SECURITY ASSESSMENT REPORT

Target: juice-shop.herokuapp.com
Date: November 24, 2025
Scan ID: 1

Prepared by Sarral Scan

1. Executive Summary

Sarral Scan performed a comprehensive security assessment of **juice-shop.herokuapp.com** on 2025-11-24. The objective was to identify potential security vulnerabilities and provide recommendations for remediation.

Findings Summary

Severity	Count
Critical	0
High	0
Medium	2
Low	0
Info	0

2. Detailed Findings

1. SSH Connection Refused/Timeout

Severity: MEDIUM **Tool:** Passive Recon

Description:

The target host (10.77.145.71) refused or timed out the SSH connection attempt on port 22. This could indicate that the SSH service is not running, a firewall is blocking the connection, or there are network connectivity problems. If the SSH service is intentionally disabled, this is less of a concern. However, if it should be running, this could indicate a misconfiguration or a potential denial-of-service.

Remediation:

1. Verify that the SSH service is running on the target host (10.77.145.71). 2. Check the firewall configuration on the target host and any intermediary firewalls to ensure that SSH traffic (port 22) is allowed. 3. Investigate network connectivity between the scanning host and the target host. 4. If SSH is intentionally disabled, document the reason and ensure appropriate alternative access methods are in place.

2. SSH Connection Refused/Timeout

Severity: MEDIUM **Tool:** Active Recon

Description:

The scan was unable to establish an SSH connection to the target host. This could indicate that the SSH service is not running, is blocked by a firewall, or that there is a network connectivity issue preventing access to port 22. While not a vulnerability in itself, it prevents further security assessment of the SSH service and could indicate a misconfiguration or denial-of-service.

Remediation:

1. Verify that the SSH service is running on the target host. 2. Check firewall rules on the target host and any intermediary firewalls to ensure that port 22 is open for the scanning source IP. 3. Investigate network connectivity between the scanning host and the target host. 4. If SSH is intentionally blocked, document the reason and ensure alternative secure access methods are in place if needed.

3. Appendix: Raw Tool Output

The following section contains raw output from the security tools used during the assessment.

Tool: Passive Recon


```
{"error": "SSH Error: [Errno 10060] Connect call failed ('10.77.145.71', 22)"}
```


Tool: Active Recon


```
{"error": "SSH Error: [Errno 10060] Connect call failed ('10.77.145.71', 22)"}
```