

# Web Application Security Assessment Report

## Introduction

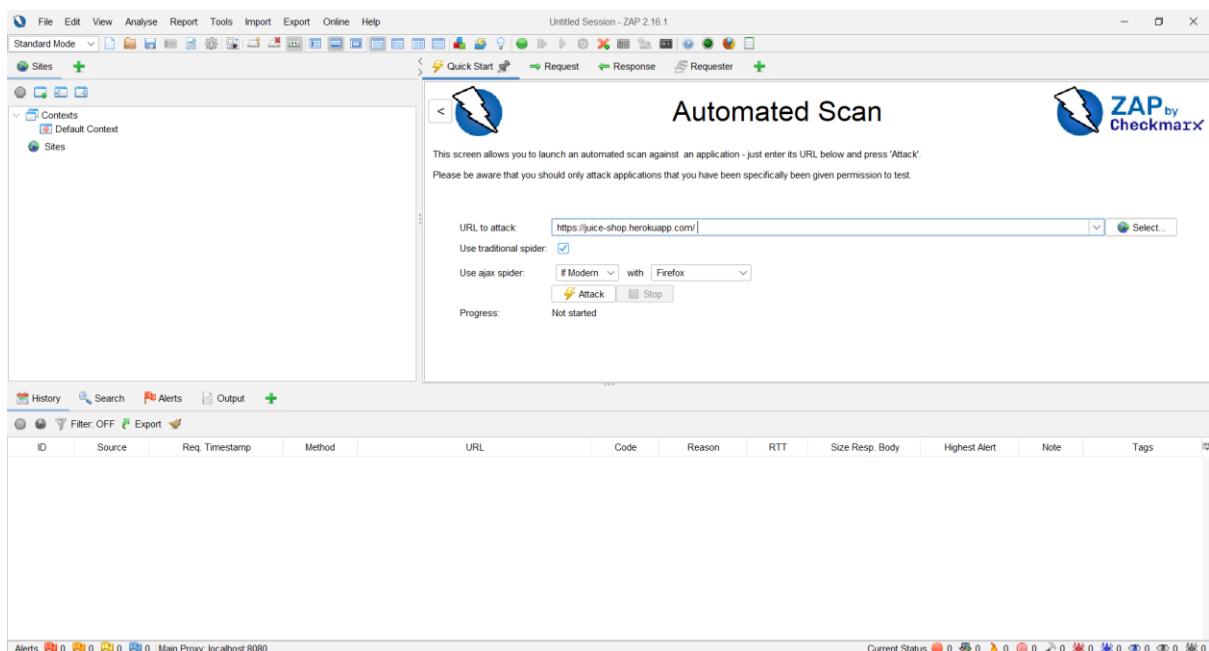
- Objective: Identify security vulnerabilities
  - Application Tested: OWASP Juice Shop
  - Reference: <https://owasp.org/www-project-juice-shop/>
  - Tool Used: OWASP ZAP
  - Testing Type: Automated security assessment

## 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 image displays three vertically stacked screenshots of the ZAP (Zed Attack Proxy) application version 2.16.1. Each screenshot shows an 'Automated Scan' dialog box with the URL <https://juice-shop.herokuapp.com/> entered. The dialog box contains a warning message: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test."

In the first screenshot, the 'Content Security Policy (CSP) Header Not Set' alert is selected. The details pane shows:

- 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:

In the second and third screenshots, the 'Content Security Policy (CSP) Header Not Set' alert is also selected, but the details pane shows a different set of alert references:

- Key: OWASP\_2021\_A05
- Value: https://owasp.org/Top10/A05\_2021-Security\_Misconfiguration/
- Key: POLICY\_QA\_STD
- Value: https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
- Key: POLICY\_PENTEST
- Value: https://cwe.mitre.org/data/definitions/693.html
- Key: SYSTEMIC
- Value: https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
- Key: CWE-693
- Value: https://cwe.mitre.org/data/definitions/693.html

## 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:**

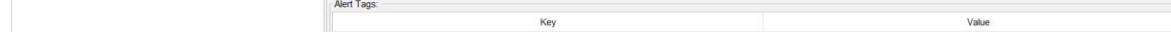
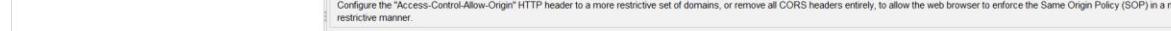
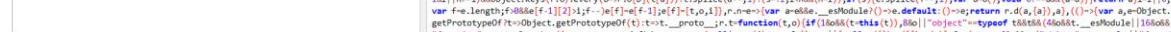
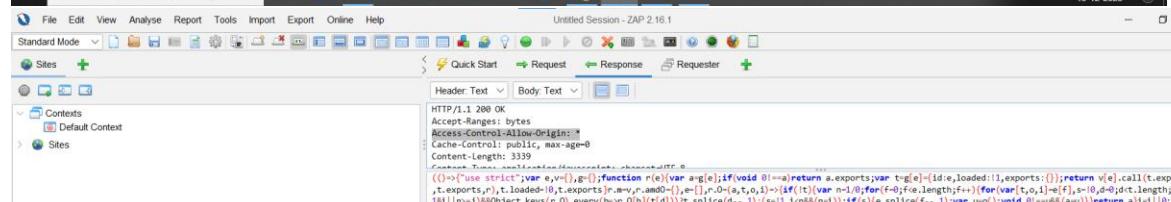
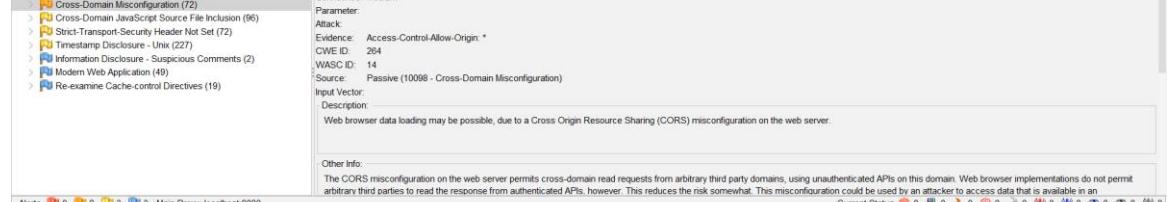
Attackers may exploit this misconfiguration to access or manipulate data from other domains.

## OWASP Category:

## A05 – Security Misconfiguration

## Screenshot:

The screenshot shows the ZAP interface with a captured session named "Untitled Session - ZAP 2.16.1". A request is being analyzed for a POST to "/script.js" with a JSON payload. The response is a 200 OK with a large, obfuscated JavaScript payload. The browser tab shows the page is loading.



### **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:**

Strict-Transport-Security Header Not Set

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

Risk: Low

Confidence: High

Attack: Strict-Transport-Security Header Not Set

Evidence:

- CWE ID: 319
- WASC ID: 15
- Source: Passive (10035 - Strict-Transport-Security Header)
- Alert Reference: 10035-1

Input Vector:

Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Reference:

### **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.

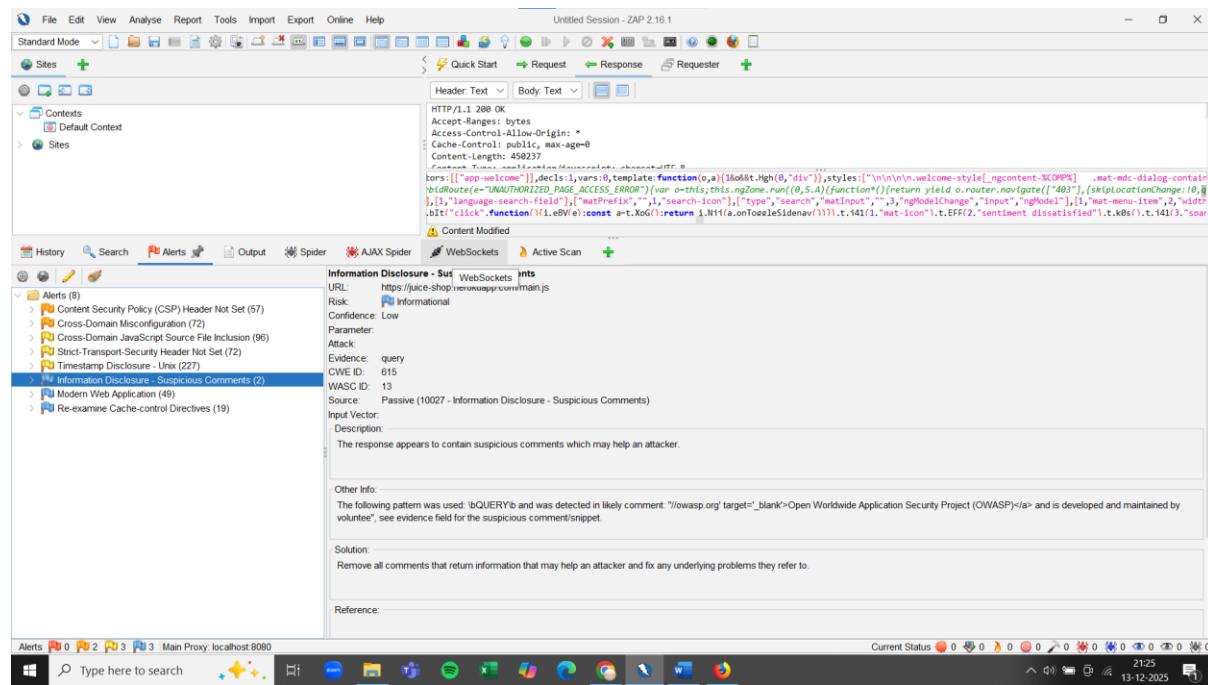
### **Impact:**

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 screenshot displays two instances of the ZAP (Zed Attack Proxy) application interface. Both instances show an 'Alerts' tab selected, indicating a 'Timestamp Disclosure - Unix' issue. The details pane shows the following information:

- Timestamp Disclosure - Unix**
- URL:** https://juice-shop.herokuapp.com/assets/public/favicon\_js.ico
- Risk:** Low
- Confidence:** Low
- Parameter:** Reporting-Endpoints
- Attack:**
- Evidence:** 1765640450
- CWE ID:** 497
- WASC ID:** 13
- Source:** Passive (10096 - Timestamp Disclosure)
- Input Vector:**
- 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 ZAP interface includes a top navigation bar with tabs like File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help, and a bottom status bar showing current status and date/time.

## 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:

Screenshot of ZAP 2.16.1 showing the Spider tool running against the URL <https://juice-herokuapp.com/>. The spider has found 111 URLs and added 71 nodes. The interface displays the following details:

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	886 bytes	28 bytes	Medium	
	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	960 bytes	15,086 bytes	Medium	
	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	
	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	
	13/12/25, 9:10:50 pm	GET	<a href="https://juice-shop.herokuapp.com/polylis.js">https://juice-shop.herokuapp.com/polylis.js</a>	200	OK	713 ms	989 bytes	34,844 bytes	Medium	
	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	Upload
	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	215 s	993 bytes	1,692,128 bytes	Medium	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	618 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/acquisition_md">https://juice-shop.herokuapp.com/ftp/acquisition_md</a>	200	OK	617 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/announcement_enc">https://juice-shop.herokuapp.com/ftp/announcement_enc</a>	200	OK	1.29 s	986 bytes	369,237 bytes	Medium	
	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	
	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/easter_eggs">https://juice-shop.herokuapp.com/ftp/easter_eggs</a>	403	Forbidden	253 ms	856 bytes	1,864 bytes	Medium	
	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/encrypt_pyc">https://juice-shop.herokuapp.com/ftp/encrypt_pyc</a>	403	Forbidden	252 ms	856 bytes	1,864 bytes	Medium	
	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/incident-support_kdt">https://juice-shop.herokuapp.com/ftp/incident-support_kdt</a>	200	OK	251 ms	978 bytes	3,246 bytes	Medium	
	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	
	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/package-lock.json.bak">https://juice-shop.herokuapp.com/ftp/package-lock.json.bak</a>	403	Forbidden	683 ms	856 bytes	1,864 bytes	Medium	
	13/12/25, 9:10:56 pm	GET	<a href="https://juice-shop.herokuapp.com/ftp/package.json.bak">https://juice-shop.herokuapp.com/ftp/package.json.bak</a>	403	Forbidden	674 ms	856 bytes	1,864 bytes	Medium	
	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	

The interface also shows the Headers and Response tabs, and the bottom status bar indicates the current status and date (21:34, 13-12-2025).

## Websockets:

Header/Request Tab (Selected):

```

HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Content-Length: 15886
Content-Type: image/x-icon
Date: Sat, 13 Dec 2025 15:40:50 GMT
Etag: W/"3ae-19a@cfcae038"
    
```

Channel Tab (Selected):

Channel	Timestamp	Opcode	Bytes	Payload
#2.1	13/12/2025, 21:11:35.993	1=TEXT	58	{"messageType": "hello", "broadcasts": [], "use_webpu": 113}
#2.2	13/12/2025, 21:11:36.225	1=TEXT	0	
#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": 96}
#2.8	13/12/2025, 21:25:43.542	1=TEXT	96	{"messageType": "broadcast", "broadcasts": [{"remote": 100}], "use_webpu": 113}
#2.9	13/12/2025, 21:26:36.648	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": 113}
#3.2	13/12/2025, 21:31:41.536	1=TEXT	100	{"messageType": "hello", "uid": "c7fbc157aca442d9", "use_webpu": 113}

## Active scan:

Header/Request Tab (Selected):

```

HTTP/1.1 200 OK
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Content-Length: 15886
Content-Type: image/x-icon
Date: Sat, 13 Dec 2025 15:40:50 GMT
Etag: W/"3ae-19a@cfcae038"
    
```

Sent Messages Tab (Selected):

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/info.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/_wepnprivate/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/_dars	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/_BitKeeper	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