# OWASP Juice Shop Security Assessment Report

---

**Performed by:** Zikra Abdusemed Mohammed
**Date:** November 7, 2025
**Tool Used:** OWASP ZAP v2.16.1

## Executive Summary

The OWASP Juice Shop application running locally at http://localhost:3000 was scanned using OWASP ZAP. A total of 12 alerts were identified: 5 Medium, 4 Low, and 3 Informational. The majority of the findings are related to security misconfigurations such as missing headers and outdated components. No High or Critical vulnerabilities were detected.

## Scope & Methodology

Target: OWASP Juice Shop (http://localhost:3000) Tools: OWASP ZAP v2.16.1 Testing Date: November 7, 2025 Method: Automated active scanning using default ZAP policies. Vulnerabilities
are mapped to the OWASP Top 10 (2021) categories.

## Overall Risk Summary

| Risk Level | Counts | Percentage |
|---|---|---|
| High | 0 | 0% |
| Medium | 5 | 41.7% |
| Low | 4 | 33.3% |
| Informational | 3 | 25% |

---

**Delaited Findings**

| Vulnerabilities | Risk | OWASP Mapping | Remediation |
|---|---|---|---|
| CSP Header Not Set | Medium | A05: Security Misconfiguration | Add Content-Security-Policy header restricting sources. |
| Cross-Domain Misconfiguration | Medium | A05: Security Misconfiguration | Restrict CORS to trusted origins only. |
| Missing Anti-clickjacking Header | Medium | A05: Security Misconfiguration | Add X-Frame-Options or CSP frame-ancestors directive. |
| Session ID in URL Rewrite | Medium | A07: Identification & Authentication | Use secure Failures cookies instead of URL parameters for sessions |
| Vulnerable JS Library | Medium | A06: Vulnerable and OutdatedUpdate Components | Update or replace outdated JavaScript libraries. |
| Cross-Domain JS Inclusion | Low | A05: Security Misconfiguration | Implement Subresource Integrity (SRI) and limit external scripts |
| Private IP Disclosure | Low | A01: Broken Access Control | Remove internal IPs from responses and logs. |
| Timestamp Disclosure | Low | A05: Security Misconfiguration | Remove server timestamps from responses. |
| X-Content-Type-Options Missing | Low | A05: Security Misconfiguration | Add X-Content-Type-Options: nosniff header. |
| Suspicious Comments | Info | A05: Security Misconfiguration | Remove developer comments from source code. |

| | | | |
|---|---|---|---|
| Retrieved from Cache | Info | A05: Security Misconfiguration | Add Cache-Control: no-store for sensitive data. |
| Modern Web Application | Info | N/A | No remediation needed. |

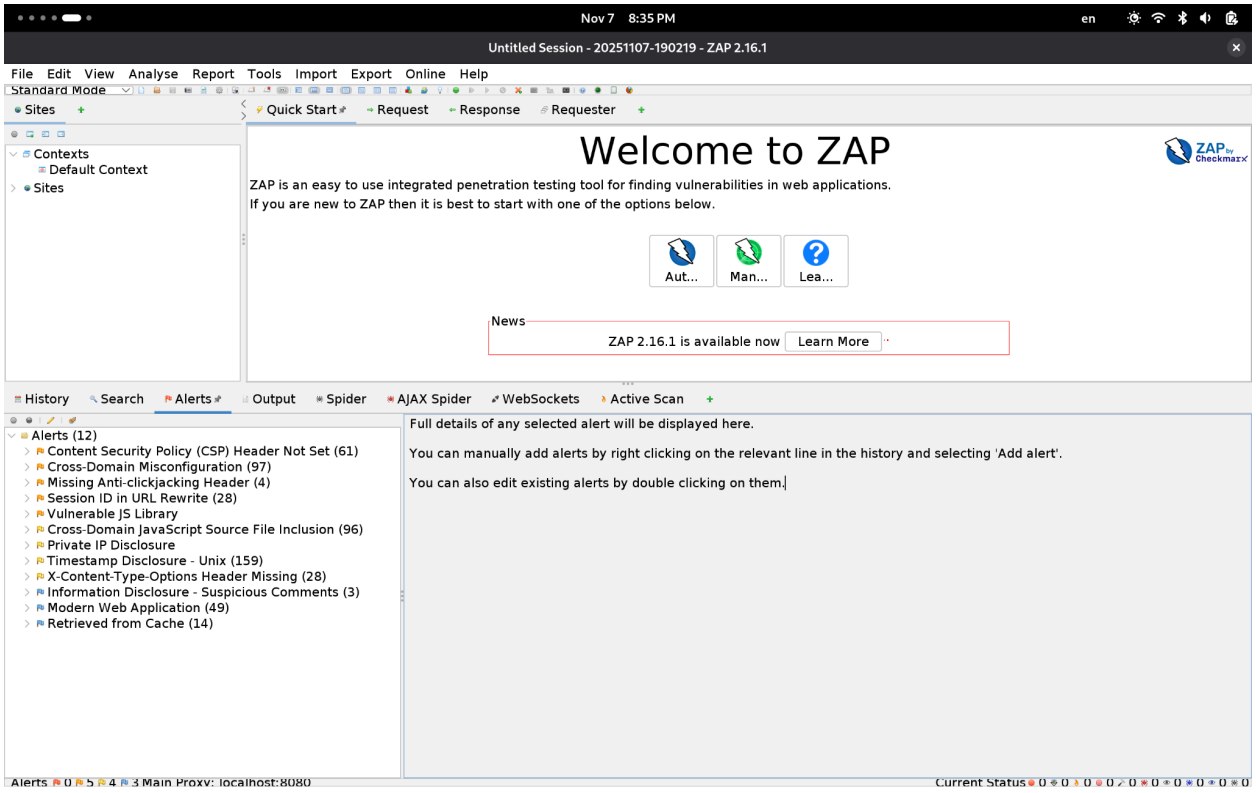
---

## Remediation Roadmap

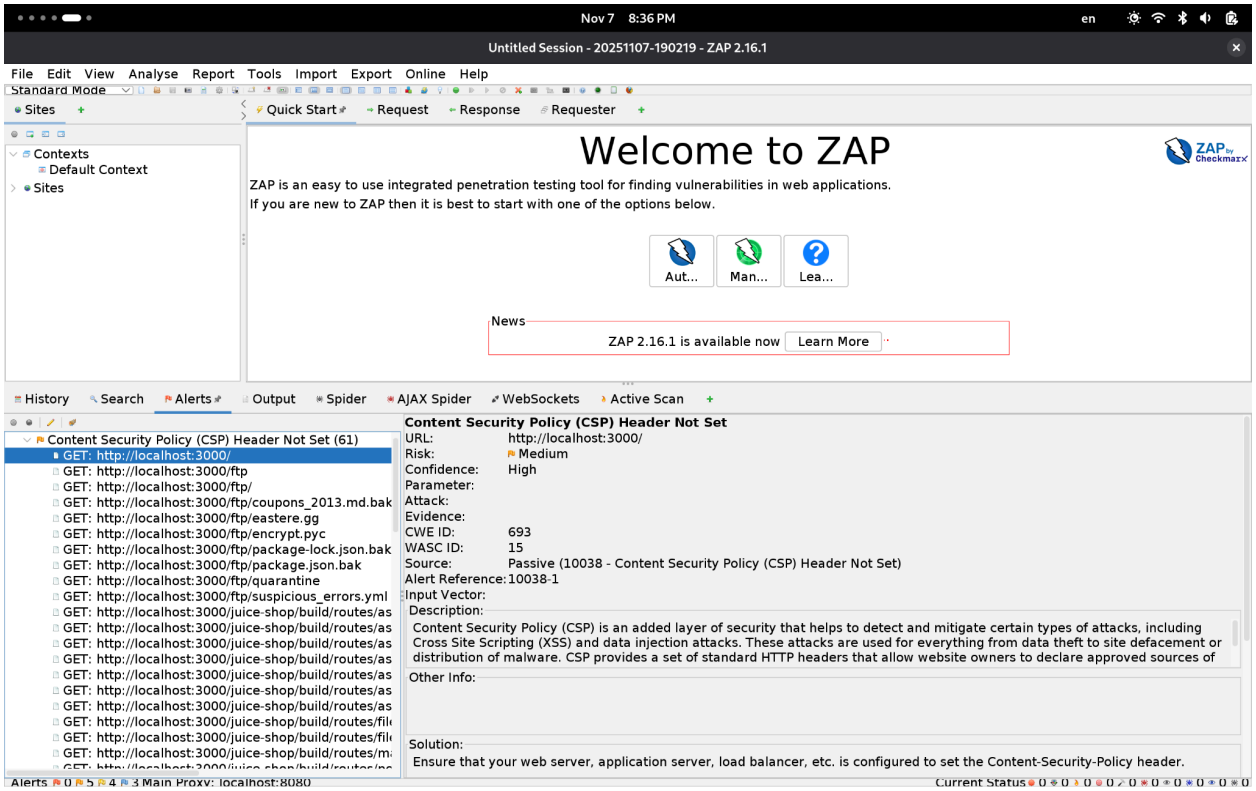
Immediate Fixes: Add security headers (CSP, X-Frame-Options, X-Content-Type-Options). • Short-Term: Update vulnerable libraries and restrict CORS to trusted origins. • Long-Term: Implement secure development lifecycle and continuous scanning.

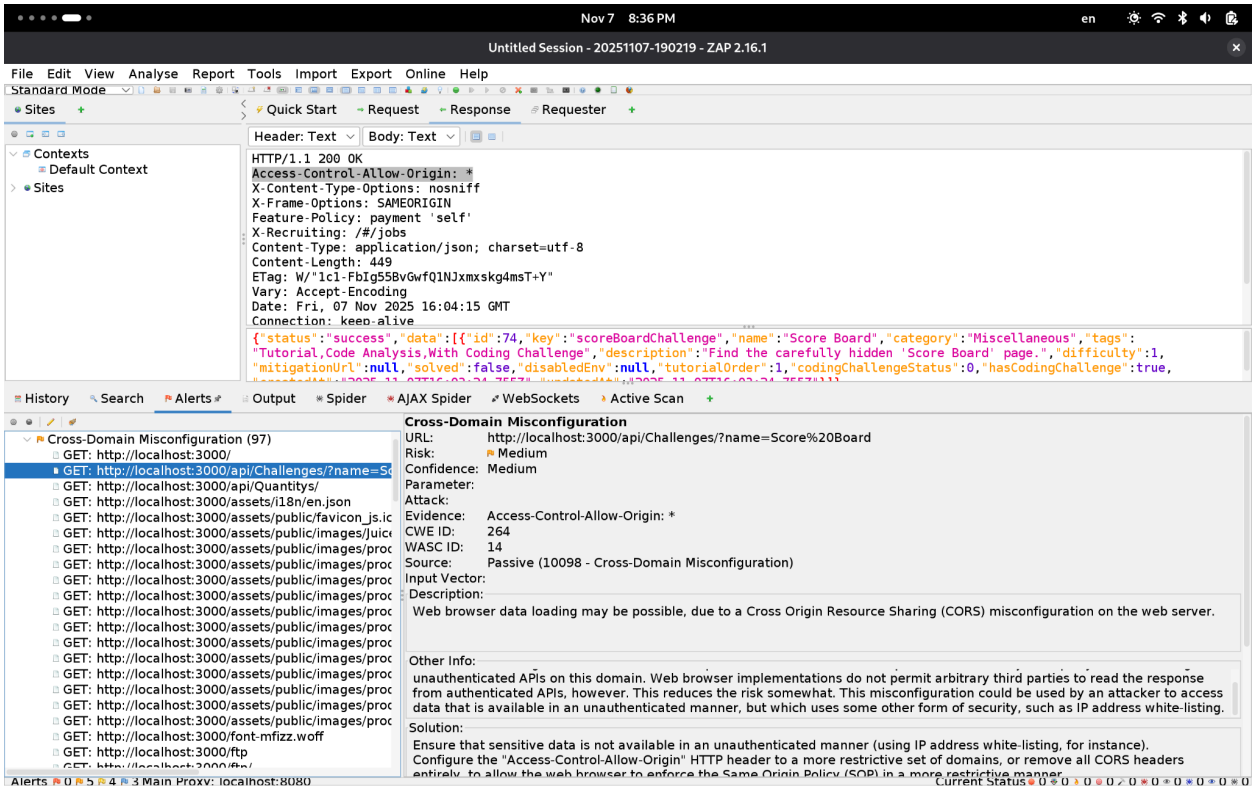
---

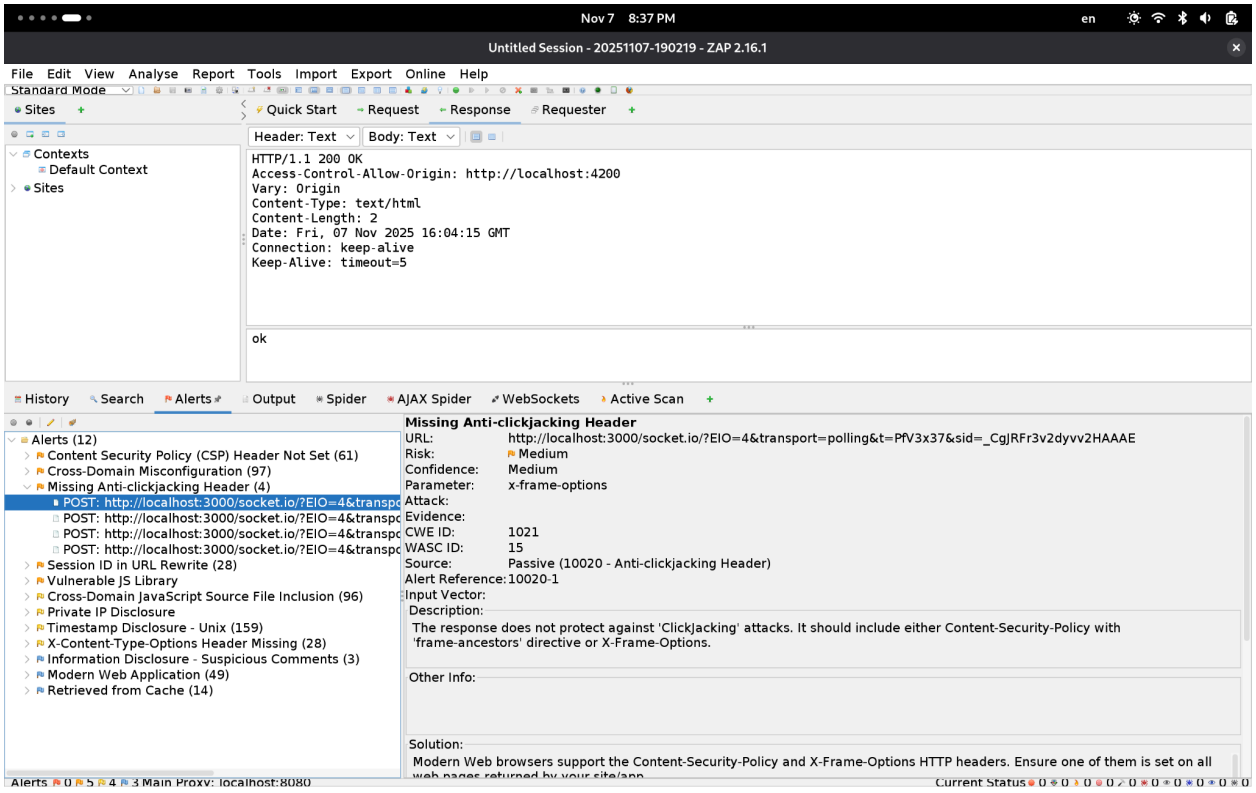
## Screen Shot of the Alerts From ZAP

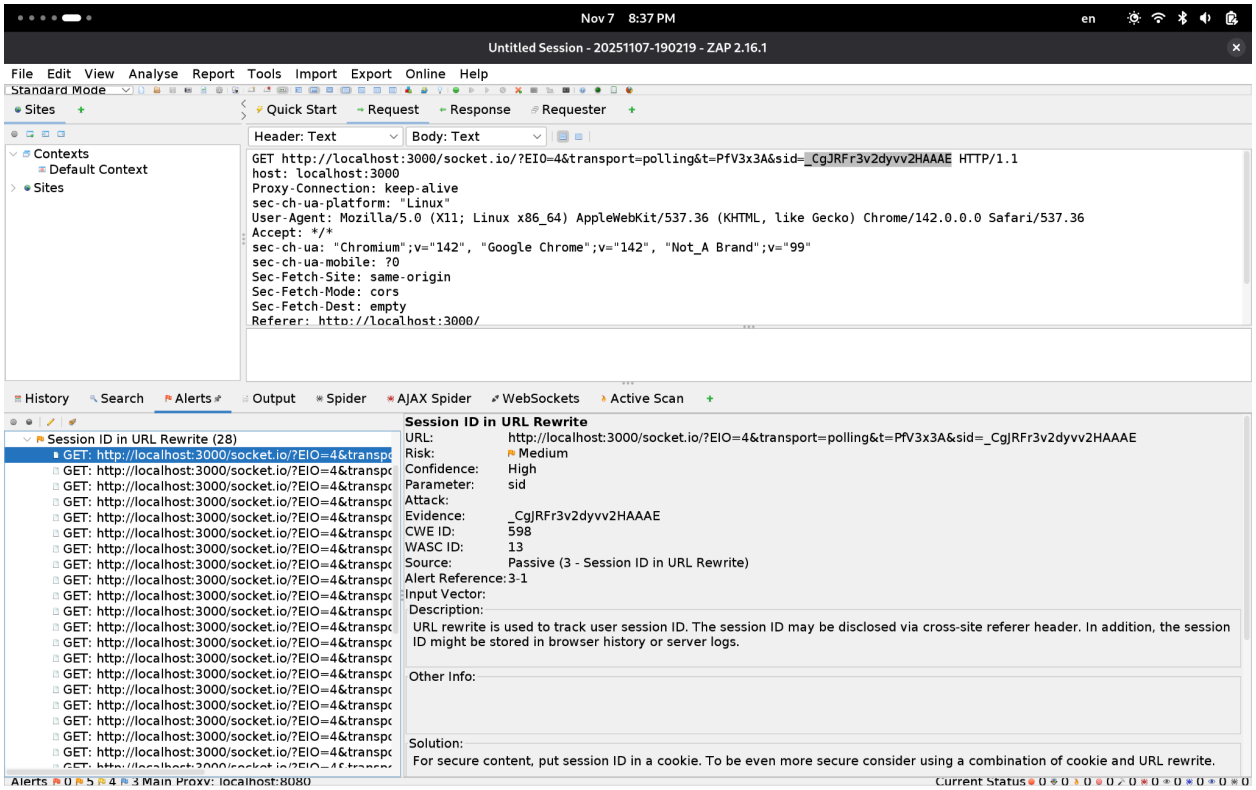


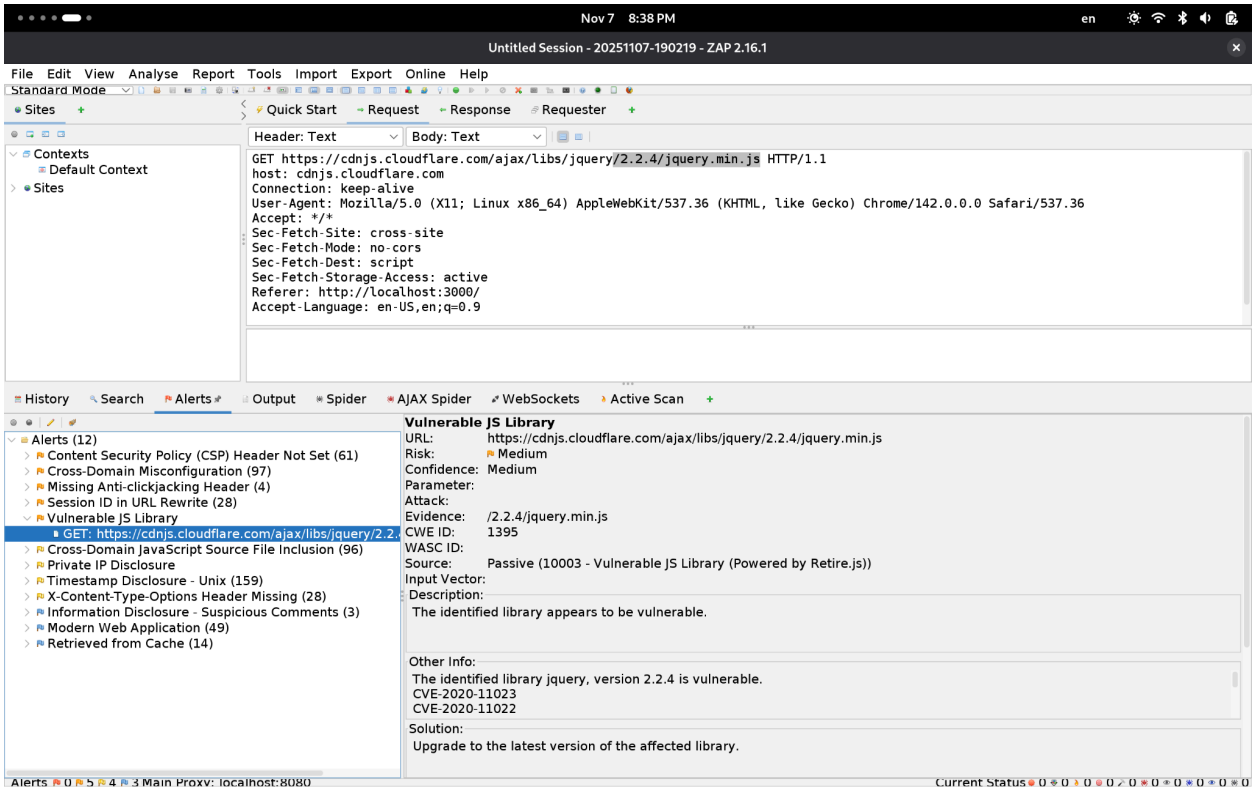
## Detailed Screenshots for the Medium Risks




Nov 7 8:36 PM
en
Untitled Session - 20251107-190219 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Header: Text
Body: Text
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 449
ETag: W/"1c1-FbIg55BvGwfQ1NJxmxskg4msT+Y"
Vary: Accept-Encoding
Date: Fri, 07 Nov 2025 16:04:15 GMT
Connection: keep-alive
{"status":"success","data":[{"id":74,"key":"scoreBoardChallenge","name":"Score Board","category":"Miscellaneous","tags":
"Tutorial,Code Analysis,With Coding Challenge","description":"Find the carefully hidden 'Score Board' page.","difficulty":1,
"mitigationUrl":null,"solved":false,"disabledEnv":null,"tutorialOrder":1,"codingChallengeStatus":0,"hasCodingChallenge":true,
History
Search
Alerts
Output
Spider
AJAX Spider
WebSockets
Active Scan
Cross-Domain Misconfiguration (97)
GET: http://localhost:3000/
GET: http://localhost:3000/api/Challenges/?name=Sc
GET: http://localhost:3000/api/Quantitys/
GET: http://localhost:3000/assets/i18n/en.json
GET: http://localhost:3000/assets/public/favicon_js.ic
GET: http://localhost:3000/assets/public/images/Juic
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/assets/public/images/proc
GET: http://localhost:3000/font-mfizz.woff
GET: http://localhost:3000/ftp
Cross-Domain Misconfiguration
URL: http://localhost:3000/api/Challenges/?name=Score%20Board
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
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:
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
Alerts 0 5 4 3 Main Proxy: localhost:8080
Current Status


Nov 7 8:37 PM
en
Untitled Session - 20251107-190219 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Header: Text
Body: Text
HTTP/1.1 200 OK
Access-Control-Allow-Origin: http://localhost:4200
Vary: Origin
Content-Type: text/html
Content-Length: 2
Date: Fri, 07 Nov 2025 16:04:15 GMT
Connection: keep-alive
Keep-Alive: timeout=5
ok
History
Search
Alerts
Output
Spider
AJAX Spider
WebSockets
Active Scan
Alerts (12)
Content Security Policy (CSP) Header Not Set (61)
Cross-Domain Misconfiguration (97)
Missing Anti-clickjacking Header (4)
POST: http://localhost:3000/socket.io/?EIO=4&transpo
POST: http://localhost:3000/socket.io/?EIO=4&transpo
POST: http://localhost:3000/socket.io/?EIO=4&transpo
POST: http://localhost:3000/socket.io/?EIO=4&transpo
Session ID in URL Rewrite (28)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (96)
Private IP Disclosure
Timestamp Disclosure - Unix (159)
X-Content-Type-Options Header Missing (28)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (49)
Retrieved from Cache (14)
Missing Anti-clickjacking Header
URL: http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PfV3x37&sid=_CgJRFr3v2dyvv2HAAAE
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:
Description:
The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with
'frame-ancestors' directive or X-Frame-Options.
Other Info:
Solution:
Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all
Alerts 0 5 4 3 Main Proxy: localhost:8080
Current Status


Nov 7 8:37 PM
en
Untitled Session - 20251107-190219 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
GET http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PfV3x3A&sid=_CgJRFr3v2dyvv2HAAAE HTTP/1.1
host: localhost:3000
Proxy-Connection: keep-alive
sec-ch-ua-platform: "Linux"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Accept: */*
sec-ch-ua: "Chromium";v="142", "Google Chrome";v="142", "Not_A Brand";v="99"
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
History
Search
Alerts
Output
Spider
AJAX Spider
WebSockets
Active Scan
Session ID in URL Rewrite (28)
GET: http://localhost:3000/socket.io/?EIO=4&transpo
Session ID in URL Rewrite
URL: http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PfV3x3A&sid=_CgJRFr3v2dyvv2HAAAE
Risk: Medium
Confidence: High
Parameter: sid
Attack:
Evidence: _CgJRFr3v2dyvv2HAAAE
CWE ID: 598
WASC ID: 13
Source: Passive (3 - Session ID in URL Rewrite)
Alert Reference: 3-1
Input Vector:
Description:
URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
Other Info:
Solution:
For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Alerts 0 5 4 3 Main Proxy: localhost:8080
Current Status


Nov 7 8:38 PM
en
Untitled Session - 20251107-190219 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
GET https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js HTTP/1.1
host: cdnjs.cloudflare.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Sec-Fetch-Storage-Access: active
Referer: http://localhost:3000/
Accept-Language: en-US,en;q=0.9
History
Search
Alerts
Output
Spider
AJAX Spider
WebSockets
Active Scan
Alerts (12)
Content Security Policy (CSP) Header Not Set (61)
Cross-Domain Misconfiguration (97)
Missing Anti-clickjacking Header (4)
Session ID in URL Rewrite (28)
Vulnerable JS Library
GET: https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2
Cross-Domain JavaScript Source File Inclusion (96)
Private IP Disclosure
Timestamp Disclosure - Unix (159)
X-Content-Type-Options Header Missing (28)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (49)
Retrieved from Cache (14)
Vulnerable JS Library
URL: https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: /2.2.4/jquery.min.js
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
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.
Alerts 0 5 4 3 Main Proxy: localhost:8080
Current Status

For additional report you can check the git repository that contains the ZAP generated html report

**Github Repo: FUTURE_CS_01**