BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem Informasi Manajemen Kepegawaian adalah sistem informasi terpadu, yang meliputi pendataan pegawai, pengolahan data, prosedur, tata kerja, sumber daya manusia dan teknologi informasi untuk menghasilkan informasi yang cepat, lengkap dan akurat dalam rangka mendukung administrasi kepegawaian (Agung & Arifin, 2020) .

Sistem Informasi Manajemen Kepegawaian (SIMPEG) adalah sistem informasi yang terpadu yang memungkinkan pengelolaan data kepegawaian yang efektif dan efisien. SIMPEG memudahkan pegawai dalam mengelola informasi kepegawaian dan memahami syarat-syarat untuk peningkatan jabatan, golongan, atau jenis pekerjaan. Selain itu, sistem ini memungkinkan pengolahan data, prosedur, tata kelola kerja, sumber daya manusia, dan teknologi informasi untuk menghasilkan informasi yang cepat dan akurat (Misrul Amri, Dina Fara Waidah, 2023).

Pembuatan Sistem Informasi Kepegawaian (SIMPEG) di universitas merdeka malang bertujuan untuk mengelola data pegawai secara efisien dan efektif. SIMPEG membantu universitas dalam mencatat informasi lengkap tentang setiap pegawai, termasuk riwayat pendidikan, pengalaman kerja, dan prestasi. Selain itu, SIMPEG mempermudah pencatatan kehadiran, absensi, dan pengelolaan cuti, memungkinkan universitas untuk menjadwalkan kegiatan akademik dan administratif dengan lebih baik. Melalui SIMPEG, proses penggajian dan pengelolaan tunjangan juga dapat dilakukan dengan cepat dan akurat, sesuai dengan kebijakan dan peraturan yang berlaku (Widyawan & Idris, 2021). Data yang terdapat dalam SIMPEG juga digunakan untuk mengevaluasi kinerja pegawai, serta merencanakan pengembangan sumber daya manusia yang sesuai. Dengan demikian, SIMPEG membantu universitas dalam memenuhi kebutuhan administrasi dan manajemen SDM, serta menjaga kepatuhan terhadap peraturan yang berlaku.

Seringkali, aplikasi web yang telah dipublikasikan di internet rentan terhadap serangan dari pihak yang tidak diinginkan, seperti *hacker* atau peretas (Prasetyo Taufan, 2022). Aplikasi web, termasuk Sistem Informasi Kepegawaian Universitas Merdeka Malang, rentan terhadap berbagai jenis serangan siber seperti SQL injection, cross-site scripting (*XSS*), dan denial of service (DoS), yang dapat mengancam keamanan data dari Dosen, Mahasiswa, dan petugas universitas. Ancaman dari pihak yang tidak diinginkan, seperti *hacker* atau peretas, memiliki potensi untuk mengeksploitasi kerentanan dalam aplikasi web SIMPEG untuk mengakses, memanipulasi, atau bahkan mencuri data sensitif. Oleh karena itu, penting untuk mengambil tindakan pencegahan yang efektif guna melindungi data tersebut dari akses yang tidak sah. Analisis kerentanan menjadi langkah awal yang krusial untuk mengevaluasi keamanan aplikasi web secara menyeluruh, sehingga potensi risiko keamanan yang mungkin terjadi dapat diidentifikasi dengan tepat. Perlindungan data dari Dosen, Mahasiswa, dan petugas universitas menjadi fokus utama, mengingat informasi pribadi, akademik, dan administratif yang sensitif harus dijaga kerahasiaannya.

Nessus Scanner merupakan Pemindai kerentanan yang memiliki tingkat akurasi tinggi, dengan insiden false positive yang rendah. Tenable telah menguji dan membuktikan bahwa ia hanya menghasilkan 32 false positives dalam satu juta pemindaian (TrustRadius, 2023). *Nessus* menyediakan cakupan kerentanan yang luas dengan harga yang terjangkau. Sebagai platform open-source, *Nessus* menggunakan Arsitektur Common Vulnerabilities and Exposure. *Nessus* dapat diintegrasikan dengan produk Tenable lainnya seperti Tenable.io dan Tenable.sc. *Nessus* tersedia dalam berbagai versi, termasuk *Nessus* Expert, *Nessus* Professional, *Nessus* Manager, dan *Nessus* Agent (*Nessus Vulnerability Scanner*: *Network Security* Solution, n.d.). *OWASP ZAP* adalah scanner vulnerabilities yang dibuat oleh organisasi *OWASP*. Ini adalah proyek *OWASP* yang paling aktif karena terus dikembangkan dan bersifat open source (Yudiana et al., 2021).

Penelitian ini bertujuan untuk menganalisis kerentanan website Sistem Informasi Kepegawaian Universitas Merdeka Malang. Hasil penelitian kerentanan ini dapat menjadi rekomendasi untuk melakukan tindakan pengamanan. Penelitian serupa telah dilakukan oleh peneliti sebelumnya antara lain Analisis Kerentanan

Situs Web KopKar Ayariah PT BSIN menggunakan *OWASP Zed Attack Proxy* yang berhasil menunjukan kerentanan dengan tingkat risiko Medium, Low, Informational dan tidak ditemukan adanya risiko yang High (Wahidin et al., 2024).

Penelitian lainnya melakukan Analisis Uji Kualitas Keamanan Website PPDB SMK X Menggunakan Metode Isaff menunjukan bahwa website PPDB SMK X dapat diakses dengan baik tanpa masalah besar meskipun ditemukan beberapa kerentanan pada server-side software namun secara keseluruhan tidak ada masalah signifikan yang dapat membahayakan situs web ini (Susanti, 2024). Penggunaan *Nessus Scanner* sebagai metode analisis kerentanan dilakukan penelitian menggunakan Sistematic Literature Review menghasilkan analisis website terbaik adalah yang lolos tahapan pengujian tahapan pengujian *OWASP* terbanyak

Alasan peneliti mengambil judul "Peningkatan Keamanan Situs Web SIAKAD Universitas Merdeka Malang Melalui Analisis Kerentanan dengan Tenable *Nessus Scanner* & *Owasp* Zed Attack Proxy", sebab proyek ini sangat penting dalam menghadapi potensi ancaman keamanan siber yang mungkin dihadapi oleh Sistem Informasi Kepegawaian (SIMPEG) di Universitas Merdeka Malang. Sebagai pusat pengelolaan data kepegawaian, keamanan SIMPEG menjadi fokus utama, terutama di masa di mana aplikasi web rentan terhadap serangan tidak diinginkan. Dengan penekanan pada analisis kerentanan menggunakan *Nessus Scanner* & *Owasp* Zed Attack Proxy, penelitian ini bertujuan untuk memberikan pemahaman mendalam mengenai risiko keamanan yang mungkin terjadi, sehingga dapat menyusun rekomendasi tindakan pengamanan yang sesuai dan efektif untuk menjaga keamanan data dosen, mahasiswa, dan staf universitas.

1.2 Rumusan Masalah

1. Bagaimana kondisi keamanan situs web Sistem Informasi Kepegawaian Universitas Merdeka Malang saat ini dan potensi risiko keamanan yang mungkin dihadapi?
2. Apa saja kerentanan yang dapat diekspos oleh serangan siber terhadap Sistem Informasi Kepegawaian, dan sejauh mana tingkat urgensi penanganan terhadap kerentanan tersebut?
3. Bagaimana implementasi analisis kerentanan menggunakan Tenable *Nessus Scanner* & *Owasp Zed Attack Proxy* dapat memberikan kontribusi terhadap peningkatan keamanan situs web Sistem Informasi Kepegawaian di Universitas Merdeka Malang?

1.3 Tujuan Penelitian

1. Menganalisis kerentanan pada situs web Sistem Informasi Kepegawaian Universitas Merdeka Malang untuk mengidentifikasi potensi risiko keamanan.
2. Menyusun rekomendasi tindakan pengamanan yang sesuai dan efektif berdasarkan hasil analisis kerentanan.
3. Mengimplementasikan Tenable *Nessus Scanner* & *Owasp Zap* sebagai alat analisis kerentanan untuk meningkatkan keamanan situs web Sistem Informasi Kepegawaian.

1.4 Manfaat Penelitian

1. Meningkatkan pemahaman terhadap potensi risiko keamanan yang dihadapi oleh Sistem Informasi Kepegawaian di lingkungan Universitas Merdeka Malang.
2. Memberikan panduan tindakan pengamanan yang dapat diimplementasikan untuk menjaga keamanan data dosen, mahasiswa, dan staf universitas.
3. Menjadi referensi bagi pihak universitas dalam mengoptimalkan keamanan situs web Sistem Informasi Kepegawaian melalui penerapan analisis kerentanan dengan Tenable *Nessus Scanner*.

1.5 Batasan Penelitian

1. Penelitian akan memfokuskan pada analisis kerentanan pada situs web Sistem Informasi Kepegawaian Universitas Merdeka Malang
2. Analisis kerentanan dilakukan menggunakan Tenable *Nessus Scanner* & *Owasp Zed Attack Proxy* sebagai metode utama.
3. Penelitian ini tidak akan melibatkan implementasi langsung dari rekomendasi Tindakan pengamanan yang disusun
4. Faktor-faktor eksternal seperti perubahan regulasi atau perkembangan teknologi tidak akan dibahas secara mendalam