ABSTRAK

Internet menjadi salah satu kebutuhan yang tidak akan pernah lepas dari kehidupan masyarakat saat ini. Internet menjadi media yang digunakan masyarakat untuk berkomunikasi, mencari data atau informasi, menyalurkan kreativitas, mendukung kegiatan ekonomi dan bisnis, serta masih banyak lagi. Saat masyarakat melakukan akses ke internet salah satu unsur dari internet yang akan selalu diakses adalah situs web. Setiap informasi yang diberikan di internet dari sumber manapun akan memiliki situs web masing-masing yang pemiliknya buat untuk menampilkan informasi atau data yang diperlukan. Tidak terkecuali Yayasan Kesehatan XYZ yang memiliki situs web agar dapat dengan mudah memberikan informasi dan data yang dapat diketahui oleh masyarakat umum. Dengan tingginya penggunaan akses internet dan situs web, ancaman keamanan terhadap integritas dan kerahasiaan suatu informasi serta sumber daya yang ada pada situs web menjadi masalah besar. Pengujian kerentanan dan keamanan dapat mencegah terjadinya insiden siber pada situs web terkait. Pengujian yang dilakukan dalam penelitian ini menggunakan metode *black box testing* dan standar NIST SP 800 – 115. Analisis kerentanan dilakukan menggunakan beberapa *tools* seperti Zenmap, OWASP ZAP, dan Burp Suite. Dari analisis kerentanan ditemukan bahwa pada situs web Yayasan Kesehatan XYZ terdapat 12 celah kerentanan yang terdiri dari 4 kerentanan dengan tingkat *risk medium*, 6 kerentanan dengan tingkat *risk low*, dan 2 kerentanan dengan tingkat *risk informational*. Pada tahap pengujian kerentanan dengan Burp Clickbandit menghasilkan informasi adanya celah potensi serangan *ClickJacking*. Setelah dilakukan pengujian dan analisis dihasilkan rekomendasi yang dapat dijadikan acuan untuk membuat situs web Yayasan Kesehatan XYZ lebih aman.

Kata kunci: situs web, analisis kerentanan, keamanan, NIST SP 800 – 115.