENDICES

## Appendix A: Security Testing Tools

The following security testing tools were utilized during this assessment: • Burp Suite • Manual Review • Nikto • Nmap • OWASP ZAP • SQLMap

## Appendix B: Testing Methodology

The security assessment followed a structured methodology including: **1. Reconnaissance and Information Gathering** • Network discovery and port scanning • Service enumeration and fingerprinting • Web application discovery **2. Vulnerability Assessment** • Automated vulnerability scanning • Manual security testing • Configuration review **3. Penetration Testing** • Exploitation of identified vulnerabilities • Privilege escalation testing • Lateral movement assessment **4. Analysis and Reporting** • Risk assessment and prioritization • Documentation of findings • Remediation recommendations



## CONFIDENTIALITY DISCLAIMER

**CONFIDENTIAL AND PROPRIETARY** This document contains confidential and proprietary information of Cybrty Security Services and is intended solely for the use of the client organization. This report contains sensitive security information that could be used to compromise systems if disclosed to unauthorized parties. **Distribution and Handling:** • This report is classified as CONFIDENTIAL • Distribution is restricted to authorized personnel only • This document should be stored securely and protected from unauthorized access • Electronic copies should be encrypted and password protected • Physical copies should be stored in locked containers **Legal Notice:** The information contained in this report is protected by applicable laws and regulations. Unauthorized disclosure, copying, or distribution is strictly prohibited and may result in legal action. **Disclaimer:** This assessment was conducted based on the systems and configurations present at the time of testing. Security postures can change rapidly, and this report represents a point-in-time assessment. Cybrty Security Services makes no warranties regarding the completeness or accuracy of this assessment beyond the scope and timeframe of the engagement. For questions regarding this report or its contents, please contact: Cybrty Security Services Email: security@cybrty.com Phone: +1 (555) 123-4567 Report ID: test-123 Generated: September 17, 2025 at 02:34 AM UTC