# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Saat ini, teknologi informasi memainkan peran yang sangat penting dalam semua lapisan masyarakat dan bidang kehidupan, dan dalam kehidupan bisnis, ekonomi dan politik. Sebab, teknologi sistem informasi saat ini dapat segera menjawab kebutuhan masyarakat. Sehingga membuat pengolahan data dan menghasilkan informasi yang diperlukan menjadi lebih sederhana, lebih akurat, lebih efisien dan efektif. Namun banyak pihak yang mengambil keuntungan dari perkembangan teknologi secara tidak bertanggung jawab. Mulai dari kasus peretasan, penipuan, bahkan kejahatan siber yang tidak hanya menyerang perorangan namun juga perusahaan/perusahaan dan instansi pemerintah.

Di Indonesia, kejahatan yang umum terjadi di dunia komputer melalui *Internet* adalah serangan virus, worm, dorm, korupsi *cyber* dan pencurian informasi pribadi, pinjaman online dan kartu kredit. Kejahatan dunia maya biasanya merupakan kejahatan dunia maya yang menggunakan jaringan komputer sebagai alatnya dan *Internet* sebagai alatnya. Kejahatan siber dalam arti luas adalah setiap aktivitas ilegal yang dilakukan melalui jaringan komputerdan *Internet* dengan tujuan memperoleh keuntungan dengan menimbulkan kerugian bagi pihak lain, sedangkan kejahatan siber dalam arti sempit adalah setiap aktivitas ilegal yang bertujuan untuk menyerang. sistem keamanan informasi dan data. mereka memprosesnya dengan sistem computer [1].

Keamanan sistem informasi harus mewaspadai ancaman internal dan eksternal, yaitu ancaman dari dalam sistem maupun dari luar sistem, yang berdampak pada ketidakstabilan sistem. Mekanisme, organisasi, kelompok, dan individu dapat menyebabkan pemicu pertahanan sistem informasi yang menyebabkan gangguan sistem dan kerusakan data. Langkah pengamanan sistem informasi harus terlebih dahulu mengetahui dan mencegah ancaman yang timbul karena serangan tidak ada sebelum ancaman itu terjadi, untuk meminimalisir ketidakstabilan sistem akibatserangan dengan melakukan tindakan yang telah diantisipasi. Yaitu memprediksi ancaman sebelum serangan.

Perhitungan untuk meminimalkan bahaya tersebut menggunakan metode penilaian risiko (Marakas dan O'Brien (2017, 2018). G. J. Simons berpendapat bahwakeamanan informasi adalah upaya untuk mencegah penipuan (fraud) atau mendeteksipenipuan dalam sistem berbasis informasi dimana informasi itu sendiri tidak memiliki arti fisik [2]. Menurut John D. Howard dalam bukunya "*Analysis of Security Incidents On The Internet*", keamanan komputer adalah pencegahan terhadap serangan yang dilakukan oleh pengguna komputer atau pengguna *Internet* yang tidak bertanggung jawab. Sementara itu, Gollman berpendapat dalam bukunya

"Keamanan Komputer" tahun 1999 bahwakeamanan komputer adalah tentang penghindaran diri dan deteksi aktivitas mengganggu yang tidak diketahui dalam sistem komputer. Sedangkan menurut pakar keamanan Garfinkel dan Spafford, sebuah komputer aman jika dipercaya dan perangkat lunaknya berfungsi sesuai harapan (Rahim, 1999).

*Website* sekolah SDN 50 Bengkalis menggunakan *Website* untuk pengolahan data. Semua informasi sekolah dipublikasikan di *Website*. Hal ini tentunya sangat efektif untuk memanipulasidata, karena memudahkan siswa atau guru dalam mengakses dan mengambildata. Namun jika *Website* yang digunakan oleh Sekolah yang berada di pulau Bengkalis kurang aman maka banyak resiko yang akan muncul, banyak pula ancaman dari pihak-pihak yang tidak bertanggung jawab yang dapat memanfaatkan celah keamanan tersebut untuk merugikan *Website* sekolah SDN 50 Bengkalis.

Penilaian kerentanan adalah proses mendefinisikan, mengidentifikasi, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan, serta memberikan organisasi yang melakukan penilaian informasi, kesadaran, dan latar belakang risiko yang diperlukan untuk mengatasi ancaman. Lingkungan dan memberikan respons yang tepat. Untuk mengidentifikasi ancaman dan risiko yang diakibatkannya, proses penilaian kerentanan yang diusulkanbiasanya menggunakan alat pengujian otomatis, seperti pemeriksaan keamanan jaringan, yang hasilnya tercantum dalam laporan penilaian kerentanan [3].

Di Indonesia, pemahaman dan penerapan metode penetration testing masih terbatas. Banyak orang belum mengenal berbagai metode penetration testing dan seringkali hanya menggunakan satu metode saja. Penggunaan satu metode ini kurang efektif karena pengujiannya tidak menyeluruh dan cakupannya terbatas. Setiap metode penetration testing memiliki fokus dan keahlian tertentu, sehingga menggunakan hanya satu metode tidak mampu mengidentifikasi semua potensi kerentanan yang ada dalam suatu sistem atau aplikasi. Penelitian lebih lanjut sangat penting karena aplikasi web sering digunakan oleh lembaga swasta dan pemerintah. Banyak kasus pembobolan situs web dan kebocoran data pada lembaga pemerintahan yang disebabkan oleh berbagai serangan, seperti SQL injection, broken authentication, dan web defacement. Oleh karena itu, pemahaman yang mendalam tentang berbagai metode penetration testing sangat diperlukan untuk meningkatkan keamanan aplikasi web.[16][17].

Pada Penelitian, ini di analisis celah keamanan pada *Website* Sekolah SDN 50 Bengkalis yang di ambil dari domain *.sch.id. bertujuan untuk menganalisis dan melakukan pengujian keamanan dan perbaikan pada website menggunakan metode VAPT dan *Website Vulnerability Assesment scanning* yang di gunakan adalah Owasp ZAP, Nmap Nikto & Analisis Manul. Hasil dari penelitian ini diharapkan

menjadi informasi sekaligus evaluasi bagi sekolah SDN 50 Bengkalis dalam menjaga dan mengembangkan *Website*.

## 1.2 Permasalahan

Masalah yang ada di *Website* sekolah SDN 50 Bengkalis pada era yang semakin digital ini adalah Kurangnya pengetahuan dalam bidang IT yang mengelola atau yang mengoperasikan *Website* tersebut dan *Website* sekolah sering kali menyimpan informasi sensitif, seperti data pribadi siswa dan staf, banyak *Website* sekolah di Pulau Bengkalis yang tidak menerapkan standar keamanan yang baik sehingga rentan terhadap berbagai serangan *cyber* seperti *SQL Injection*, *Cross-Site Scripting* (XSS), dan DoS (*Denial of Service*).

## 1.3 Tujuan

Tujuan penelitian "Analisis Kerentanan Pada Website Sdn 50 Bengkalis Menggunakan Metode VAPT" ini adalah:

1. Mengidentifikasi kerentanan pada website SDN 50 Bengkalis melalui tahapan Vulnerability assesment menggunakan *information gathering* dan *vulnerability scanning*.
2. Eksploitasi Website untuk mengetahui seberapa rentan website SDN 50 Bengkalis untuk mengetahui sejauh mana celah keamanan dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab dan apa dampak yang mungkin terjadi terhadap website.
3. Melakukan mitigasi dan perbaikan terhadap *website* SDN 50 Bengkalis, dengan melakukan update coding yang berfokus pada database.
4. Meningkatkan Kesadaran Betapa Pentingnya Keamanan Website.

## 1.4 Manfaat

Manfaat penelitian "Analisis tingkat kerentanan pada *Website* Sekolah yang berada di pulau Bengkalis menggunakan Metode VAPT" ini adalah:

a. Meningkatkan Keamanan *Website* sekolah
   1) Deteksi kerentanan: Penelitian ini akan membantu mengidentifikasi beberapa celah keamanan pada *Website* sekolah di Pulau Bengkalis. Dengan mengetahui kerentanan tersebut, sekolah dapat mengambil langkah untuk memperbaikinya.
   2) Pencegahan serangan dunia maya: dengan mengurangi atau menghilangkan kerentanan yang ditemukan, situs *web* sekolah menjadi lebih aman dari serangan dunia maya seperti peretasan, vandalisme, atau pencurian data.

b. Perlindungan data siswa dan guru

1) Perlindungan data pribadi: Situs *web* sekolah sering kali menyimpan data pribadi siswa dan guru. Studi ini membantu memastikan bahwa informasi aman dan terlindungi dari akses tidak sah.
2) Ketahanan Operasional: Dengan mengurangi risiko kerentanan keamanan, operasional situs *web* dapat berjalan lebih lancar tanpa gangguan akibat serangan *cyber*.