SECURITY ASSESSMENT

Juice Shop Vulnerabilities Report

Submitted to: Udacity
Security Analyst: Samar Abdulaziz

Date of Testing: 1/5/2023
Date of Report Delivery: <<DATE>

Table of Contents

Contents

Security Engagement Summary

Engagement Overview

the leadership of the development team has requested engagement to assess the vulnerability for legacy web application

Scope

The scop is a web application for Juice shop which runs on 192.168.44.140:3000.

Executive Risk Analysis

The assessment was completed on 1/5/2023, the purpose of this assessment was to detect vulnerabilities on a legacy web application and assess the risk and what list of possible mitigation

After scanning the juice shop web server using OWASP zap, there is no high vulnerability detected, there are four medium-risk and five low risks, recommend to do this assement each month to detect any issue before incident happen.

Executive Recommendation

recommend the configuration and maintenance of the legacy web application there is a misconfiguration in its recurring assessment using an automated method to do maintenance when needed, there is some medium vulnerability that need to be fixed to secure the web application such as CORS and Session ID in URL rewrite

also CSP header , these weaknesses important to fix because configuring CSP for example will mitigate XSS and data injection attack, misconfiguring these will makes the site vulnerable.

Significant Vulnerability Summary

High Risk Vulnerabilities

- No High risk has been detected

Medium Risk Vulnerabilities

- cross-domain misconfiguration
- missing anti clickjacking
- session ID in URL Rewrite

Low Risk Vulnerabilities

- private IP disclosure.
- application error disclosure.
- X-content type option header missing

Significant Vulnerability Detail

cross-domain misconfiguration

occurs when the web server allows third-party domains to perform privileged tasks through the browsers of legitimate users.

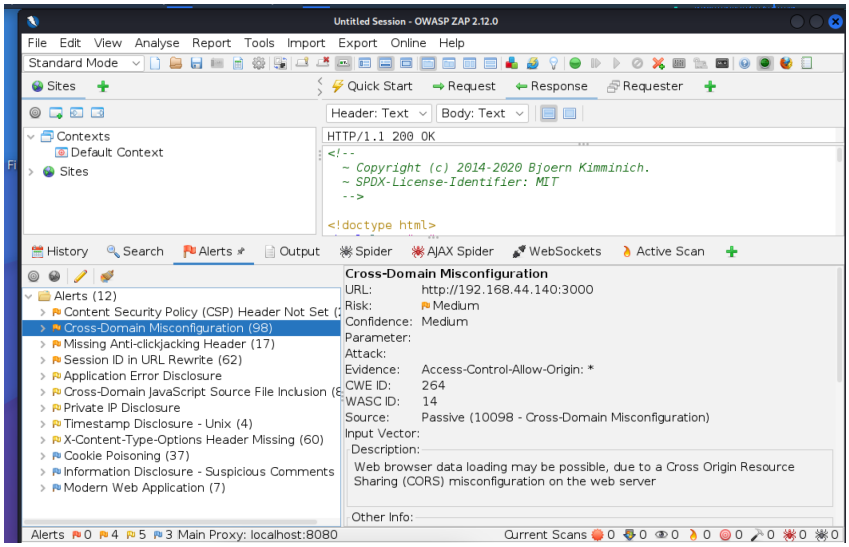
Source raised by a passive scanner (Cross-Domain Misconfiguration)

CWE ID 264

WASC ID 14

Reference
https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

MEDIUM



Remediation :

- Ensure that sensitive data is not available in an unauthenticated manner
- Configure the 'Access-Control-Allow-Origin' HTTP header
- remove all CORS headers entirely

Risk=Medium, Confidence=Medium

The probability that the vulnerability could be exploited is high if the origin site is vulnerable

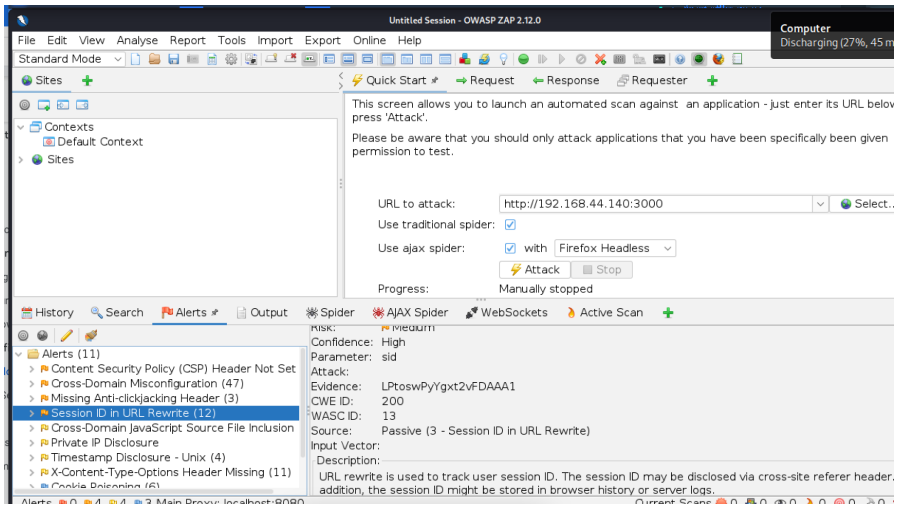
Session ID in URL rewrite

MEDIUM

“ 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.”

“The Session Tokens (Cookie, SessionID, Hidden Field), if exposed, will usually enable an attacker to impersonate a victim and access the application illegitimately. As such, it is important that they are protected from eavesdropping at all times – particularly whilst in transit between the Client browser and the application servers.”

Source	**raised by a passive scanner (Session ID in URL Rewrite)**
CWE ID	**200**
WASC ID	**13**
Reference	**http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html**



Remideiton :

- Ensure using HTTPS on your website.
- Store session ID in a cookie.
- For even more security use the combination of cookie and URL rewrite.

Risk=Medium, Confidence=High

The impacted assets are Web application which is high, its important to protect data and customers.

The probability that the vulnerability could be exploited is low it requires the skilled hacker to exploit

Methodology

Assessment Toolset Selection

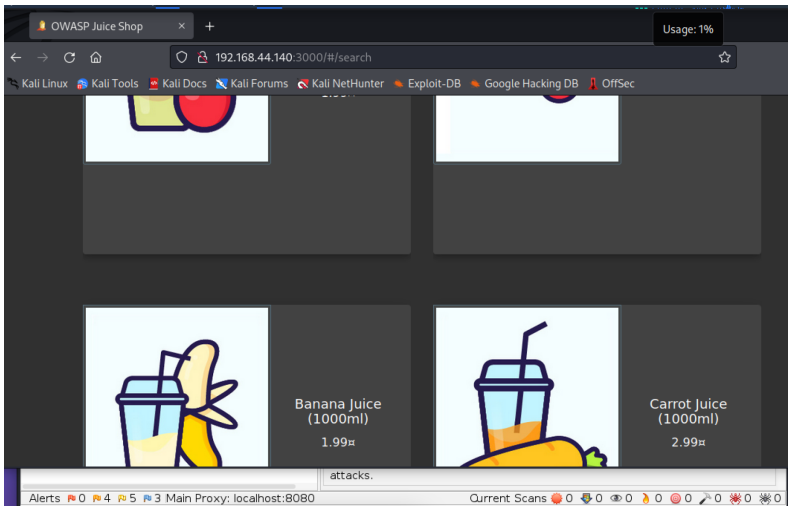
OWASP ZAP

Virtual box

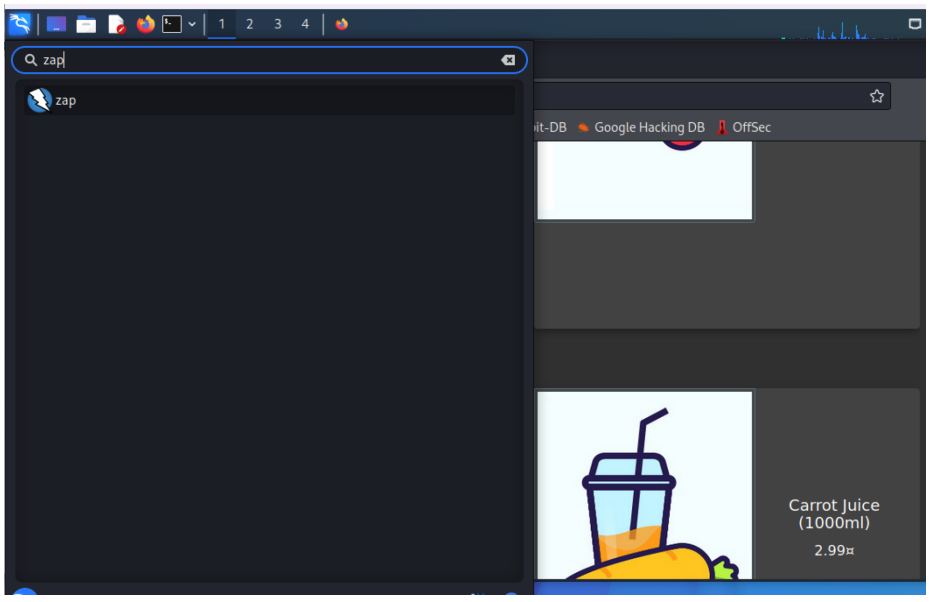
browser

Assessment Methodology Detail

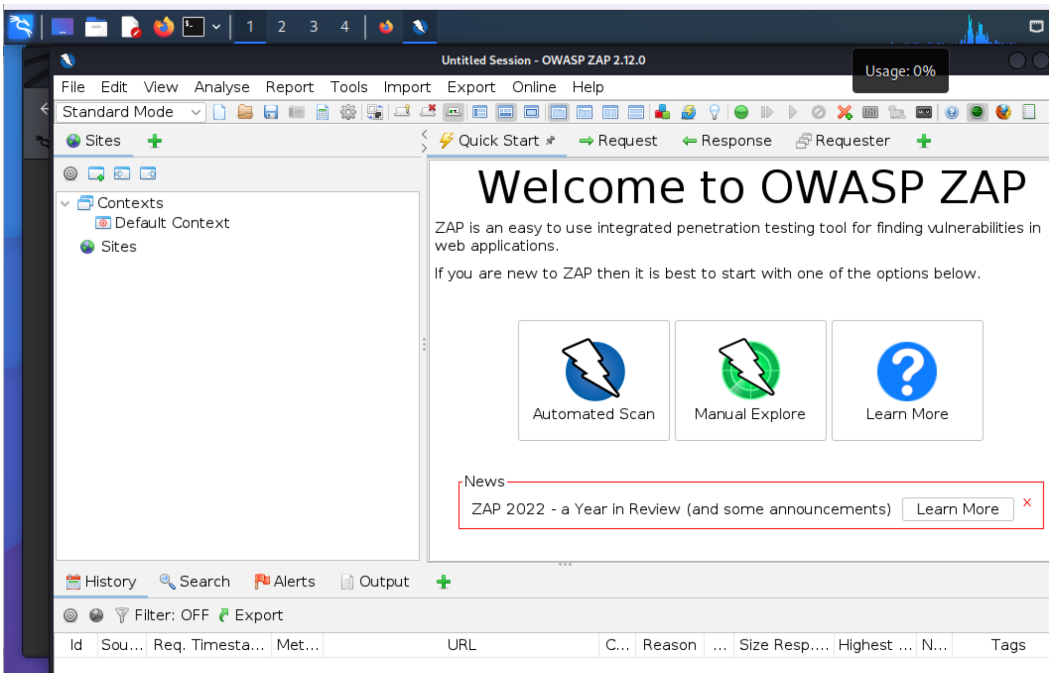
First : make sure the website are connected by ping or type the URL 192.168.44.140:3000 in the browser



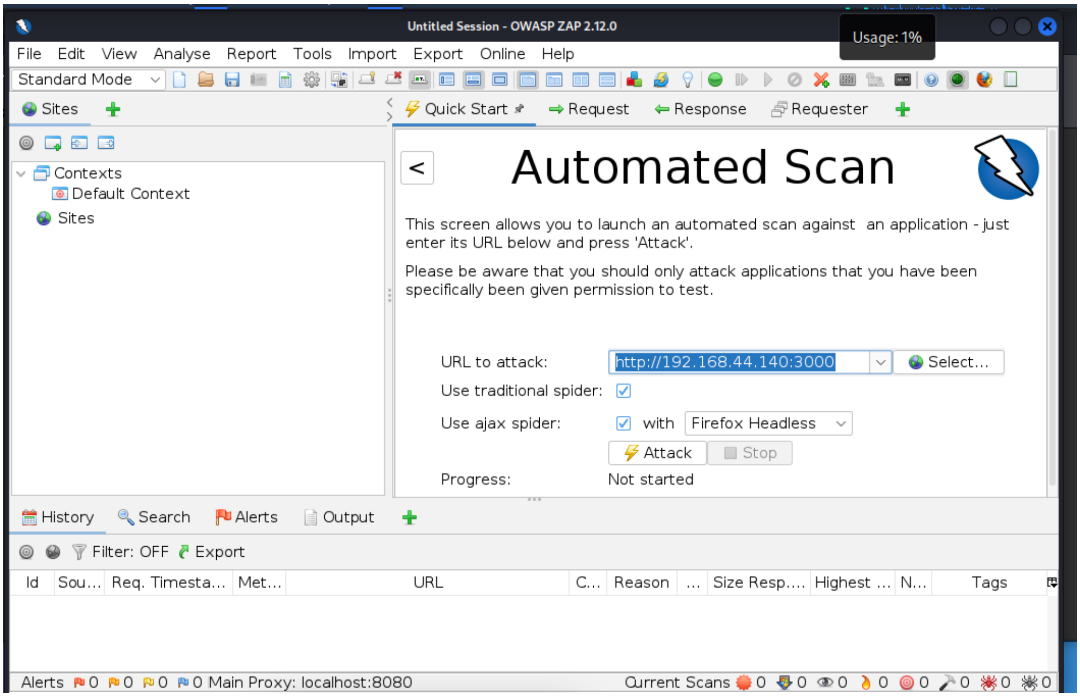
Second: after make sure everything is connected we can do scan using any tool I will use OWSAP ZAP



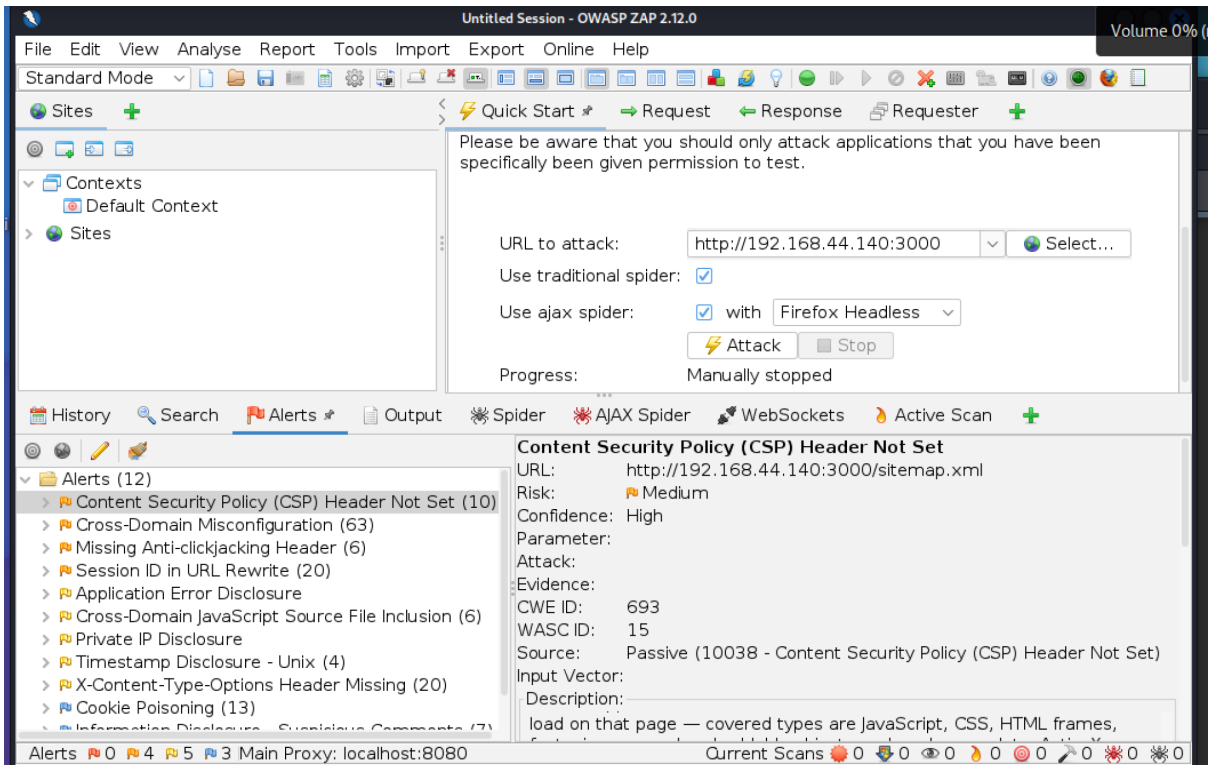
Third: select Automated Scan to Start



Fourth : type the URL to start the Scan



Finally : As you can see there is 4 medium Risk and 5 low risk that should be fixed



This concluded the vulnerability assessment methodology portion of this report.