LAB 004 / TRAINING CASE STUDY

# 2FA Bypass

Akses akun sebelum faktor kedua diverifikasi

| | |
|---|---|
| CATEGORY | **CWE-287 / CWE-306** |
| RESULT | **Solved (screenshot)** |
| METHOD | **Browser, direct route** |

EXECUTIVE SUMMARY

## Ringkasan pengujian

Lab mengizinkan akun latihan carlos membuka /my-account setelah login kata sandi, tanpa memasukkan kode 2FA.

VALIDATED FINDING

## Apa yang ditemukan

Kontrol akses sisi server tidak memastikan tahap verifikasi faktor kedua telah diselesaikan sebelum halaman akun ditampilkan.

POTENTIAL IMPACT

## Mengapa temuan penting

Dalam sistem nyata, desain seperti ini dapat melemahkan proteksi 2FA dan memungkinkan akses akun ketika kata sandi telah diketahui.

**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**

Login ke aplikasi latihan membawa pengguna ke formulir kode 2FA.

**2 / Auth workflow**

Sesi akun latihan carlos berada pada keadaan menunggu faktor kedua.

**3 / Direct access**

Penguji meminta /my-account tanpa memasukkan kode 2FA.

**4 / Evidence**

Akun carlos tampil dan status lab Solved pada screenshot.

SUGGESTED REMEDIATION

## Perbaikan yang direkomendasikan

Terapkan status autentikasi bertahap di server. Batasi seluruh rute sensitif sampai faktor kedua tervalidasi; gunakan session state yang terikat akun, rotasi sesi, dan tes regresi untuk akses langsung.

EXTERNAL REFERENCE

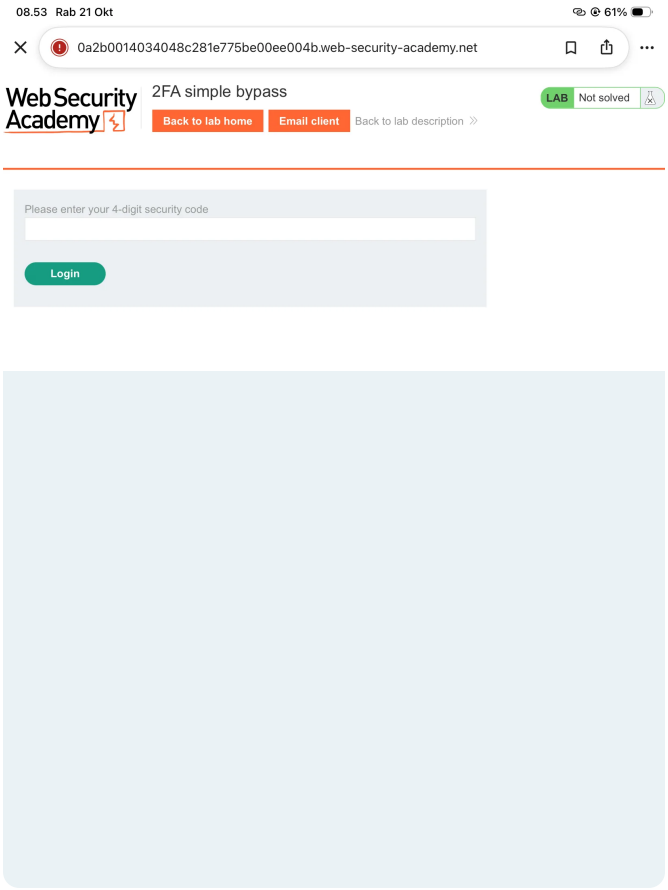
## Sumber laboratorium

https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass

SOURCE EVIDENCE

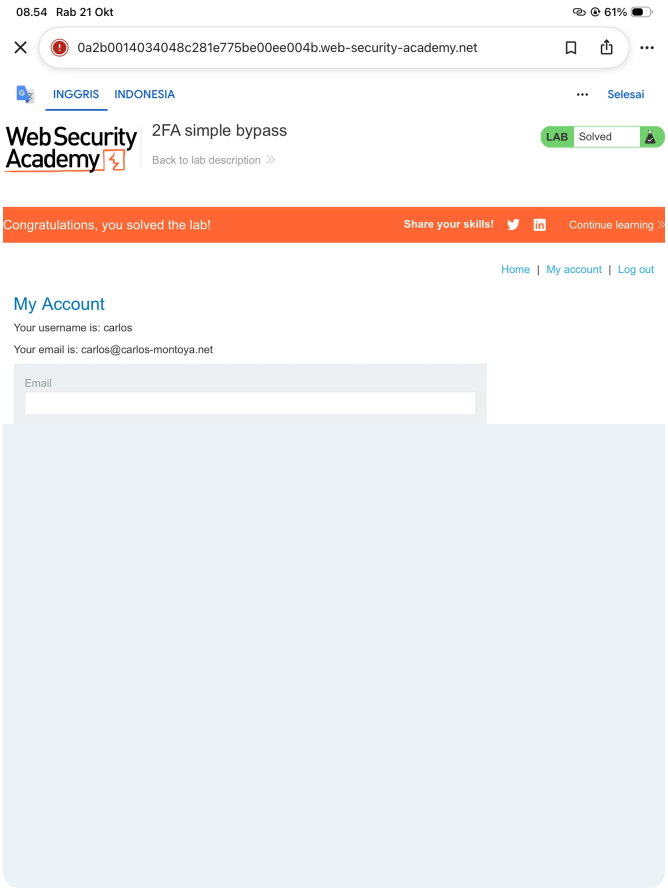
# Bukti yang tersedia

Screenshot PortSwigger memperlihatkan LAB Solved dan username carlos pada halaman akun.




## Layar kode 2FA

Halaman menuntut kode 4 digit.




## Akses tanpa kode

Akun carlos terbuka; lab Solved.

### 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.