BAB V

PENUTUP

5.1 Kesimpulan

Dengan ditemukannya kerentanan pada situs web rsjsh.co.id dalam penelitian ini, serta kerentanan tersebut dapat dibuktikan kebenarannya. Hasil pengujian keamanan situs web rsjsh.co.id mengidentifikasi 11 kerentanan, terdiri dari 3 kerentanan bertingkat risiko sedang, 4 kerentanan risiko rendah, dan 4 kerentanan bersifat informasional. Ketiga kerentanan sedang meliputi *Content Security Policy (CSP), clickjacking*, dan *mixed content*, yang masing-masing dieksploitasi melalui metode validasi, injeksi XSS, injeksi SQL, penggunaan skrip HTML dengan iframe, serta alat seography.io untuk mendeteksi halaman HTTP pada koneksi HTTPS. Dampak dari kerentanan tersebut beragam, seperti peningkatan risiko serangan XSS yang dapat mencuri data sensitif, eksploitasi clickjacking yang dapat mengecoh pengguna untuk tindakan yang tidak disadari, serta potensi serangan man-in-the-middle akibat mixed content yang mengancam privasi data dan menurunkan kepercayaan pengguna. Untuk mengatasi masalah ini, implementasi kebijakan CSP menjadi rekomendasi utama, diikuti dengan perbaikan konfigurasi header keamanan dan penghapusan konten campuran. Berdasarkan analisis CVSS v3.1 dan *OWASP Risk Rating*, tingkat risiko keseluruhan sistem dikategorikan sedang (*medium*).

5.2 Saran

Berikut merupakan saran yang dapat diberikan berdasarkan hasil pengujian keamanan yang telah dilakukan:

1. Melakukan perbaikan kerentanan sesegera mungkin guna mengurangi potensi eksploitasi yang dapat merugikan sistem maupun Rumah Sakit.

2. Lakukan *penetration testing* secara berkala guna mengidentifikasi dan memperbaiki kerentanan keamanan.
3. Pembaruan sistem secara rutin guna menjaga keamanan sistem dari ancaman yang baru ditemukan.

Untuk penelitian selanjutnya, disarankan untuk melakukan pengujian yang lebih mendalam menggunakan alat-alat lain untuk pengujian seperti *Nessus Professional* untuk mencari kerentanan dan *ParamSpider*,dan *Dalfox* yang dapat dijalankan pada Kali Linux untuk melakukan simulasi serangan XSS guna membandingkan hasi analisa yang diperoleh dan menilai sejauh mana metode *penetration testing* dapat diimplementasikan secara luas.