CERBERUS

Security Assessment Report

Date: March 19, 2025

Report ID: CERB-20250319-001

Table of Contents

1. Executive Summary

This report details the security vulnerabilities identified during a scan of the application hosted at `https://juice-shop.herokuapp.com`. The scan revealed several security configuration issues that could potentially compromise the application's security. These vulnerabilities include missing security headers and potential information leakage via ETags. The report also includes a risk assessment and practical remediation steps to address these issues. Integrating knowledge graph insights, we note that the IP address resolution for the host is not detected, which could imply potential issues with DNS resolution or network configuration.

2. Key Findings

1. Missing X-XSS-Protection Header

- OWASP Reference: This aligns with the OWASP Top 10 category A7:2021-Cross-Site Scripting (XSS).
- Impact: Without the X-XSS-Protection header, the application is vulnerable to Cross-Site Scripting (XSS) attacks, which can allow attackers to inject malicious scripts into web pages viewed by other users.
- Risk: High. XSS attacks can lead to session hijacking, data theft, and account compromise.

2. Missing X-Content-Type-Options Header

- OWASP Reference: This aligns with the OWASP Top 10 category A6:2021-Security Misconfiguration.
- Impact: The absence of the X-Content-Type-Options header can lead to MIME type sniffing, where browsers may interpret files as a different MIME type than intended, potentially executing malicious code.
- Risk: Medium. This vulnerability can be exploited to deliver malicious content to users.

3. Server May Leak Inodes via ETags

- OWASP Reference: This aligns with the OWASP Top 10 category A6:2021-Security Misconfiguration.
- Impact: ETags can expose internal file paths and inode numbers, which can be used to map out the server's file structure and potentially exploit vulnerabilities.
- Risk: Medium. This information can aid attackers in launching more targeted attacks.

4. Missing Anti-Clickjacking X-Frame-Options Header

- OWASP Reference: This aligns with the OWASP Top 10 category A6:2021-Security Misconfiguration.
- Impact: The absence of the X-Frame-Options header allows the application to be embedded in an iframe on another site, potentially leading to clickjacking attacks.
- Risk: Medium. Clickjacking can be used to deceive users into performing unintended actions.

5. IP Address Resolution Issue

- Impact: The knowledge graph indicates that the IP address for `https://juice-shop.herokuapp.com` is not detected, which could imply issues with DNS resolution or network configuration.
- Risk: Medium. Undetected IP addresses can lead to potential network misconfigurations and accessibility issues.

3. Risk Assessment

Vulnerability	Severity	Impact Description
Missing X-XSS-Protection Header	High	Allows XSS attacks, leading to session hijacking, data theft, and account compromise.
Missing X-Content-Type-Options Header	Medium	Enables MIME type sniffing, potentially executing malicious content.
Server May Leak Inodes via ETags	Medium	Exposes internal file paths and inode numbers, aiding in mapping out the server's file structure.
Missing Anti-Clickjacking X-Frame-Options Header	Medium	Allows clickjacking, deceiving users into performing unintended actions.
IP Address Resolution Issue	Medium	Potential network misconfigurations and accessibility issues.

4. Recommendations

1. Implement X-XSS-Protection Header

- Action: Configure the server to include the `X-XSS-Protection` header with the value `1; mode=block`.
- Example: `X-XSS-Protection: 1; mode=block`

2. Set X-Content-Type-Options Header

- Action: Configure the server to include the `X-Content-Type-Options` header with the value `nosniff`.
- Example: `X-Content-Type-Options: nosniff`

3. Disable ETags or Mask Inodes

- Action: Configure the server to disable ETags or mask inode numbers to prevent exposure of internal file paths.
- Example: In Apache, add `FileETag None` to the configuration file.

4. Implement X-Frame-Options Header

- Action: Configure the server to include the `X-Frame-Options` header with the value `DENY` or `SAMEORIGIN`.
- Example: `X-Frame-Options: DENY`

5. Resolve IP Address Resolution Issue

- Action: Investigate and resolve the DNS resolution issue to ensure the application is accessible and properly configured.
- Example: Verify DNS settings and network configurations to ensure the IP address is correctly resolved.

By addressing these vulnerabilities and ensuring proper network configuration, the application can significantly enhance its security posture and protect against common web application attacks and network misconfigurations.