

## ABSTRAK

Perkembangan pesat teknologi berbasis *website*, telah membuat kemudahan dalam memperoleh dan melihat data yang ada di internet semakin mudah. Pemanfaatan *website* melalui aplikasi telah mendorong penggunaan di berbagai sektor secara luas, termasuk sektor pemerintahan. Namun, kemudahan yang diberikan berbanding lurus dengan meningkatnya resiko keamanan siber juga semakin nyata, yang mengakibatkan perlu adanya keamanan terhadap kerahasiaan dan integritas data publik. Penelitian dilakukan karena aplikasi *website* Lapormasbup mengelola data pribadi sensitif warga seperti Nama Lengkap, Nomor Induk Kependudukan (NIK), dan alamat, serta mengalami lonjakan traffic IP address yang tidak wajar pada periode Februari–Maret 2026 yang mengindikasikan adanya percobaan serangan siber. Tujuan penelitian ini adalah menganalisis tingkat keamanan aplikasi *website* Lapormasbup menggunakan metode *penetration testing* berbasis framework ISSAF yang mencakup tiga fase, yaitu *Planning and Preparation*, *Assessment*, dan *Reporting, Clean Up and Destroy Artifacts*. Pengujian dilakukan menggunakan tools ZAP, Nmap, Whatweb, Whois, SQLmap, Burp Suite, dan Metasploit Framework. Hasil pemindaian menggunakan ZAP (Zed Attack Proxy) mengidentifikasi 17 kerentanan yang terdiri dari 6 kerentanan berlevel medium, 6 berlevel low, dan 5 bersifat informational, tanpa ditemukan kerentanan berlevel high. Percobaan serangan *Cross-Site Request Forgery* (CSRF), *Cross-Site Scripting* (XSS), SQL Injection, dan *brute force* seluruhnya tidak berhasil menembus sistem karena *website* telah dilindungi oleh *Web Application Firewall* (WAF) dan *reCAPTCHA*. Kesimpulan penelitian menunjukkan bahwa tingkat keamanan *website* Lapormasbup berada pada level cukup baik, meskipun masih terdapat celah konfigurasi yang perlu diperbaiki melalui penambahan header keamanan dan audit berkala.

Kata kunci: Keamanan *Website*, *Penetration Testing*, ISSAF, ZAP (*Zed Attack Proxy*), Lapormasbup.

## ABSTRACT

*The rapid development of website-based technology has made it increasingly easier to obtain and view data on the internet. The use of websites through applications has driven widespread adoption across various sectors, including the government sector. However, the convenience provided is directly proportional to the increasing risk of cybersecurity threats, making it necessary to protect the confidentiality and integrity of public data. This research was conducted because the Lapormasbup website application manages sensitive personal data of citizens such as full names, National Identity Numbers (NIK), and addresses, and experienced an abnormal surge in IP address traffic during the period of February–March 2026, indicating attempted cyberattacks. The purpose of this study is to analyze the security level of the Lapormasbup website application using the ISSAF-based penetration testing method, which encompasses three Phases: Planning and Preparation, Assessment, and Reporting, Clean Up and Destroy Artifacts. Testing was conducted using ZAP, Nmap, Whatweb, Whois, SQLmap, Burp Suite, and Metasploit Framework. The scan results using ZAP (Zed Attack Proxy) identified 17 vulnerabilities consisting of 6 medium-level, 6 low-level, and 5 informational vulnerabilities, with no high-level vulnerabilities found. Attempted attacks including Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS), SQL Injection, and brute force all failed to penetrate the system as the website is protected by a Web Application Firewall (WAF) and reCAPTCHA. The study concludes that the security level of the Lapormasbup website is at a reasonably good level, although configuration gaps remain that need to be addressed through the addition of security headers and regular security audits.*

**Keywords:** Website Security, Penetration Testing, ISSAF, ZAP (Zed Attack Proxy), Lapormasbu