

EVALUASI KERENTANAN WEBSITE POLBENG MENGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)

Nama : Novan Rusdy Ardiansyah
NIM : 6404211076
Dosen Pembimbing : Rezki Kurniati, M.Kom

ABSTRAK

Keamanan website merupakan aspek penting dalam menjaga integritas dan ketersediaan layanan informasi. Penelitian ini bertujuan untuk menganalisis tingkat keamanan website polbeng.ac.id dengan menggunakan beberapa teknik pengujian, yaitu pemindaian kerentanan, pengujian brute-force, dan pengujian Cross-Site Scripting (XSS). Alat yang digunakan meliputi WPScann, Hydra, XSSStrike, dan XSSer. Pengujian brute-force pada halaman login WordPress tidak berhasil karena sistem keamanan server mampu mendeteksi dan membatasi percobaan login berulang. Pengujian XSS menggunakan XSSStrike menemukan adanya refleksi input pada parameter pencarian, namun payload tidak dapat dieksekusi sehingga tidak terbukti sebagai kerentanan XSS. Sementara itu, XSSer hanya berhasil menjalankan payload pada URL simulasi dan bukan pada halaman asli website, sehingga tidak dapat dikategorikan sebagai kerentanan nyata. Hasil penelitian menunjukkan bahwa website telah memiliki mekanisme keamanan yang cukup baik dalam mencegah serangan brute-force dan XSS, meskipun pemantauan keamanan dan pembaruan sistem tetap perlu dilakukan secara berkala. Penelitian ini diharapkan dapat menjadi referensi dalam meningkatkan keamanan website serta mendorong upaya pemeliharaan berkelanjutan pada sistem yang digunakan.

Kata Kunci: Keamanan Website, Penetration Testing, WPScann, Hydra, XSS, XSSStrike, XSSer

VULNERABILITY EVALUATION OF POLBENG WEBSITE USING THE PENETRATION TESTING EXECUTION STANDARD (PTES) METHOD

Name : Novan Rusdy Ardiansyah
Student ID : 6404211076
Supervisor : Rezki Kurniati, M.Kom

ABSTRACT

Website security plays a critical role in maintaining the integrity and availability of information services. This research aims to analyze the security level of the polbeng.ac.id website using several penetration testing techniques, including vulnerability scanning, brute-force testing, and Cross-Site Scripting (XSS) evaluation. The tools used in this study include WPScann, Hydra, XSSStrike, and XSSer. The brute-force testing conducted on the WordPress login page did not succeed, as the server's security system was able to detect and limit repeated login attempts. XSS testing using XSSStrike identified reflected input in the search parameter, but the payloads could not be executed, indicating that the website is not vulnerable to XSS through that vector. Meanwhile, XSSer was only able to execute payloads on a simulated URL and not on the actual website, meaning that no real vulnerability could be confirmed. Overall, the results show that the website has implemented adequate security mechanisms to mitigate brute-force and XSS attacks, although continuous monitoring and regular system updates remain essential. This research is expected to serve as a reference for improving website security and supporting ongoing maintenance efforts within the system.

Keywords: Website Security, Penetration Testing, PTES, WPScann, Hydra, XSS, XSSStrike, XSSer.