OWASP Juice Shop – A07 Identification And Authentication Failures
Praktikum Keamanan Jaringan

Dosen Pembimbing :
Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :

Fifin Nur Rahmawati (3122640040)

Lula Rania Salsabilla (3122640045)

1 D4 – IT B LJ

D4 TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023

Laporan Praktikum

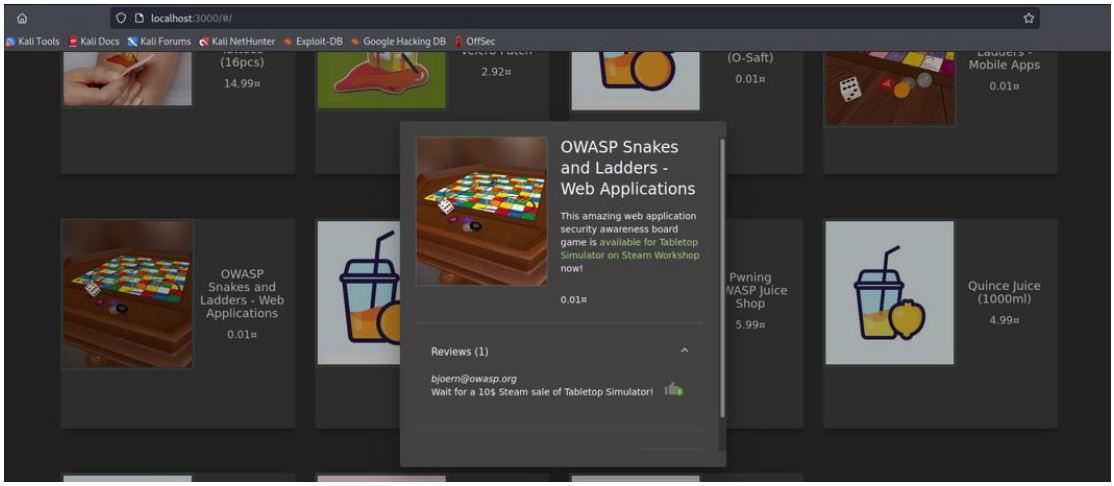
Identification and Authentication Failures

Pada aplikasi OWASP Juice Shop, "Identification and Authentication Failures" adalah salah satu kategori kerentanan yang mungkin terjadi. Ini mengacu pada kegagalan dalam proses identifikasi dan otentikasi pengguna, yang dapat menyebabkan celah keamanan dalam sistem. Beberapa contoh kerentanan yang termasuk dalam kategori ini mungkin mencakup:

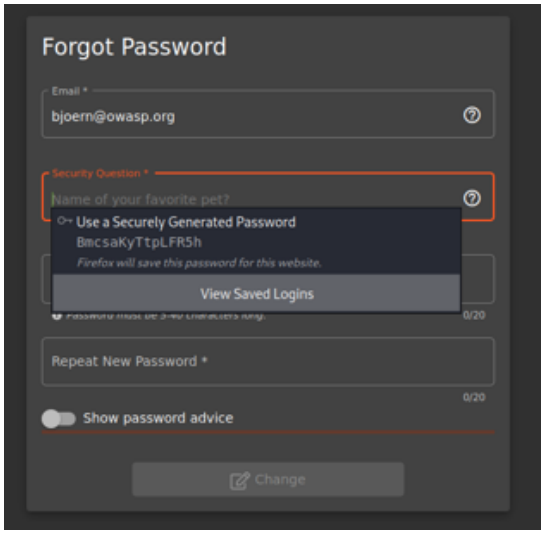
1. Weak Passwords: Aplikasi tidak memberlakukan kebijakan keamanan yang kuat terkait pemilihan kata sandi, sehingga pengguna dapat menggunakan kata sandi yang lemah atau mudah ditebak.
2. Broken Authentication: Terdapat kerentanan dalam proses otentikasi yang dapat dimanfaatkan oleh penyerang untuk mengakses akun pengguna tanpa izin.
3. Session Management: Implementasi yang buruk dalam manajemen sesi dapat menyebabkan serangan seperti pencurian sesi, penggunaan ganda sesi, atau serangan perusakan sesi.
4. Credential Stuffing: Serangan ini melibatkan penyerang yang mencoba menggunakan kombinasi email dan kata sandi yang dicuri dari pelanggaran data di situs web lain untuk mengakses akun pengguna di Juice Shop.
5. Insecure Remember Me: Jika fitur "Ingat Saya" tidak diimplementasikan dengan benar, maka serangan dapat dilakukan dengan mencuri token autentikasi yang disimpan di sisi klien atau server.
6. Weak Account Recovery: Jika proses pemulihan akun dilakukan dengan cara yang tidak aman, penyerang dapat memanfaatkannya untuk mendapatkan akses ke akun pengguna.
7. User Enumeration: Dalam situasi ini, penyerang dapat menggunakan metode seperti pesan kesalahan yang berbeda atau waktu respons yang berbeda untuk mengidentifikasi apakah suatu akun pengguna valid atau tidak.
8. Brute Force Attacks: Penyerang dapat mencoba menebak kata sandi pengguna dengan mencoba kombinasi yang berbeda secara otomatis hingga berhasil.

Semua kerentanan ini dapat menyebabkan pelanggaran keamanan yang serius jika tidak ditangani dengan benar.

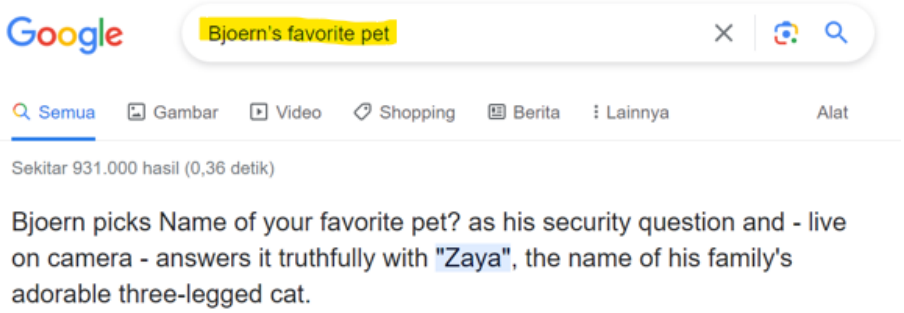
1. Mencari akun OWASP Snakes and Ladders dengan menggunakan reviews pada user bjoern@owasp.org



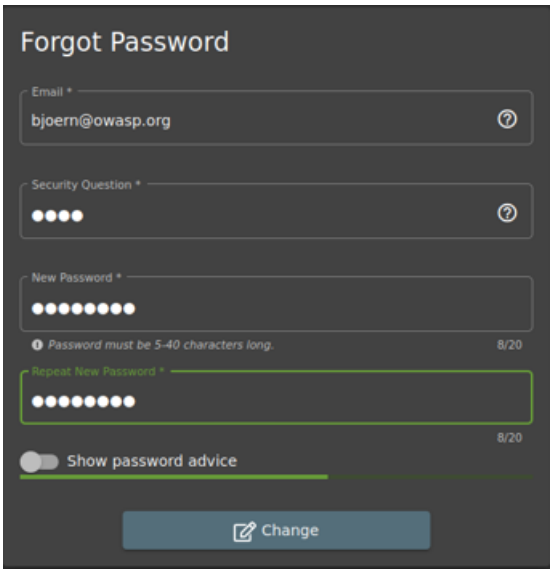
2. Copy email bjoern@owasp.org → Login → Forgot ur pw (Belum mengetahui pw pada email bjoern@owasp.org)lalu akan tampil pertanyaan keamanan dari akun tersebut yaitu nama hewan favorit nya



3. Seacrh keyword pada browser “Bjoern’s favorite pet”



4. Security Questions “Zaya” password Admin123



5. Berhasil login seperti gambar dibawah ini!!!