BAB I. Pendahuluan

1.1. Latar Belakang Masalah

Dalam beberapa dekade ini lajunya perkembangan teknologi telah membawa perubahan mendalam dalam cara kita hidup, bekerja, dan berinteraksi. Transformasi yang sangat cepat dalam teknologi informasi, komunikasi, dan ilmu pengetahuan telah menciptakan peluang besar dan tantangan seiring perkembangan zaman. Teknologi telah menjadi pendorong utama kemajuan sosial, ekonomi, dan budaya di seluruh dunia. Dampak signifikan yang ditimbulkan oleh perubahan ini sangat berpengaruh pada berbagai sektor, termasuk bisnis, pendidikan, kesehatan, pemerintahan, hiburan, dan banyak lagi. Salah satu sektor yang sangat terdampak teknologi adalah pada penyampaian informasi.

Salah satu contoh perkembangan tekonologi dalam bidang penyampaian informasi adalah dengan terciptanya sebuah *website. Website* atau laman memiliki definisi sebuah kumpulan halaman yang berfungsi untuk menyajikan informasi yang bisa berupa teks, gambar, animasi, media, atau kombinasi dari semuanya, baik dalam bentuk statis maupun dinamis, yang membentuk sistem terkait satu sama lain[1]. Seiring dengan perkembangan zaman penggunaan *website* tidak hanya digunakan hanya untuk penyampaian informasi saja, karena *website* juga banyak digunakan untuk pengelolaan sistem suatu lembaga atau organisasi. Oleh karena hal tersebut dalam pembuatan *website* untuk sebuah sistem suatu lembaga keamanan dari sistem tersebut perlu diperhatikan.

Meningkatkan keamanan dari sebuah sistem *website* adalah upaya yang digunakan untuk memastikan bahwa sistem *website* tidak mempunyai celah, kerentanan dan risiko untuk diserang oleh para penyerang yang dapat merugikan suatu organisasi atau perusahaan[2]. Semakin tinggi keamanan dari suatu *website* maka semakin tinggi juga keamanan dari informasi

yang ada pada sistem *website* tersebut. Dengan semakin tingginya keamanan dari suatu *website* maka *website* tersebut tentu akan lebih aman dari serangan yang sering terjadi pada sistem suatu *website*. Namun saat ini masih ada pengembang atau pemilik suatu sistem *website* yang masih mengabaikan keamanan *website* tersebut[1].

Keamanan dari *website* PPDB SMK Muhammadiyah Gamping menjadi hal yang perlu diperhatikan. Karena pada *website* PPDB SMK Muhammadiyah Gamping terdapat risiko celah keamanan pada sistem *website* tersebut, oleh karena hal tersebut perlu dilakukannya analisis keamanan pada *website* PPDB SMK Muhammadiyah Gamping guna menemukan celah keamanannya. Ada 2 teknik yang bisa digunakan untuk menemukan kerentanan keamanan sistem pada sebuah *website*, adapun 2 teknik tersebut ialah *vulnerabillity assessment* dan *penetration testing*[3] . *Vulnerabillity assessment* adalah sebuah teknik mencari celah keamanan *website* melalui proses *scanning* sistem untuk menemukan celah keamanan dari suatu *website* dan melakukan peninjauan terhadap kerentanan yang ditemukan, sedangkan *penetration testing* merupakan analisis keamanan suatu sistem dengan mensimulasikan serangan terkontrol guna mengidentifikasi kerentanan terhadap sistem yang sudah ada[4].

Penelitian ini akan melakukan pengujian pada *website* PPDB SMK Muhammadiyah Gamping dengan melakukan *vulnerability assessment* dan *penetration testing* pada *website* guna menemukan celah keamanan sistem *website* dan melakukan analisis terhadap celah yang ditemukan serta melakukan perbaikan pada kerentanan pada keamanan sistem yang ditemukan. Selain itu, pada penelitian ini menggunakan metode *penetration testing execution standard* untuk menguji keamanan dari *website* PPDB SMK Muhammadiyah Gamping terhadap kerentanan *Open Web Application Security Project* (OWASP) 2021. Penelitian ini juga menggunakan alat bantu seperti OWASP ZAP, Acunetix yang digunakan untuk melakukan *vulnerability assessment* dan Burp Suite yang digunakan untuk melakukan *penetration testing*.

Diharapkan pada penelitian ini dapat memberikan hasil berupa temuan celah keamanan pada *website website* PPDB SMK Muhammadiyah Gamping serta memberikan rekomendasi perbaikan terhadap celah yang ditemukan untuk meningkatkan keamanan *website* tersebut.

1.2. Batasan Masalah Penelitian

Adapun batasan masalah dalam penelitian ini ditetapkan untuk mencegah penelitian menjadi terlalu luas, yaitu sebagai berikut :

1. Pengujian dilakukan pada *website* PPDB SMK Muhammadiyah Gamping
2. Penelitian ini akan melakukan *vulnerability asesment* dan *penetration testing* pada *Website* PPDB SMK Muhammadiyah Gamping dan melakukan perbaikan pada celah yang ditemukan
3. Penelitian ini menggunakan metode *penetration testing execution standard* (PTES) untuk melakukan pengujian keamanan *Website* PPDB SMK Muhammadiyah Gamping terhadap kerentanan OWASP TOP 10 2021 yang ditemukan.

1.3. Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang yang ada,maka rumusan masalah dalam penelitian ini dijabarkan sebagai berikut::

1. Bagaimana cara melakukan *vulnerability* asesment pada *Website* PPDB SMK Muhammadiyah Gamping?
2. Bagaimana cara melakukan pengujian terhadap kerentanan sistem yang ditemukan pada *Website* PPDB SMK Muhammadiyah Gamping?
3. Bagaimana cara memperbaiki kerentanan sistem yang ditemukan pada *website* PPDB SMK Muhammadiyah Gamping?

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk mencapai beberapa sasaran utama, antara lain:

1. Menguji tingkat keamanan dari *website* PPDB SMK Muhammadiyah Gamping
2. Mencari kerentanan sistem yang terdapat pada *website* PPDB SMK Muhammadiyah Gamping
3. Meningkatkan keamanan dari *website* PPDB SMK Muhammadiyah Gamping dengan memberikan rekomendasi perbaikan pada celah keamanan yang ditemukan.

1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan berbagai manfaat, antara lain :

1 Mengetahui tingkat keamanan sistem pada *website* PPDB SMK Muhammadiyah Gamping

2 Meningkatkan keamanan sistem *website* PPDB SMK Muhammadiyah Gamping

3 Menjadi tambahan refrensi untuk penelitian bagi peneliti selanjutnya.