BAB I
PENDAHULUAN

1.1. Latar Belakang

Pengujian pada sistem keamanan berbasis *website* adalah hal yang penting pada era perkembangan aplikasi berbasis *website* yang begitu pesat dari masa ke masa. Semakin melaju pesat berkembang aplikasi yang berbasis *website* ini diiringi dengan serangan keamanan yang tinggi dari berbagai teknik ancaman. Sering kali pada masalah keamanan ada pada urutan kedua, atau bisa berada diurutan terakhir dalam hal-hal yang sangat dianggap penting [1]. Penggunaan *website* ini adalah salah satu bentuk dari canggihnya penggunaan teknologi masa kini. Oleh karena itu, sangat penting bagi organisasi untuk melakukan *assessment* pada aplikasi yang berbasis *website* agar organisasi mampu mendeteksi kerentanan keamanan dan memahami risiko yang akan dihadapi. Dengan adanya *website* desa warga dapat dengan mudah mengakses informasi mengenai layanan desa tanpa warga datang ke kantor desa untuk layanan yang akan di lakukan dan mendapatkan informasi desa.

Cara yang paling andal untuk menilai sikap keamanan informasi suatu organisasi adalah melalui observasi terhadap responsnya terhadap serangan. Untuk memastikan keamanan sistem secara menyeluruh, melakukan pengujian penetrasi menjadi strategi yang paling terbaik, dimana sering kali memungkinkan para peneliti yang menganalisis keamanan akan menemukan celah baru [2]. Analisis *website* kelurahan Rimba Sekampung ini dilakukan untuk menemukan kerentanan keamanan pada *website* untuk mengidentifikasi dampak negatif yang dihasilkan dari analisis kerentanan keamanan.

Sebelum peneliti melaksanakan pengujian keamanan aplikasi berbasis *website* ini, peneliti melakukan tinjauan literatur dan menemukan beberapa penelitian terkait [1]. Mitha dalam penelitiannya mendeteksi kerentanan keamanan pada aplikasi berbasis *website* milik SMA Negeri 2 Amplapura menggunakan OWASP untuk melakukan penilaian risiko agar hasil penelitian mereka diharapkan dapat membantu pihak pengelola dan pengembang sistem untuk dapat mencegah dan mengatasi risiko yang ditemukan pada keamanan sistem informasi *website*

tersebut [1]. Tamsir dalam penelitiannya menganalisis kerentanan keamanan pada Sistem Informasi Akademik Universitas Bina Darma dengan menggunakan OWASP. Hasil penelitian menunjukkan bahwa terdapat beberapa kerentanan keamanan yang ditemukan, antara lain *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF), dan SQL *Injection*. Berdasarkan analisis OWASP *Risk Rating*, ketiga kerentanan tersebut memiliki tingkat risiko yang berbeda-beda, mulai dari risiko sedang hingga tinggi. Rekomendasi perbaikan dan mitigasi diusulkan untuk meningkatkan keamanan Sistem Informasi Akademik Universitas Bina Darma [3]. Nurholis dalam penelitiannya ini melakukan analisis kerentanan keamanan *website* Dinas Tenaga Kerja menggunakan metode OWASP *(Open Web Application Security Project*) pada Dinas Tenaga Kerja untuk membantu pihak pengelola dan pengembang sistem mendeteksi dan mengatasi risiko keamanan yang ditemukan pada aplikasi berbasis *website* yang dibangun DisnakerTrans [4].

OWASP *(Open Web Application Security Project)* Top 10 merupakan sebuah metodologi yang digunakan untuk menguji keamanan sistem berbasis *website*. Metode ini dikembangkan oleh komunitas OWASP dan berisi daftar 10 ancaman keamanan utama yang dapat mempengaruhi keamanan suatu situs *website* [2]. Metode ini memprioritaskan 10 ancaman tersebut berdasarkan beberapa faktor, yaitu tingkat kemudahan dalam melakukan eksploitasi, seberapa umum atau sering ditemukan ancaman tersebut, kemudahan dalam mendeteksi adanya ancaman, serta dampak parah yang dapat ditimbulkan oleh ancaman tersebut. Dengan menggunakan OWASP Top 10, para pengembang atau penguji keamanan akan dapat mengidentifikasi dan memitigasi kerentanan keamanan kritis yang mungkin ada pada aplikasi *website* mereka ini, sehingga metode ini menjadi acuan penting dalam memastikan keamanan sistem berbasis *website* [2].

Hasil analisis kerentanan yang didapatkan akan membantu pengelola dan pengembang sistem dalam mencegah dan mengatasi dampak risiko yang teridentifikasi pada sistem [4]. Belum adanya analisis *Security Assesment* (Penilaian Kemananan) pada sistem informasi *website* kelurahan rimba sekampung. Analisis perlu dilakukan pada keamanan *website* untuk mencegah serangan injeksi agar mencegah kebocoran informasi sensitif, seperti surat dan data masyarakat.

Namun belum melakukan pengujian sistem sehingga belum mengetahui secara pasti celah keamanan sistem yang sudah dibangun. Oleh karena itu perlu adanya *Security Assessment* (penilaian keamanan) pada sistem tersebut.

Terdapat beberapa faktor yang mengakibatkan rendahnya tingkat keamanan pada aplikasi *website*, termasuk kesalahan dalam penulisan kode program dan salah konfigurasi [1]. Kesalahan dalam penulisan kode program pada aplikasi berbasis *website* sering dimanfaatkan oleh penyerang. Beberapa jenis serangan yang umum digunakan oleh penyerang meliputi SQL *Injection*, *Authentication*, dan XSS [1]. Dengan menggunakan alat pemindai kerentanan dan mengacu pada standar OWASP, proses pengujian dapat mengungkap berbagai jenis kerentanan informasi pada aplikasi *website*. Melalui pendekatan ini, dapat ditemukan informasi sensitif seperti versi *server website*, pola permintaan *GET* dan *POST*, struktur URL, kerangka kerja (*framework*) yang digunakan, komponen pembangun *website*, serta arsitektur *website* secara keseluruhan. Lebih lanjut, pengujian dengan OWASP ini juga akan dapat mengidentifikasi kerentanan terkait dengan proses autentikasi pada aplikasi *website*. Pendekatan ini memungkinkan pengembang atau penguji keamanan untuk menganalisis dan memitigasi kelemahan-kelemahan kritis yang dapat mengancam keamanan aplikasi *website* [2].

Dalam penggunaan OWASP untuk menguji kerentanan aplikasi *website*, selain menggunakan alat pemindai kerentanan, diperlukan juga konfigurasi yang tepat untuk memaksimalkan tingkat akurasi hasil pengujian. Konfigurasi yang tepat pada alat pemindai kerentanan dapat membantu mengoptimalkan deteksi kerentanan yang ada, sehingga proses pengujian dapat memberikan hasil yang lebih komprehensif dan akurat. Hal ini penting dilakukan agar peneliti atau pengembang atau tim keamanan dapat memperoleh informasi yang akurat terkait kelemahan-kelemahan keamanan pada aplikasi *website* yang sedang diuji, sehingga dapat dilakukan tindakan perbaikan yang tepat sasaran [2].

Dalam penelitian ini, terdapat beberapa metode untuk mendeteksi kerentanan keamanan pada aplikasi *website*, termasuk ISSAF, OSSTMM, OWASP, dan NIST [4]. Namun, metode yang paling tepat untuk dapat melakukan pengujian penetrasi adalah OWASP [4]. OWASP, yang didirikan pada tahun 2004, juga dikenal sebagai

organisasi nirlaba amal di Amerika Serikat dan menyediakan panduan standar untuk memudahkan pengujian penetrasi.

1.2. Permasalahan

Permasalahan yang dihadapi belum adanya analisis Penilaian Keamanan pada sistem informasi *website* Kelurahan Rimba Sekampung untuk mengidentifikasi celah keamanan yang ada. Akibatnya, risiko-risiko keamanan seperti serangan injeksi yang dapat menyebabkan kebocoran informasi sensitif seperti surat dan data masyarakat belum dapat dicegah secara efektif. Selain itu, belum diketahuinya secara pasti celah keamanan yang ada pada sistem informasi *website* Kelurahan Rimba Sekampung yang telah dibangun. Oleh karena itu perlu adanya *Security Assesment* pada sistem tersebut.

1.3. Batasan Masalah

a. Penelitian ini hanya fokus pada analisis keamanan pada *website* Kelurahan Rimba Sekampung.
b. Penelitian ini berfokus pada penerapan pedoman dan alat OWASP, tanpa membandingkannya dengan pendekatan keamanan lainnya.

1.4 Tujuan

Melakukan analisis kerentanan keamanan pada *website* kelurahan rimba sekampung dengan menggunakan *framework* owasp zap untuk mencari celah dan menilai keamanan *website* tersebut.

1.5 Manfaat

Manfaat penelitian dari judul “Analisis Kerentanan Keamanan pada Website Kelurahan Rimba Sekampung Menggunakan *Framework* OWASP ZAP” adalah:

1. Menemukan atau mengidentifikasi celah keamanan pada sistem informasi *website* Kelurahan Rimba Sekampung.
2. Mengetahui risiko-risiko keamanan yang dapat terjadi, seperti risiko serangan injeksi yang dapat menyebabkan kebocoran informasi sensitif.

3. Memberikan gambaran komprehensif tentang kerentanan keamanan *website* Kelurahan Rimba Sekampung dan tingkat risikonya.
4. Menjadi referensi untuk penelitian serupa di masa depan.

Dengan manfaat-manfaat ini, penelitian ini diharapkan dapat memberikan dampak positif pada perusahaan, organisasi, dan komunitas penelitian keamanan *website* secara keseluruhan.

1.6 Sistematika Penulisan

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 Deskripsi 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.