ABSTRAK

Seiring bertumbuhnya teknologi informasi secara pesat dapat memberikan hal yang positif dalam persebaran informasi. *Website* merupakan salah satu hasil dari perkembangan teknologi informasi sebagai media penyampaian informasi. XYZ sebagai *partner* transformasi pendidikan memiliki *website* yang berisi data-data sensitif seperti data pembelian paket kelas *bootcamp*, namun belum pernah dilakukan *penetration testing* untuk meningkatkan keamanan sistemnya. Penelitian ini menggunakan *framework* OWASP Top – 10 2021 dengan metode *black box testing* untuk melakukan pengujian penetrasi pada website XYZ. Pengujian dilakukan untuk mengidentifikasi potensi kerentanan keamanan yang mungkin dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Hasil pengujian menemukan beberapa kerentanan signifikan seperti masalah pada *user agent fuzzer*, *improper input validation*, *information disclosure*, kerentanan terkait *header* keamanan, *plugin* dan tema yang perlu diperbarui, risiko *brute force* dan *user enumeration*, serta *insufficient logging*. Rekomendasi perbaikan yang diberikan meliputi implementasi validasi input, *header* keamanan yang tepat, mekanisme anti-CSRF, perbaikan konfigurasi *cookie*, pembaruan *plugin* dan tema, implementasi rate limiting dan CAPTCHA, serta peningkatan sistem *logging* dan *monitoring*.

Kata kunci— **Kali Linux, Kejahatan *Cyber, Penetration Testing, Website***