XYNY / SECURITY SERVICES

SECURITY ASSESSMENT LAB-001

Broken Access Control | Unprotected Admin Functionality

LAB SOLVED

AUTHORIZED TRAINING LAB

RUANG LINGKUP

PortSwigger Web Security Academy - lab simulasi yang sengaja dibuat rentan. Pengujian manual dilakukan melalui browser pada instance lab milik peserta.

Tanggal observasi	**21 Oktober 2026 (WIB)**
Status pengujian	**Selesai - bukti keberhasilan tersedia**
Metode	**Pemeriksaan manual pada lab resmi**
Klasifikasi kasus	**Access control / administrasi tanpa login**

Dokumen portofolio latihan. BUKAN audit komersial, bukan sertifikasi pentest, dan bukan laporan dari sistem produksi pelanggan.

Hasil pengujian

Berdasarkan tiga bukti screenshot yang diberikan oleh penguji

HIGH - PENILAIAN LAB

Hasil: fungsi administratif dapat diakses tanpa login

RINGKASAN EKSEKUTIF

Dalam instance laboratorium PortSwigger, lokasi panel admin terekspos melalui robots.txt. Saat dibuka langsung tanpa autentikasi, panel tersebut menampilkan daftar pengguna dan kontrol penghapusan akun. Tindakan menghapus akun target latihan berhasil; status lab berubah menjadi Solved.

TEMUAN TEKNIS

Judul: Unprotected Admin Functionality

Kategori: Broken Access Control / Missing Authorization Check

Indikator: /robots.txt mengungkap jalur /administrator-panel

Verifikasi: panel memuat tautan Delete tanpa sesi admin

Dampak yang terbukti: akun latihan carlos berhasil dihapus

PROSEDUR REPRODUKSI (LAB)

01 Buka instance lab PortSwigger: Unprotected admin functionality.

02 Akses /robots.txt; baca petunjuk Disallow: /administrator-panel.

03 Kunjungi /administrator-panel tanpa login; amati daftar user dan kontrol Delete.

04 Klik Delete pada akun latihan carlos; amati User deleted successfully dan Solved.

DAMPAK & BATAS PENILAIAN

Pada aplikasi nyata, celah serupa dapat mengizinkan perubahan atau penghapusan akun oleh pihak tanpa hak. Label High pada dokumen ini adalah penilaian kualitatif untuk skenario lab, bukan skor CVSS resmi. Tidak ada pemindaian menyeluruh, enumerasi endpoint lain, atau pengujian produksi.

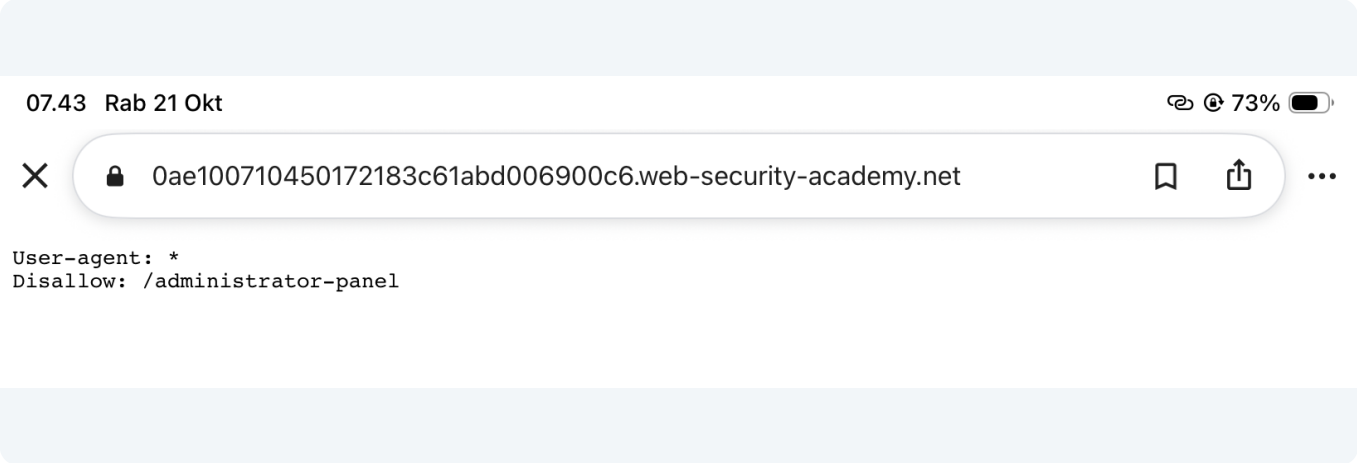
BUKTI PENGUJIAN

Evidence 01 & 02

Cuplikan screenshot asli untuk fokus pada elemen yang terbukti

EVIDENCE 01 / ADMIN PATH DISCLOSURE

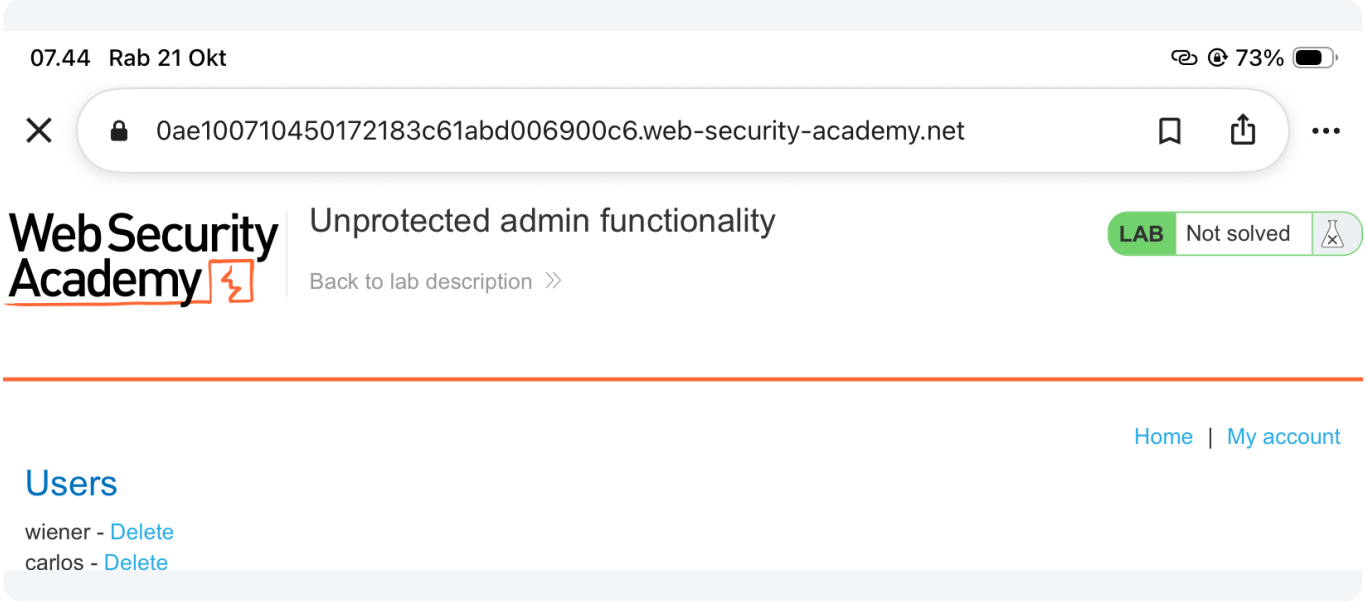
robots.txt memuat: Disallow: /administrator-panel



Catatan: robots.txt saja bukan mekanisme autentikasi atau bukti akses admin.

EVIDENCE 02 / UNAUTHENTICATED ADMIN ACCESS

Panel menampilkan akun wiener dan carlos beserta kontrol Delete.



Status lab pada tahap ini: Not solved. Panel terlihat tanpa login admin.

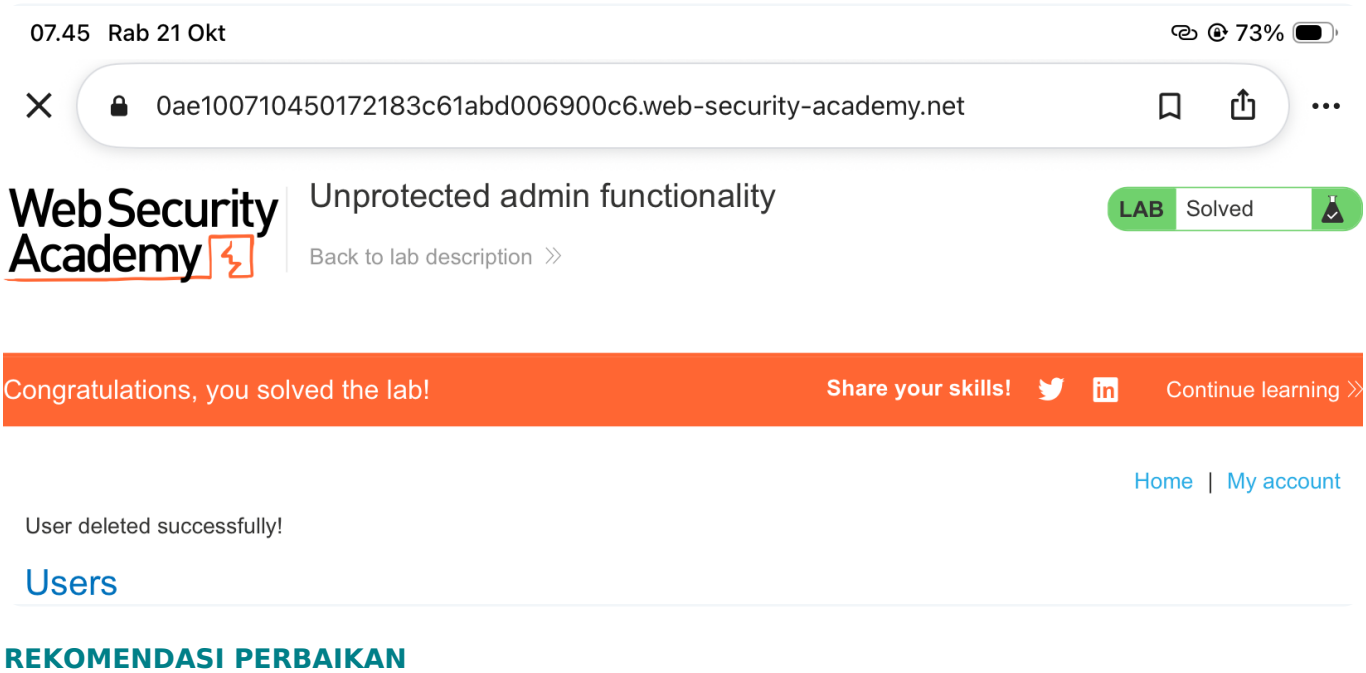
Gambar asli beresolusi penuh turut disertakan dalam paket arsip bukti.

Lab berhasil diselesaikan

Bukti akhir, rekomendasi, dan batasan penggunaan portofolio

EVIDENCE 03 / OBJECTIVE COMPLETED

Terlihat status Solved dan pesan User deleted successfully!



REKOMENDASI PERBAIKAN

- Wajibkan autentikasi sebelum setiap endpoint dan aksi administratif.
- Terapkan pemeriksaan otorisasi di sisi server untuk peran administrator.
- Tolak akses tanpa hak (403/redirect login); jangan andalkan robots.txt.
- Gunakan pengujian regresi untuk endpoint admin termasuk operasi DELETE.

VERIFIKASI SETELAH PERBAIKAN (RENCANA)

Dari sesi tanpa login, GET ke panel admin dan aksi penghapusan harus ditolak. Dari pengguna biasa, aksi administratif juga ditolak. Hanya peran yang berwenang yang dapat mengakses dan mengubah data. Perbaikan ini belum diimplementasikan atau diuji ulang karena kode lab tidak dikelola peserta.

PENGUNGKAPAN UNTUK CALON KLIEN

Studi kasus ini merupakan demonstrasi latihan berizin pada PortSwigger Web Security Academy. Tidak boleh disajikan sebagai audit klien nyata atau referensi pekerjaan berbayar.