

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, *website* telah menjadi salah satu elemen penting bagi perusahaan, organisasi, dan individu dalam menjalankan berbagai aktivitas, mulai dari penyediaan informasi, layanan transaksi, hingga layanan komunikasi. seiring dengan meningkatnya penggunaan *website*, timbul beragam potensi serangan yang berusaha mencuri data atau mengambil informasi sensitif dari sebuah *website* [1]. berbagai serangan siber sering kali dimanfaatkan oleh peretas atau pihak yang tidak bertanggung jawab untuk mengeksploitasi celah keamanan dalam suatu *website*. Misalnya serangan *Cross-Site Scripting* (XSS) yang merupakan salah satu jenis serangan pada *website* yang berbahaya. Serangan ini digunakan untuk mencuri informasi pengguna (*phishing*), bahkan dapat menjalankan *script* berbahaya pada browser pengguna [2]. Jenis serangan lain yang juga berbahaya adalah serangan *SQL Injection*. *SQL injection* merupakan celah keamanan yang ada pada aplikasi *website* berbasis database, di mana penyerang memanipulasi input pengguna untuk menyisipkan perintah *SQL* berbahaya, guna untuk mendapatkan akses yang tidak sah ke informasi sensitif [3].

Serangan-serangan ini dapat menyebabkan organisasi mengalami kerugian finansial, pencurian data, hingga penurunan reputasi akibat serangan yang tidak terdeteksi atau tertangani dengan baik. Berdasarkan laporan tahunan Badan Siber dan Sandi Negara (BSSN), pada tahun 2024 tercatat sebanyak 330.527.636

serangan siber di Indonesia, dengan lonjakan tertinggi pada bulan Desember yang mencapai 112.085.045 serangan, sementara jumlah terendah terjadi pada bulan Mei dengan 12.273.078 serangan. Statistik ini menunjukkan bahwa keamanan siber di Indonesia masih memiliki banyak celah yang dapat dieksploitasi oleh peretas atau pihak yang tidak bertanggungjawab, sehingga meningkatkan risiko kebocoran data sensitif, penurunan reputasi, serta berkurangnya tingkat kepercayaan terhadap institusi yang terkena dampaknya [4].

SMK Taruna Bangsa dipilih sebagai objek penelitian karena *website* sekolah ini merupakan sarana utama dalam penyampaian informasi akademik dan administrasi. Berdasarkan hasil wawancara dengan pengelola *website*, diketahui bahwa sebelumnya *website* ini pernah mengalami insiden keamanan, seperti serangan yang mengeksploitasi celah pada fitur formulir dan informasi kontak, bahkan *website* mengarah pada situs judi online melalui *malicious redirect* atau *unwanted redirect*. Selain itu, ditemukan sebuah *backdoor* yang terindikasi disisipkan melalui sebuah kolom komentar yang dimana hal ini dapat memberikan akses yang tidak sah kedalam sistem atau *website*. *Website* ini juga belum pernah menjalani proses pengujian keamanan secara menyeluruh, tidak memiliki standar operasional prosedur (SOP) penanganan insiden keamanan, dan belum pernah dilakukan audit sistem informasi. Sementara itu, *log access user* masih terbatas pada IP yang terekam melalui *CPanel*.

Dari hasil wawancara tersebut menunjukkan bahwa sistem keamanan pada *website* SMK Taruna Bangsa masih rentan terhadap potensi eksploitasi. Oleh karena itu, dilakukan analisis kerentanan dengan pendekatan *penetration testing*

menggunakan metode *OWASP* untuk memberikan rekomendasi khusus dan teknis yang relevan dalam meningkatkan keamanan *website* sekolah SMK Taruna Bangsa.

Berdasarkan permasalahan yang telah diuraikan, penelitian ini akan berfokus pada Analisis Kerentanan *Website* dengan Pendekatan *Penetration Testing* Menggunakan Metode *OWASP* pada *Website* SMK Taruna Bangsa.

Penelitian ini bertujuan untuk mengidentifikasi tingkat keamanan *website*, menemukan potensi celah keamanan, serta memberikan rekomendasi teknis guna meningkatkan perlindungan terhadap serangan siber. Hasil penelitian ini diharapkan dapat meningkatkan kesadaran serta pemahaman pihak sekolah terhadap pentingnya keamanan siber, serta menjadi acuan bagi institusi pendidikan lainnya dalam mengembangkan sistem keamanan *website* yang lebih baik.

1.2 Identifikasi Masalah

Berikut beberapa permasalahan utama yang menjadi fokus dalam penelitian ini, yaitu.

1. *Website* SMK Taruna Bangsa belum pernah dilakukan pengujian keamanan secara menyeluruh sehingga perlu dianalisis untuk mengetahui seberapa besar potensi risiko terhadap serangan siber yang dapat mengancam data dan operasional *website*.
2. Jenis-jenis kerentanan yang ada pada *website* perlu diidentifikasi secara sistematis melalui pendekatan pengujian keamanan *penetration testing* menggunakan metode *OWASP*.

3. Dampak dari kerentanan yang ditemukan perlu dianalisis untuk memahami sejauh mana ancaman tersebut dapat memengaruhi *confidentiality*, *integrity*, dan *availability* data serta layanan pada *website*.
4. SMK Taruna Bangsa belum terdapat standar operasional prosedur (SOP) dalam menangani insiden keamanan maupun audit sistem informasi.
5. Dalam sistem manajemen log, *website* SMK Taruna Bangsa masih terbatas pada *log* IP melalui *CPanel* dan belum mampu memberikan informasi yang memadai untuk mendeteksi potensi serangan.
6. Rekomendasi peningkatan keamanan sistem perlu dirumuskan berdasarkan hasil analisis kerentanan untuk memperkuat keamanan *website* SMK Taruna Bangsa terhadap potensi ancaman siber.

1.3 Rumusan Masalah

Berdasarkan identifikasi permasalahan di atas, maka dapat diperoleh rumusan masalah:

1. Bagaimana tingkat kerentanan *website* SMK Taruna Bangsa terhadap serangan siber berdasarkan hasil *penetration testing* menggunakan metode OWASP?
2. Jenis kerentanan apa saja yang ditemukan pada *website* SMK Taruna Bangsa setelah berdasarkan OWASP Top 10?
3. Bagaimana dampak dari kerentanan yang ditemukan terhadap keamanan data dan operasional *website*?
4. Rekomendasi keamanan apa yang dapat diterapkan untuk meningkatkan perlindungan *website* SMK Taruna Bangsa dari ancaman siber?

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, penelitian ini bertujuan untuk:

1. Melakukan pengujian keamanan pada *website* SMK Taruna Bangsa menggunakan pendekatan *penetration testing* menggunakan metode *OWASP* untuk mengidentifikasi potensi kerentanan.
2. Mengklasifikasikan dan menganalisis jenis-jenis kerentanan yang ditemukan berdasarkan kategori dalam *OWASP Top 10*.
3. Melakukan evaluasi dampak dari kerentanan yang teridentifikasi terhadap operasional *website* serta potensi ancaman terhadap data pengguna.
4. Menyusun rekomendasi perbaikan keamanan yang dapat diterapkan pengelola *website* untuk meningkatkan perlindungan terhadap serangan siber.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Penelitian ini diharapkan dapat memberikan kontribusi baik pada keamanan siber melalui pengujian *website* dengan metode *OWASP*.
2. Dapat menjadi referensi untuk penelitian selanjutnya dengan pengujian keamanan *website*, dan membantu akademisi serta mahasiswa memahami teknik mitigasi kerentanan.
3. Penelitian ini membantu pengelola situs SMK Taruna Bangsa menemukan masalah keamanan dan menawarkan solusi untuk meningkatkan pertahanan terhadap serangan siber.
4. Penelitian ini dapat diterapkan pada institusi Pendidikan lainnya dan menjadi referensi bagi praktisi keamanan siber dalam penerapan metode

OWASP.

5. Penelitian ini meningkatkan kesadaran akan pentingnya menjaga keamanan data pada institusi pendidikan dan mendorong penguatan sistem digital untuk melindungi data dari kebocoran dan ancaman siber.

1.6 Batasan Masalah

Berdasarkan rumusan masalah yang telah diuraikan, maka berikut batasan masalah dalam penelitian ini:

1. Penelitian ini hanya berfokus pada analisis keamanan *website* SMK Taruna Bangsa menggunakan pendekatan *penetration testing* dengan metode OWASP dan kategori OWASP Top 10, tanpa mencakup uji keamanan infrastruktur jaringan sekolah.
2. Analisis hanya dilakukan pada *website* utama SMK Taruna Bangsa tanpa mencakup sistem internal sekolah seperti jaringan, *server mail*, atau sistem informasi sekolah (SIS).
3. Pendekatan yang digunakan terbatas pada *penetration testing* dengan metode OWASP, tanpa melibatkan metode pengujian lain.
4. Penelitian hanya berfokus pada analisis, identifikasi serta eksploitasi kerentanan teknis, tanpa membahas secara mendalam tentang ancaman *non-teknis*, seperti serangan berbasis sosial seperti *social engineering* atau *insider threat*.
5. Pada penelitian ini, *tools* yang digunakan untuk pemindaian dan eksploitasi kerentanan telah sesuai dengan standar industri, akan tetapi penelitian ini tidak

mencakup perbandingan antara berbagai *tools* yang digunakan.

6. Penelitian ini berfokus pada pengujian teknis, dan tidak menguji secara mendalam aspek kebijakan atau tingkat kesadaran keamanan siber di kalangan staf sekolah atau pihak terkait.

1.7 Sistematika Tugas Akhir

Sistematika penulisan dalam tugas akhir mengikuti aturan yang menentukan susunan teks secara sistematis, sehingga memberikan gambaran yang jelas dan menyeluruh. Adapun sistematika penulisan dalam penelitian ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi penjelasan umum mengenai latar belakang penelitian, identifikasi masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, manfaat penelitian, serta sistematika tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang landasan teori yang berkaitan tentang pembahasan dalam penelitian *penetration testing* dan pembahasan tentang metode *OWASP*.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metode yang digunakan dalam penelitian, seperti pendekatan penelitian, Teknik pengumpulan data, dan objek penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang proses pengujian *website* yang di uji dan dapat melihat hasil kerentanan apa saja yang ada pada *website* tersebut.

BAB V PENUTUP

Bab ini menjelaskan kesimpulan terhadap penelitian yang telah dilakukan serta saran yang diberikan kepada pembaca untuk dilanjutkan atau di kembangkan oleh penelitian selanjutnya.

