Web Application Security Assessment Report

Name: Okoro Destiny Nkem

Task 1: Web Application Security Testing

Program: Future Intern Cybersecurity Analyst

Tools Used:

- Kali Linux,
- OWASP Juice Shop,
- OWASP ZAP (AJAX Spider).

Date: August 2025

Task Summary

This assessment involved conducting a security evaluation of OWASP Juice Shop using OWASP ZAP. The main objective was to detect vulnerabilities outlined in the OWASP Top 10, such as Cross-Site Scripting (XSS), SQL Injection and security misconfigurations. OWASP ZAP was utilized to perform automated scans of the application, through which significant vulnerabilities were discovered. Corresponding remediation measures are also recommended to address and mitigate the identified risks.

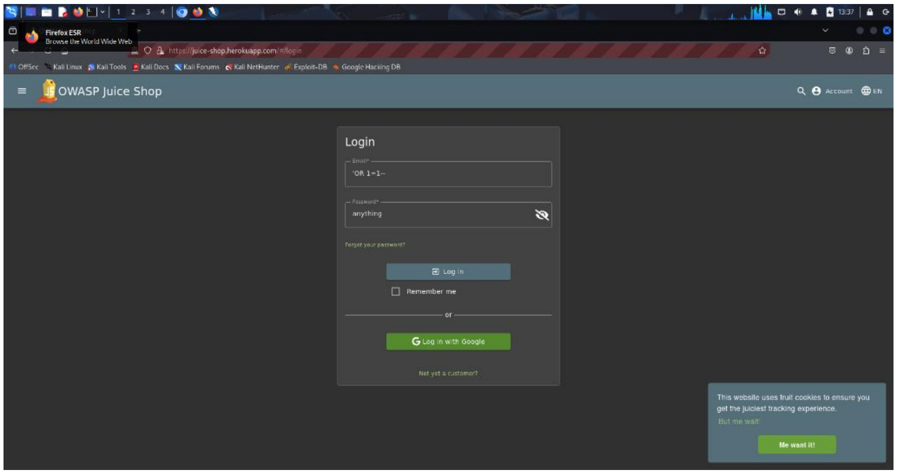
Procedure

- The OWASP Juice Shop application was accessed via its publicly available deployment on Heroku (https://juice-shop.herokuapp.com). This hosted instance provided a realistic environment to simulate web application attacks without the need for local setup.
- The Heroku deployment was used as the target system for all automated and manual security testing conducted with OWASP ZAP.
- The tool executed active scanning processes to identify input fields, user interactions, and potential vulnerabilities.
- The findings were examined and systematically aligned with the corresponding categories in the OWASP Top 10 framework and corrective measures were also recommended to address the identified vulnerabilities.

Identified Vulnerabilities

1. **SQL Injection Vulnerability**

   During the assessment, an SQL Injection vulnerability was identified in the login functionality of the OWASP Juice Shop application by entering the payload (or 1=1--). The authentication mechanism was bypassed, granting unauthorized access to the application. This injection technique manipulated the underlying SQL query, causing the system to return a valid result without verifying legitimate credentials and I was able to gain access with elevated privileges, including administrative level access to the application. This poses a critical security risk, as it could allow attackers to compromise sensitive data or take full control of the application.



Login

Email*: 'OR 1=1--

Password*: anything

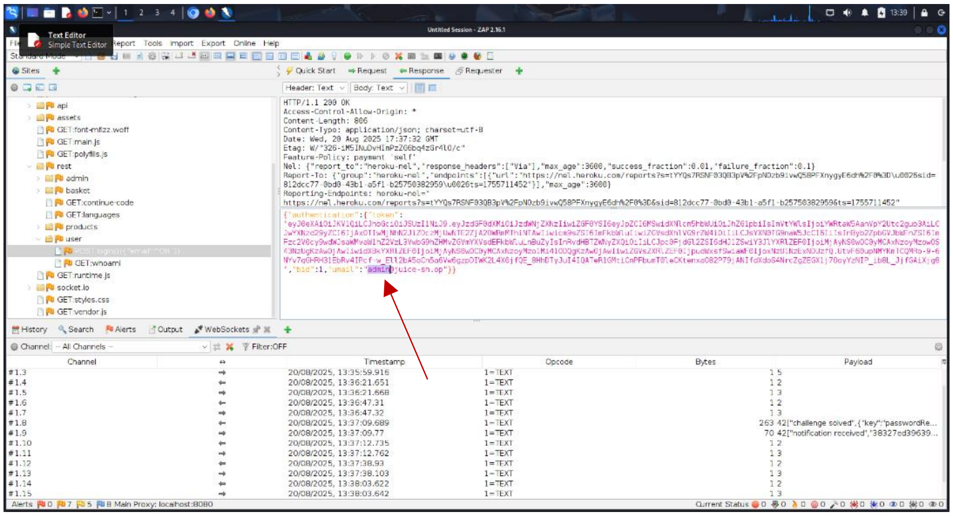
Forgot your password?

□ Remember me

Not yet a customer?

This website uses fruit cookies to ensure you get the juiciest tracking experience.

But me wait!



```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Length: 806
Content-Type: application/json; charset=utf-8
Date: Wed, 20 Aug 2025 17:37:32 GMT
Etag: W/"326-iM5INuDvHImPzZG6bq4zGr4l0/c"
Feature-Policy: payment 'self'
Nel: {"report_to":"heroku-nel","response_headers":["Via"],"max_age":3600,"success_fraction":0.01,"failure_fraction":0.1}
Report-To: {"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku.com/reports?s=tYYQs7RSNF03QB3pV%2FpNDzb9ivwQ58PFXnygyE6dh%2F0%3D\u0026sid=
812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=1755711452"}],"max_age":3600}
Reporting-Endpoints: heroku-nel="
https://nel.heroku.com/reports?s=tYYQs7RSNF03QB3pV%2FpN0zb9ivwQ58PFXnygyE6dh%2F0%3D&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&ts=1755711452"
```

```
{"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiJhZG1pbiIsImVtYWlsIjoiYWRtaW5AanVpY2Utc2gub3AiLC
JwYXNzd29yZCI6IjAxOTIwMjNhN2JiZDczMjUwNTE2ZjA2OWRmMThiNTAwIiwicm9sZSI6ImFkbWluIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IiIsInByb2ZpbGVJbWFnZSI6Im
Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdEFkbWluLnBuZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNS0wOC0yMCAxNzoyMzowOS
43NzUgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNS0wOC0yMCAxNzoyMzoIMi41ODQgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzU1NzExNDUzfQ.UtvF69upNMYKmICQMRo-9-6
NYv7qGHRH31EbRv4IPcf-w_El12bA5oCn5a6Vw6gzpOIWK2L4X0jfQE_8HhDTyJuI4IQATeR1GMtiCnPFbumT0leCKtenxa082P79jANIfdXdoS4NrcZgZEGX1j70oyYzNIP_ib8L_JjfGAiXjg0
","bid":1,"umail":"admin@juice-sh.op"}}
```

Channel	↔	Timestamp	Opcode	Bytes	Payload
#1.3	→	20/08/2025, 13:35:59.916	1=TEXT	1	5
#1.4	←	20/08/2025, 13:36:21.651	1=TEXT	1	2
#1.5	→	20/08/2025, 13:36:21.668	1=TEXT	1	3
#1.6	←	20/08/2025, 13:36:47.31	1=TEXT	1	2
#1.7	→	20/08/2025, 13:36:47.32	1=TEXT	1	3
#1.8	←	20/08/2025, 13:37:09.689	1=TEXT	263	42["challenge solved",{"key":"passwordRe...
#1.9	→	20/08/2025, 13:37:09.77	1=TEXT	70	42["notification received","38327ed39639...
#1.10	←	20/08/2025, 13:37:12.735	1=TEXT	1	2
#1.11	→	20/08/2025, 13:37:12.762	1=TEXT	1	3
#1.12	←	20/08/2025, 13:37:38.93	1=TEXT	1	2
#1.13	→	20/08/2025, 13:37:38.103	1=TEXT	1	3
#1.14	←	20/08/2025, 13:38:03.622	1=TEXT	1	2
#1.15	→	20/08/2025, 13:38:03.642	1=TEXT	1	3

Severity Level

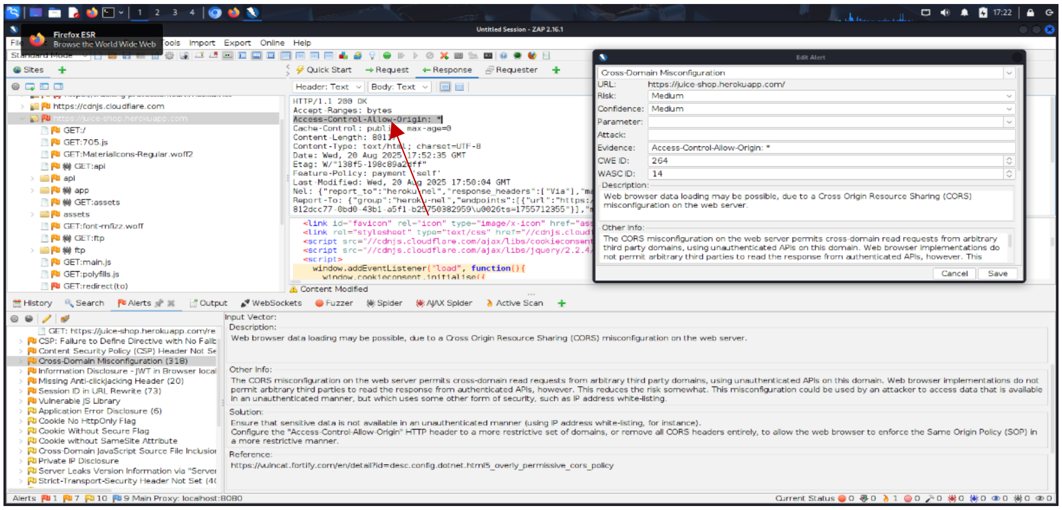
High because it is a critical vulnerability that allows privilege escalation and full application compromise.

Corrective Action

- ✓ Apply strict server-side input validation and sanitization.
- ✓ Enforce least-privilege principles for database accounts.
- ✓ Perform regular code reviews and penetration testing to detect injection flaws early.

2. **Cross Domain Misconfiguration**

During the automated assessment with OWASP ZAP, a potential Cross-Domain Misconfiguration was detected in the application's Cross-Origin Resource Sharing (CORS) policy. The server was observed to include overly permissive response headers, such as the "Access-Control-Allow-Origin: * " header. This configuration allows requests from any external domain, thereby bypassing the browser's same origin policy. As a result, a malicious website could potentially send crafted requests to the web app on behalf of authenticated users, exposing sensitive information such as session tokens or personal data.



https://cdnjs.cloudflare.com
https://juice-shop.herokuapp.com
GET:/
GET:705.js
GET:MaterialIcons-Regular.woff2
GET:api
api
app
GET:assets
assets
GET:font-mfizz.woff
GET:ftp
ftp
GET:main.js
GET:polyfills.js
GET:redirect(to)

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Content-Length: 8011
Content-Type: text/html; charset=UTF-8
Date: Wed, 20 Aug 2025 17:52:35 GMT
Etag: W/"138f5-198c89a2dff"
Feature-Policy: payment 'self'
Last-Modified: Wed, 20 Aug 2025 17:50:04 GMT
Nel: {"report_to":"heroku-nel","response_headers":["Via"],"ma
Report-To: {"group":"heroku-nel","endpoints":[{"url":"https:/
812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=1755712355"}],"m
```

```
<link id="favicon" rel="icon" type="image/x-icon" href="ass
<link rel="stylesheet" type="text/css" href="//cdnjs.cloudf
<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/
<script>
  window.addEventListener("load", function(){
    window.cookieconsent.initialise({
```

Cross-Domain Misconfiguration
URL: https://juice-shop.herokuapp.com/
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Other Info:
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This

GET: https://juice-shop.herokuapp.com/re
CSP: Failure to Define Directive with No Fallb
Content Security Policy (CSP) Header Not Se
Cross-Domain Misconfiguration (318)
Information Disclosure - JWT in Browser local
Missing Anti-clickjacking Header (20)
Session ID in URL Rewrite (73)
Vulnerable JS Library
Application Error Disclosure (6)
Cookie No HttpOnly Flag
Cookie Without Secure Flag
Cookie without SameSite Attribute
Cross-Domain JavaScript Source File Inclusion
Private IP Disclosure
Server Leaks Version Information via "Server
Strict-Transport-Security Header Not Set (40

Input Vector:
Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Other Info:
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Solution:
Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference:
https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Alerts 1 7 10 9 Main Proxy: localhost:8080
Current Status 0 0 1 0 0 0 0 0 0 0

Severity Level

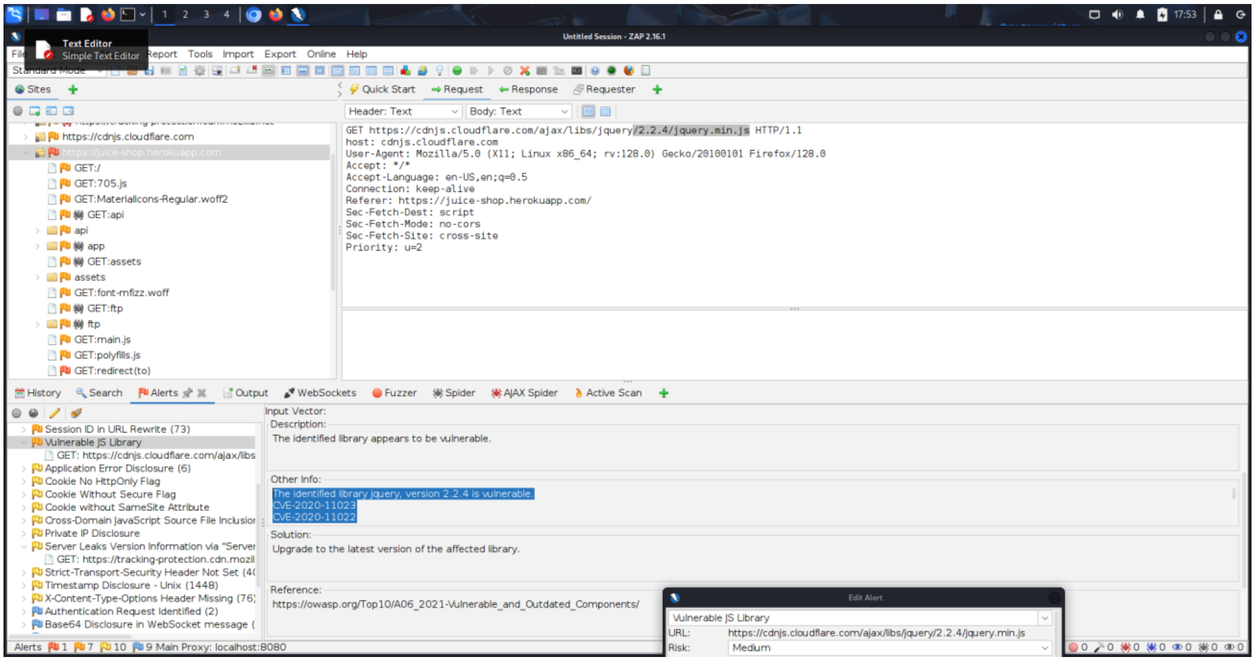
Medium because while not immediately granting full system compromise, it significantly increases the attack surface and can lead to serious data exposure when combined with other vulnerabilities.

Corrective Action

- ✓ Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing)
- ✓ Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains.

3. **Vulnerable JS Library**

OWASP ZAP identified the use of an outdated JavaScript library within the OWASP Juice Shop application and it relates to OWASP Top 10 vulnerabilities which is the "Vulnerable and Outdated Components" vulnerability. The scan reported that one or more client-side libraries in use contained known security flaws. Attackers can exploit weaknesses in outdated JavaScript frameworks or libraries to launch attacks such as Cross-Site Scripting (XSS), denial of service, or client-side code injection and the affected URL identified was "https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"



https://cdnjs.cloudflare.com
https://juice-shop.herokuapp.com
GET:/
GET:705.js
GET:MaterialIcons-Regular.woff2
GET:api
api
app
GET:assets
assets
GET:font-mfizz.woff
GET:ftp
ftp
GET:main.js
GET:polyfills.js
GET:redirect(to)

```
GET https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js HTTP/1.1
host: cdnjs.cloudflare.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://juice-shop.herokuapp.com/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Priority: u=2
```

Session ID in URL Rewrite (73)
Vulnerable JS Library
GET: https://cdnjs.cloudflare.com/ajax/libs
Application Error Disclosure (6)
Cookie No HttpOnly Flag
Cookie Without Secure Flag
Cookie without SameSite Attribute
Cross-Domain JavaScript Source File Inclusion
Private IP Disclosure
Server Leaks Version Information via "Server
GET: https://tracking-protection.cdn.mozil
Strict-Transport-Security Header Not Set (4(
Timestamp Disclosure - Unix (1448)
X-Content-Type-Options Header Missing (76)
Authentication Request Identified (2)
Base64 Disclosure in WebSocket message (

Input Vector:

Description:
The identified library appears to be vulnerable.

Other Info:
The identified library jquery, version 2.2.4 is vulnerable.
CVE-2020-11023
CVE-2020-11022

Solution:
Upgrade to the latest version of the affected library.

Reference:
https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Vulnerable JS Library
URL: https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Risk: Medium

Alerts 1 7 10 9 Main Proxy: localhost:8080

Severity Level

Medium because exploitation depends on the specific library and version in use. While it may not immediately lead to full system compromise, it provides an entry point for attackers.

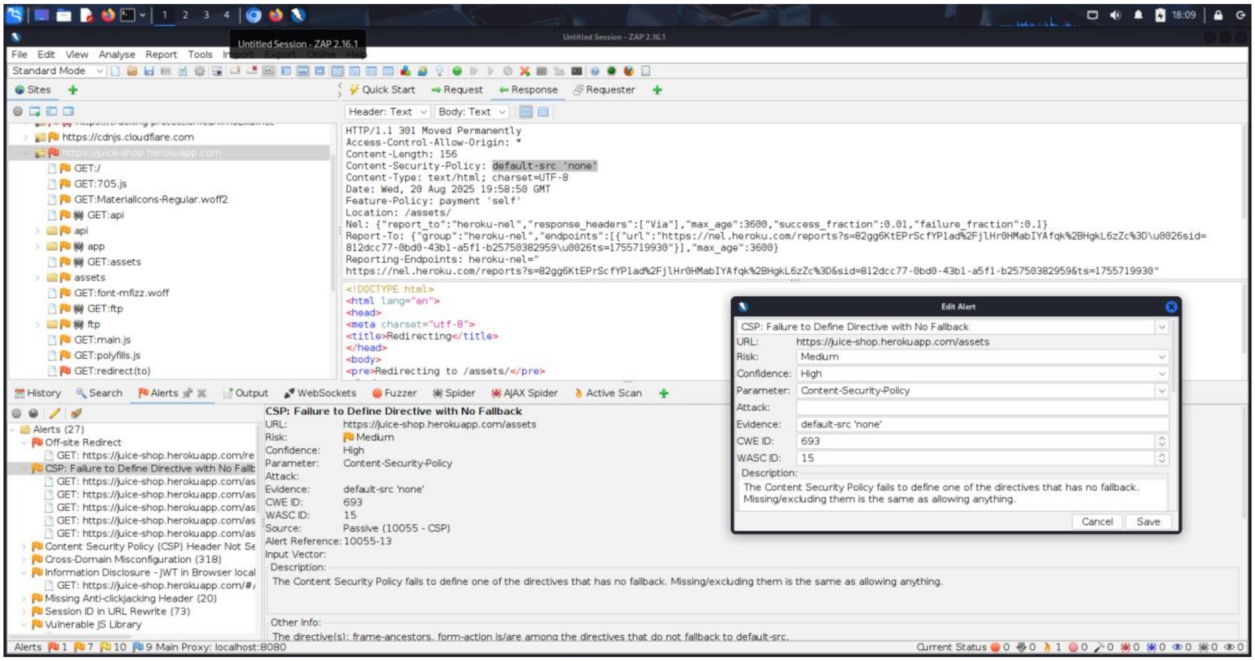
Corrective Action

- ✓ Upgrade to the latest version of the affected library.
- ✓ Remove unused or unnecessary libraries from the application.

4. Control Security Policy Misconfiguration

OWASP ZAP identified that the application has a Content Security Policy (CSP) misconfiguration, specifically a failure to define certain directives without fallback options. This relates to Security Misconfiguration as part of the OWASP Top 10 vulnerabilities. A properly configured CSP helps prevent client-side attacks such as Cross-Site Scripting, data injection, and clickjacking by restricting the sources from which content can be loaded.

But in this case, OWASP ZAP flagged that one or more directives were either missing or not backed by fallback policies and the affected URL was the https://juice-shop.herokuapp.com/assests .



```
https://cdnjs.cloudflare.com
https://juice-shop.herokuapp.com
    GET:/
    GET:705.js
    GET:MaterialIcons-Regular.woff2
    GET:api
  api
  app
    GET:assets
  assets
    GET:font-mfizz.woff
    GET:ftp
  ftp
    GET:main.js
    GET:polyfills.js
    GET:redirect(to)
```

```
HTTP/1.1 301 Moved Permanently
Access-Control-Allow-Origin: *
Content-Length: 156
Content-Security-Policy: default-src 'none'
Content-Type: text/html; charset=UTF-8
Date: Wed, 20 Aug 2025 19:58:50 GMT
Feature-Policy: payment 'self'
Location: /assets/
Nel: {"report_to":"heroku-nel","response_headers":["Via"],"max_age":3600,"success_fraction":0.01,"failure_fraction":0.1}
Report-To: {"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku.com/reports?s=82gg6KtEPrScfYPlad%2FjlHr0HMabIYAfqk%2BHgkL6zZc%3D\u0026sid=
812dcc77-0bd0-43b1-a5f1-b25750382959\u0026ts=1755719930"}],"max_age":3600}
Reporting-Endpoints: heroku-nel="
https://nel.heroku.com/reports?s=82gg6KtEPrScfYPlad%2FjlHr0HMabIYAfqk%2BHgkL6zZc%3D&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&ts=1755719930"
```

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Redirecting</title>
</head>
<body>
<pre>Redirecting to /assets/</pre>
```

Edit Alert

CSP: Failure to Define Directive with No Fallback

URL: https://juice-shop.herokuapp.com/assets
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'none'
CWE ID: 693
WASC ID: 15
Description:
The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.

Cancel Save

```
Alerts (27)
  Off-site Redirect
    GET: https://juice-shop.herokuapp.com/re
  CSP: Failure to Define Directive with No Fallb
    GET: https://juice-shop.herokuapp.com/as
    GET: https://juice-shop.herokuapp.com/as
    GET: https://juice-shop.herokuapp.com/as
    GET: https://juice-shop.herokuapp.com/as
    GET: https://juice-shop.herokuapp.com/as
  Content Security Policy (CSP) Header Not Se
  Cross-Domain Misconfiguration (318)
  Information Disclosure - JWT in Browser local
    GET: https://juice-shop.herokuapp.com/#/
  Missing Anti-clickjacking Header (20)
  Session ID in URL Rewrite (73)
  Vulnerable JS Library
```

CSP: Failure to Define Directive with No Fallback

URL: https://juice-shop.herokuapp.com/assets
Risk: Medium
Confidence: High
Parameter: Content-Security-Policy
Attack:
Evidence: default-src 'none'
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Alert Reference: 10055-13
Input Vector:
Description:
The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.

Other Info:
The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

Alerts 1 7 10 9 Main Proxy: localhost:8080 Current Status 0 0 1 0 0 0 0 0 0 0

Severity Level

Medium because while not always directly exploitable on its own, a weak or misconfigured CSP significantly increases the likelihood of successful XSS or other client side attacks when combined with other vulnerabilities**.**

Corrective Action

- ✓ Ensure that that web server, application server, load balancer are properly configured to set the Content Security Policy header.
- ✓ Avoid using wildcards (*) in CSP directives.