BAB I

PENDAHULUAN

1.1 Latar Belakang

Pengujian sistem keamanan *website* adalah hal yang penting di era perkembangan yang melaju dengan pesat, Semakin berkembangnya sistem informasi juga di lihat dengan tingginya serangan keamanan dari berbagai teknik ancaman, Seringkali masalah keamanan berada pada urutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang di anggap penting, Oleh karena itu organisasi atau instansi perlu melakukan *Vullnerabillity Assesment,* agar dapat mampu mendeteksi kerentanan dan memahami resiko yang dihadapi (Ghozali, 2019)

Keamanan merupakan aspek yang begitu penting bagi sistem informasi berbasis *web* yang dapat diakses oleh orang banyak. Tingginya ancaman juga di ikuti dengan perkembangan teknologi informasi saat ini, serta ancaman terhadap website, ini sudah banyak di selediki oleh berbagai penelitian, lembaga riset, ataupun komunitas independen (Moh.Yunus, 2019)

Data serangan Cyber menunjukan tingkat keamanan dalam negeri cukup rentan, dengan jumlah total serangan mencapai 100 juta kasus hinggah 1 agustus 2023 dengan jenis serangan meliputi serangan *malware* dan *ransomalware,* terdapat juga 4 potensi yang mengundang serangan cyber diranah digital yaitu kredensial,phising dan server untuk kredensial ini seperti password yang masih default (BSSN)

Data serangan cyber yang baru baru ini adalah bocornya informasi pribadi dimana dalam keamanan data pribadi ini pretas yang viral dengan nama Bjorka mengumbar data informasi pribadi instansi pada twiter dari serangan tersebut kelemahan dan kurangnya pememelihara sistem hinggah terdapat bug, menjadi alasan kenapa pada data tersebut bocor, serta pada kasus yang kemarin viral dimana data nasabah pada instansi perbankan di retas dan diduga data nasabah di exploitasi di internet data tersebut di retas dengan serangan ransomalware dan juga malware yang dikirim peretas (BSSN)

Analisa Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi *Security Tools Project* Berdasarkan *Framework* Owasp Versi 4 OWASP Versi 4 Menggunakan *tools vulnerability scanner* dengan kolaborasi beberapa *tools security project* dalam mencari celah keamanan, kemudian melakukan pengujian untuk mengetahui keamanan suatu aplikasi (Moh Yunus, 2019)

Scanning *Vullnerabillity Assesment* menjadi solusi Dengan Semakin Kompleksnya ancaman siber, perlindungan pada website sangat penting, celah keamanan website dapat menyebabkan akses yang tidak sah, sehinggah dengan masalah di atas dengan melakukan Scaning *Vullnerabillity Assesement* akan timbul suatu rekomendasi untuk mengatasi kerentanan tersebut untuk keamanan data dan juga mengamankan website dari tindakan pencurian data dan exploitasi dari pihak yang tidak berkepentingan.

Penelitian ini dilakukan dengan tujuan untuk peningkatan keamanan website SMK Negeri 2 Kota Ternate, Berdasarkan Vullnerabillity Assesment menggunakan Framework OWASP Versi 4 dengan mengevaluasi potensi kerentanan sehinggah dapat mengambil

langkah langkah pencegahan yang efektif dan memberikan rekomendasi kepada pengelolah website

1.2 Rumusan Masalah

Berdasarkan Latar Belakang di atas, maka rumusan masalah yang penulis angkat dalam peneitian ini adalah

1. Apa langkah langkah konkret yang perlu di ambil untuk memitigasi kerentanan pada website smkn2ternate.sch.id
2. Bagaimana menyusun rekomendasi yang sesuai dengan hasil analisa vulnerability assessment untuk meningkatkan keamanan website

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini yaitu:

1. Penelitian ini menggunakan *website* SMK Negeri 2 Ternate
2. Pengujian ini hanya berdasarkan pada Framework Owasp Versi 4
3. Pengujian ini Mengikuti pedoman pada Document OWASP

1.4 Tujuan Penelitian

1. Untuk mengidentifikasi langkah-langkah kongkret yang dapat diambil untuk memitigasi kerentanan pada website smkn2ternate.sch.id.
2. Untuk menyusun rekomendasi yang tepat berdasarkan hasil analisa *Vulnerability Assessment* untuk meningkatkan keamanan pada website

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah untuk meningkatkan keamanan website smkn2ternate.sch.id dengan mengidentifikasi dan mengatasi kerentanan yang ada, serta memberikan rekomendasi kepada pengelolah website untuk meningkatkan keamanan secara efektif.

1.6 Sistematika Penulisan

Sistematika penulisan laporan ini, merupakan pembahasan singkat dari setiap bab yang ada beserta penjelasan terkait hubungan-hubungan antara bab pada laporan penelitian ini yang terdiri dari 3 bab yaitu sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi pengantar dalam memahami dan mengenal materi pokok secara garis besar yang terdiri dari latar belakang dan alasan memilih judul , rumusan masalah, batasan masalah serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan teori-teori yang berkaitan dengan judul penulisan, Hal ini di maksudkan untuk memberikan landasan teoritis dalam menganalisa permasalahan yang di dapat peneliti.

BAB III METODE PENELITIAN

Bab ini menguraikan tentang metode dan teknik yang di gunakan untuk mengumpulkan data sehinggah dapat menjawab atau menjelaskan masalah penelitian.

BAB IV HASIL DAN PEBAHASAN

bab ini membahasa tentang hasil dalam pengujian sebuah kerentanan pada website dimana kerentanan kerentanan tersebut di analisa dan di uraikan dalam tahapan implementasi framework owasp versi 4

BAB V PENUTUP

Bab ini adalah bab yang mengurainkan kesimpulan dan saran dari hasil penelitian dan pengujian