UJI PENETRASI KEAMANAN *WEBSITE* DINAS KOMUNIKASI DAN INFORMATIKA

Nama	:	Rimba Dirgantara
NIM	:	6404211035
Dosen Pembimbing Utama	:	Rezki Kurniati, M.Kom.
Dosen Pembimbing Pendamping	:	Nurmi Hidayasari, ST., M.Kom.

ABSTRAK

Website resmi Dinas Komunikasi dan Informatika Kabupaten XYZ adalah sarana publikasi, interaksi, dan promosi potensi daerah. Website ini memiliki peran penting dalam menyebarkan informasi pemerintah kepada masyarakat. Namun, kerentanannya terhadap serangan seperti *SQL Injection*, *Brute Force*, *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF), dan *Distributed Denial of Service* (DDoS) dapat mengancam integritas data dan ketersediaan layanan. Penelitian ini bertujuan mengidentifikasi celah keamanan melalui serangan otomatis dan manual. Hasilnya menunjukkan bahwa *SQL Injection* berhasil mengekstrak data, sementara *Brute Force* gagal memperoleh kredensial *valid*. Proteksi yang ada mampu mencegah serangan XSS dan CSRF. Serangan DDoS tidak berdampak signifikan berkat penggunaan layanan mitigasi. Rekomendasi keamanan meliputi validasi dan sanitasi *input*, penggunaan *Query Builder* dan *prepared statement*, pembaruan *framework*, serta penerapan CAPTCHA dan pembatasan *login*. Sebagai solusi deteksi dan respons *real-time*, *Snort* direkomendasikan sebagai *Intrusion Detection System* (IDS). Penelitian ini diharapkan meningkatkan kesadaran akan pentingnya pengamanan *website* dan menyediakan langkah konkret untuk mengurangi risiko serangan pada *website* Dinas Komunikasi dan Informatika Kabupaten XYZ.

Kata Kunci: Uji Penetrasi, Keamanan *Website*, *SQL Injection*, *Brute Force*, XSS, CSRF, *Snort*, *Intrusion Detection System*

WEBSITE SECURITY PENETRATION TEST FOR THE COMMUNICATIONS AND INFORMATICS OFFICE

Name	:	*Rimba Dirgantara*
NIM	:	*6404211035*
Primary Supervisor	:	*Rezki Kurniati, M.Kom.*
Co-Supervisor	:	*Nurmi Hidayasari, ST., M.Kom.*

ABSTACT

The official website of the Department of Communication and Informatics of XYZ Regency serves as a medium for publication, interaction, and promotion of regional potential. This website plays a crucial role in disseminating government information to the public. However, its vulnerability to attacks such as SQL Injection, Brute Force, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and Distributed Denial of Service (DDoS) poses threats to data integrity and service availability. This research aims to identify security loopholes through automated and manual attacks. The results show that SQL Injection successfully extracted data, while Brute Force failed to obtain valid credentials. Existing protections were effective in preventing XSS and CSRF attacks. The DDoS attack had no significant impact due to mitigation services in place. Security recommendations include input validation and sanitization, the use of Query Builder and prepared statements, framework updates, as well as implementing CAPTCHA and login attempt restrictions. For real-time attack detection and response, Snort is recommended as an Intrusion Detection System (IDS). This study is expected to raise awareness of the importance of website security and provide practical measures to reduce the risk of attacks on the official website of the Department of Communication and Informatics of XYZ Regency.

Keywords*: Penetration testing, Website security, SQL Injection, Brute Force, XSS, CSRF, Snort*, *Intrusion Detection System*