**Security Testing Report – OWASP ZAP**

**Target Application:** https://juice-shop.herokuapp.com  
**Tool Used:** OWASP ZAP (v2.16.1)  
**Date:** May 18, 2025

**Top Vulnerabilities Found:**

1. **Cross-Domain Misconfiguration**
   * *Description:* Site allows cross-origin resource sharing (CORS) from any origin.
   * *Impact:* Can lead to sensitive data exposure.
   * *Remediation:* Configure strict CORS policies.
2. **Content Security Policy Header Missing**
   * *Description:* CSP header is not set.
   * *Impact:* Increases risk of Cross-Site Scripting (XSS).
   * *Remediation:* Implement a proper CSP in response headers.
3. **Strict-Transport-Security Header Not Set**
   * *Description:* Site does not enforce HTTPS using HSTS.
   * *Impact:* Vulnerable to SSL stripping attacks.
   * *Remediation:* Add the Strict-Transport-Security header.
4. **Cross-Domain JavaScript Source File Inclusion**
   * *Description:* Site loads JS from external domains.
   * *Impact:* May introduce malicious scripts.
   * *Remediation:* Only allow trusted scripts, use Subresource Integrity (SRI).
5. **Hidden Files Found**
   * *Description:* Files like .git, .bak, or debug pages are accessible.
   * *Impact:* May reveal internal code or credentials.
   * *Remediation:* Remove or restrict access to sensitive files.

**Recommendations:**

* Implement secure headers.
* Regularly scan for hidden or outdated files.
* Harden CORS and CSP policies.
* Perform periodic security testing.

**Top Vulnerabilities Identified**

|  |  |  |  |
| --- | --- | --- | --- |
| **s.no** | **Vulnerability** | **Description** | **Remediation** |
| 1 | **Content Security Policy (CSP) Header Missing** | No CSP header, increases XSS risk | Add a strong CSP header in all responses |
| 2 | **Cross-Domain Misconfiguration** | CORS allows any origin | Restrict Access-Control-Allow-Origin to trusted domains |
| 3 | **Hidden Files Found** | Unintended debug files exposed | Remove or secure these files |
| 4 | **Strict-Transport-Security Not Set** | HSTS header missing | Enable HSTS to force HTTPS |
| 5 | **Cross-Domain JS Source Inclusion** | External scripts included | Load only trusted scripts; use SRI |

**Steps Performed**

1. Launched OWASP ZAP.
2. Started **Automated Scan** on the target URL.
3. Let it run the **spider** and **active scan**.
4. Reviewed the vulnerabilities under **Alerts**.
5. Generated a detailed HTML report.

**Attachments:**

* 🔹 2025-05-18-ZAP-Report.html (Detailed ZAP Scan Report)
* 🔹 Security\_Testing\_Summary.docx (This summary document)