INTISARI

Perkembangan teknologi informasi mendorong pemerintah desa untuk memanfaatkan website sebagai media layanan publik dan penyampaian informasi yang transparan serta akuntabel. Website Desa Kalipelus Kabupaten Banjarnegara berfungsi sebagai pusat informasi desa, namun pemanfaatannya belum optimal, baik dari sisi pembaruan konten, fitur interaktif, maupun aspek teknis. Selain itu, website desa umumnya belum melalui pengujian keamanan yang memadai sehingga berpotensi menimbulkan risiko terhadap kerahasiaan dan integritas data. Penelitian ini bertujuan untuk menganalisis tingkat keamanan Website Desa Kalipelus Kabupaten Banjarnegara dengan mengidentifikasi kerentanan sistem menggunakan metode Penetration Testing Execution Standard (PTES). Metode PTES diterapkan melalui tahapan pre-engagement interaction, intelligence gathering, threat modeling, vulnerability analysis, exploitation, dan reporting. Pengujian difokuskan pada website kalipelus-banjarnegara.desa.id dengan ruang lingkup eksploitasi kerentanan SQL Injection, Absence of Anti-CSRF Tokens, dan Cross Site Scripting (XSS). Proses pengujian dilakukan secara legal dan terukur untuk memastikan keamanan sistem tanpa mengganggu layanan publik. Hasil penelitian menunjukkan bahwa Website Desa Kalipelus masih memiliki beberapa kerentanan keamanan, khususnya SQL Injection, Absence of Anti-CSRF Tokens, dan Cross Site Scripting (XSS), yang berpotensi dimanfaatkan oleh pihak tidak berwenang untuk mengakses, memodifikasi, atau merusak data. Temuan ini menunjukkan bahwa meskipun tingkat keamanan website tergolong cukup aman, peningkatan keamanan dan pengujian berkala tetap diperlukan guna mendukung perlindungan data serta peningkatan kualitas layanan publik desa.

Kata Kunci: PTES, Situs Web Desa, Keamanan Informasi, Pengujian Penetrasi, Kerentanan.

ABSTRACT

Advances in information technology have encouraged village governments to utilize websites as a medium for public services and the dissemination of transparent and accountable information. The Kalipelus Village website in Banjarnegara Regency serves as a village information center, but its utilization has not been optimal in terms of content updates, interactive features, and technical aspects. In addition, village websites generally have not undergone adequate security testing, which could potentially pose a risk to data confidentiality and integrity. This study aims to analyze the security level of the Kalipelus Village website in Banjarnegara Regency by identifying system vulnerabilities using the Penetration Testing Execution Standard (PTES) method. The PTES method is applied through the stages of pre-engagement interaction, intelligence gathering, threat modeling, vulnerability analysis, exploitation, and reporting. The testing focused on the kalipelus-banjarnegara.desa.id website with the scope of exploiting SQL Injection, Absence of Anti-CSRF Tokens, and Cross Site Scripting (XSS) vulnerabilities. The testing process was carried out legally and measurably to ensure system security without disrupting public services. The results of the study show that the Kalipelus Village Website still has several security vulnerabilities, particularly SQL Injection, Absence of Anti-CSRF Tokens, and Cross Site Scripting (XSS), which could potentially be exploited by unauthorized parties to access, modify, or damage data. These findings indicate that although the website's security level is relatively secure, security enhancements and periodic testing are still necessary to support data protection and improve the quality of public services in the village.

Keywords: PTES, Village Website, Information Security, Penetration Testing, Vulnerabilities.