# INTISARI

SMK Negeri Jateng Di Purbalingga menyediakan informasi dalam sebuah website, di dalam website tersebut terdapat informasi seperti profil sekolah, informasi terkait pendaftaran online, informasi pengumuman seleksi calon siswa dan informasi lainnya. Berdasarkan hasil obervasi dan wawancara pengelola website, website tersebut belum pernah dilakukan pengujian sistem keamanan seperti scanning untuk mengetahui celah keamanan. Jika tidak memiliki sistem keamanan yang baik maka bisa mengakibatkan hal buruk bisa terjadi seperti pencurian data atau perubahan data yang tersimpan di website, serta adanya ancaman yang dapat menyerang sistem keamanan dan bisa menyebabkan kerugian. Tujuan dari penelitan ini adalah melakukan vulnerability scanning untuk mengetahui potensi celah keamanan pada website SMK Negeri Jawa Tengah Di Purbalingga. Metode yang digunakan vulnerability assessment, karena metode ini dapat memberikan berbagai informasi tentang kelemahan keamanan atau potensi ancaman terhadap sistem website. Dalam proses vulnerability assessment juga melibatkan penggunaan alat pengujian otomatis, seperti pemindai keamanan jaringan contohnya OWASP ZAP, acunetix, dan nessus. Dari pengujian kerentanan menggunakan OWASP ZAP, berhasil mengidentifikasi 1 kerentanan tingkat tinggi, 3 kerentanan tingkat menengah, 5 kerentanan tingkat rendah, dan 5 kerentanan tingkat informasi. Sementara itu, acunetix menghasilkan 27 kerentanan tingkat menengah, 2 kerentanan tingkat rendah, dan 3 kerentanan tingkat informasi. Nessus mendeteksi 1 kerentanan tingkat menengah dan 10 kerentanan tingkat informasi. Berdasarkan hasil ini, jika mengklasifikasikan tingkat keamanan situs web SMK Negeri Jawa Tengah Di Purbalingga dalam skala 1 hingga 3, maka tingkat keamanannya akan berada pada tingkat 2 (menengah). Hal ini menunjukan bahwa sistem keamanan pada website SMK Negeri Jawa Tengah Di Purbalingga belum cukup aman dan masih banyak hal yang harus dievaluasi dan diperbaiki.

Kata kunci: kerentanan, vulnerability assessment, OWASP, website

## *ABSTRACT*

*SMK Negeri Jateng Di Purbalingga provides information on a website, on the website there is information such as school profiles, information related to online registration, information on prospective student selection announcements and other information. Based on the results of observations and interviews with website managers, the website has never been tested for security systems such as scanning to find out security gaps. If it does not have a good security system, it can cause bad things to happen such as data theft or changes to data stored on the website, as well as threats that can attack the security system and can cause losses. The purpose of this research is to conduct vulnerability scanning to find out the potential security holes on the website of the Central Java State Vocational High School in Purbalingga. The method used is vulnerability assessment, because this method can provide various information about security weaknesses or potential threats to the website system. The vulnerability assessment process also involves the use of automated testing tools, such as network security scanners, for example OWASP ZAP, acunetix, and nessus. From vulnerability testing using OWASP ZAP, it successfully identified 1 high-level vulnerability, 3 medium-level vulnerabilities, 5 low-level vulnerabilities, and 5 information-level vulnerabilities. Meanwhile, acunetix produced 27 medium-level vulnerabilities, 2 low-level vulnerabilities, and 3 information-level vulnerabilities. Nessus detected 1 medium-level vulnerability and 10 information-level vulnerabilities. Based on these results, if classifying the security level of the website of SMK Negeri Jawa Tengah Di Purbalingga on a scale of 1 to 3, then the security level will be at level 2 (medium). This shows that the security system on the website of SMK Negeri Jawa Tengah Di Purbalingga is not secure enough and there are still many things that must be evaluated and improved.*



*Keyword: vulnerability, vulnerability assessment, OWASP, website*