

ABSTRAK

Website saat ini menjadi keperluan bersama dengan meningkatnya pengguna yang tersambung ke jaringan internet. Yang mana hal ini dapat menimbulkan tindakan kejahatan *cyber* oleh pihak yang tidak bertanggung jawab. Maka diperlukannya Keamanan Sistem Informasi, yang dapat mengantisipasi adanya kejahatan *cyber*. *Website* PPDB sekolah XYZ memiliki peran penting, dimana terdapat data siswa baru hingga proses melakukan pembayaran pendaftaran. Oleh karena itu, penelitian ini melakukan analisis keamanan sistem informasi sebagai bentuk melindungi data pribadi siswa hingga *financial* yang ada pada *website* tersebut. Dalam penelitian ini, pendekatan *information system security assesment framework* (ISSAF) dapat digunakan untuk mengevaluasi keamanan sistem, jaringan komputer, hingga aplikasi atau *website*. Dalam pendekatan ISSAF terdapat 3 tahapan dalam evaluasi penilaian yaitu *planning and preparation, assesment, reporting, clean up and destroy artifacts*. Dari hal tersebut didapatkan beberapa hasil setelah melakukan hasil *penetration testing* berdasarkan *framework* ISSAF, yaitu teridentifikasinya profil perusahaan setelah melakukan *scan whois*, terdapat kerentanan pada *vulnerability scan*, dan adanya kerentanan XSS dan *file upload user* pada *penetration test*. Namun terdapat hasil tes yang tidak berhasil dilakukan untuk mendapatkan hak akses yaitu pada tahap *gaining access and privilege escalation* sehingga tidak dapat dilakukan tahap selanjutnya hingga *corvering tracks* karena *website* telah di konfigurasi dengan baik. Kemudian dilakukannya pemberian rekomendasi dan solusi untuk mengatasi celah keamanan yang ada pada *website* PPDB sekolah XYZ.

Kata Kunci: *Keamanan, Website, PPDB, ISSAF, Penetration Testing*

ABSTRACT

The website is now a shared necessity with the increasing number of users connected to the internet network. Which can lead to cyber crimes by irresponsible parties. So the need for Information System Security, which can anticipate the existence of cyber crimes. The XYZ school of registration website has an important role, where there is data on new students to the process of making registration payments. Therefore, this study conducts an analysis of information system security as a form of protecting students' personal and financial data on the website. In this study, the information system security assessment framework (ISSAF) approach can be used to evaluate the security of systems, computer networks, and applications or websites. In the ISSAF approach there are 3 stages in the evaluation of the assessment, namely planning and preparation, assessment, reporting, clean up and destroy artifacts. From this, several results were obtained after carrying out the results of penetration testing based on the ISSAF framework, namely the identification of company profiles after carrying out a whois scan, there were vulnerabilities in the vulnerability scan, and there were XSS vulnerabilities and user file uploads in the penetration test. However, there were test results that were not successfully carried out to obtain access rights, namely at the gaining access and privilege escalation stage so that the next stage could not be carried out until the bordering tracks because the website had been properly configured. Then provide recommendations and solutions to overcome security holes on the XYZ school registration website.

Keywords: Security, Website, Student Registration, ISSAF, Penetration Testing.