BAB I

PENDAHULUAN

1.1 Latar Belakang

PT XYZ, sebuah perusahaan yang mengembangkan aplikasi apotek dan klinik bernama XYZ, memiliki peran krusial dalam manajemen data bisnis apotek dan klinik. Aplikasi ini mendukung manajemen data obat, pasien, rekam medis, keuangan, dan analisis data. Penggunaan sistem informasi *website* juga menjadi suatu kebutuhan penting dalam menjalankan operasional perusahaan. Seiring berjalannya waktu, perkembangan digital seperti *website* telah menjadi sumber informasi berharga yang meluas di berbagai sektor industri (Nisa, Adi Putra, et al., 2022). Keamanan informasi menjadi prioritas bagi setiap instansi guna menghindari gangguan atau tindakan kejahatan. Ancaman keamanan, seperti serangan malware, eksploitasi, injeksi database, dan lain sebagainya, tersebar luas di internet (Darojat et al., 2022a). Salah satu ancaman utama adalah serangan web, yang dapat terjadi baik dari pengguna terhadap situs web maupun sebaliknya. Meskipun sering kali ditargetkan pada server web karena menyimpan data berharga dari banyak pengguna, serangan semacam itu dapat mencoba memanipulasi sistem manajemen basis data untuk mengakses informasi yang sensitif (Wibowo, 2021). Dengan meningkatnya ancaman keamanan *cyber*, perusahaan seperti PT XYZ perlu memastikan bahwa sistem informasi *website* mereka terlindungi dari serangan. Ancaman *cyber* yang umum terjadi pada laman web adalah gangguan atau peretasan pada layanan sistem, ini menjadi salah satu faktor krusial yang sering dihadapi berbagai perusahaan yang menggunakan layanan berbasis teknologi digital (Dermawan et al., 2023). Seiring dengan ramainya penggunaan teknologi, peningkatan ancaman siber sebesar 6,15% yang terjadi di Indonesia dari tahun 2020 s/d 2021, ancaman yang sering terjadi di antaranya serangan Injeksi dan *Denial of Service (Dos) Attack* yang berupa serangan *synflood* dan ICMP *flood, phising*, serta pencurian data pribadi. Berdasarkan kasus serangan cyber yang menargetkan instansi Kesehatan pada 2020 sekitar 279 juta data warga Indonesia, termasuk mereka yang sudah meninggal dunia diretas dan dijual di forum daring. Data itu diduga berasal dari badan penyelenggara layanan kesehatan, BPJS Kesehatan (Parulian et al., 2021). Maka sistem informasi pada klinik atau layanan kesehatan juga beresiko menjadi sasaran serangan cyber, hal ini didukung dengan hasil wawancara kepada koordinator perusahaan XYZ yang menyatakan bahwa website XYZ pernah terjadi tindakan peretasan berupa serangan injeksi. Konteks kajian penelitian ini yaitu khususnya berhubungan dengan PT XYZ yang mana perusahaan ini memiliki basis data pribadi dan terdaftar secara resmi di Pemerintah RI. Tentunya juga mendapatkan perlindungan secara hukum. Dalam aspek ekonomi

politik, kedaulatan data suatu negara dihadapkan pada posisi negara dengan sektor swasta dalam konteks global. Peran negara utamanya adalah untuk menghasilkan regulasi perlindungan data siber dan keamanan siber. Jaminan perlindungan data pribadi merupakan hak warga negara yang membutuhkan kapasitas dan kapabilitas warga negara (Aji, 2023). Upaya menjaga keamanan data dan informasi, metode penetration testing menjadi relevan. Penetration testing, atau pentesting, merupakan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan (Azis & Fattah, 2019a). Pada penerapan penetration testing pada *website*, PT XYZ mengacu pada standar OWASP (Open Web Application Security Project) TOP 10 sebagai panduan untuk menganalisis keamanan *website* mereka. OWASP, sebuah organisasi nirlaba yang menyediakan sumber daya dan framework pengujian keamanan aplikasi berbasis web, memiliki keanggotaan yang terdiri dari ilmuwan, peneliti, dan sektor swasta (Elanda & Buana, 2020). OWASP TOP 10 2021 adalah daftar sepuluh kerentanan keamanan umum yang ditemukan pada aplikasi web. Daftar ini diperbarui secara berkala oleh komunitas keamanan OWASP untuk mencerminkan tren dan ancaman terbaru dalam dunia keamanan *cyber*. Dengan menggunakan panduan ini, perusahaan dapat mengidentifikasi dan mengatasi kerentanan yang sering dieksploitasi oleh penyerang . Melalui analisis keamanan sistem informasi *website* menggunakan metode penetration testing dengan OWASP TOP 10 2021, PT XYZ dapat memahami lebih baik tentang kelemahan dan kerentanan dalam sistem mereka. Mereka dapat mengambil langkah-langkah untuk memperbaiki dan meningkatkan keamanan sistem, termasuk penerapan tindakan pencegahan dan perubahan konfigurasi yang diperlukan. Oleh karena itu, OWASP TOP 10 menjadi rujukan mengenai keamanan sistem oleh banyak *cyber* security expert. Berikut beberapa penelitian yang menggunakan OWASP TOP 10 diantarannya pada penelitian pertama yang ditulis oleh Hidayatulloh dan Saptadiaji pada penelitiannya melakukan pengujian pada *website* Universitas ARS menggunakan Open Web Application Security Project (OWASP), adapun pengujian ini menggunakan metode penetration testing dengan mengacu pada parameter OWASP TOP 10 tahun 2021 dan *tools* yang digunakan pada penelitian ini adalah OWASP ZAP, burp suite dan nikto (Hidayatulloh & Saptadiaji, 2021). Kemudian pada penelitian kedua yang ditulis oleh Yunus metode yang digunakan untuk penetration testing adalah OWASP versi 4, terkait *website* vulnerability scanning *tools* yang digunakan adalah acunetix dengan objek yang diteliti adalah aplikasi berbasis web (Yunus, 2019). Beberapa literatur penelitian sebelumnya, para peneliti telah menggunakan OWASP TOP 10 tahun 2017 dan versi 4. Namun, pada penelitian ini, dipilih penggunaan OWASP TOP 10 tahun 2021 karena keberlanjutan pembaruan informasi terkait kerentanan *website* yang sedang marak dan memberikan rekomendasi perbaikan. Keberlanjutan pembaruan ini menjadi krusial karena kerentanan *website* terus berkembang. Dengan demikian, penerapan penetration testing dengan menggunakan panduan OWASP TOP 10

2021 diharapkan dapat memberikan hasil yang lebih relevan dan akurat untuk memastikan keamanan sistem informasi *website* PT XYZ

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat kerentanan sistem informasi website PT XYZ terhadap ancaman siber berdasarkan standar OWASP TOP 10 tahun 2021?
2. Apa saja jenis kerentanan yang ditemukan pada sistem informasi website PT XYZ melalui metode penetration testing?
3. Bagaimana rekomendasi perbaikan yang dapat diterapkan untuk meningkatkan keamanan sistem informasi website PT XYZ?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah melakukan evaluasi keamanan pada *website* PT. XYZ dan memberikan rekomendasi kepada pihak *programmer* dalam pengamanan *website*. Hasil penelitian ini diharapkan dapat membantu pihak *programmer* PT. XYZ dalam pengamanan *website*. Secara rinci maka dapat dijabarkan sebagai berikut:

1. Menganalisis tingkat kerentanan sistem informasi website PT XYZ dengan menggunakan standar OWASP TOP 10 tahun 2021.
2. Menganalisis jenis-jenis kerentanan yang ditemukan dalam sistem informasi website PT XYZ melalui metode penetration testing.
3. Memberikan rekomendasi perbaikan guna meningkatkan keamanan sistem informasi website PT XYZ

1.4 Batasan dan Asumsi Penelitian

Dalam penulisan penelitian, batasan masalah ditetapkan sehingga solusi dapat memenuhi harapan. Namun penelitian ini juga mempunyai batasan-batasan masalah yang disesuaikan oleh kemampuan dari peneliti, batasan tersebut adalah sebagai berikut:

1. Penelitian ini akan berfokus pada penggunaan metode *penetration testing* dengan menggunakan OWASP *Top* 10 2021, pada analisis kerentanan dalam sistem informasi *website* PT. XYZ.
2. Penelitian ini dibatasi pada penerapan metode penetration testing berdasarkan OWASP Top 10 2021, dengan fokus utama pada menganalisis kerentanan dalam sistem serta pelaporan hasil temuan dan memberikan rekomendasi perbaikan.

1.5 Manfaat Penelitian

Berdasarkan latar belakang yang telah diuraikan sebelumnya maka dapat dituliskan manfaat dari penelitian ini adalah:

1. Mencegah serangan *cyber* dengan menutup potensi celah yang bisa dimanfaatkan oleh penyerang. Dengan melakukan analisis keamanan secara teratur, perusahaan dapat meminimalkan risiko serangan dan gangguan layanan.
2. Dapat mengetahui seberapa rentan *website* PT. XYZ terhadap serangan dari luar atau pihak yang tidak bertanggung jawab.

1.6 Sistematika Penulisan

Metodologi penelitian ini menggunakan penetration testing dengan menggunakan OWASP Top 10 2021 melibatkan beberapa tahapan penting. Website yang diuji aktif dengan menggunakan domain xyz.com, menjadi salah satu website yang dikembangkan oleh PT. XYZdalam bidang layanan kesehatan pada apotek dan klinik. Sedangkan, tahapan yang akan dilaksanakan terdiri dari beberapa langkah. Pertama, persiapkan penelitian dengan menentukan tujuan dan mengumpulkan informasi tentang sistem *website* yang akan diuji. Selanjutnya, buat rencana penelitian yang mencakup ruang lingkup, waktu, sumber daya, dan metode yang akan digunakan. Setelah itu, melakukan pemindaian awal untuk mengumpulkan informasi tentang sistem *website* yang akan diuji dan identifikasi celah keamanan yang mungkin ada. Selanjutnya, analisis hasil pemindaian awal dan evaluasi tingkat keparahan serta dampak dari setiap celah keamanan yang ditemukan. Memprioritaskan celah keamanan berdasarkan tingkat keparahan dan dampaknya. Setelah itu, melakukan serangan terhadap celah keamanan yang ditemukan untuk menguji keefektifan sistem keamanan. Dengan melaporkan hasil penelitian, termasuk celah keamanan yang ditemukan, tingkat keparahan, dan rekomendasi perbaikan. Terakhir, mengimplementasikan rekomendasi perbaikan yang disarankan dalam laporan dan uji ulang sistem *website* setelah perbaikan dilakukan untuk memastikan celah keamanan telah tertutup.