TRAINING CASE / 009

Unrestricted File Upload / RCE

Eksekusi file PHP di direktori avatar

KATEGORI

CWE-434

PENYELENGGARA

PortSwigger Web Security Academy

TANGGAL PENGUJIAN

21 Oktober 2026

LINGKUNGAN

Instance laboratorium resmi yang sengaja rentan

BUKTI STATUS

Screenshot Solved tersedia

BATASAN & TRANSPARANSI

Dokumen ini merupakan laporan pembelajaran pada laboratorium resmi, bukan audit keamanan terhadap sistem klien atau sertifikasi pentest profesional. Screenshot diambil dari bukti pengujian peserta; nilai sensitif disamarkan.

ASSESSMENT BRIEF / 01

Unrestricted File Upload / RCE

Ringkasan temuan dan metode latihan pada lingkungan terotorisasi

RINGKASAN TEMUAN

Pada lab upload avatar, aplikasi menerima file PHP dan memprosesnya sebagai skrip saat file itu diakses melalui URL publik. Pengujian dimulai dari penanda teks sederhana lalu membaca berkas rahasia simulasi yang ditentukan lab.

APA YANG BENAR-BENAR TERAMATI

Terdapat screenshot bahwa lab009.php berhasil diunggah, respons browser menampilkan marker XYNY-LAB009-TEST, serta bukti file latihan dapat dibaca. Screenshot terakhir memperlihatkan LAB Solved.

DAMPAK POTENSIAL PADA SISTEM NYATA

Dalam aplikasi nyata, unggahan skrip executable tanpa pemisahan eksekusi dapat berujung pada kendali eksekusi kode server, akses data, dan dampak terhadap integritas layanan.

PROSEDUR YANG DIDOKUMENTASIKAN

01 Unggah file PHP pada fitur avatar di lingkungan lab

02 Akses berkas di /files/avatars/ dan amati eksekusi marker

03 Validasi pembacaan berkas simulasi milik lab; rahasia disamarkan

04 Konfirmasi status LAB Solved di PortSwigger

SUMBER LATIHAN

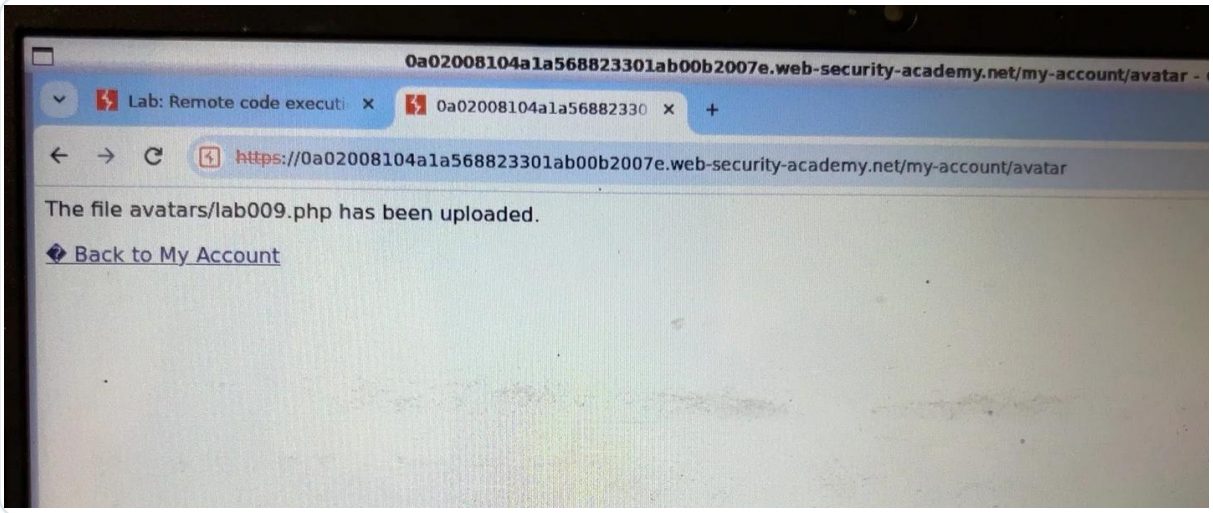
https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload

EVIDENCE / 02

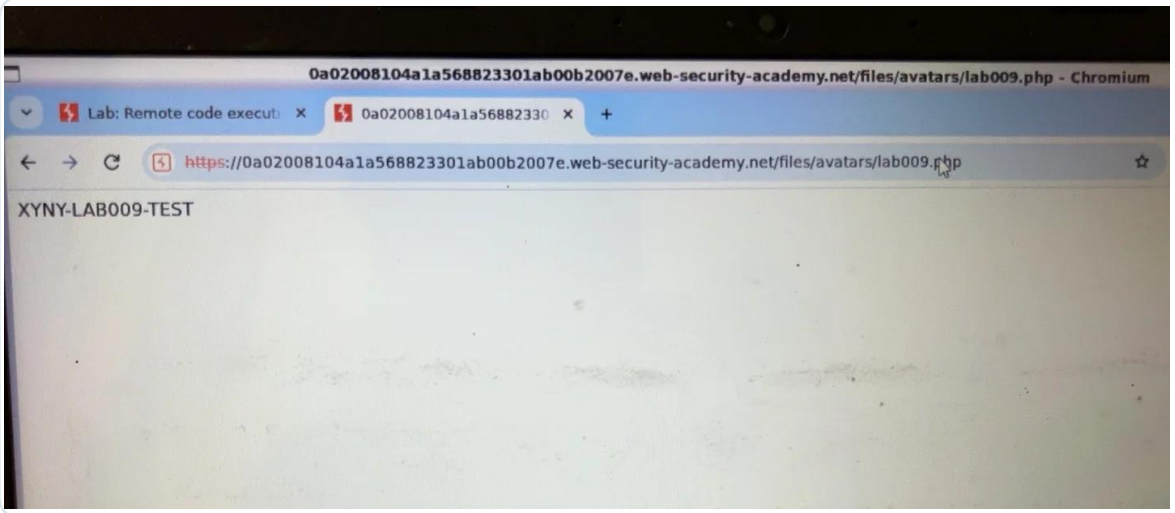
Bukti pengujian

Screenshot pengujian yang dirotasi, dipotong bila perlu, dan disanitasi

01 Pesan upload PHP berhasil



02 Eksekusi marker PHP via URL avatar



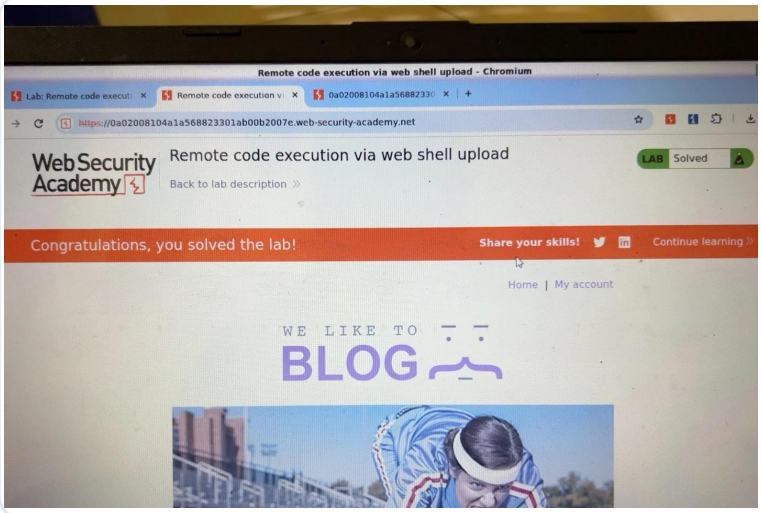
Catatan: Screenshot menampilkan lingkungan PortSwigger. String sesi dan nilai rahasia tidak dicantumkan dalam versi publik.

EVIDENCE / 03

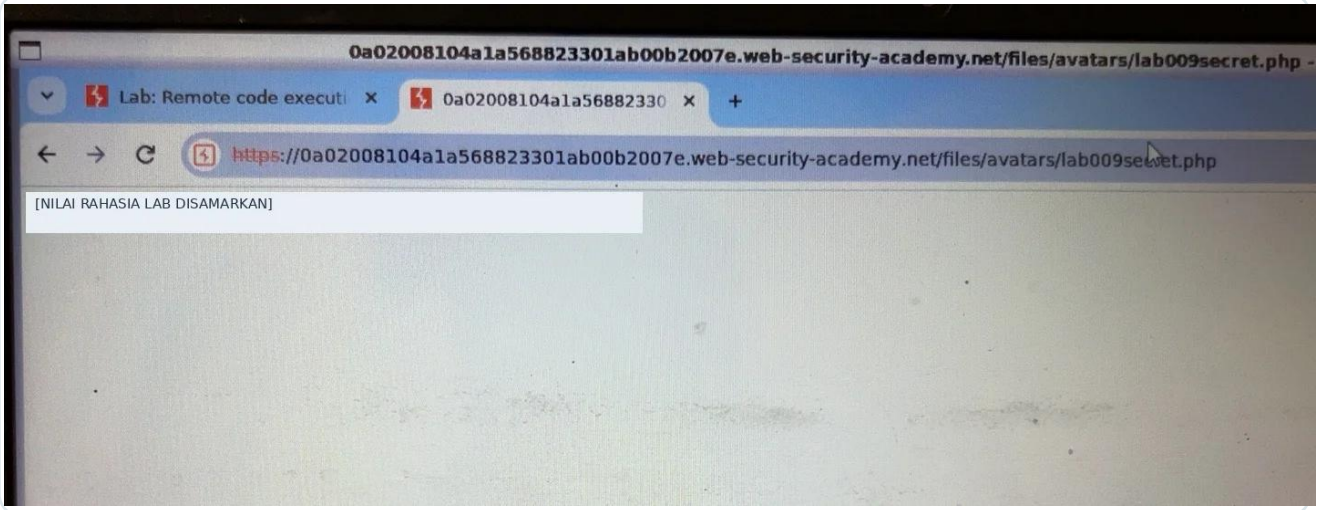
Penyelesaian & validasi

Konfirmasi status Solved dan redaksi nilai rahasia simulasi

03 Status PortSwigger: LAB Solved



04 Hasil file simulasi; nilai rahasia ditutup



REMEDIATION NOTES / 04

Rekomendasi perbaikan

Prinsip mitigasi yang relevan untuk aplikasi produksi

01 Batasi tipe dan konten unggahan melalui allowlist dan pemeriksaan server-side.

02 Simpan unggahan di luar web root, dengan nama acak serta izin baca/tulis minimum.

03 Nonaktifkan interpretasi/eksekusi skrip di direktori file pengguna.

04 Terapkan autentikasi, batas ukuran, antivirus, dan logging untuk unggahan.

PENGUJIAN BUKAN PENGESAHAN KETAHANAN SISTEM

Status Solved membuktikan keberhasilan menjalankan skenario latihan yang disediakan PortSwigger. Temuan pada aplikasi nyata hanya dapat disimpulkan dari penilaian terpisah, dengan izin dan ruang lingkup yang disepakati.