XYNY / SECURITY

AUTHENTIC LAB PORTFOLIO / 003

REFLECTED XSS

Unencoded HTML Context

PortSwigger Web Security Academy

TEMUAN TERKONFIRMASI

Input pencarian dieksekusi sebagai JavaScript

Payload uji: <script>alert(1)</script>

Bukti: dialog browser muncul; status lab "Solved".

SOLVED

21 OKT 2026 | PORTOFOLIO LABORATORIUM RESMI

Bukan audit klien dan bukan sertifikasi pentester.

RINGKASAN EKSEKUTIF

Pengujian pada laboratorium resmi yang sengaja dibuat rentan menunjukkan bahwa input pencarian dipantulkan tanpa encoding HTML yang memadai dan dapat mengeksekusi JavaScript pada browser. Respons berhasil divalidasi dengan dialog alert dan konfirmasi Solved dari platform latihan.

LAB	KATEGORI	CWE	STATUS
003	Reflected XSS	79	SOLVED

RUANG LINGKUP DAN BUKTI

01 **LINGKUNGAN**

Instance latihan PortSwigger Web Security Academy: "Reflected XSS into HTML context with nothing encoded".

02 **PERMUKAAN INPUT**

Form pencarian blog; nilai pencarian tercermin pada halaman hasil.

03 **PENGUJIAN AWAL**

Pencarian XYNYTEST ditampilkan ulang dalam teks halaman, belum membuktikan XSS.

04 **PEMBUKTIAN**

Input <script>alert(1)</script> menghasilkan dialog JavaScript bernilai 1.

05 **VALIDASI AKHIR**

Halaman menunjukkan pesan keberhasilan dan status LAB Solved.

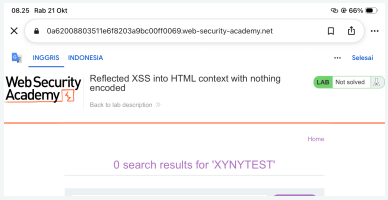
BATAS TEMUAN

Bukti hanya menunjukkan eksekusi JavaScript dalam lab. Tidak ada bukti pengambilalihan akun, akses data pengguna nyata, ataupun pengujian pada domain produksi.

BUKTI TEKNIS

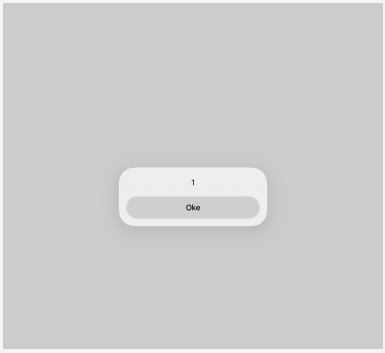
Tiga screenshot original dari sesi pengujian disimpan di paket ZIP. Pratinjau berikut memperlihatkan tahapan dari reflection sampai konfirmasi hasil.

01 INPUT REFLECTED



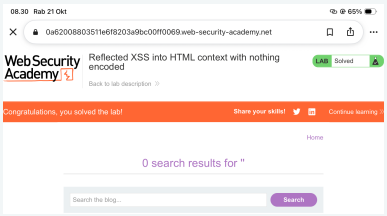
XYNYTEST tercermin dalam hasil pencarian; status awal Not solved.

02 JAVASCRIPT EXECUTION



Dialog "1" ditampilkan browser setelah payload XSS dijalankan.

03 CHALLENGE SOLVED



PortSwigger menampilkan "Congratulations" dan status Solved.

EVIDENCE CHAIN

Screenshot 01: tampilan hasil pencarian biasa. Screenshot 02: dialog alert sebagai bukti runtime JavaScript. Screenshot 03: status Solved sebagai konfirmasi dari platform.

REKOMENDASI PERBAIKAN

Pada aplikasi riil, uji ini perlu dilanjutkan dengan pengecekan konteks output dan penerapan perlindungan pada sisi server maupun browser.

01 **Contextual output encoding**

Encode karakter HTML pada setiap data tidak tepercaya sebelum dirender sebagai HTML. Pilih encoding sesuai konteks HTML, atribut, JavaScript, atau URL.

02 **Safe DOM APIs**

Hindari memasukkan input tidak tepercaya ke innerHTML. Untuk teks biasa, gunakan textContent atau rendering framework yang meng-escape input.

03 **Trusted sanitization**

Jika aplikasi harus menerima HTML terbatas, lakukan sanitasi dengan pustaka terawat dan konfigurasi allowlist yang tepat.

04 **Defense in depth**

Terapkan Content Security Policy (CSP) yang ketat, cookie HttpOnly/SameSite sesuai kebutuhan, dan monitoring untuk menambah lapisan pengamanan.

05 **Regression testing**

Uji ulang seluruh endpoint yang memantulkan input, termasuk variasi karakter khusus, setelah perubahan kode diterapkan.

KERANGKA PENILAIAN

Klasifikasi: High (indikatif pada skenario latihan; bukan hasil CVSS resmi). Status: kerentanan terkonfirmasi di lab, remediasi dan retest aplikasi nyata tidak termasuk.

ETIKA & KEABSAHAN

Latihan dilakukan pada lab resmi yang dibuat untuk eksplorasi keamanan. Dokumen ini merupakan studi kasus pembelajaran, tidak menyatakan pernah mengaudit sistem klien.