ANALISIS KEAMANAN *WEBSITE* SMAN 77 JAKARTA MENGGUNAKAN METODE *WEB SECURITY TESTING GUIDE*

Muhamad Safar Astakusuma

ABSTRAK

Pesatnya perkembangan teknologi informasi di era digital membawa berbagai kemudahan, namun di sisi lain juga meningkatkan risiko keamanan siber yang dapat merugikan banyak pihak. Website sekolah sebagai salah satu media informasi publik dan layanan administratif tidak terlepas dari ancaman tersebut, termasuk kemungkinan adanya serangan siber seperti injeksi SQL, kontrol akses yang lemah, serta kebijakan kata sandi yang tidak memadai. Oleh karena itu, penelitian ini dilakukan dengan tujuan untuk menganalisis tingkat keamanan website SMAN 77 Jakarta terhadap serangan yang paling umum, yaitu kerentanan terhadap kontrol akses file atau direktori, *Injection*, kegagalan identifikasi dan otentikasi, dan kesalahan konfigurasi keamanan. Metode yang digunakan mengacu pada panduan OWASP Web Security Testing Guide (WSTG) dengan pendekatan penetration testing yang dilakukan pada salinan lokal website menggunakan akun admin untuk memeriksa form login dan halaman admin secara spesifik. Terdapat beberapa kerentanan dari hasil pengujian yang dilakukan analisis dengan bantuan CVSS pada aspek base score metrics untuk mengukur tingkat keparahan kerentanan.

Kata Kunci: *Website*, Burp Suite, OWASP WSTG, *Penetration Testing*, CVSS

SECURITY ANALYSIS OF THE SMAN 77 JAKARTA WEBSITE USING THE WEB SECURITY TESTING GUIDE METHOD

Muhamad Safar Astakusuma

ABSTRACT

The rapid development of information technology in the digital era brings various conveniences, but on the other hand also increases cybersecurity risks that can harm many parties. School websites as one of the public information media and administrative services are not free from these threats, including the possibility of cyber attacks such as SQL injection, weak access control, and inadequate password policies. Therefore, this study was conducted with the aim to analyze the security level of SMAN 77 Jakarta's website against the most common attacks, namely vulnerabilities to file or directory access control, Injection, identification and authentication failures, and security configuration errors. The method used refers to the OWASP Web Security Testing Guide (WSTG) with a penetration testing approach conducted on a local copy of the website using an admin account to check the login form and admin page specifically. There are several vulnerabilities from the test results that are analyzed with the help of CVSS on the base score metrics aspect to measure the severity of the vulnerability.

Keywords: Website, Burp Suite, OWASP WSTG, Penetration Testing, CVSS