BAB I

PENDAHULUAN

1.1 Latar Belakang

Aplikasi web adalah salah satu platform paling umum untuk menyampaikan informasi dan layanan melalui Internet. Bahkan saat ini, aplikasi web banyak digunakan dalam layanan penting. Namun penggunaan yang meluas ini membuat aplikasi web menjadi target populer berbagai ancaman dalam bentuk serangan cyber [1]. Meskipun sebagian besar teknologi telah dikembangkan untuk melindungi aplikasi web dan setidaknya meminimalkan serangan cyber, hanya sedikit yang telah dilakukan untuk membangun hubungan antara teknologi-teknologi ini dan memberikan gambaran menyeluruh tentang penelitian keamanan aplikasi web.

Pada penelitian ini akan dilakukan Analisis pada Website SIMPKN Informatika yang nantinya Analisis tersebut menampilkan kerentanan-kerentanan yang ada pada website dan juga cara mengatasi kerentanan pada website. Kerentanan dapat membuat website terancam seperti terdapat penyerang atau hacker yang ingin untuk website tersebut dirusak maka dari itu penelitian dilakukan untuk mengatasi penyerangan dari hacker yang tidak bertanggung jawab. Hacker dapat membuat website tidak berjalan normal dengan mencari celah keamanan yang ada pada website yang nantinya penyerang atau hacker dapat menyusupkan program yang dapat memanipulasi sistem website agar tidak berjalan dengan normal.

OWASP merupakan singkatan dari Open Web Application Security Project, adalah sebuah organisasi nirlaba yang menitikberatkan pada peningkatan keamanan perangkat lunak. Sebagai suatu kerangka kerja, OWASP digunakan oleh para pengembang dan profesional teknologi untuk mengamankan website. OWASP menyediakan platform bagi pengembang untuk meningkatkan keamanan sistem melalui kontribusi open-source dan menggunakan beragam alat yang disediakan oleh OWASP [7].

Dalam penelitian Analisis Kerentanan pada website memilih metode OWASP ZAP sebagai alat untuk melakukan penyerangan terhadap website. Open Web Application Security Project (OWASP) adalah komunitas terbuka yang mengembangkan dan memelihara aplikasi tepercaya [2]. Hal ini memungkinkan untuk mengirimkan informasi terkait keamanan aplikasi. ZAP (Zed Attack Proxy) merupakan aplikasi yang dapat menjalankan pentesting untuk menemukan kerentanan website dengan mudah. ZAP memiliki beberapa keunggulan seperti open source, active scanner, capture proxy, tradisional dan ajax spider [2]

Open Web Application Security Project (OWASP) merupakan aplikasi berbasis web pengujian yang digunakan sebagai framework pengujian keamanan [5]. Dengan menggunakan (Open Web Application Security) OWASP memudahkan dalam mengetahui kerentanan pada website dan dapat mengurangi resiko yang terjadi. Mengetahui celah keamanan sendiri tidak akan membantu manajemen untuk meningkatkan keamanan pada aplikasi. Melakukan penilaian pada resiko aplikasi dengan mempertimbangkan perbedaan faktor-faktor terkait dengan aplikasi [5].

Berdasarkan beberapa penelitian di atas dan pengamatan terhadap beberapa penelitian lainnya yang melakukan Analisa Celah Keamanan Pada website belum menjelaskan mengenai kelemahan yang paling banyak terjadi pada sebuah website pada [1]-[4] hanya menjelaskan mengenai fitur upload yang menjadi aspek dalam kerentanan pada website tetapi tidak hanya fitur upload saja, pada [2] menjelaskan mengenai keseluruhan kerentanan yang terdapat pada sebuah website menggunakan ZAP tanpa menjelaskan versi tools yang digunakan [5]. Selanjutnya hanya menjelaskan pengecekan-pengecekan yang ada pada OWASP tanpa menjelaskan tools yang digunakan pada percobaan OWASP

Penelitian lainnya yang menerapkan metode OWASP hanya menjelaskan beberapa permasalahan yang muncul pada penelitian ini akan menjelaskan pada kerentanan-kerentanan yang muncul menggunakan Tools ZAP (Zed Attack Proxy) dengan versi 2.14.0 yang lebih detail dalam melakukan scanning untuk mendapatkan kerentanan pada sebuah website.

Tujuan dari penelitian ini adalah untuk melakukan analisis terhadap faktor-faktor keamanan pada website SIMPKN Informatika dengan mempertimbangkan potensi terjadinya ancaman dan gangguan yang dapat mengancam keamanan data yang disimpan dalam website tersebut, sehingga dapat mencegah akses ilegal dari pihak yang tidak bertanggung jawab. Seperti sebelumnya Website SIMPKN Informatika yang beberapa waktu lalu pernah tidak dapat diakses yang membuat website dialihkan terus-menerus mengakibatkan website tidak dapat digunakan oleh mahasiswa dan membuat Mahasiswa kesulitan dalam melakukan pendaftaran PKN (Program Kerja Nyata) dan MBKM (Merdeka Belajar Kampus Merdeka). Kerentanan tersebut membuat para hacker akan melakukan penyerangan seperti SQL Injection, Click-Jacking, dan lainnya.

Berdasarkan hal tersebut, maka penelitian ini menggunakan OWASP (OpenWeb Application Security Method) versi 4 dengan alat ZAP (Zed Attack Proxy) untuk Pengujian keamanan website. Hasil pengujian menunjukan celah atau kerentanan yang ada pada website untuk diklasifikasikan dalam resiko tingkat penyerangannya. Penelitian ini memberikan rekomendasi terhadap permasalahan yang ditemui. Dalam penelitian ini menjelaskan risk rating yang ada pada website dan pengamanan website terhadap kerentanan yang ada untuk menyempurnakan kinerja website.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan dan dirincikan di atas, maka dapat diperoleh rumusan masalah sebagai berikut:

A. Bagaimana mendeteksi, mengklasifikasi, dan memitigasi serangan pada keamanan Website SIMPKN Informatika ?.

B. Bagaimana rekomendasi perbaikan keamanan pada Website SIMPKN Informatika ?.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disebutkan di atas, maka dapat diperoleh pula tujuan dari penelitian ini sebagai berikut:

A. Mengetahui tingkat keamanan pada Website SIMPKN Informatika.

B. Merekomendasi perbaikan keamanan pada Website SIMPKN Informatika.

1.4 Batasan Masalah

Ruang lingkup penelitian diperlukan supaya proses penelitian tidak meluas cakupannya dan hanya berdasarkan rumusan masalah yang telah disebutkan di atas, sehingga dapat diperoleh cakupan masalah untuk penelitian ini sebagai berikut:

A. Metode pengecekan keamanan pada Website SIMPKN Informatika menggunakan metode OWASP Zed Attack Proxy (ZAP).

B. Pengujian penetrasi melibatkan evaluasi keamanan informasi pada sistem komputer atau jaringan dengan cara mengidentifikasi kerentanan, meninjau pengaturan firewall, serta hotspot Wi-Fi. Hal ini bertujuan untuk mendeteksi kelemahan keamanan pada suatu situs web.