**Summary Report from the ZAP Scan on 10/26/24**

**\*All the information in this document was provided by OWASP ZAP\***

1. **Risk = High, Confidence = Medium (1)**

* **SQL Injection Vulnerability Lite**

**------------------------------------------**

**Alert Tags:**

**------------------------------------------**

* [OWASP\_2017\_A01](https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html)
* [OWASP\_2021\_A03](https://owasp.org/Top10/A03_2021-Injection/)
* [CWE-89](https://cwe.mitre.org/data/definitions/89.html)
* [WSTG-v42-INPV-05](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection)

**Site:** GET https://juice-shop.herokuapp.com/rest/products/search?q=%27%28

**SQL injection may be possible.**

-------------------------------------------

**Other information:** RDBMS [SQLite] likely, given error message regular expression [SQLITE\_ERROR] matched by the HTML results.

The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.

**Request Information:** GET https://juice-shop.herokuapp.com/rest/products/search?q=%27%28 HTTP/1.1

host: juice-shop.herokuapp.com

user-agent: Mozilla/5.0 (Windows NT 10.0; rv:125.0) Gecko/20100101 Firefox/125.0

pragma: no-cache

cache-control: no-cache

**Response:** HTTP/1.1 500 Internal Server Error

Server: Cowboy

Report-To: {"group":"heroku-nel","max\_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1729975518&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=0FE%2F0jZvcFl4ZnQkbGbnnrT%2BvJCWrKkXpM85Osbd64o%3D"}]}

Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1729975518&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=0FE%2F0jZvcFl4ZnQkbGbnnrT%2BvJCWrKkXpM85Osbd64o%3D

Nel: {"report\_to":"heroku-nel","max\_age":3600,"success\_fraction":0.005,"failure\_fraction":0.05,"response\_headers":["Via"]}

Connection: keep-alive

Access-Control-Allow-Origin: \*

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

Feature-Policy: payment 'self'

X-Recruiting: /#/jobs

Content-Type: text/html; charset=utf-8

Vary: Accept-Encoding

Date: Sat, 26 Oct 2024 20:45:18 GMT

Via: 1.1 vegur

content-length: 974

Response body (974 bytes)

<html>

<head>

<meta charset='utf-8'>

<title>Error: SQLITE\_ERROR: near &quot;(&quot;: syntax error</title>

<style>\* {

margin: 0;

padding: 0;

outline: 0;

}

body {

padding: 80px 100px;

font: 13px "Helvetica Neue", "Lucida Grande", "Arial";

background: #ECE9E9 -webkit-gradient(linear, 0% 0%, 0% 100%, from(#fff), to(#ECE9E9));

background: #ECE9E9 -moz-linear-gradient(top, #fff, #ECE9E9);

background-repeat: no-repeat;

color: #555;

-webkit-font-smoothing: antialiased;

}

h1, h2 {

font-size: 22px;

color: #343434;

}

h1 em, h2 em {

padding: 0 5px;

font-weight: normal;

}

h1 {

font-size: 60px;

}

h2 {

margin-top: 10px;

}

ul li {

list-style: none;

}

#stacktrace {

margin-left: 60px;

}

</style>

</head>

<body>

<div id="wrapper">

<h1>OWASP Juice Shop (Express ^4.17.1)</h1>

<h2><em>500</em> Error: SQLITE\_ERROR: near &quot;(&quot;: syntax error</h2>

<ul id="stacktrace"></ul>

</div>

</body>

</html>

**Parameter:** q

**Attack Evidence:** ‘ (

**Evidence**: SQLITE\_ERROR

**Solution:**

------------------------------------

Do not trust client side input, even if there is client side validation in place.

In general, type check all data on the server side.

If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

If database Stored Procedures can be used, use them.

Do \*not\* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!

Do not create dynamic SQL queries using simple string concatenation.

Escape all data received from the client.

Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.

Apply the principle of least privilege by using the least privileged database user possible.

In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.

Grant the minimum database access that is necessary for the application.

1. **Risk = Medium, Confidence = High (1 of 3)**

* **CSP: Wildcard Directive:**

-------------------------------------------

**Alert Tags:**

**-----------------------------**

* [CWE-693](https://cwe.mitre.org/data/definitions/693.html)
* [OWASP\_2021\_A05](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)
* [OWASP\_2017\_A06](https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html)

**Site:** GET <https://juice-shop.herokuapp.com/assets>

**Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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 Information:** The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:

frame-ancestors, form-action

The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

**Request Information:** GET https://juice-shop.herokuapp.com/assets HTTP/1.1

host: juice-shop.herokuapp.com

user-agent: Mozilla/5.0 (Windows NT 10.0; rv:125.0) Gecko/20100101 Firefox/125.0

pragma: no-cache

cache-control: no-cache

**Response**: HTTP/1.1 301 Moved Permanently

Server: Cowboy

Report-To: {"group":"heroku-nel","max\_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1729974946&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=%2BVzUnqjk8Pz3eEZHvLcW5WJLeKL8HEiEyus3AyLf2hU%3D"}]}

Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1729974946&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=%2BVzUnqjk8Pz3eEZHvLcW5WJLeKL8HEiEyus3AyLf2hU%3D

Nel: {"report\_to":"heroku-nel","max\_age":3600,"success\_fraction":0.005,"failure\_fraction":0.05,"response\_headers":["Via"]}

Connection: keep-alive

Access-Control-Allow-Origin: \*

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

Feature-Policy: payment 'self'

X-Recruiting: /#/jobs

Content-Type: text/html; charset=UTF-8

Content-Length: 179

Content-Security-Policy: default-src 'none'

Location: /assets/

Vary: Accept-Encoding

Date: Sat, 26 Oct 2024 20:35:46 GMT

Via: 1.1 vegur

Response body (179 bytes)

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Redirecting</title>

</head>

<body>

<pre>Redirecting to <a href="/assets/">/assets/</a></pre>

</body>

</html>

**Parameter:** Content-Security-Content

**Evidence:** default-src 'none'

**Solution:**

----------------------------

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

1. **Risk = Medium, Confidence = (Medium 2 of 3)**

* **Cross-Domain-Misconfiguration**

--------------------------------------------------

**Alert Tags:**

**----------------------------**

* [**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)
* [**OWASP\_2021\_A01**](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)

**Site: GET** <https://juice-shop.herokuapp.com/runtime.js>

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

**---------------------------------------------------------------------------------------------------------------------------**

**Other Information**: 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.

**Request Information**: GET https://juice-shop.herokuapp.com/runtime.js HTTP/1.1

host: juice-shop.herokuapp.com

Connection: keep-alive

Origin: https://juice-shop.herokuapp.com

sec-ch-ua-platform: "Windows"

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36

sec-ch-ua: "Chromium";v="130", "Google Chrome";v="130", "Not?A\_Brand";v="99"

sec-ch-ua-mobile: ?0

Accept: \*/\*

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: script

Referer: https://juice-shop.herokuapp.com/

Accept-Language: en-US,en;q=0.9

Cookie: language=en; welcomebanner\_status=dismiss; cookieconsent\_status=dismiss; continueCode=pphytRIVi1SkUqt8ckIvFxf4H5hqsMoupNtvPIQxuWlh9zFrptpZc19SknuqVcjzC8QS2zTa8IwQ

If-None-Match: W/"ce1-191d788a008"

If-Modified-Since: Mon, 09 Sep 2024 16:05:41 GMT

**Response**: HTTP/1.1 304 Not Modified

Server: Cowboy

Content-Length: 0

Report-To: {"group":"heroku-nel","max\_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1729974709&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=feITDpMIgVNMoVJuckeXUFjiKn4pqH9uikCZr990Ij0%3D"}]}

Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1729974709&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=feITDpMIgVNMoVJuckeXUFjiKn4pqH9uikCZr990Ij0%3D

Nel: {"report\_to":"heroku-nel","max\_age":3600,"success\_fraction":0.005,"failure\_fraction":0.05,"response\_headers":["Via"]}

Connection: keep-alive

Access-Control-Allow-Origin: \*

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

Feature-Policy: payment 'self'

X-Recruiting: /#/jobs

Accept-Ranges: bytes

Cache-Control: public, max-age=0

Last-Modified: Mon, 09 Sep 2024 16:05:41 GMT

Etag: W/"ce1-191d788a008"

Date: Sat, 26 Oct 2024 20:31:49 GMT

Via: 1.1 vegur

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

**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.

**This Summary’s End**.

**Completed**: on 10-27-2024

**By:** Thomas Kolenda

**\*All the information in this document was provided by OWASP ZAP\***