ABSTRAK

Berkembangnya teknologi *website*, semakin banyak pihak yang memanfaatkannya sebagai media pendukung penyampaian informasi, termasuk lembaga daerah di Indonesia. Keamanan aplikasi *website* penting untuk memastikan integritas, kerahasiaan, dan ketersediaan data dalam lingkungan digital. Perusahaan Daerah XYZ merupakan salah satu unit usaha milik daerah yang bergerak di bidang mendistandaribusikan air bersih di daerah Surabaya, Pasuruan, Sidoarjo dan Gresik. Perusahaan Daerah XYZ mempunyai *website* yang bernama *Customer Information System* (CIS). *Website* sebagai media untuk membantu memberi informasi kepada pelanggan tentang pasang baru, pengaduan, tagihan dan pemakaian, informasi tagihan *online*, dan sebagainya. Dengan hal ini, keamanan sistem *website* rentan akan *bug* maupun virus dan itu perlu diuji menggunakan *Penetration Testing. Penetration Testing* adalah kegiatan mensimulasikan serangan yang dapat dilakukan terhadap jaringan organisasi atau perusahaan tertentu untuk menemukan kerentanan dan menguji ketahanan dalam sistem *website* jaringan berdasarkan standar kerangka ISSAF. Standar ini menawarkan beberapa keunggulan dibandingkan fitur keamanan lainnya dan bertindak sebagai penghubung antara perspektif teknis. Kerangka kerja ISSAF terdapat 9 penilaian pengujian yang mencakup *Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites dan Maintaining Access, Covering Tracks.* Tujuan dari tugas akhir ini adalah untuk mengetahui kerentanan keamanan informasi situs *website* dari *bug* maupun virus menggunakan *Penetration Testing* berdasarkan *Framework* ISSAF untuk membuat rekomendasi peningkatan keamanan pada situs *website* Perusahaan Daerah XYZ. Hasil penelitian dari tugas akhir ini analisis kerentanan pada situs web Perusahaan Daerah XYZ menunjukkan adanya beberapa kerentanan keamanan, namun situs tersebut masih dapat dianggap aman. Kerentanan yang ditemukan dapat diperbaiki melalui pembaruan server dengan mengupgrade OS pada sistem situs web.

Kata Kunci: Keamanan Sistem Informasi, Aplikasi *Website*, ISSAF, *Penetration Testing*, Perusahaan Daerah XYZ

ABSTRACT

With the development of website technology, more and more parties are using it as a supporting medium for conveying information, including regional institutions in Indonesia. Website application security is important to ensure the integrity, confidentiality and availability of data in a digital environment. XYZ Regional Company is a regionally owned business unit which operates in the field of standardizing clean water in the Surabaya, Pasuruan, Sidoarjo and Gresik areas. Regional Company XYZ has a website called Customer Information System (CIS). Website as a medium to help provide information to customers about new installations, complaints, bills and usage, online billing information, and so on. With this, the security of the website system is vulnerable to bugs or viruses and this needs to be tested using Penetration Testing. Penetration Testing is the activity of simulating attacks that can be carried out against a particular organization's or company's network to find vulnerabilities and test resilience in the network's website system based on the ISSAF framework standards. This standard offers several advantages over other security features and acts as a link between technical perspectives. The ISSAF framework contains 9 test assessments which include Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromising Remote Users/Sites and Maintaining Access, Covering Tracks. The aim of this final assignment is to determine the information security vulnerabilities of website sites from bugs and viruses using Penetration Testing based on the ISSAF Framework to make recommendations for improving security on the XYZ Regional Company website. The research results from this final project, vulnerability analysis on the XYZ Regional Company website show that there are several security vulnerabilities, but the site can still be considered safe. The vulnerabilities found can be fixed through server updates by upgrading the OS on the website system.

Keywords: Information System Security, Website Application, ISSAF, Penetration Testing, XYZ Regional Company