

# Web Application Security Assessment Report

## Introduction

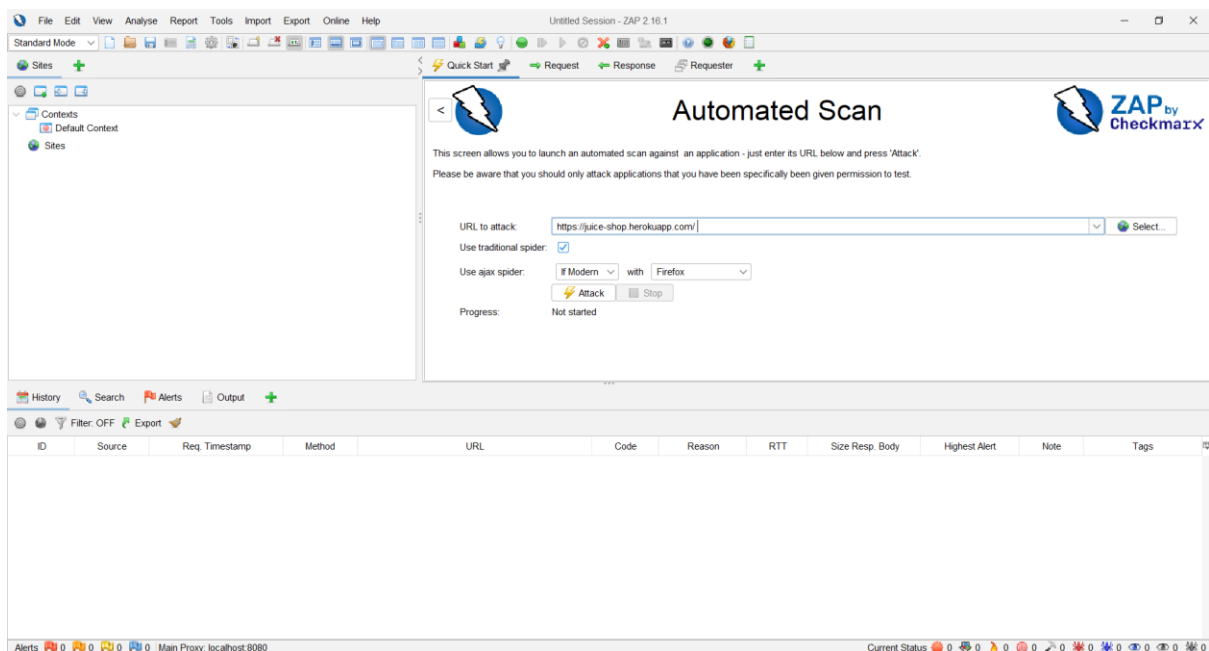
- Objective: Identify security vulnerabilities
- Application Tested: OWASP Juice Shop
- Reference: <https://owasp.org/www-project-juice-shop/>
- Tool Used: OWASP ZAP
- Testing Type: Automated security assessment

## Methodology

- Automated Scan using OWASP ZAP
- Crawling using Spider and AJAX Spider
- OWASP Top 10 used for classification

## Vulnerability Findings

The screenshot below contains the automated Zap scan



## Vulnerability 1: Content Security Policy (CSP) Header Not Set

**Risk Rating:** Medium

### Description:

The application does not define a Content Security Policy header, which may allow malicious scripts to execute.

## Impact:

Attackers may inject unauthorized scripts, leading to data theft.

## OWASP Category:

A05 – Security Misconfiguration

## Screenshot:

The top screenshot shows the ZAP interface with the 'Automated Scan' screen. The URL to attack is <https://juice-shop.herokuapp.com/>. The bottom screenshot shows the 'Alerts' tab with a list of alerts. The alert 'Content Security Policy (CSP) Header Not Set' is selected, showing details such as URL, Risk, Confidence, Parameter, Attack, Evidence, CWE ID, WASC ID, Source, Alert Reference, Input Vector, Description, Other Info, Solution, and Reference.

**Alert Details:**

- URL: <https://juice-shop.herokuapp.com/>
- Risk: Medium
- Confidence: High
- Parameter: Attack
- Evidence: CWE ID: 693, WASC ID: 15
- Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
- Alert Reference: 10038-1
- Input Vector:
- Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
- Other Info:
- Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
- Reference: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP>, [https://cheatsheetseries.owasp.org/cheatsheets/Content\\_Security\\_Policy\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html), <https://www.w3.org/TR/CSP/>

**Alert Tags:**

Key	Value
OWASP_2021_A05	<a href="https://owasp.org/Top10/A05_2021-Security_Misconfiguration/">https://owasp.org/Top10/A05_2021-Security_Misconfiguration/</a>
POLICY_QA_STD	
POLICY_PENTEST	
SYSTEMIC	<a href="https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic">https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic</a>
CWE-693	<a href="https://cwe.mitre.org/data/definitions/693.html">https://cwe.mitre.org/data/definitions/693.html</a>

## Recommendation:

Implement a strict CSP header to restrict script execution.

# Vulnerability 2: Cross-Domain Misconfiguration

**Risk Rating:** Medium

## Description:

The application allows cross-domain interactions without proper restrictions, which may expose sensitive resources.

## Impact:

Attackers may exploit this misconfiguration to access or manipulate data from other domains.

## OWASP Category:

A05 – Security Misconfiguration

## Screenshot:

The screenshot displays the ZAP (Zed Attack Proxy) interface, showing a list of alerts on the left and the details of a selected alert on the right.

**Alerts List (Left):**

- Alerts (8)
- Content Security Policy (CSP) Header Not Set (57)
- Cross-Domain Misconfiguration (72)**
- Cross-Domain JavaScript Source File Inclusion (96)
- Strict-Transport-Security Header Not Set (72)
- Timestamp Disclosure - Unix (227)
- Information Disclosure - Suspicious Comments (2)
- Modern Web Application (49)
- Re-examine Cache-control Directives (19)

**Alert Details (Right):**

**Alert:** Cross-Domain Misconfiguration

**URL:** https://juice-shop.herokuapp.com/runtime.js

**Risk:** Medium

**Confidence:** Medium

**Parameter:** Access-Control-Allow-Origin \*

**Attack:** Access-Control-Allow-Origin \*

**Evidence:** Access-Control-Allow-Origin \*

**CWE ID:** 264

**WASC ID:** 14

**Source:** Passive (10098 - Cross-Domain Misconfiguration)

**Input Vector:** Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

**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://vuln.catfortify.com/en/detail?category=HTML5&subcategory=Overly%520Permissive%520CORS%520Policy>

**Alert Tags:**

Key	Value
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
CWE-264	https://cwe.mitre.org/data/definitions/264.html
POLICY_QA_STD	
POLICY_PENTEST	

### Recommendation:

Restrict cross-domain access by configuring proper CORS (Cross-Origin Resource Sharing) policies.

## Vulnerability 3: Strict-Transport-Security (HSTS) Header Not Set

**Risk Rating:** Medium

### Description:

The application does not include the HTTP Strict Transport Security (HSTS) header, allowing browsers to communicate over insecure HTTP connections.

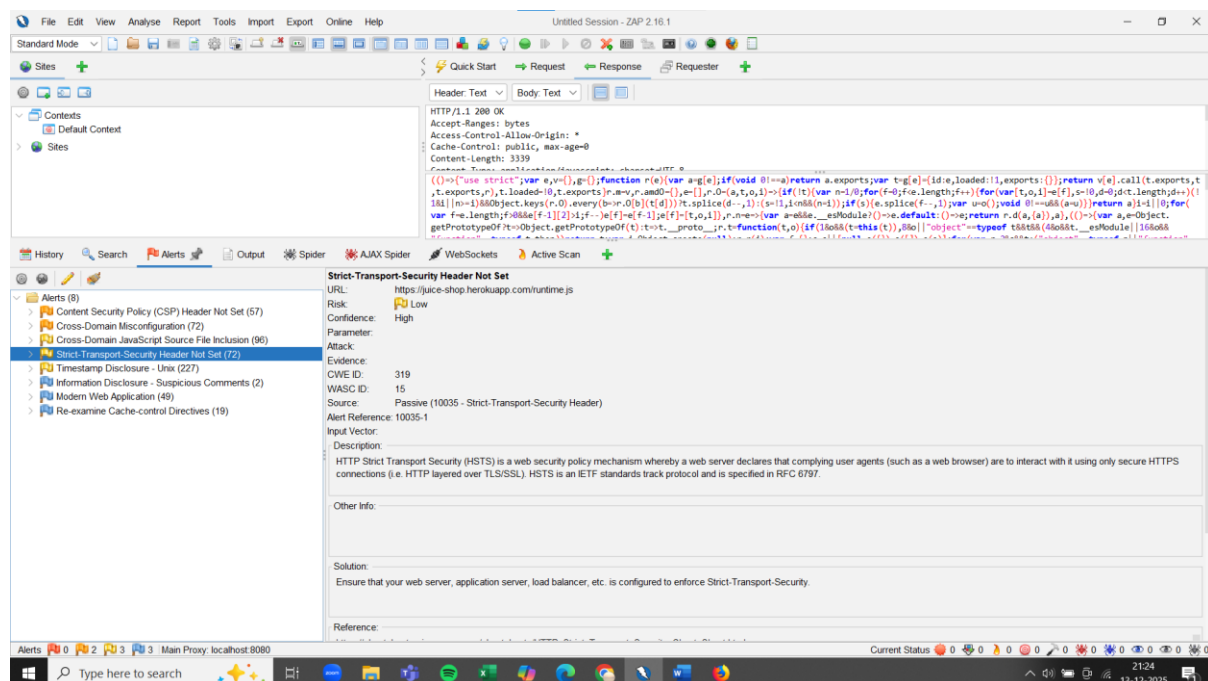
### Impact:

An attacker could perform man-in-the-middle attacks and intercept sensitive data.

### OWASP Category:

A02 – Cryptographic Failures

### Screenshot:



### Recommendation:

Enable the HSTS header to ensure all communications occur over HTTPS.

## Vulnerability 4: Information Disclosure – Suspicious Comments

**Risk Rating:** Low

### Description:

The application contains suspicious comments in the source code that may reveal internal implementation details.

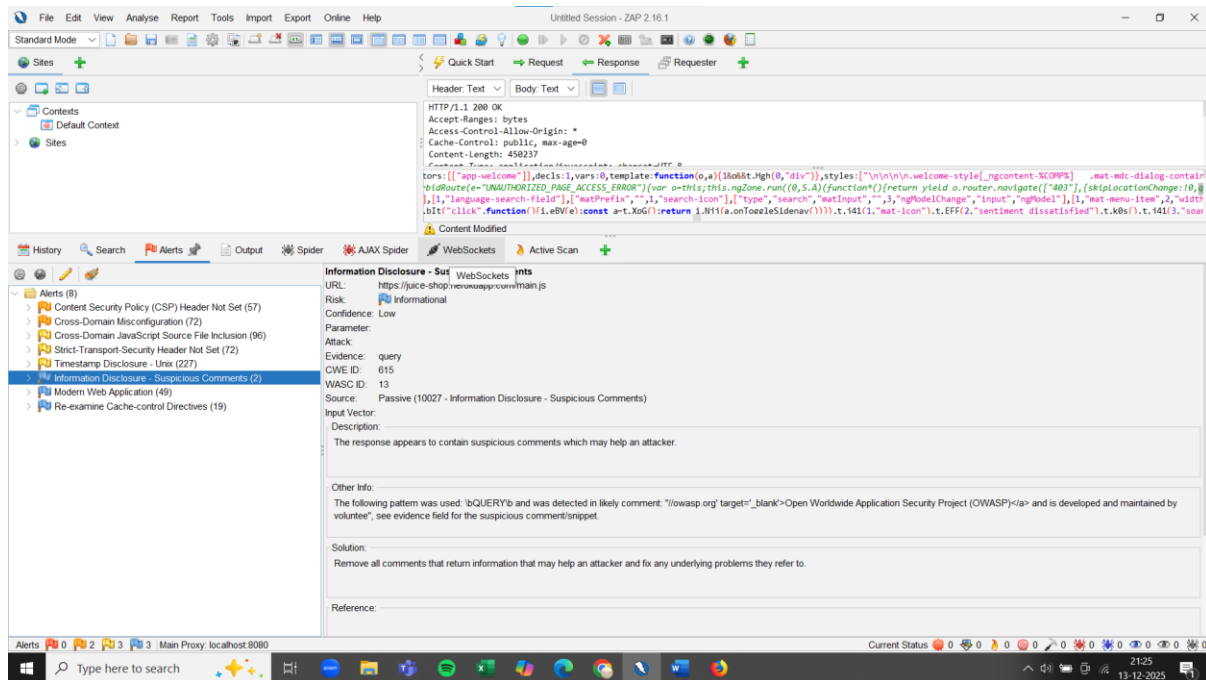
## Impact:

Attackers could use this information to understand the application structure and plan further attacks.

## OWASP Category:

A01 – Broken Access Control

## Screenshot:



## Recommendation:

Remove all unnecessary comments from production code before deployment.

## Vulnerability 5: Timestamp Disclosure – Unix

### Risk Rating: Low

### Description:

The application discloses Unix timestamps in server responses, which may reveal system information.

### Impact:

Attackers could use timing information to analyse server behaviour or plan targeted attacks.

## OWASP Category:

A01 – Broken Access Control

## Screenshot:

The top screenshot shows the ZAP 2.16.1 interface with the 'Timestamp Disclosure - Unix' alert selected. The alert details are as follows:

- URL: <https://juice-shop.herokuapp.com/assets/public/favicon.ico>
- Risk: Low
- Confidence: Low
- Parameter: Reporting-Endpoints
- Attack: 1765640450
- Evidence: 1765640450
- CWE ID: 497
- WASC ID: 13
- Source: Passive (10096 - Timestamp Disclosure)
- Input Vector: Reporting-Endpoints
- Description: A timestamp was disclosed by the application/web server. - Unix
- Other Info: 1765640450, which evaluates to: 2025-12-13 21:10:50.
- Solution: Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
- Reference: <https://cwe.mitre.org/data/definitions/200.html>

The bottom screenshot shows the same alert with the 'Alert Tags' table expanded:

Key	Value
OWASP_2021_A01	<a href="https://owasp.org/Top10/A01_2021-Broken_Access_Control/">https://owasp.org/Top10/A01_2021-Broken_Access_Control/</a>
OWASP_2017_A03	<a href="https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html">https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html</a>
POLICY_PENTEST	
CWE-497	<a href="https://cwe.mitre.org/data/definitions/497.html">https://cwe.mitre.org/data/definitions/497.html</a>
SYSTEMIC	<a href="https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/systemic">https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/systemic</a>

## Recommendation:

Avoid exposing internal timestamp information in responses unless required.

## OWASP Top 10 Category mapping

OWASP Top 10 Category	Status
A01: Broken Access Control	Issues Found in vulnerabilities 5,4
A02: Cryptographic Failures	Issues Found in vulnerabilities 3
A03: Injection	Not found
A04: Insecure Design	Not found
A05: Security Misconfiguration	Issues Found in vulnerabilities 1,2
A06: Vulnerable and Outdated Components	Not found
A07: Identification and Authentication Failures	Not found
A08: Software and Data Integrity Failures	Not found
A09: Security Logging and Monitoring Failures	Not found
A10: Server Side Requested Forgery	Not found

Tool logs:

ZAP scan report:

[ZAP by Checkmarx Scanning Report](#)



## Additional screenshots:

### Spider running:

The top screenshot shows the ZAP interface with the Spider tool running a scan on <https://juice-shop.herokuapp.com/>. The scan progress is 100%. The current status shows 0 URLs Found, 111 Nodes Added, and 71 Export. The scan results table shows the following data:

Processed	Req	Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Tags
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/">https://juice-shop.herokuapp.com/</a>	200 OK	212 ms	973 bytes	75,055 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/robots.txt">https://juice-shop.herokuapp.com/robots.txt</a>	200 OK	584 ms	880 bytes	28 bytes	Medium	Script, Comment		
Not Text	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/sitemap.xml">https://juice-shop.herokuapp.com/sitemap.xml</a>	200 OK	973 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/assets/public/favicon.js">https://juice-shop.herokuapp.com/assets/public/favicon.js</a>	200 OK	187 ms	860 bytes	15,088 bytes	Medium	Comment		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/styles.css">https://juice-shop.herokuapp.com/styles.css</a>	200 OK	272 s	977 bytes	640,267 bytes	Medium	Comment		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/runtime.js">https://juice-shop.herokuapp.com/runtime.js</a>	200 OK	544 ms	987 bytes	3,339 bytes	Medium	Upload		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/polyfills.js">https://juice-shop.herokuapp.com/polyfills.js</a>	200 OK	713 ms	989 bytes	34,844 bytes	Medium	Comment		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/main.js">https://juice-shop.herokuapp.com/main.js</a>	200 OK	1.74 s	991 bytes	450,237 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/vendor.js">https://juice-shop.herokuapp.com/vendor.js</a>	200 OK	2.15 s	993 bytes	1,692,128 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp">https://juice-shop.herokuapp.com/ftp</a>	200 OK	6.18 s	846 bytes	11,318 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/quarantine">https://juice-shop.herokuapp.com/ftp/quarantine</a>	200 OK	6.17 s	849 bytes	9,592 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/questions.md">https://juice-shop.herokuapp.com/ftp/questions.md</a>	200 OK	258 ms	981 bytes	909 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/announcement_enc">https://juice-shop.herokuapp.com/ftp/announcement_enc</a>	200 OK	1.28 s	986 bytes	369,237 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/coupons_2013.md">https://juice-shop.herokuapp.com/ftp/coupons_2013.md</a>	403 Forbidden	255 ms	856 bytes	1,864 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/easteregg">https://juice-shop.herokuapp.com/ftp/easteregg</a>	403 Forbidden	253 ms	856 bytes	1,864 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/encrypt.py">https://juice-shop.herokuapp.com/ftp/encrypt.py</a>	403 Forbidden	252 ms	856 bytes	1,864 bytes	Medium	Script, Comment		
Not Text	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/incident-support.kit">https://juice-shop.herokuapp.com/ftp/incident-support.kit</a>	200 OK	251 ms	978 bytes	3,246 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/legal.md">https://juice-shop.herokuapp.com/ftp/legal.md</a>	200 OK	677 ms	982 bytes	3,047 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/package-lock.json">https://juice-shop.herokuapp.com/ftp/package-lock.json</a>	403 Forbidden	683 ms	856 bytes	1,864 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/package.json">https://juice-shop.herokuapp.com/ftp/package.json</a>	403 Forbidden	674 ms	856 bytes	1,864 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/suspicious_errors.y">https://juice-shop.herokuapp.com/ftp/suspicious_errors.y</a>	403 Forbidden	675 ms	856 bytes	1,864 bytes	Medium	Script, Comment		

The bottom screenshot shows the ZAP interface with the Spider tool running a scan on <https://juice-shop.herokuapp.com/>. The scan progress is 100%. The current status shows 0 URLs Found, 111 Nodes Added, and 71 Export. The scan results table shows the following data:

Processed	Req	Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Tags
✓	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	240 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	232 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	218 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
✓	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	205 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	1.04 s	977 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	250 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	1.4 s	977 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	230 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	211 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	209 ms	977 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	425 ms	973 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	612 ms	973 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	371 ms	973 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	415 ms	973 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	420 ms	973 bytes	75,055 bytes	Medium	Script, Comment		
Max Depth	13/12/25, 9:10:58 pm	GET	<a href="https://juice-shop.herokuapp.com/app/node_modules/ser">https://juice-shop.herokuapp.com/app/node_modules/ser</a>	200 OK	379 ms	973 bytes	75,055 bytes	Medium	Script, Comment		
Not Text	13/12/25, 9:11:03 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms">https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms</a>	200 OK	179 ms	968 bytes	166 bytes	Medium	Script, Comment		
Not Text	13/12/25, 9:11:03 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/">https://juice-shop.herokuapp.com/ftp/</a>	200 OK	6.19 s	842 bytes	11,275 bytes	Medium	Script, Comment		
Not Text	13/12/25, 9:11:03 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms">https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms</a>	200 OK	178 ms	968 bytes	166 bytes	Medium	Script, Comment		
Not Text	13/12/25, 9:11:03 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms">https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms</a>	200 OK	177 ms	968 bytes	162 bytes	Medium	Script, Comment		
Not Text	13/12/25, 9:11:03 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms">https://juice-shop.herokuapp.com/ftp/quarantine/juicy_ms</a>	200 OK	176 ms	968 bytes	168 bytes	Medium	Script, Comment		



## Websockets:

The screenshot shows the ZAP WebSockets interface. The top panel displays the 'Header Text' of a response, which is an HTTP 200 OK status. The main panel shows a list of messages with columns for Channel, Timestamp, Opcode, Bytes, and Payload. The messages are numbered #2.1 through #3.2. The bottom panel shows the 'Alerts' section with a search bar and a list of alerts.

Channel	Timestamp	Opcode	Bytes	Payload
#2.1	13/12/2025, 21:11:35.993	1=TEXT	58	["messageType":"hello","broadcasts":[],"use_webpu
#2.2	13/12/2025, 21:11:36.225	1=TEXT	113	["messageType":"hello","uuid":"08a32d8291b54dd3a
#2.3	13/12/2025, 21:16:36.213	9=PING	0	
#2.4	13/12/2025, 21:16:36.213	10=PONG	0	
#2.5	13/12/2025, 21:21:36.417	9=PING	0	
#2.6	13/12/2025, 21:21:36.417	10=PONG	0	
#2.7	13/12/2025, 21:25:43.325	1=TEXT	94	["messageType":"broadcast_subscribe","broadcast
#2.8	13/12/2025, 21:25:43.542	1=TEXT	96	["messageType":"broadcast","broadcasts":["remote
#2.9	13/12/2025, 21:26:36.646	9=PING	0	
#2.10	13/12/2025, 21:26:36.648	10=PONG	0	
#3.1	13/12/2025, 21:31:41.306	1=TEXT	100	["messageType":"hello","broadcasts":[],"use_webpu
#3.2	13/12/2025, 21:31:41.536	1=TEXT	113	["messageType":"hello","uuid":"c7fbcb157aca442d9

## Active scan:

The screenshot shows the ZAP Active Scan interface. The top panel displays the 'Header Text' of a response, which is an HTTP 200 OK status. The main panel shows a list of messages with columns for ID, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Header, and Size Resp. Body. The messages are numbered 369 through 389. The bottom panel shows the 'Alerts' section with a search bar and a list of alerts.

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
369	13/12/25, 9:13:16 pm	13/12/25, 9:13:16 pm	GET	https://juice-shop.herokuapp.com/info.php	200 OK		222 ms	981 bytes	75,055 bytes
370	13/12/25, 9:13:16 pm	13/12/25, 9:13:16 pm	GET	https://juice-shop.herokuapp.com/.php	200 OK		200 ms	981 bytes	75,055 bytes
371	13/12/25, 9:13:16 pm	13/12/25, 9:13:17 pm	GET	https://juice-shop.herokuapp.com/test.php	200 OK		201 ms	981 bytes	75,055 bytes
372	13/12/25, 9:13:17 pm	13/12/25, 9:13:17 pm	GET	https://juice-shop.herokuapp.com/_wpeprivate/config.json	200 OK		371 ms	981 bytes	75,055 bytes
373	13/12/25, 9:13:17 pm	13/12/25, 9:13:17 pm	GET	https://juice-shop.herokuapp.com/_framework/blazor/boot.js	200 OK		197 ms	977 bytes	75,055 bytes
374	13/12/25, 9:13:17 pm	13/12/25, 9:13:17 pm	GET	https://juice-shop.herokuapp.com/hg	200 OK		234 ms	977 bytes	75,055 bytes
375	13/12/25, 9:13:17 pm	13/12/25, 9:13:18 pm	GET	https://juice-shop.herokuapp.com/bzr	200 OK		383 ms	977 bytes	75,055 bytes
376	13/12/25, 9:13:18 pm	13/12/25, 9:13:18 pm	GET	https://juice-shop.herokuapp.com/_darc	200 OK		369 ms	977 bytes	75,055 bytes
377	13/12/25, 9:13:18 pm	13/12/25, 9:13:18 pm	GET	https://juice-shop.herokuapp.com/BKKeeper	200 OK		185 ms	981 bytes	75,055 bytes
378	13/12/25, 9:13:18 pm	13/12/25, 9:13:19 pm	GET	https://juice-shop.herokuapp.com/	200 OK		208 ms	981 bytes	75,055 bytes
379	13/12/25, 9:13:19 pm	13/12/25, 9:13:19 pm	GET	https://juice-shop.herokuapp.com/	200 OK		185 ms	981 bytes	75,055 bytes
380	13/12/25, 9:13:19 pm	13/12/25, 9:13:19 pm	GET	https://juice-shop.herokuapp.com/	200 OK		193 ms	981 bytes	75,055 bytes
381	13/12/25, 9:13:19 pm	13/12/25, 9:13:19 pm	GET	https://juice-shop.herokuapp.com/	200 OK		192 ms	977 bytes	75,055 bytes
382	13/12/25, 9:13:19 pm	13/12/25, 9:13:20 pm	GET	https://juice-shop.herokuapp.com/	200 OK		449 ms	977 bytes	75,055 bytes
383	13/12/25, 9:13:20 pm	13/12/25, 9:13:20 pm	GET	https://juice-shop.herokuapp.com/	200 OK		173 ms	977 bytes	75,055 bytes
384	13/12/25, 9:13:20 pm	13/12/25, 9:13:20 pm	GET	https://juice-shop.herokuapp.com/	200 OK		195 ms	977 bytes	75,055 bytes
385	13/12/25, 9:13:20 pm	13/12/25, 9:13:20 pm	GET	https://juice-shop.herokuapp.com/	200 OK		193 ms	973 bytes	75,055 bytes
386	13/12/25, 9:13:20 pm	13/12/25, 9:13:20 pm	GET	https://juice-shop.herokuapp.com/	200 OK		216 ms	973 bytes	75,055 bytes
387	13/12/25, 9:13:20 pm	13/12/25, 9:13:21 pm	GET	https://juice-shop.herokuapp.com/	200 OK		198 ms	973 bytes	75,055 bytes
388	13/12/25, 9:13:21 pm	13/12/25, 9:13:21 pm	GET	https://juice-shop.herokuapp.com/	200 OK		191 ms	973 bytes	75,055 bytes
389	13/12/25, 9:13:21 pm	13/12/25, 9:13:21 pm	GET	https://juice-shop.herokuapp.com/	200 OK		200 ms	973 bytes	75,055 bytes