ABSTRAK

Perkembangan teknologi digital telah membawa dampak signifikan terhadap berbagai sektor, termasuk sektor perdagangan aset kripto. Salah satu platform pertukaran aset digital terbesar di Indonesia adalah Indodax.com. Seiring meningkatnya aktivitas dan transaksi pengguna, risiko terhadap serangan siber juga semakin tinggi, seperti serangan SQL *Injection*, *Cross-Site Scripting* (XSS), dan *eksploitasi* terhadap kerentanan sistem lainnya. Penelitian ini bertujuan untuk menguji kualitas celah keamanan informasi pada website Indodax.com dengan menggunakan *metode penetration testing* yang mengacu pada kerangka kerja *Information System Security Assessment Framework* (ISSAF). Proses penelitian dibagi menjadi tiga fase utama, yaitu: perencanaan dan persiapan (*planning and preparation),* penilaian *(assessment),* serta pelaporan dan *pembersihan (reporting and clean-up)*. Pada *fase assessment*, dilakukan serangkaian pengujian yang mencakup pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, dan pengujian penetrasi. Sistem operasi Kali Linux digunakan sebagai lingkungan pengujian dengan dukungan *tools* seperti Nmap, SQLMap, dan OWASP ZAP. Hasil penelitian menunjukkan adanya sejumlah kerentanan, antara lain konfigurasi header keamanan yang belum optimal, penggunaan pustaka *JavaScript* yang tidak diperbarui, serta potensi celah XSS yang berhasil diblokir oleh sistem keamanan *Web Application Firewall* (WAF). Sementara itu, uji *SQL Injection* tidak berhasil dilakukan karena tidak ditemukan parameter dinamis yang rentan dan sistem keamanan memblokir akses dengan kode status HTTP 403. Selain itu, konfigurasi SSL pada *website* ini sudah mendukung TLS 1.2, meskipun TLS 1.3 belum aktif. Secara keseluruhan, website Indodax.com memiliki tingkat keamanan yang cukup baik, namun masih memerlukan penyempurnaan teknis untuk meningkatkan perlindungan terhadap ancaman siber yang terus berkembang.

Kata kunci: keamanan informasi, *penetration testing*, ISSAF, Indodax.com, Kali Linux

ABSTRACT

The advancement of digital technology has significantly impacted various sectors, including cryptocurrency trading. One of the largest digital asset exchange platforms in Indonesia is Indodax.com. As user activity and transaction volumes increase, so do the risks of cyberattacks such as SQL Injection, Cross-Site Scripting (XSS), and exploitation of other system vulnerabilities. This research aims to evaluate the quality of information security vulnerabilities on the Indodax.com website using a penetration testing method based on the Information System Security Assessment Framework (ISSAF). The research process is divided into three main phases: planning and preparation, assessment, and reporting and clean-up. During the assessment phase, a series of tests were conducted, including information gathering, network mapping, vulnerability identification, and penetration testing. The Kali Linux operating system was used as the testing environment, supported by tools such as Nmap, SQLMap, and OWASP ZAP. The results of the study revealed several security issues, including suboptimal security header configurations, outdated JavaScript libraries, and XSS vulnerabilities that were successfully blocked by the Web Application Firewall (WAF). Meanwhile, SQL Injection testing was unsuccessful due to the absence of injectable dynamic parameters and automatic blocking by the security system, indicated by HTTP 403 responses. Additionally, the website's SSL configuration supports TLS 1.2, although TLS 1.3 has not yet been activated. Overall, the Indodax.com website demonstrates a fairly strong security posture, but some technical improvements are still needed to enhance protection against evolving cyber threats.

***Keywords**: information security, penetration testing, ISSAF, Indodax.com, Kali Linux*