

BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet sebagai jaringan komunikasi global telah menjadi media dan sumber informasi yang sangat berguna untuk berbagai kebutuhan seperti ilmu pengetahuan, teknologi, hiburan, bisnis, dan lainnya. Kemudahan dan kenyamanan yang ditawarkan oleh internet membuatnya semakin sering digunakan. Namun, di balik semua manfaat tersebut, ada satu aspek yang sering diabaikan oleh pengguna, yaitu keamanan. Keamanan adalah elemen penting dalam aplikasi web, namun masih banyak pengguna yang kurang memperhatikannya. Hingga kini, belum ada website yang bisa dianggap sepenuhnya aman [1]. Oleh karena itu, keamanan pada website menjadi sangat penting untuk mengidentifikasi dan menutup celah-celah yang dapat dimanfaatkan untuk mengakses situs secara tidak sah. Ini berfungsi untuk melindungi data sensitif dan menjaga integritas serta ketersediaan layanan yang disediakan oleh website tersebut [2].

e-Pinter adalah inovasi layanan publik Kabupaten Bengkalis yang mempercepat dan menyederhanakan proses perizinan. Platform ini memungkinkan masyarakat dan pelaku usaha untuk mengurus berbagai jenis izin secara online, dari izin usaha hingga izin lingkungan, dengan prosedur yang lebih mudah dan waktu yang lebih singkat.

Keamanan website sangat penting karena menyimpan data penting seperti informasi Perizinan Usaha dan Perizinan Bangunan. Tanpa perlindungan yang memadai, data ini dapat hilang atau disalahgunakan. Oleh karena itu, penting untuk melakukan pemindaian website menggunakan alat seperti *OASWP* dan *ZAP* untuk mendeteksi celah keamanan [3]. Setelah pemindaian, perlu dilakukan analisis lebih lanjut, termasuk pengujian kelemahan seperti *SQL Injection (SQLI)* dan *Cross-Site Scripting (XSS)*. *SQLI* memungkinkan penyerang memanipulasi perintah *SQL* yang dikirimkan ke database *back-end* [1], sementara *XSS* melibatkan penyisipan kode atau skrip berbahaya ke dalam halaman web melalui URL situs [2].

Beberapa penelitian sejenis yang pernah dilakukan di antaranya adalah penelitian dengan judul "Analisis Keamanan Menggunakan Web Aplikasi Bwapp Terhadap Serangan *XSS (Cross Site Scripting)* dan *SQL Injection*", penulis mengidentifikasi beberapa masalah utama. Pertama, meskipun internet berkembang pesat sebagai media dan sumber informasi yang sering digunakan, aspek keamanan seringkali diabaikan oleh pengguna. Kedua, kerentanan *SQL Injection* terjadi ketika penyerang dapat memanipulasi *query SQL* yang dikirimkan melalui aplikasi ke database back-end. Ketiga, serangan *XSS (Cross Site Scripting)* melibatkan penyisipan kode *HTML* atau script klien lainnya. Untuk mengatasi masalah-masalah ini, penulis melakukan simulasi serangan *SQL Injection* dan *XSS* pada web aplikasi bwapp sebagai upaya untuk menganalisis celah keamanan pada web aplikasi tersebut [1].

Penelitian dengan judul "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik *SQL Injection* dan *XSS*" Jurnal ini membahas optimalisasi keamanan website melalui penetrasi testing menggunakan teknik *SQL Injection (SQLI)* dan *Cross-Site Scripting (XSS)*. Permasalahan yang diangkat adalah website yang tidak memiliki keamanan yang memadai dapat menjadi sasaran serangan *SQLI* dan *XSS*, di mana hacker memanfaatkan celah pada menu login, pencarian, unggahan, masukan, dan URL dengan parameter angka. Solusi yang ditawarkan adalah melakukan penetrasi testing pada website rental mobil CV. Merdeka Auto Rental, mengidentifikasi celah keamanan, lalu membuat skrip fungsi PHP untuk membuang karakter berbahaya, dan menyisipkannya pada file input, proses, dan output. Meskipun skrip fungsi ini hanya menangani serangan *SQLI* dan *XSS*, pendekatan ini terbukti efektif dalam mencegah serangan tersebut pada website yang diuji [2].

Penelitian dengan Judul "Uji Penetrasi untuk Menganalisis Keamanan Website STIE Samarinda Menggunakan Teknik *SQL Injection* dan *XSS*". Fokus permasalahan dalam penelitian ini adalah website universitas yang menyimpan banyak data dan informasi penting, seperti data mahasiswa, dosen, staf, dan kurikulum, namun rentan terhadap ancaman penetrasi website, khususnya serangan *SQL injection* dan *cross-site scripting (XSS)*, yang dapat menyebabkan kehilangan

data atau penyalahgunaan informasi. Untuk menangani masalah ini, peneliti melakukan analisis kerentanan keamanan website STIE Samarinda menggunakan teknik uji penetrasi, dengan fokus pada metode *SQL injection* dan *XSS* [3].

1.2 Permasalahan

Website e-Pinter menghadapi masalah utama terkait keamanan website mereka yang menyimpan data penting seperti informasi Perizinan Usaha dan Perizinan Bangunan. Tanpa perlindungan memadai, data ini rentan disalahgunakan. Website sekolah ini kemungkinan memiliki kelemahan keamanan seperti *SQL Injection (SQLi)* dan *Cross-Site Scripting (XSS)*, di mana *SQLi* memungkinkan manipulasi perintah *SQL* ke database, dan *XSS* memungkinkan penyisipan kode berbahaya ke halaman web. Selain itu, belum ada analisis keamanan komprehensif pada sistem informasi mereka, sehingga celah-celah keamanan yang ada belum teridentifikasi dan diatasi secara efektif. Ketidakpastian mengenai keberadaan celah keamanan ini meningkatkan risiko eksploitasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, sangat penting bagi e-pinter untuk melakukan analisis keamanan menyeluruh dan memperkuat sistem informasi mereka guna melindungi data penting dan mencegah serangan potensial.

1.3 Batasan Masalah

Penelitian ini hanya fokus pada analisis keamanan website e-Pinter terhadap serangan *SQL Injection* dan *Cross-Site Scripting (XSS)*. Tujuan utamanya adalah menemukan celah keamanan yang ada dan memberikan saran untuk meningkatkan keamanan serta melakukan perbaikan. Semua pengujian dilakukan di lingkungan yang aman dan terkendali, sehingga tidak mengganggu operasional website. Hasil penelitian hanya berupa saran dan rekomendasi.

1.4 Tujuan

Penelitian ini bertujuan untuk menganalisis keamanan website E-Pinter terhadap serangan *SQL Injection* dan *XSS*. Adapun tujuan spesifik dari penelitian ini meliputi:

1. Mengidentifikasi potensi celah keamanan pada website E-Pinter yang bisa dieksploitasi untuk serangan *SQL Injection* dan *XSS*.
2. Menganalisis dampak dan risiko yang mungkin timbul akibat serangan *SQL Injection* dan *XSS* pada website E-Pinter.
3. Memberikan rekomendasi perbaikan dan peningkatan keamanan website E-Pinter untuk melindungi dari serangan *SQL Injection* dan *XSS*.

Melalui analisis keamanan ini, diharapkan potensi celah keamanan yang dapat dimanfaatkan untuk serangan *SQL Injection* dan *XSS* pada website E-Pinter dapat diidentifikasi dan diminimalisir. Hasil penelitian ini diharapkan dapat berkontribusi dalam meningkatkan keamanan website sekolah dan melindungi data-data penting yang tersimpan di dalamnya.

1.5 Manfaat

Berdasarkan judul skripsi "ANALISIS KEAMANAN WEBSITE E-PINTER TERHADAP SERANGAN *SQL INJECTION* DAN *XSS*", penelitian ini memiliki beberapa manfaat penting:

1. Memberikan analisis menyeluruh terkait potensi kerentanan sistem sebagai acuan dalam peningkatan mekanisme keamanan, guna menjaga integritas dan kerahasiaan data perizinan yang dikelola.
2. Penelitian ini memberikan referensi teknis terkait penerapan langkah-langkah mitigasi terhadap serangan *SQL Injection* dan *Cross-Site Scripting (XSS)*, khususnya melalui implementasi prepared statements serta validasi input dan output, yang dapat dijadikan acuan dalam proses pengembangan aplikasi berbasis web agar lebih aman.
3. Penelitian ini dapat menjadi referensi atau acuan bagi peneliti lain yang ingin mengkaji lebih dalam mengenai keamanan aplikasi web. Selain itu, metode pengujian yang digunakan dapat dijadikan sebagai panduan dalam melakukan analisis terhadap sistem informasi lainnya.

1.6 Sistematika Penulisan

Jelaskan tentang sistematika pembahasan dalam buku proyek akhir yang meliputi:

Bab 1 Pendahuluan

Jelaskan tentang apa saja yang dibahas pada Bab 1. Penjelasan memuat bagian-bagian penting pada Pendahuluan.

Bab 2 Kajian Pustaka

Jelaskan tentang apa saja yang dibahas pada Bab 2. Penjelasan memuat bagian-bagian penting pada Kajian Pustaka.

Bab 3 Deskripsi Sistem

Jelaskan tentang apa saja yang dibahas pada Bab 3. Penjelasan memuat bagian-bagian penting pada Desain Sistem.

Bab 4 Eksperimen dan Analisis

Jelaskan tentang apa saja yang dibahas pada Bab 4. Penjelasan memuat bagian-bagian penting pada Eksperimen dan Analisis.

Bab 5 Penutup

Jelaskan tentang apa saja yang dibahas pada Bab 5. Penjelasan memuat bagian-bagian penting pada Penutup.