ANALISIS KERENTANAN *WEBSITE* PT. PITJARUS DENGAN TIGA *TOOLS SCANNING* DAN *PENETRATION TESTING BLACK BOX* BERDASARKAN OWASP TOP 10

Chattelin

ABSTRAK

Pemanfaatan *website* sebagai sarana operasional bisnis berpotensi meningkatkan risiko ancaman siber terhadap data dan sistem informasi perusahaan. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan *website* PT. Pitjarus menggunakan metode *penetration testing* dengan pendekatan *black box* berdasarkan standar NIST SP 800-115 dan kerangka kerja OWASP Top 10 2021. Metodologi penelitian mencakup fase *planning, discovery, attack*, dan *reporting*. Pada fase *discovery*, penggunaan Nslookup dan Nmap mengidentifikasi bahwa domain target berada di balik layanan *reverse proxy* Cloudflare yang menyembunyikan alamat IP server origin, sedangkan pemindaian menggunakan OWASP ZAP menemukan 9 indikasi awal kerentanan (*initial findings*) pada lapisan aplikasi, termasuk potensi SQL *Injection* dan *Cross-Site Scripting* (XSS) yang masuk ke dalam kategori *A03: Injection* pada OWASP Top 10 202. Temuan ini menjadi dasar penentuan fokus pengujian pada fase *attack*. Hasil validasi pada fase attack mengonfirmasi dua kerentanan utama, yaitu SQL *Injection* pada fitur autentikasi dan XSS pada fitur pembuatan tugas. Berdasarkan penilaian menggunakan CVSS v3.1, kerentanan SQL *Injection* memperoleh skor 7.5 (*High*), sedangkan XSS memperoleh skor 3.9 (*Low*). Hasil ini menunjukkan bahwa perlindungan *reverse proxy* belum sepenuhnya mampu mencegah eksploitasi pada lapisan aplikasi. Penelitian ini merekomendasikan penerapan *parameterized query*, validasi dan sanitasi input di sisi server, serta prinsip *least privilege* pada pengelolaan basis data untuk meningkatkan keamanan *website* PT. Pitjarus.

Kata Kunci: *Penetration Testing*, *Black Box*, NIST SP 800-115, OWASP Top 10, Keamanan *Website*

VULNERABILITY ANALYSIS OF PT. PITJARUS WEBSITE USING THREE SCANNING TOOLS AND BLACK BOX PENETRATION TESTING BASED ON OWASP TOP 10

Chattelin

ABSTRACT

The use of websites as core business platforms increases the potential risk of cyber threats to organizational data and information systems. This study aims to assess security vulnerabilities on the PT. Pitjarus website through penetration testing using a black-box approach, guided by the NIST SP 800-115 standard and the OWASP Top 10 2021 framework. The research was conducted through four stages: planning, discovery, attack, and reporting. During the discovery phase, Nslookup and Nmap identified that the target domain is protected by the Cloudflare reverse proxy service, which masks the origin server's IP address. In addition, scanning with OWASP ZAP detected nine initial indicators of vulnerabilities at the application layer, including potential SQL Injection and Cross-Site Scripting (XSS), classified under the A03: Injection category in the OWASP Top 10 2021. These findings directed the execution of targeted testing in the attack phase, which confirmed two primary vulnerabilities: SQL Injection in the authentication feature and XSS in the task creation feature. Based on CVSS v3.1 scoring, SQL Injection received a score of 7.5 (High), while XSS received a score of 3.9 (Low). The findings demonstrate that reverse proxy protection alone is insufficient to mitigate attacks at the application layer. Accordingly, this study recommends implementing parameterized queries, enforcing server-side input validation and sanitization, and applying the principle of least privilege in database management to further enhance the security posture of the PT. Pitjarus website.

Keywords: *Penetration Testing, Black Box, NIST SP 800-115, OWASP Top 10, Website Security*