LAB 005 / TRAINING CASE STUDY

IDOR / Access Control

Objek akun lain dapat dibaca lewat parameter ID

CATEGORY	CWE-639 / CWE-862
RESULT	Solved (screenshot)
METHOD	Browser, parameter ID

EXECUTIVE SUMMARY

Ringkasan pengujian

Ketika login sebagai wiener di lab, parameter id diganti menjadi carlos; aplikasi menampilkan data akun dan API key simulasi milik carlos.

VALIDATED FINDING

Apa yang ditemukan

Endpoint /my-account mempercayai parameter id tanpa memverifikasi kepemilikan resource terhadap sesi pengguna yang meminta.

POTENTIAL IMPACT

Mengapa temuan penting

Pada sistem produksi, pola ini dapat mengungkap data milik pengguna lain termasuk rahasia API.

BATAS KLAIM: Penilaian ini dilakukan di lab simulasi PortSwigger, bukan di sistem pelanggan. Tidak mencakup pemindaian menyeluruh ataupun audit produksi.

TEST METHODOLOGY

Prosedur & validasi

1 / Baseline

Penguji login menggunakan akun latihan wiener.

2 / Resource ID

Parameter id pada /my-account menggambarkan akun pemilik data.

3 / Authorization check

Nilai id diganti dari wiener ke carlos; detail akun carlos terlihat.

4 / Evidence

Penyerahan solusi lab selesai dengan status Solved; API key di screenshot publik disamarkan.

SUGGESTED REMEDIATION

Perbaikan yang direkomendasikan

Lakukan pemeriksaan otorisasi per objek di sisi server. Gunakan identitas subjek dari sesi tervalidasi, bukan hanya parameter id; audit aturan akses dan tambahkan negative test lintas akun.

EXTERNAL REFERENCE

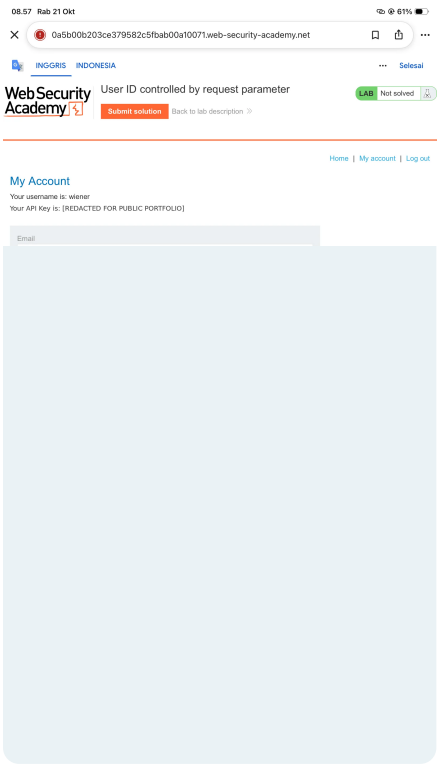
Sumber laboratorium

https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter

SOURCE EVIDENCE

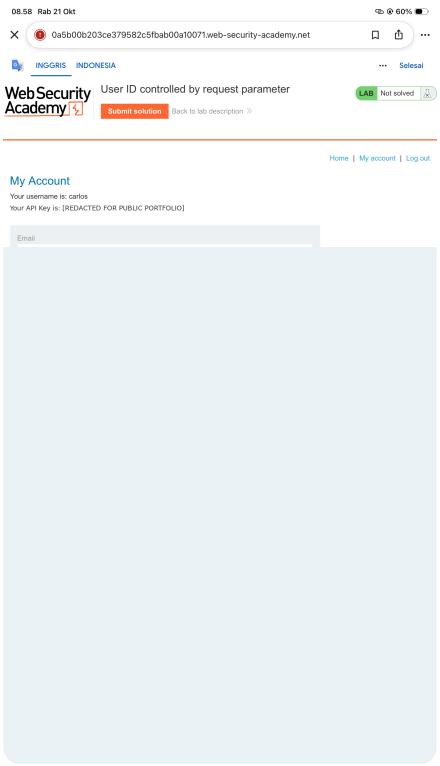
Bukti yang tersedia

Screenshot baseline, akses carlos, dan status Solved. API key lab disamarkan pada aset publik.



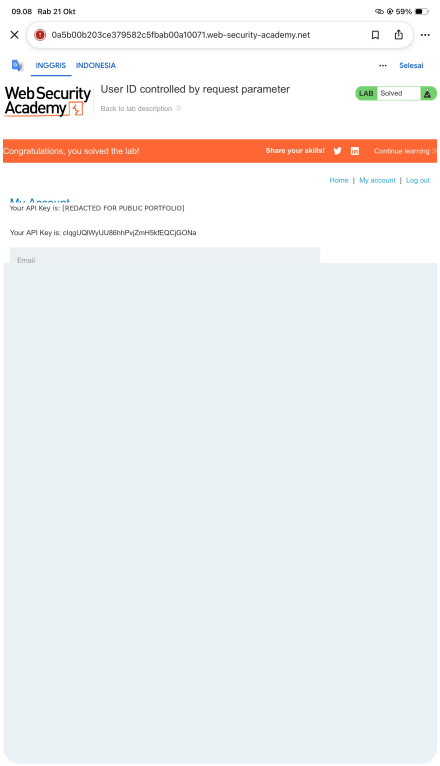
Akun sendiri

Halaman wiener sebagai baseline.



Akun lain terlihat

Halaman carlos terbuka; API key disamarkan.



Skenario selesai

Status Solved setelah penyerahan solusi.

DISCLOSURE / KETERBATASAN

Studi kasus ini hanya menunjukkan pengujian pada aplikasi yang sengaja rentan untuk edukasi. Kredensial lab bukan data pelanggan. Portofolio ini tidak setara dengan pengalaman audit enterprise atau sertifikasi profesional.