TRAINING CASE / 010

OS Command Injection

Perintah sistem operasi berjalan dari input stok

KATEGORI

CWE-78

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

OS Command Injection

Ringkasan temuan dan metode latihan pada lingkungan terotorisasi

RINGKASAN TEMUAN

Dalam lab pemeriksaan stok, parameter storeId digunakan pada eksekusi perintah server tanpa pemisahan yang aman. Pengujian melalui Burp Repeater menunjukkan hasil whoami dalam respons HTTP.

APA YANG BENAR-BENAR TERAMATI

Burp Repeater menampilkan POST /product/stock dengan nilai storeId yang disisipi pemisah perintah; respons HTTP 200 mengembalikan nama pengguna proses. Screenshot lain menunjukkan LAB Solved.

DAMPAK POTENSIAL PADA SISTEM NYATA

Kelemahan yang sama pada layanan nyata dapat memungkinkan eksekusi perintah dengan hak akses proses aplikasi, pembacaan data, atau perubahan sistem sesuai izin proses.

PROSEDUR YANG DIDOKUMENTASIKAN

01 POST /product/stock direkam melalui Burp Suite

02 Nilai parameter storeId memicu eksekusi perintah whoami

03 HTTP 200 dan nama akun sistem tampil pada response

04 PortSwigger memperlihatkan LAB Solved

SUMBER LATIHAN

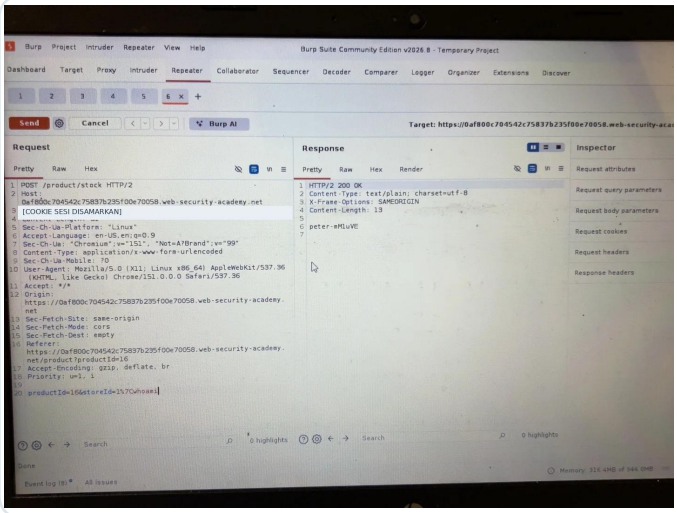
https://portswigger.net/web-security/os-command-injection/lab-simple

EVIDENCE / 02

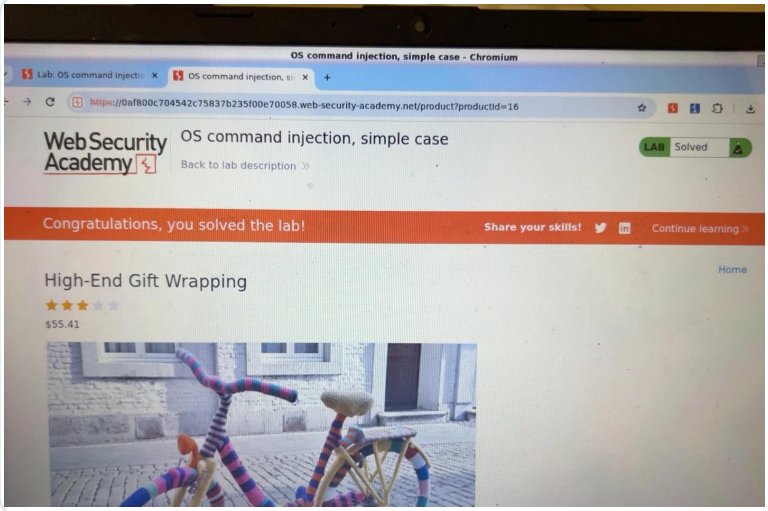
Bukti pengujian

Screenshot pengujian yang dirotasi, dipotong bila perlu, dan disanitasi

01 Burp Repeater: output whoami (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 Jangan menggabungkan input pengguna menjadi perintah shell; gunakan API sistem tanpa shell.

02 Jika tidak dapat dihindari, validasi parameter dengan allowlist tipe/nilai yang ketat.

03 Jalankan service dengan hak akses minimum, sandboxing, serta pembatasan akses host.

04 Uji parameter terhadap karakter kontrol shell; pantau aktivitas proses abnormal.

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.