

## ABSTRAK

Meningkatnya penggunaan internet dari tahun ke tahun seiring dengan perkembangan pesat teknologi informasi dan komunikasi, termasuk website, menjadikan website sebagai salah satu media penting yang digunakan pemerintah untuk menyebarkan dan memperoleh informasi. Namun, perhatian khusus perlu diberikan terhadap keamanan dalam pengembangan website pemerintah, mengingat banyaknya kasus kebocoran data masyarakat yang bersumber dari server milik pemerintah. Hal ini dapat menurunkan kepercayaan masyarakat kepada pemerintah.

Website Desa Sudagaran yang dikelola oleh Kemendikbud menjadi objek penelitian ini untuk mengidentifikasi dan mengevaluasi tingkat keamanannya. Penelitian dilakukan menggunakan metode penetration testing dan mengacu pada OWASP Top 10, dengan langkah-langkah identifikasi kerentanan dan simulasi penyerangan pada kerentanan yang ditemukan.

Hasil implementasi menunjukkan adanya beberapa kerentanan, seperti SQL Injection, Cross-Site Scripting (XSS), dan kelemahan konfigurasi keamanan. Rekomendasi mitigasi mencakup penerapan header keamanan, validasi input, penggunaan HTTPS, dan pembaruan komponen yang usang. Implementasi langkah mitigasi ini diharapkan dapat meningkatkan keamanan website dan memulihkan kepercayaan masyarakat terhadap layanan berbasis digital.

**Kata kunci:** *owasp, penetration testing, website, pemerintah, Banyumas*