BAB I

PENDAHULUAN

1.1 Latar Belakang

Berdasarkan penelitian Fortinet, kecepatan serangan siber di Indonesia meningkat 43% pada 2024 dibandingkan 2023. Serangan ini menargetkan berbagai sektor, termasuk organisasi, industri, individu, dan pemerintah. Dengan meningkatnya ancaman, kesadaran akan keamanan informasi menjadi tanggung jawab setiap pengguna internet.

Kesadaran akan keamanan informasi memiliki peran krusial dalam melindungi data sensitif dari berbagai ancaman siber. Hal ini juga membantu meningkatkan kemampuan individu dalam mengelola sistem informasi secara lebih efektif dan memastikan bahwa langkah-langkah pencegahan dapat diterapkan. Dengan kesadaran yang tinggi, kepatuhan terhadap aturan yang berlaku dapat terjaga, sehingga kerahasiaan, integritas, dan ketersediaan informasi tetap aman di era digital ini (Budiningsih et al., 2019).

Dalam jasa kesehatan, untuk dapat bersaing serta bertahan dalam hal Rumah Sakit, perlu adanya analisis pada perencanaan strategi digital (Mustajib & Kurniawati, 2023). Untuk memaksimalkan strategi digital, Rumah Sakit Soeharto Heerdjan memiliki *website* yang sudah cukup infromatif dan memiliki tampilan yang menarik. Rumah Sakit Soeharto Heerdjan memanfaatkan *website* untuk menyediakan informasi penting bagi pasien dan staf. Namun, *IBM Cost of Data Breach Report* 2024 menunjukkan bahwa sektor kesehatan mengalami kerugian terbesar akibat kebocoran data, karena tingginya risiko pencurian data sensitif seperti rekam medis pasien. Dari laporan tersebut, bisa diartikan bahwa sektor kesehatan memiliki kerentanan yang paling tinggi untuk diserang oleh peretas yang tidak bertanggung jawab.

Tanpa pengamanan yang memadai, *website* berpotensi menjadi pintu masuk peretas. Oleh karena itu, penting dilakukan pengujian keamanan untuk menurunkan risiko serangan. Rumah Sakit Dr. Soeharto Heerdjan memiliki tiga komponen utama untuk mendukung ketahanan sibernya: *website* sebagai komponen digital, ruang server sebagai komponen fisik, dan Tim SIRS sebagai komponen manusia. *Website* rumah sakit ini terus diperbarui untuk memberikan informasi terbaru kepada pasien. Mengingat peran pentingnya, pengujian keamanan diperlukan untuk menemukan dan memperbaiki kerentanan sebelum disalahgunakan peretas.

Rumah Sakit Soeharto Heerdjan, sebelumnya bernama Rumah Sakit Grogol, didirikan untuk mendukung kesehatan jiwa masyarakat Grogol. Berganti nama pada 2002, rumah sakit ini menawarkan layanan unggulan di bidang Psikiatri Anak dan Remaja, Psikiatri Dewasa, serta layanan umum seperti Gigi dan Rehabilitasi Medik. Dengan semakin pesatnya kemajuan teknologi dan tingginya serangan siber, RS Soeharto Heerdjan harus memastikan komponen-komponennya mendukung ketahanan siber untuk melindungi sistem dan menjaga kelancaran operasional.

Sebagai upaya peningkatan keamanan, pengujian dengan metode *Penetration testing* serta penilaian risiko dapat membantu Tim SIRS mengidentifikasi kerentanan sebelum dimanfaatkan oleh pihak tak bertanggung jawab. Penelitian ini berbeda dengan penelitian sebelumnya, di mana selain menggunakan metode *Penetration testing* yang mengacu pada klasifikasi kerentanan OWASP *Top* 10 2021, penelitian ini juga memanfaatkan dua alat penilaian risiko, yaitu CVSS (*Common Vulnerability Scoring System)* dan *OWASP Risk Rating Calculator*. Penggunaan kedua alat ini memungkinkan penilaian risiko yang lebih komprehensif dan akurat, sehingga setiap kerentanan dapat diprioritaskan sesuai tingkat urgensi dan dampaknya. Dengan pendekatan yang sistematis, diharapkan

keamanan dan ketahanan siber *website* rumah sakit dapat terus ditingkatkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah tertulis diatas, rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Apa saja kerentanan keamanan yang terdapat pada *website* RS Soeharto Heerdjan?
2. Bagaimana metode ekploitasi yang dapat digunakan untuk memanfaatkan kerentanan tersebut?
3. Sejauh mana dampak dari kerentanan tersebut terhadap keamanan data pasien dan operasional *website*?
4. Adakah rekomendasi perbaikan keamanan informasi yang bisa diberikan kepada rumah sakit?

1.3 Batasan Masalah

Agar terhindar dari luasnya masalah dan kerentanan yang ditemukan pada saat penelitian, maka dibuatkan Batasan – Batasan untuk membatasi masalah dan kerentanan yang ditemukan. Beberapa Batasan tersebut tercantum sebagai berikut:

1. Pengujian dibatasi hanya pada sistem ketahanan siber yang dimiliki oleh RS Soeharto Heerdjan.
2. Pengujian dan penilaian hanya pada *website* RS Soeharto Heerdjan yang beralamat rsjsh.co.id
3. Pengujian keamanan mengacu pada klasifikasi kerentanan dari 3 *Poin* yang ada pada *OWASP Top* 10 2021 yaitu *Injection* (A03), *Insecure Design* (A04) dan *Security Missconfiguration* (A05).
4. Pengujian hanya pada temuan kerentanan yang ada berdasarkan panduan *Owasp Testing Guide* v4 dengan metode *Black Box Testing*, tidak menilai kerentanan yang tidak ditemukan.
5. Pemindaian dan Ekploitasi menggunakan *tools – tools* yang sudah ada diantaranya *OWASZAP, Sqlmap, SSL Labs,*

Nslookup, Whatweb, Whois, Burp Suite, Seography.io dan Nmap.

6. Pengujian hanya dilakukan pada kerentanan yang memiliki tingkat risiko *medium* atau lebih.
7. Penilaian risiko menggunakan CVSS 3.1 *Calculator & Owasp Risk Rating Calculator*

1.4 Manfaat Penelitian

Manfaat dari penelitian ini terbagi menjadi dua manfaat yaitu manfaat bagi rumah sakit dan peneliti, untuk penjelasan lebih lanjut maka dipaparkan manfaat – manfaat tersebut dibawah ini.

1.4.1 Manfaat bagi rumah sakit

Manfaat yang didapat oleh perusahaan adalah menghasilkan laporan dan saran perbaikan yang didapat dari kerentanan yang ditemukan dari ketahanan siber yang dimiliki rumah sakit serta meningkatkan kesadaran akan pentingnya keamanan dan ketahanan siber guna menjaga lancarnya kegiatan operasional serta data – data yang tersimpan.

1.4.2 Manfaat bagi peneliti

Selain untuk menyelesaikan tugas akhir kuliah, penelitian ini sangat bermanfaat untuk peneliti karena meningkatkan skill dan ilmu baru dalam bidang keamanan informasi, serta dapat mengimplementasikan teori yang didapat didalam perkuliahan kedalam bidang industri. Manfaat yang lain yang didapat oleh peneliti yaitu keterampilan bersosial, berdiskusi, dan bekerjasama dalam memecahkan masalah.

1.5 Tujuan

Penelitian ini memiliki tujuan – tujuan sebagai berikut :

1. Mengindentifikasi kerentanan keamanan yang ada pada *website* RS Soeharto Heerdjan menggunakan metode *penetration testing.*
2. Melakukan eksploitasi terhadap kerentanan yang ditemukan untuk memahami dampak dan risiko yang mungkin terjadi.

3. Memberikan penilaian risiko berdasarkan temuan kerentanan untuk membantu prioritisasi mitigasi.
4. Menyusun rekomendasi keamanan yang praktis dan aplikatif untuk meningkatkan perlindungan *website* RS Soeharto Heerdjan dari ancaman siber.