LAB 007 / TRAINING CASE STUDY

Server-Side Request Forgery

Fitur cek stok membaca panel admin lokal

CATEGORY	**CWE-918**
RESULT	**Selesai menurut peserta; screenshot belum ada**
METHOD	**Burp Repeater, manual**

EXECUTIVE SUMMARY

Ringkasan pengujian

Di lab PortSwigger, request POST /product/stock yang menggunakan parameter stockApi diarahkan ke http://localhost/admin. Respons HTTP 200 memuat halaman panel admin internal beserta daftar pengguna.

VALIDATED FINDING

Apa yang ditemukan

Server melakukan permintaan ke tujuan yang dikendalikan melalui stockApi tanpa pembatasan alamat jaringan internal yang memadai.

POTENTIAL IMPACT

Mengapa temuan penting

Dalam konteks sistem nyata, SSRF dapat mengekspos layanan internal atau metadata cloud tergantung hak akses server dan proteksi jaringan.

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

Penguji mengakses fitur cek stok produk dan menemukan request POST /product/stock.

2 / Parameter

Request body memiliki parameter stockApi untuk URL pemeriksaan stok.

3 / SSRF proof

Melalui Burp Repeater, nilai stockApi diarahkan ke http://localhost/admin.

4 / Response

HTTP 200 OK mengandung HTML Admin panel dan daftar pengguna; Solved kemudian dikonfirmasi peserta, tanpa screenshot final.

SUGGESTED REMEDIATION

Perbaikan yang direkomendasikan

Gunakan allowlist tujuan berbasis skema, host dan port; tolak alamat loopback/private/link-local setelah DNS resolution dan setiap redirect; segmentasi outbound traffic dan logging.

EXTERNAL REFERENCE

Sumber laboratorium

https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost

SOURCE EVIDENCE

Bukti yang tersedia

Bukti teks: respons Burp Repeater HTTP/2 200 OK dan HTML panel admin diterima dari peserta. Status Solved dikonfirmasi peserta melalui chat; belum ada screenshot Solved untuk verifikasi visual.

```
REDACTED TRANSCRIPT / BURP REPEATER

POST /product/stock

stockApi -> http://localhost/admin


HTTP/2 200 OK

Content-Type: text/html; charset=utf-8


<title>Basic SSRF against the local server</title>

<a href="/admin">Admin panel</a>

<h1>Users</h1>

<span>wiener - </span> ... Delete

<span>carlos - </span> ... Delete
```

Sumber: fragmen response yang ditempel peserta. Cookie sesi dihilangkan. Konfirmasi Solved berasal dari pernyataan peserta, bukan screenshot final.

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.