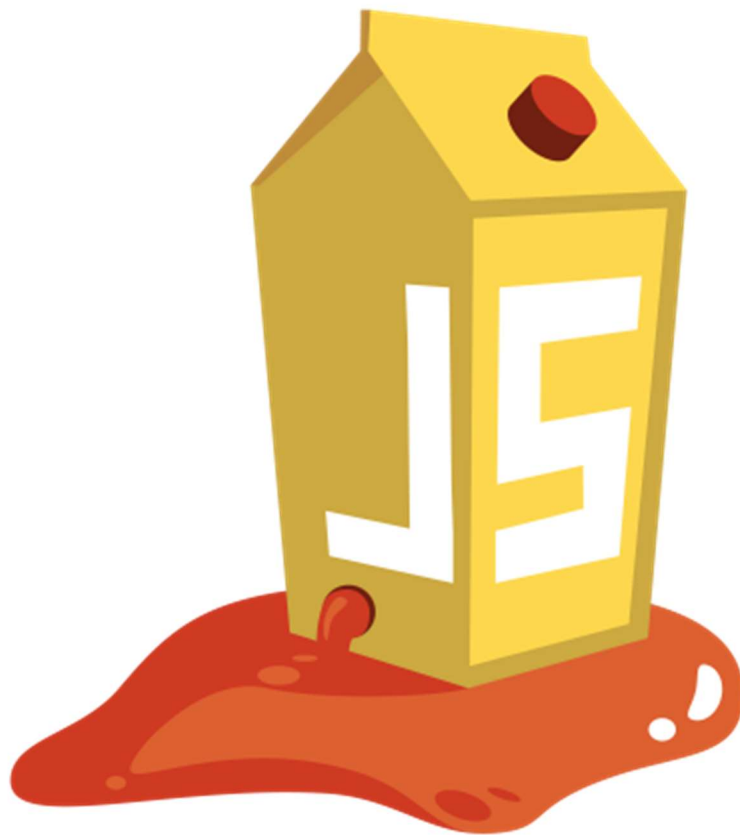


# AAF Praktika: Web penetrazio testak

## -OWASP Juice Shop-



Oier Barrutiabengoa

Euskal Herriko Unibertsitatea (UPV/EHU)

## Aurkibidea

Change Bender's password prozesua .....	3
Kontuaren bilaketa .....	3
Login Benderen kontuan .....	4
Kontuaren pasahitza aldatzen .....	5
Arazoak eta ondorioak.....	9
Ustitutako arazoak .....	9
HTTP errorearen arrazoiak.....	9
Ondorioak.....	9

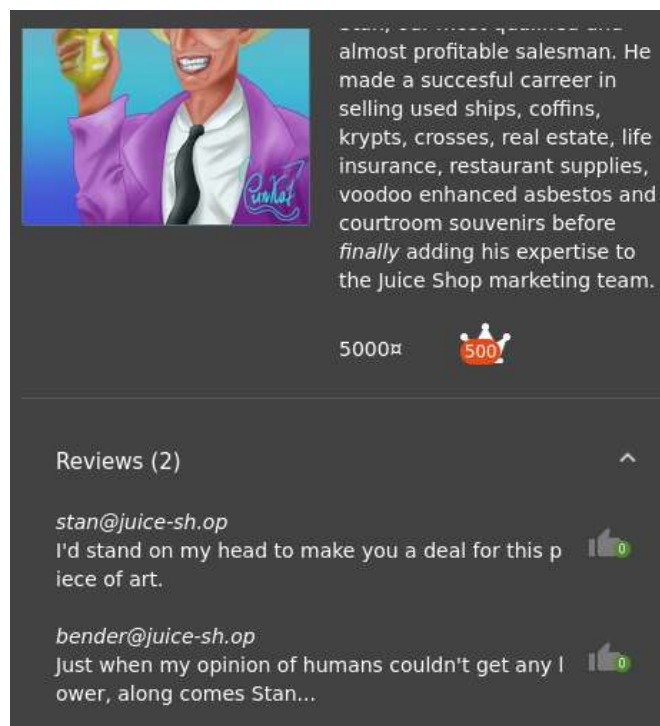
## Change Bender's password prozesua

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



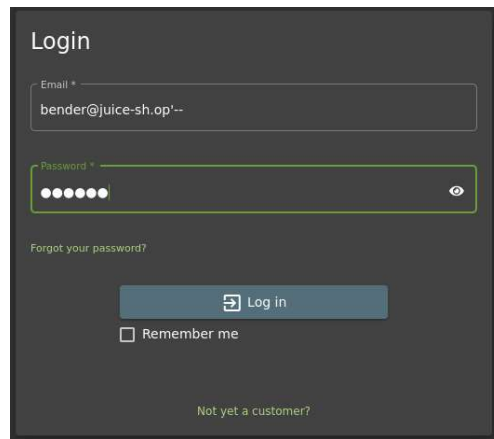
## Kontuaren bilaketa

Ariketa ebazteko lehenengo Benderen emaila lortu behar dugu, hau egiteko [192.168.56.101:3000/#/search](http://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](mailto:bender@juice-sh.op)) kopiatuko dugu.



## Login Benderen kontuan

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



Login

Email \*

bender@juice-sh.op'--

Password \*

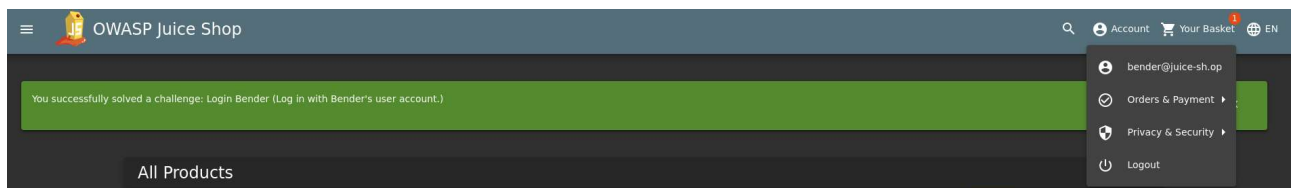
Forgot your password?

Log in

☐ Remember me

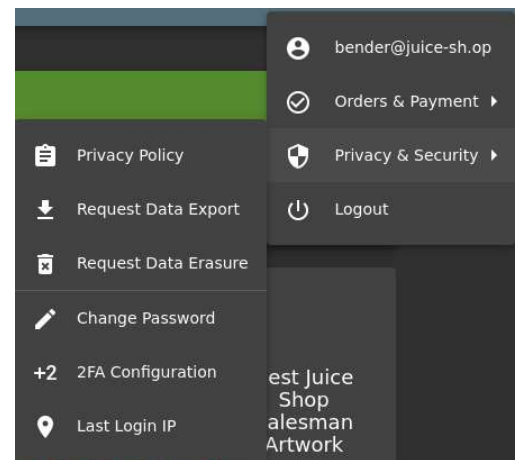
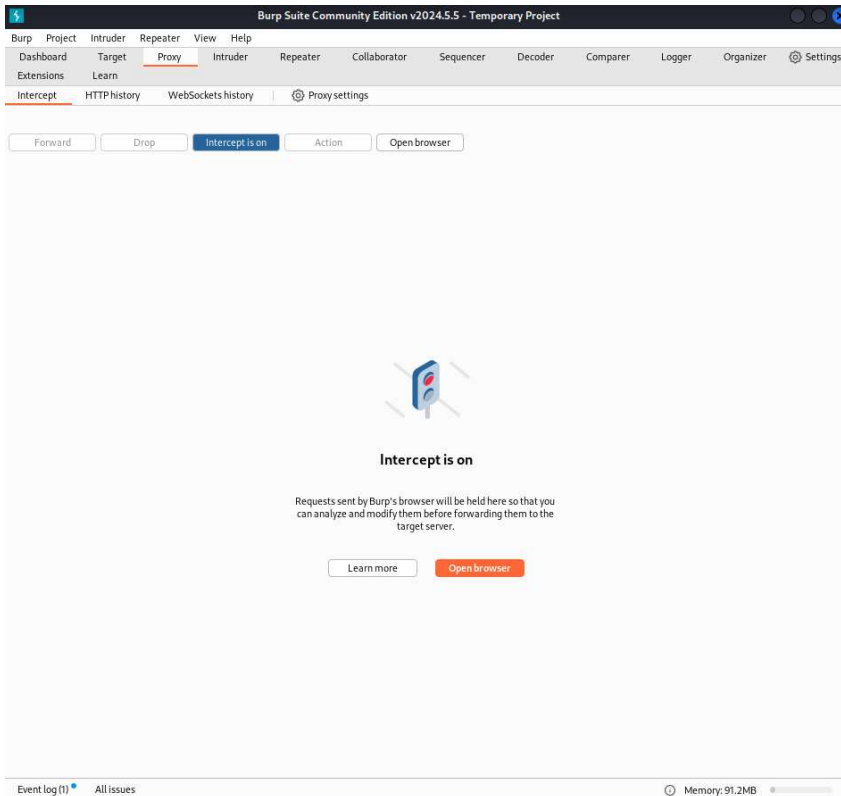
Not yet a customer?

**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** aukerara 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 Password

Current Password \*

New Password \*

Password must be 5-40 characters long.
 5/40

Repeat New Password \*

5/20

Change

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

[illegible]

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

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: text/html; charset=utf-8
8 Content-Length: 32
9 ETag: W/"20-6tKKLCLLg0nzRSqInvJyo/E13vg"
10 Vary: Accept-Encoding
11 Date: Sat, 22 Mar 2025 18:14:52 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 Current password is not correct.
```



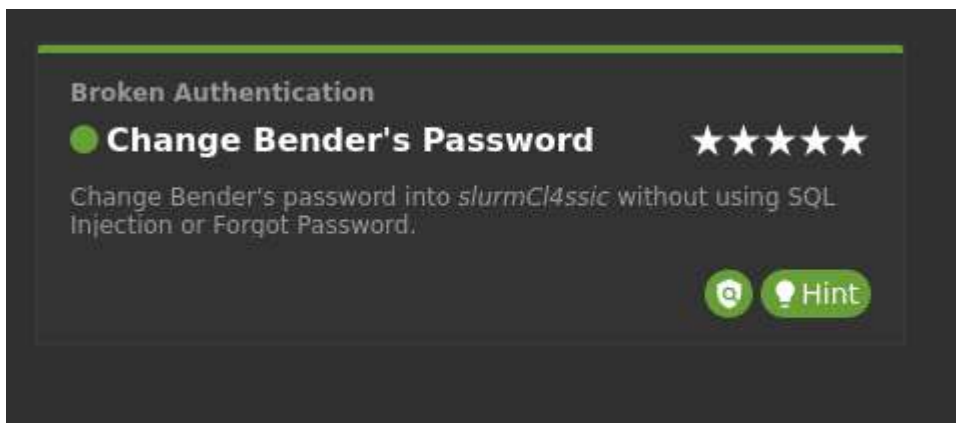
## Request

### Response

7

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 manipulatu.

### 3. HTTP eskaera manipulatzeara

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, sarreraren 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.