ABSTRAK

Perkembangan teknologi informasi telah mengubah cara organisasi beroperasi dan berkomunikasi. Salah satu implementasi penting dari teknologi informasi adalah sistem informasi aplikasi berbasis *website*. Pada perusahaan PT. XYZ (Abc), sistem informasi telah diterapkan untuk menyediakan pelayanan kepada pelanggan. Serangan *cyber* seperti kebocoran data maupun akses terhadap layanan *website* dapat merugikan pihak perusahaan dan juga dapat mengganggu kegiatan operasional. Selain itu, keamanan *cyber* yang buruk atau sering diserang dapat merusak reputasi perusahaan. Penelitian ini bertujuan untuk menganalisis keaman sistem informasi *website* Abc pada PT. XYZ dengan *penetration testing* menggunakan metode *Open Web Application Security Project* (OWASP) Top-10 2021. Metode ini membantu mengidentifikasi potensi kerentanan keamanan yang terdapat pada *website* tersebut. Dari proses pengujian dan analisis yang telah dilakukan, hasil dari 10 daftar kerentanan yang dimiliki oleh OWASP Top 10 peneliti mendapatkan 4 daftar kerentanan yang berhasil ditemukan, yaitu desain yang tidak aman dengan skala menengah (*Insecure Design (medium)*), komponen yang rentan dan telah usang dengan skala menengah (*Vulnerable and Outdated Components (Medium)*), kegagalan integritas perangkat lunak dan data dengan skala tinggi (*Software and Data Integrity Failures (High),* serta kegagalan pencatatan dan pemantauan keamanan dengan skala menengah *Security Logging and Monitoring Failures (Medium)*).

Kata Kunci: Keamanan Sistem Informasi, *Penetration Testing,* OWASP TOP 10, *Website*.