TRAINING CASE / 008

File Path Traversal

Pembacaan file di luar direktori gambar

KATEGORI

CWE-22

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

File Path Traversal

Ringkasan temuan dan metode latihan pada lingkungan terotorisasi

RINGKASAN TEMUAN

Pada instance laboratorium PortSwigger, endpoint gambar menerima parameter filename. Ketika nilai diarahkan keluar dari direktori gambar, server mengembalikan isi file sistem /etc/passwd.

APA YANG BENAR-BENAR TERAMATI

Burp Repeater memperlihatkan permintaan /image?filename=... menuju berkas sistem dan HTTP 200 dengan entri akun Linux. Screenshot status PortSwigger menunjukkan LAB Solved.

DAMPAK POTENSIAL PADA SISTEM NYATA

Dalam aplikasi nyata, kelemahan serupa dapat mengekspos konfigurasi, kode aplikasi, atau berkas lokal lain yang dapat dibaca oleh proses web.

PROSEDUR YANG DIDOKUMENTASIKAN

01 GET /image?filename=... lewat Burp Repeater

02 Perubahan nilai filename untuk menguji traversal path

03 Respons HTTP 200 menampilkan entri file sistem

04 Status penyelesaian laboratorium: Solved

SUMBER LATIHAN

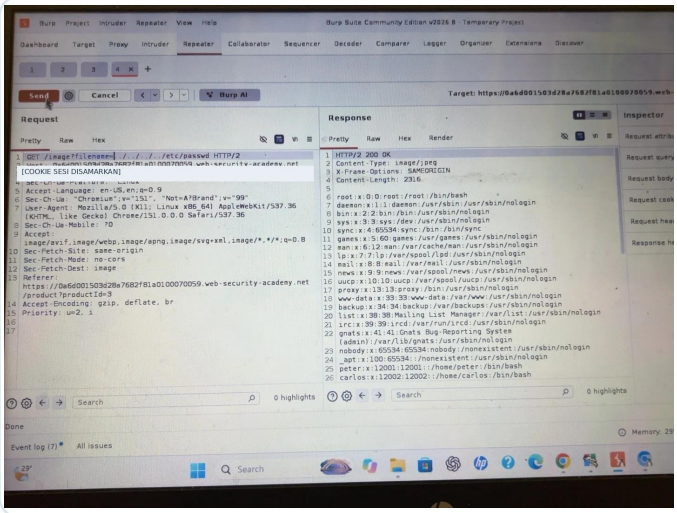
https://portswigger.net/web-security/file-path-traversal/lab-simple

EVIDENCE / 02

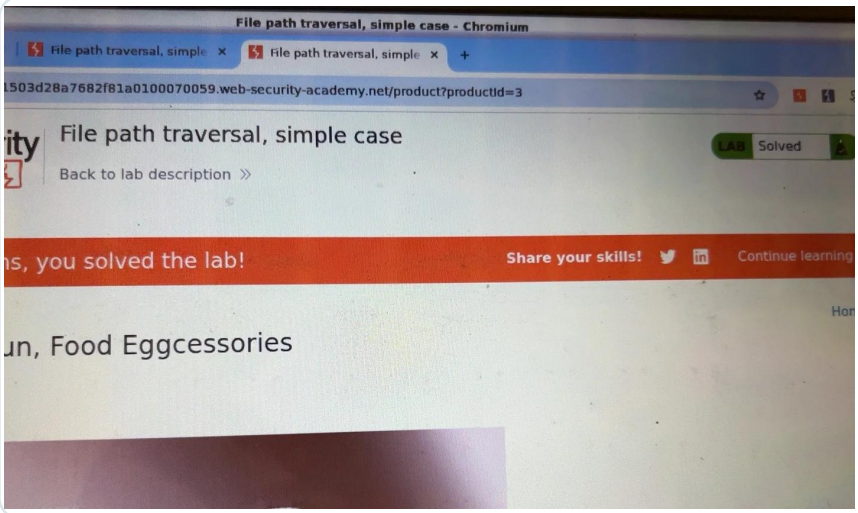
Bukti pengujian

Screenshot pengujian yang dirotasi, dipotong bila perlu, dan disanitasi

01 Burp Repeater: respons berkas sistem (cookie disamarkan)



02 Status PortSwigger: LAB Solved



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

REMEDIATION NOTES / 04

Rekomendasi perbaikan

Prinsip mitigasi yang relevan untuk aplikasi produksi

01 Gunakan identitas berkas / allowlist, bukan path filesystem dari pengguna.

02 Normalisasikan path dan pastikan hasilnya selalu berada di direktori yang diizinkan.

03 Batasi izin akses proses web dan pisahkan dokumen sensitif dari direktori publik.

04 Tambahkan pengujian otomatis terhadap traversal, absolute path, dan encoded path.

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.