

Politechnika Wrocławska, Informatyka Stosowana

# Web security cz.1

Cyberbezpieczeństwo, Laboratorium nr.13 - raport

Autor: Aleksander Stepaniuk  
Nr. Indeksu: 272644

## 4. Pytania

### Pytanie 1;

Nagłówek (http) X-Content-Type-Options – kiedy jest ustawiony na wartość nosniff, uniemożliwia przeglądarce interpretowanie plików o innym typie MIME niż zadeklarowany w odpowiedzi serwera. Chroni przed atakami, w których złośliwy plik (np. skrypt JavaScript) zostaje uruchomiony jako inny typ pliku.

Nagłówek X-Frame-Options kontroluje czy strona może być osadzona w ramkach (tzw. iframe). Ustawienia, takie jak DENY (blokowanie wszystkich ramek) lub SAMEORIGIN (dozwolone tylko z tej samej domeny) chronią przed atakami typu „clickjacking”.

Ataki SQL Injection: Pozwalają na wstrzyknięcie złośliwego nieporządanego kodu SQL poprzez niezabezpieczone pola wejściowe. Osoba atakująca może wykonać takie akcje jak:

- Kradzież danych (np. wyciąganie haseł czy adresów e-mail).
- Modyfikowanie danych (np. zmiana wartości konta).
- Usuwanie baz danych lub całych tabel.
- Uzyskanie dostępu administracyjnego do systemu.

### Pytanie 2;

Jest to istotne, bo zapewnia ochronę przed znaczną częścią ataków wykorzystujących luki w walidacji po stronie klienta czy serwera:

Po stronie klienta:

- Zapewnia lepszą wydajność i szybsze reagowanie dla użytkownika (np. walidacja e-maila przed wysłaniem formularza).

Po stronie serwera:

- Chroni przed manipulacjami, ponieważ walidacja po stronie klienta może być pominięta przez złośliwego użytkownika. Niezabezpieczony serwer jest narażony na ataki, takie jak SQL Injection, XSS lub wysyłanie nieprawidłowych danych.

### Pytanie 3;

- Uwierzytelnianie: upewnić się, że użytkownik jest zalogowany (np. JWT, sesje).
- Autoryzacja: weryfikacja ról i uprawnień użytkownika przed udzieleniem dostępu do zasobu (np. RBAC, czyli „Role-Based Access Control”).
- Mechanizmy na poziomie serwera: Korzystanie z reguł zapory sieciowej, kontroli dostępu (ACL) i odpowiednio skonfigurowanych serwerów aplikacji.
- Zasada najmniejszych uprawnień: Użytkownicy powinni mieć dostęp tylko do zasobów niezbędnych dla ich roli.

## 5. Zadania

### Zadanie 0;

Adresy IP maszyn:

**Kali linux:** 172.16.96.8/24

**Adres sieci:** 172.16.96.0/24

### Zadania 1-3;

Uruchamiam juice-shop

```
File Actions Edit View Help

(stud@kali-vm)-[~/Desktop]
$ cd 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 runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file styles.css is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Server listening on port 3000
```


OWASP Juice Shop

localhost:3000/#/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

OWASP Juice Shop

All Products



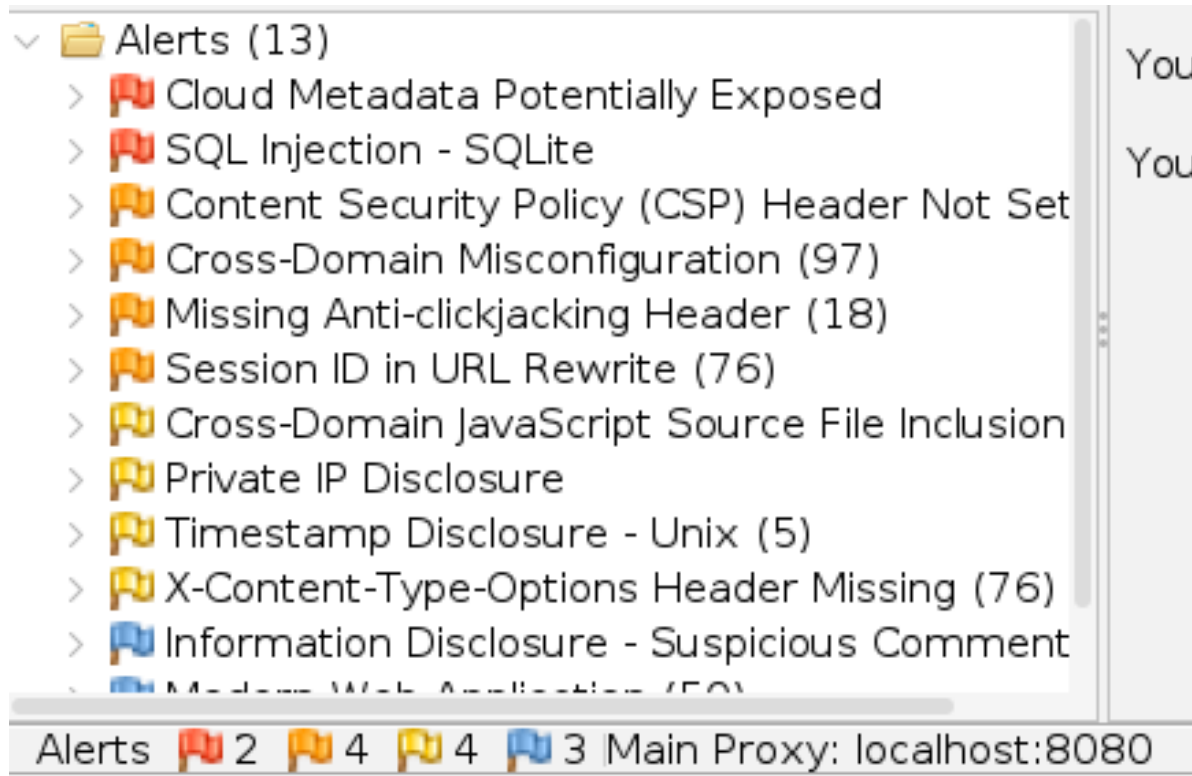
Apple Juice  
(1000ml)

1.99€

## Zadanie 4;

Skanowanie pokazało flagi: (łącznie 13):

- 2 czerwone
- 4 bursztynowe
- 4 żółte
- 3 niebieskie



Skanowanie ujawniło między innymi katalog /assets/public/image/products/ który można wyświetlić w przeglądarce:

Sent Messages		Filtered Messages							
ID	Req. Timestamp	Resp. Timestamp	Meth...	URL	Code	Reason	RTT	Size Re...	Size Re...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/api/Challenges	200	OK	69...	390 by...	79,72...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/api/Quantitys	200	OK	17...	388 by...	6,124 ...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/assets	301	Move...	1 ...	416 by...	179 by...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/assets/i18n	301	Move...	1 ...	421 by...	189 by...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/assets/public	301	Move...	7 ...	423 by...	193 by...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/assets/public/images	301	Move...	0 ...	430 by...	207 by...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/assets/public/images/products	301	Move...	1 ...	439 by...	225 by...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/home	200	OK	14...	466 by...	3,748 ...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/home/stud	200	OK	14...	466 by...	3,748 ...
11,...	1/21/25, 8:48:30 ...	1/21/25, 8:48:30 ...	GET	http://localhost:3000/home/stud/Desktop	200	OK	12...	466 by...	3,748 ...
Alerts 2 4 4 4 3 Main Proxy: localhost:8080					Current Scans 0				



## Zadania 5-7;

W historii zapa pojawia się request z naszej sesji firefoxa.

ID	Sour...	Req. Timestamp	Meth...	URL	Co...	Reason	R...	Size Resp. B...	Highest Al...	N...	Tags
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/rest/admin/applicati...	304	Not Mo...	2...	0 bytes	Medium		
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/rest/admin/applicati...	200	OK	6...	20,381 bytes	Medium		JSON
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/socket.io/?EIO=4&t...	200	OK	8...	32 bytes			
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/socket.io/?EIO=4&t...	101	Switchi...	8...	0 bytes			
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/Materialcons-Regul...	200	OK	9...	60,840 bytes	Medium		Comment
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/rest/languages	200	OK	1...	4,881 bytes	Medium		JSON
11,...	Pr...	1/21/25, 9:15:14...	GET	http://localhost:3000/socket.io/?EIO=4&t...	200	OK	1...	1 bytes	Medium		
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/rest/products/searc...	200	OK	1...	13,659 bytes			
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/api/Challenges/?na...	200	OK	2...	648 bytes	Medium		JSON
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/api/Quantities/	200	OK	2...	6,124 bytes	Medium		JSON
11,...	Pr...	1/21/25, 9:15:13...	GET	http://localhost:3000/api/Challenges/?na...	200	OK	2...	648 bytes			

Alerts 2 4 4 3 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0 0 0

## Zadania 8-11;

## User Registration

Email \*

test@test.pl

Password \*

●●●●●●●●

ⓘ Password must be 5-40 characters long.

9/20

Repeat Password \*

●●●●●●●●

9/40

Show password advice

Security Question \*

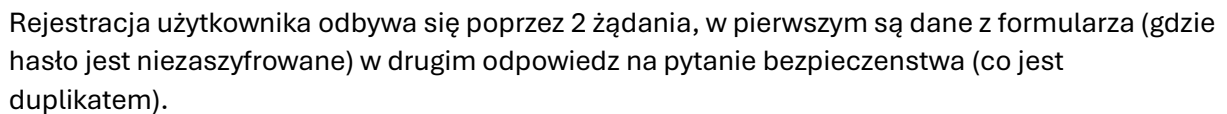
Mother's birth date? (MM/DD/YY) ▼

ⓘ This cannot be changed later!

Answer \*

01/01/01

+ Register



</

## Zadania 12-17;

Składamy complainta (file size = 25kb)

# Complaint

Customer
temp@admin.pl

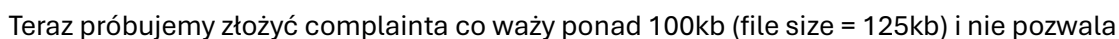
Message \*

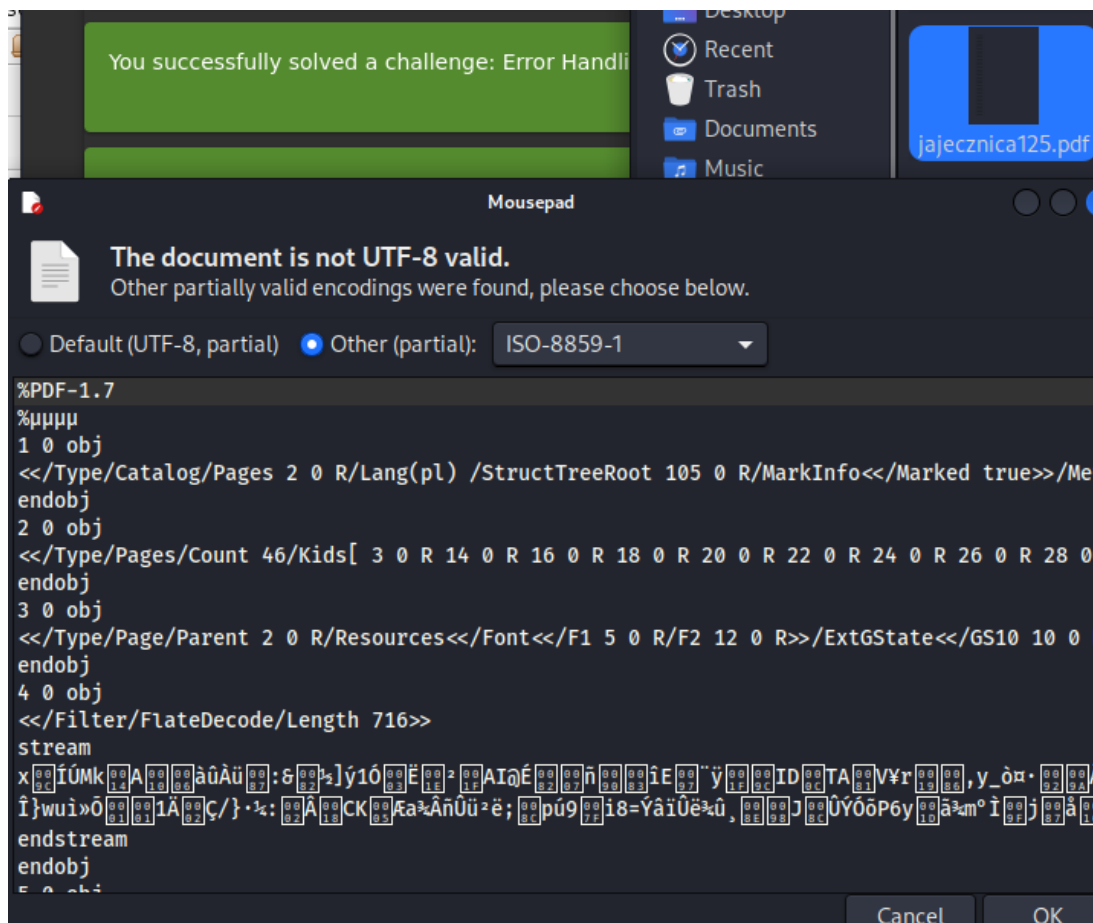
Max. 160 characters
0/160

Invoice:
Browse...
jajecznic25.pdf

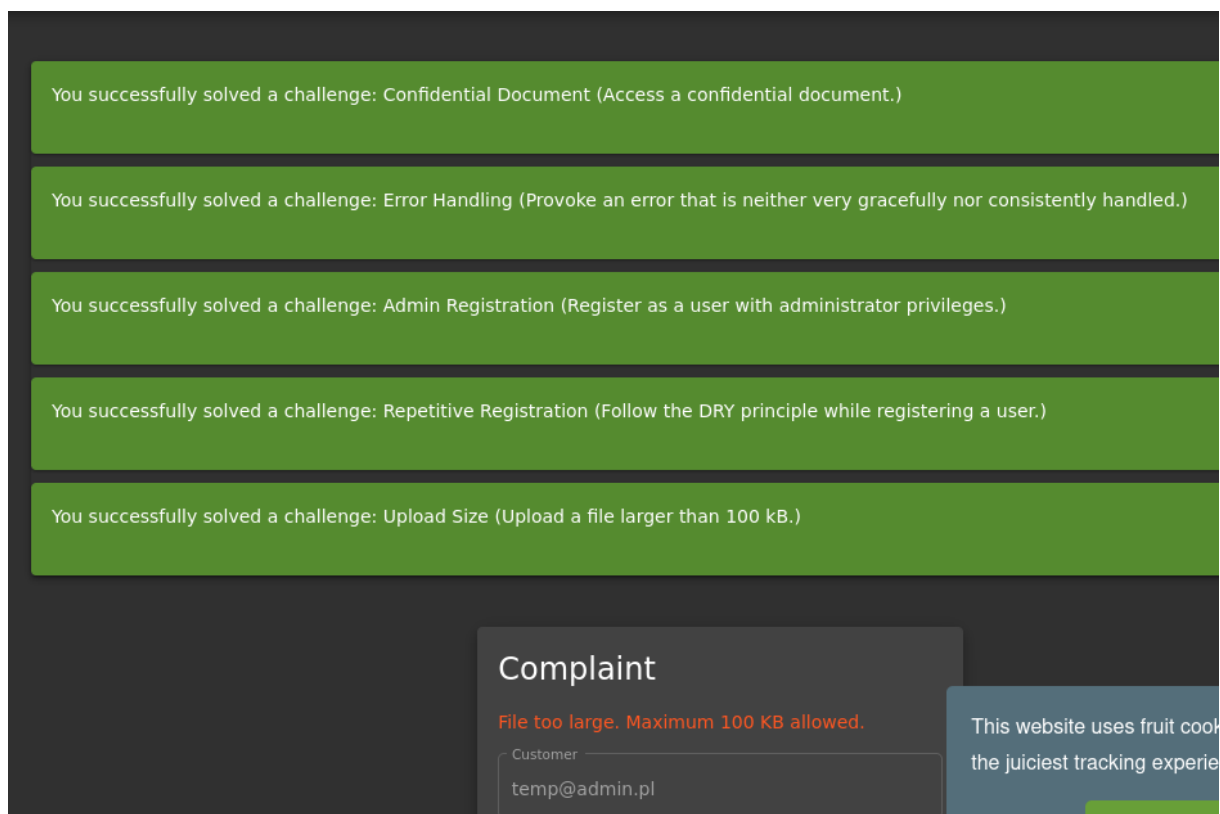
Submit



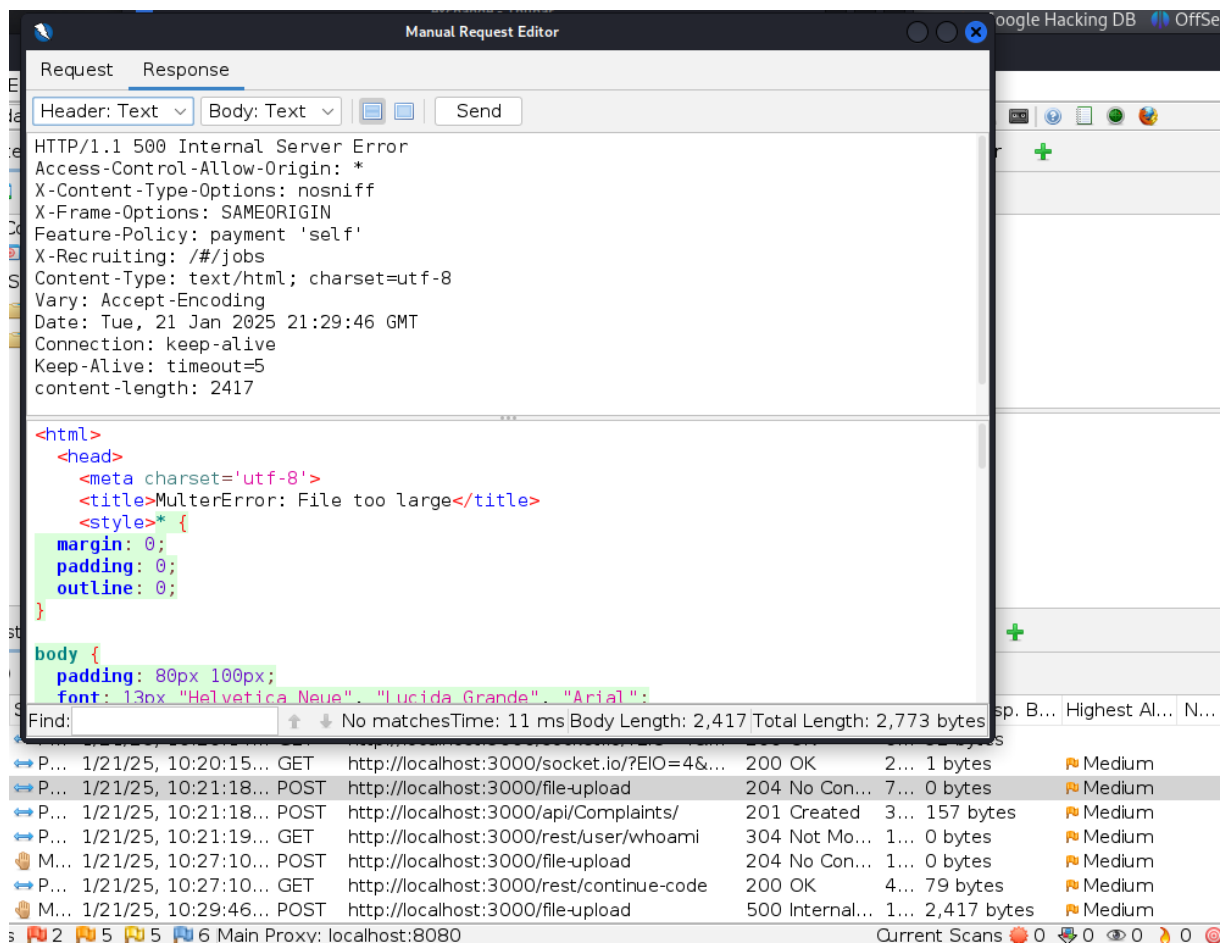




Udało się wrzucić przez ZAPa plik powyżej 100kb.

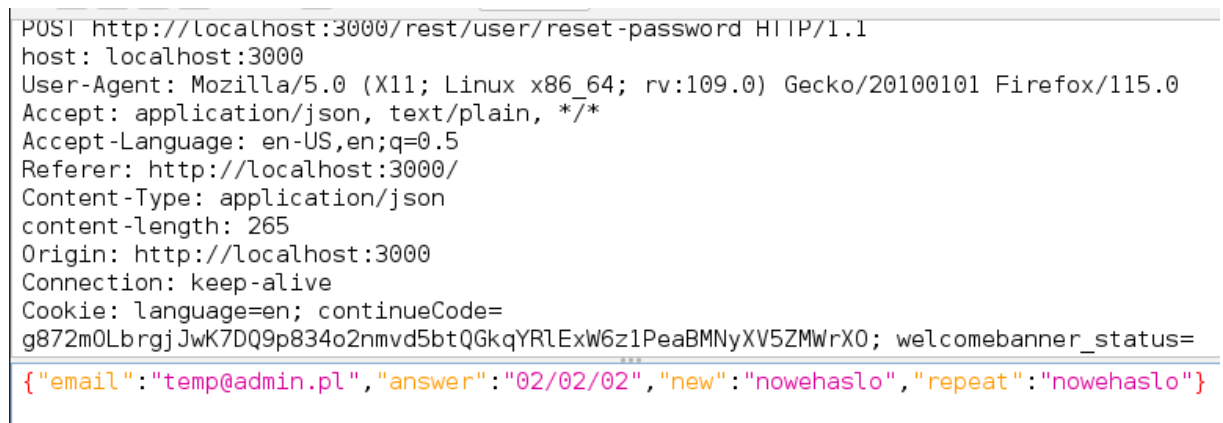


Teraz próba wrzucenia pliku powyżej 200kb: (błąd)



Teraz wniosek jest taki, że największy możliwy do wrzucenia plik przez interfejs webowy to 100kb, natomiast błędna walidacja danych wejściowych po stronie serwera sprawia, że limit ten wynosi tak naprawdę 200kb.

## Zadania 18-20;



# Forgot Password

Email \*  ?

Security Question \*  ?

New Password \*

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

Repeat New Password \*

6/20

☐ Show password advice

Change

Fuzzer

Fuzz LocationsOptionsMessage Processors

Header: TextBody: TextEdit

POST http://localhost:3000/rest/user/reset-password  
HTTP/1.1  
host: localhost:3000  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: application/json, text/plain, \*/\*  
Accept-Language: en-US,en;q=0.5  
Referer: http://localhost:3000/  
Content-Type: application/json  
content-length: 84  
Origin: http://localhost:3000  
Connection: keep-alive  
Cookie: language=en; continueCode=g872m0LbrgjJwK7DQ9p834o2nmvd5btQGkqYRLExW6z1PeaBMNyXV5ZMwRX0; welcomebanner\_status=dismiss  
  

```
{ "email": "temp@admin.pl", "answer": "02", "new": "nowehaslo", "repeat": "nowehaslo" }
```

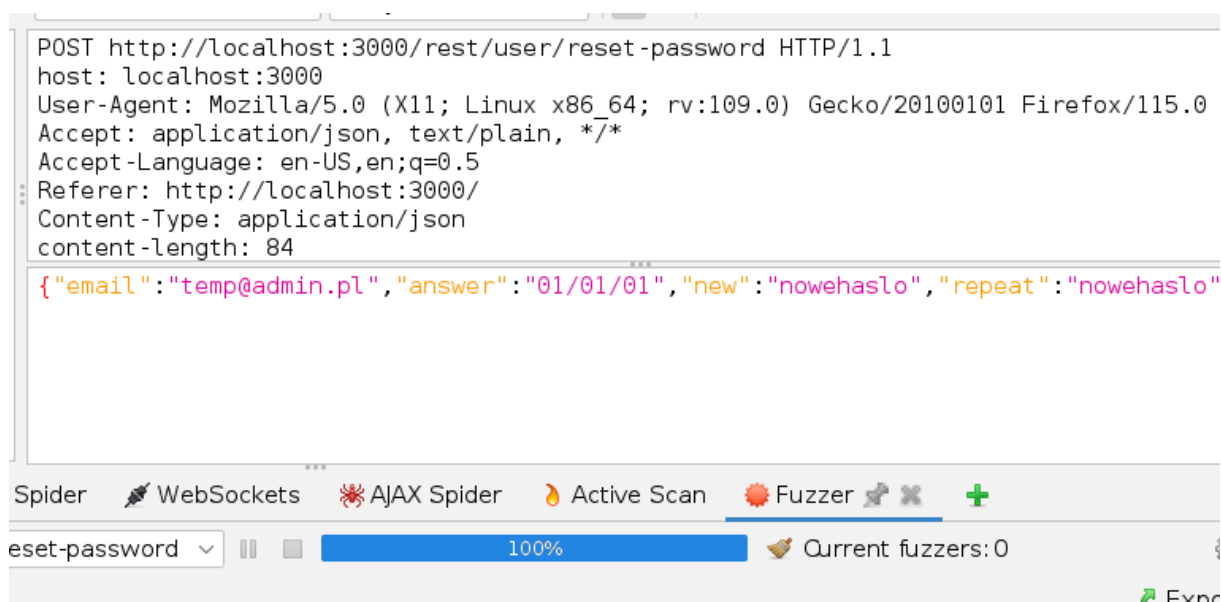
Fuzz Locations:

Locati...	Value	# of Paylo...	# of Processors
Body [3... 02		30	0
Body [3... 02		11	0
Body [4... 02		8	0

Add...RemovePayloads...Processors...

Remove without confirmation? ☒

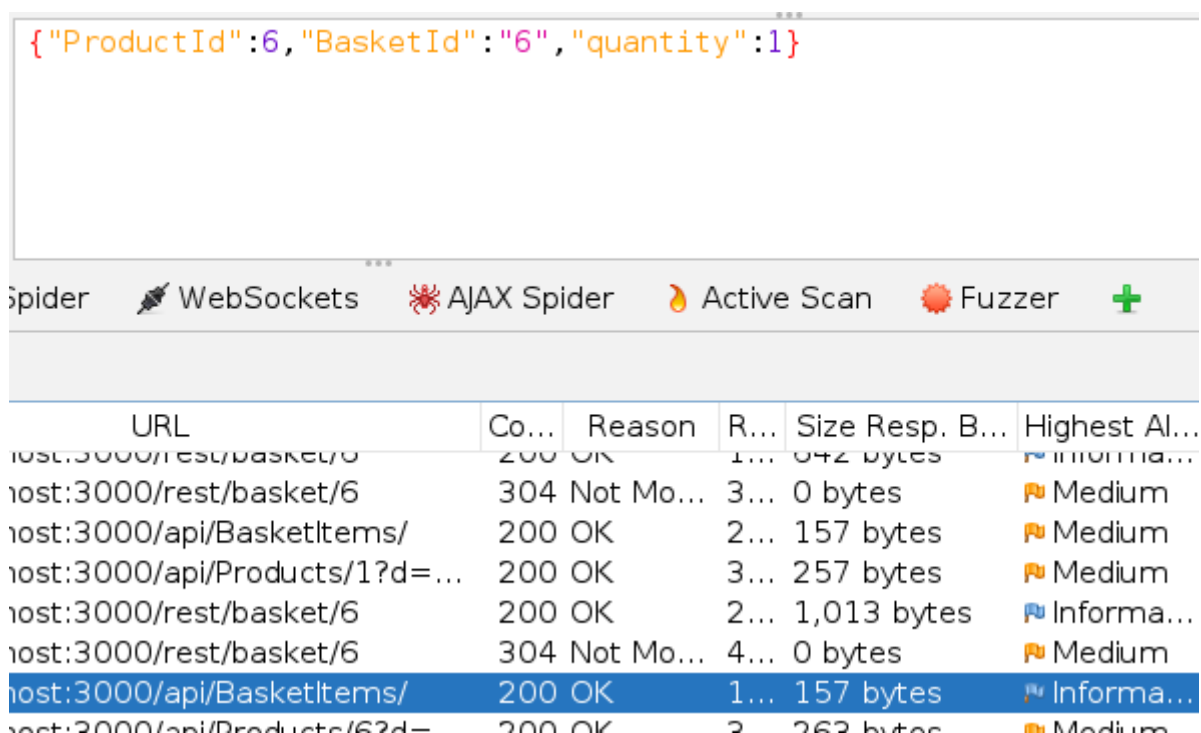
Start FuzzerResetCancel

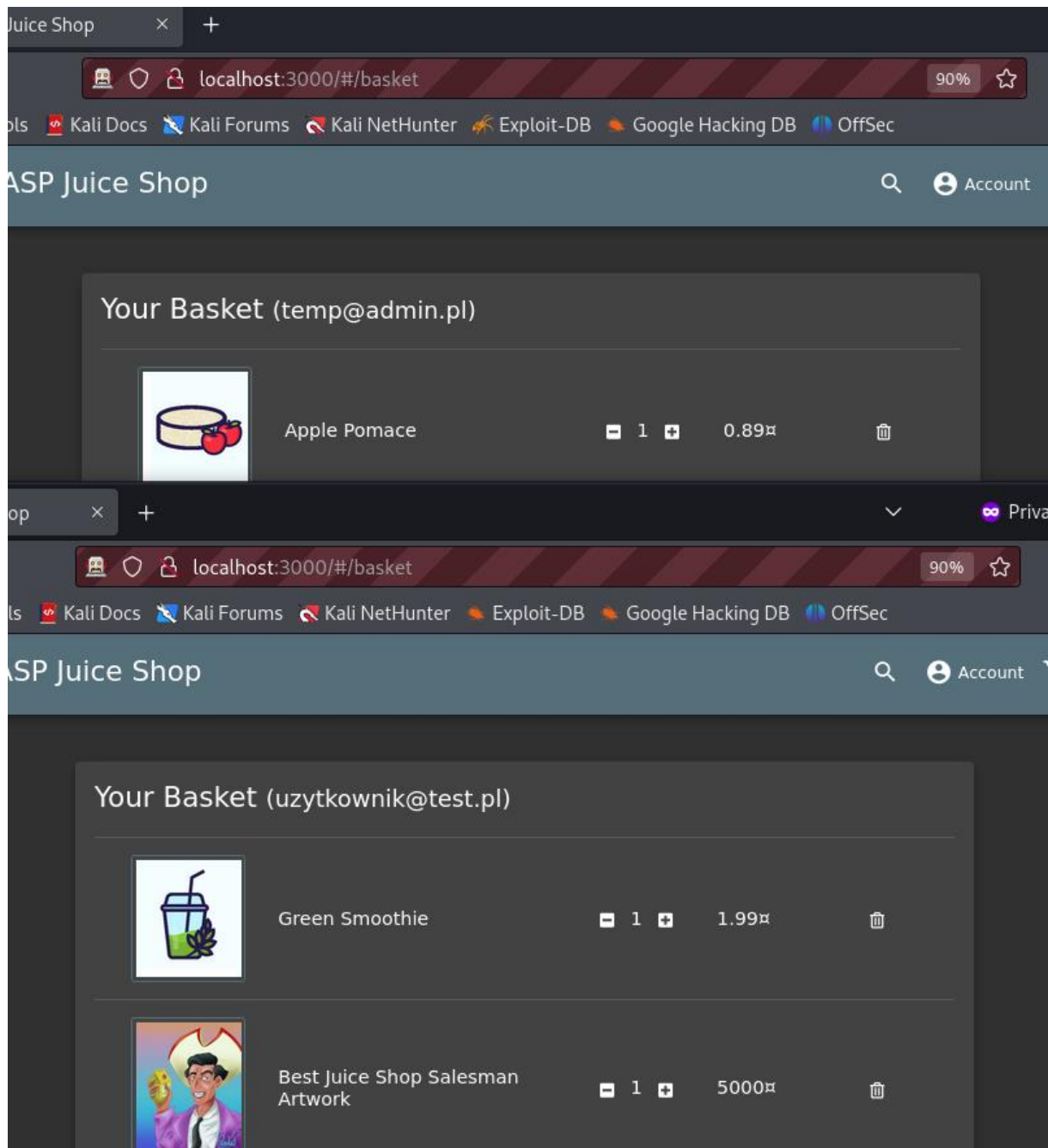


Przypadkowo przekroczyłem limit zapytań (bo w fuzzerze podałem liczby naturalne od 1 do 31, natomiast poprawna wartość to 01, więc nie wpisałem jej i wyczerpałem się limit powiadomień. Tak czy siak finalnie zgadłem poprawną odpowiedź.

## Zadania 21-25;

Id koszyka głównego: (basket id = 6);





Id nowego koszyka: (basket id = 7);

```

{"ProductId":42,"BasketId":"7","quantity":1}

```

Spider   WebSockets   AJAX Spider   Active Scan   Fuzzer   +

URL	Co...	Reason	R...	Size	Resp. B...	Highest Al...	N...
host:3000/api/Quantitys/	304	Not Mo...	2...	0 bytes		Informa...	
host:3000/rest/basket/7	304	Not Mo...	3...	0 bytes		Medium	
host:3000/api/BasketItems/	200	OK	2...	158 bytes		Medium	
host:3000/api/Products/22?d...	200	OK	4...	342 bytes		Medium	
host:3000/rest/basket/7	200	OK	3...	611 bytes		Informa...	
host:3000/rest/basket/7	304	Not Mo...	2...	0 bytes		Medium	
host:3000/api/BasketItems/	200	OK	1...	158 bytes		Informa...	

Header: Text   Body: Text



```

GET http://localhost:3000/rest/basket/7 HTTP/1.1
host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109
Accept: application/json, text/plain, */*

```

You successfully solved a challenge: View Basket (View another user's shopping basket.)

### Your Basket (uzytkownik@test.pl)

	Green Smoothie	1	1.99zł	
---	----------------	---	--------	---