202110370311022
Muhammad Daffa Raihan Syalwa
Prodi Informatika

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, *website* telah menjadi alat penting untuk menyediakan informasi, layanan publik, dan interaksi antara pemerintah dengan warga. Namun, seiring dengan meningkatnya ketergantungan pada teknologi digital, ancaman keamanan siber juga semakin kompleks dan beragam [1][2]. Serangan siber seperti *SQL Injection*, *Cross-Site Scripting* (XSS), dan *Distributed Denial of Service* (DDoS) menjadi ancaman serius yang dapat mengakibatkan kebocoran data sensitif, kerugian finansial, dan penurunan kepercayaan publik [3][4].

Website pemerintah sering menjadi target serangan siber karena menyimpan informasi pribadi warga, seperti data kependudukan, informasi keuangan, dan layanan publik. Serangan siber dapat menyebabkan kebocoran data, gangguan layanan, dan bahkan kerusakan reputasi institusi pemerintah jika keamanan *website* pemerintah tidak dijaga dengan baik [5][6][7]. Oleh karena itu, sangat penting bagi pemerintah untuk melakukan pengujian keamanan rutin untuk menemukan dan memperbaiki kesalahan sebelum mereka dimanfaatkan oleh individu yang tidak bertanggung jawab [8][9].

Penetration testing adalah cara yang efektif untuk menguji keamanan situs web dengan mensimulasikan serangan pada suatu sistem untuk menemukan dan menggunakan kerentanan. Menurut, "Penetration testing adalah teknik evaluasi keamanan yang melibatkan simulasi serangan terhadap sistem untuk menemukan kerentanan yang dapat digunakan oleh penyerang." Proses ini dinilai sangat krusial, "Untuk website pemerintah karena dapat membantu menemukan kerentanan sebelum mereka digunakan oleh pihak yang tidak bertanggung jawab" [10][11].

Salah satu alat populer untuk pengujian penetrasi adalah OWASP ZAP (Zed Attack Proxy), alat *open source* yang membantu pengembang dan pakar keamanan mengidentifikasi sensitivitas keamanan situs web. Ekstensi seperti pemindaian otomatis, analisis manual dan integrasi ke alat lain memungkinkan pengguna untuk melakukan tes keamanan yang komprehensif. Sebuah studi terkait juga menyimpulkan bahwa "OWASP ZAP efektif untuk identifikasi kerentanan kritis pada *website* pemerintah" [12][13].

Fokus penelitian ini adalah situs web Pemerintah Kota Malang (https://malangkota.go.id/), yang merupakan salah satu portal resmi yang memberikan layanan publik dan informasi penting bagi warga Kota Malang. Karena tanggung jawab strategisnya untuk menyediakan layanan publik dan informasi, situs web harus dijaga dengan baik. Sejalan dengan penelitian sebelumnya, "Keamanan aplikasi web sangat penting karena situs web pemerintah sering menyimpan data sensitif", sehingga evaluasi keamanan pada website ini menjadi suatu keharusan [14][15].

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalahnya adalah:

1. Bagaimana implementasi OWASP ZAP berdasarkan standar PTES dapat mengidentifikasi dan memvalidasi kerentanan keamanan pada *website* Pemerintah Kota Malang?
2. Jenis kerentanan apa saja dalam kategori OWASP Top 10 yang terdeteksi oleh OWASP ZAP dan bagaimana membuktikan validitas temuan tersebut?
3. Bagaimana melakukan analisis dalam penggunaan OWASP ZAP serta bagaimana rekomendasi mitigasi yang terukur berdasarkan standar NIST SP 800-115 atau ISO/IEC 27001?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan penelitiannya adalah:

1. Mengimplementasikan OWASP ZAP dalam *penetration testing* pada *website* Pemerintah Kota Malang dengan mengikuti standar PTES (Penetration Testing Execution Standard) dan memvalidasi temuan kerentanan menggunakan *tools* pendukung (seperti SQLmap untuk SQL Injection atau Burp Suite untuk XSS).Untuk mengidentifikasi jenis-jenis kerentanan yang dapat ditemukan pada *website* pemerintah Kota Malang melalui penggunaan OWASP ZAP.
2. Mengklasifikasikan kerentanan keamanan berdasarkan OWASP Top 10 (fokus pada kriteria seperti SQL Injection, XSS, atau CSRF) yang ditemukan pada *website*, disertai bukti eksploitasi dan analisis dampak terhadap keamanan data warga.
3. Tantangan teknis dalam penggunaan OWASP ZAP (misalnya false positive/negative) dan memberikan rekomendasi solusi yang terukur berdasarkan standar keamanan (seperti NIST SP 800-115 atau ISO/IEC 27001) untuk meningkatkan keamanan *website*.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian di atas, maka manfaat penelitiannya adalah:

1. Bagi pemerintah Kota Malang, penelitian ini dapat menjadi panduan dalam meningkatkan keamanan *website* dan melindungi data warga.
2. Bagi akademisi, penelitian ini dapat menjadi referensi untuk studi lebih lanjut mengenai keamanan *website* pemerintah Kota Malang.
3. Bagi masyarakat, penelitian ini dapat meningkatkan kesadaran akan pentingnya keamanan informasi dalam layanan publik.

1.5 Ruang Lingkup Penelitian

Ruang lingkup penelitiannya adalah:

1. Penggunaan OWASP ZAP untuk *penetration testing* pada *website* pemerintah Kota Malang.
2. Analisis kerentanan yang ditemukan selama proses pengujian.
3. Tantangan dan solusi dalam implementasi OWASP ZAP untuk meningkatkan keamanan *website* pemerintah Kota Malang.