ABSTRAK

Seiring dengan perkembangan teknologi, informasi sangat mudah untuk diperoleh dan disebarluaskan serta menjadi salah satu aset penting bagi perusahaan. Keamanan sistem menjadi salah satu bagian dalam perkembangan teknologi. Sistem informasi harus memastikan kerahasiaan, ketersediaan, dan integritas pada semua sumber daya informasi. Instansi XYZ adalah salah satu instansi kesehatan yang menggunakan sistem informasi berbasis *website* untuk media informasi kesehatan. Namun bedasarkan hasil wawancara kepada koordinator IT pada instansi XYZ yang menyatakan bahwa *website* instansixyz.com pernah terjadi tindakan peretasan dengan mengganti tampilan *website*. Hal ini membuktikan bahwa *website* instansixyz.com rentan terhadap serangan, serta *website* antrianinstansixyz.com yang berisi data sensitif pasien seperti KTP, NIK, Alamat, dll, juga berpotensi mendapatkan serangan serupa seperti instansixyz.com, maka perlu dilakukan pengujian keamanan untuk meminimalisir celah kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Tujuan dilakukan penelitian ini adalah melakukan analisis kerentanan pada *website* Instansi XYZ untuk mengetahui apa saja kerentanan pada *website* dan memberikan rekomendasi kepada pihak Instansi. Metode yang digunakan pada penelitian ini adalah penetration testing dengan pendekatan framework OWASP. Hasil penelitian ditemukan berapa kerentanan dengan menggunakan *tools* yang berbeda. Ditemukan sebanyak 21 kerentanan yang berbeda pada kedua *wesbite*. Dari kerentanan yang ditemukan peneliti membuat rekomendasi perbaikan untuk pengembang *website* dalam meningkatkan keamanan bagi kedua *website*.

Kata Kunci: Keamanan Sistem, OWASP, *Penetration Testing*.