LAB 006 / TRAINING CASE STUDY

Cross-Site Request Forgery

Perubahan email dipicu oleh situs luar

CATEGORY	CWE-352
RESULT	Solved (screenshot)
METHOD	Exploit Server, HTML form

EXECUTIVE SUMMARY

Ringkasan pengujian

Pada lab PortSwigger, halaman HTML eksternal menggunakan form POST otomatis untuk memicu perubahan email akun simulasi yang sedang login.

VALIDATED FINDING

Apa yang ditemukan

Endpoint perubahan email tidak memiliki perlindungan CSRF yang memadai untuk memastikan perubahan berasal dari tindakan sengaja pemilik sesi.

POTENTIAL IMPACT

Mengapa temuan penting

Dalam aplikasi nyata, serangan CSRF dapat mendorong pengguna yang login melakukan tindakan tanpa sengaja, tergantung cookie, browser, dan kontrol server.

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

Akun latihan wiener menampilkan form perubahan email.

2 / Request context

Form perubahan email menggunakan POST tanpa pertahanan CSRF yang efektif.

3 / Simulation

Exploit Server menyediakan form HTML otomatis menuju endpoint perubahan email.

4 / Evidence

Setelah pengiriman ke korban simulasi, status lab Solved terlihat pada screenshot.

SUGGESTED REMEDIATION

Perbaikan yang direkomendasikan

Gunakan anti-CSRF token yang terikat sesi dan divalidasi server, verifikasi Origin/Referer bila sesuai, atur SameSite cookies, dan minta reauthentication pada perubahan sensitif.

EXTERNAL REFERENCE

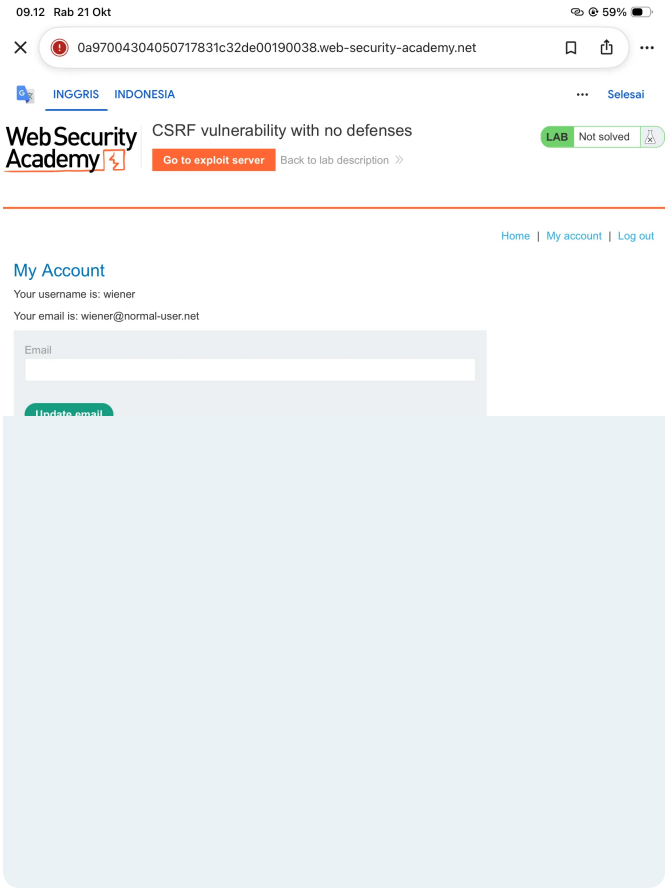
Sumber laboratorium

https://portswigger.net/web-security/csrf/lab-no-defenses

SOURCE EVIDENCE

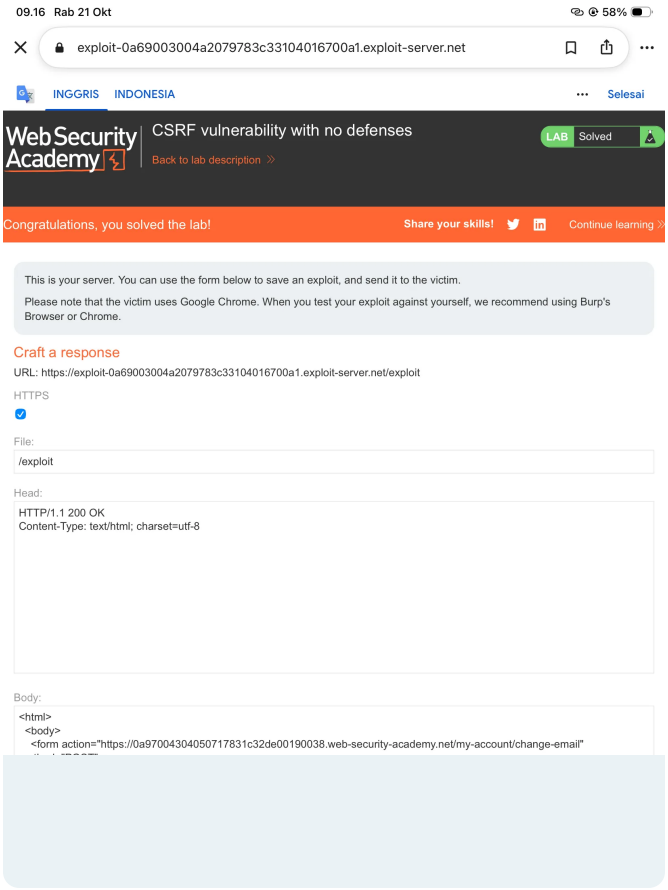
Bukti yang tersedia

Exploit Server resmi menunjukkan payload latihan dan label LAB Solved pada halaman yang sama.



Akun sebelum uji

Halaman perubahan email akun latihan.



Exploit terkirim

Eksploit HTML lab dan status 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.