BAB I PENDAHULUAN

I.1 Latar Belakang

Evolusi sistem teknologi informasi telah berkembang dengan cepat sejak kemunculan *World Wide Web* atau yang lebih dikenal sebagai *Website* pada tahun 1989. Tujuan utama pembuatan sistem ini adalah untuk mendukung manusia dalam pertukaran dan pembaruan informasi. Namun, seiring berjalannya waktu, tuntutan meningkatnya kebutuhan manusia mendorong teknologi untuk terus meningkatkan fungsinya. Penelitian ini akan merinci perkembangan *website* mulai dari era Web 1.0, Web 2.0, hingga Web 3.0.

Pada era Web 1.0, fungsi utama *website* adalah sebagai *platform* pencarian informasi atau berita dengan akses satu arah. Seiring berjalannya waktu, terutama pada era Web 2.0, *website* mengalami peningkatan fungsi signifikan dengan pertukaran informasi yang bersifat masif. Web 2.0 memungkinkan interaksi dua arah dan aktivitas sosial di dunia maya melalui *platform* media sosial seperti media messengers, Facebook, dan Twitter. Era Web 3.0 melihat inovasi yang luar biasa dengan kemunculan *Semantic* Web, di mana *website* dapat memahami bahasa manusia tidak hanya melalui teks tetapi juga bahasa suara (Ashri, 2022).

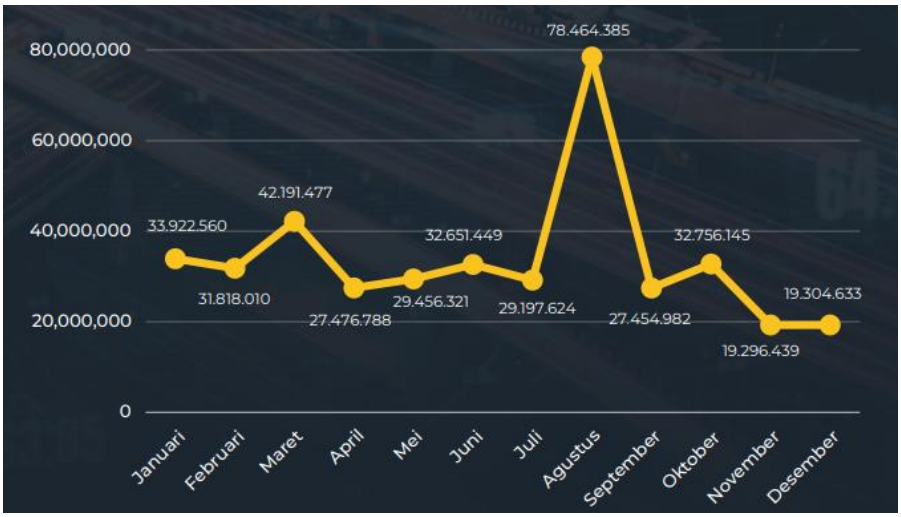
Teknologi Informasi dan Komunikasi (TIK) telah membawa perubahan mendasar dalam pendidikan di Indonesia. Dalam beberapa tahun terakhir, kemajuan TIK telah signifikan dalam meningkatkan aksesibilitas dan kualitas pembelajaran, serta mempromosikan keadilan sosial. Pandemi COVID-19 telah mempercepat adopsi teknologi digital di sektor pendidikan. Dengan adanya berbagai platform dan teknologi pembelajaran, siswa dan guru kini dapat mengakses materi pembelajaran sesuai dengan kebutuhan belajar individu, serta pengembangan media pembelajaran yang inovatif meningkatkan interaksi siswa dengan materi pelajaran, menciptakan pengalaman belajar yang lebih menarik dan mendalam (Hidayatullah et al., 2023).

Sebelumnya, pelajar terbiasa dengan metode penyelenggaraan ujian

berbasis kertas atau PBT (*Paper Based Test*) yang tentunya beresiko kebocoran dalam penyebaran soal-soal ujian yang dianggap sensitif. dengan adanya pemanfaatan teknologi membuka peluang baru untuk efisiensi dan efektivitas dalam penyelenggaraan ujian dengan menerapkan ujian berbasis komputer atau CBT (*Computer Base Test*), tetapi juga membawa risiko terhadap keamanan data.

Perkembangan terus-menerus dalam teknologi informasi telah secara signifikan merubah konsep keamanan, mengembangkan ruang interaksi dari sebatas fisik menjadi melibatkan dunia maya (*cyber*). Akibatnya, negara harus beradaptasi dengan perkembangan konsep keamanan dunia maya, yang kini diakui sebagai salah satu "wilayah" yang perlu dijaga oleh negara sebagaimana halnya dengan kewajiban menjaga keamanan teritorialnya. Serangan *cyber* tidak hanya terbatas pada institusi publik, tetapi juga merambah ke institusi pemerintah. Keamanan *cyber* mencakup berbagai aspek yang berkaitan dengan pengawasan komputer, *monitoring*, hingga penerapan kontrol yang sangat ketat (Wardana, 2021).

Menurut data statistika dari Badan Siber dan Sandi Negara Republik Indonesia (BSSN) terdapat terdapat 403.990.813 total trafik dari anomali dan serangan siber di Indonesia selama tahun 2023 Seperti pada gambar 1.1 (BSSN, 2023).



Gambar I.1 Statistik Trafik Anomali dan Serangan *Cyber* di Indonesia selama Tahun 2023

Dikarenakan terdapat kenaikan signifikan tidak menutup kemungkinan bahwa dapat terjadinya penyerangan, oleh karena itu, perlindungan terhadap keamanan jaringan menjadi kritis, terutama dalam konteks institusi pendidikan yang menyimpan data siswa dan informasi sensitif lainnya seperti soal ujian sekolah.

Sebagai sekolah yang memiliki sejarah panjang sejak penerimaan siswa baru pada tahun 1986, SMAN 20 Bandung juga telah berupaya mengadopsi teknologi informasi dalam proses pembelajaran, salah satunya melalui pelaksanaan ujian berbasis komputer (CBT). *Website* ujian tersebut dijalankan melalui server lokal berbasis Bitnami WAMP Stack, yang dari hasil observasi awal menunjukkan bahwa sistem ini telah digunakan dalam waktu yang cukup lama dan belum memiliki dokumentasi yang jelas terkait versi maupun pembaruan layanan yang digunakan. Kondisi ini menimbulkan potensi risiko keamanan, terutama ketika server dibuka secara publik pada waktu tertentu selama ujian berlangsung, sehingga permukaan serangan terhadap sistem menjadi lebih luas.

Berdasarkan hasil tinjauan lapangan, sistem ini belum pernah menjalani pengujian keamanan secara menyeluruh sejak pertama kali diterapkan. Padahal, sistem ujian tersebut menyimpan dan mengelola berbagai data penting seperti akun siswa, nilai hasil ujian, serta data guru. Dengan mempertimbangkan sensitivitas data tersebut, perlindungan terhadap kerahasiaan, keutuhan, dan ketersediaan sistem menjadi krusial. Penelitian ini dilaksanakan berdasarkan surat permohonan penelitian *final project* dan koordinasi dengan tim IT SMAN 20 Bandung untuk memastikan proses penelitian dilakukan secara etis dan terkoordinasi. Kondisi ini menjadikan pengujian keamanan sebagai kebutuhan nyata yang belum terpenuhi, dan penting untuk dilakukan secara metodologis menggunakan pendekatan standar seperti *Penetration Testing Execution Standard* (PTES).

Untuk menjawab kebutuhan tersebut, penelitian ini menggunakan pendekatan pengujian keamanan berbasis *Penetration Testing Execution*

Standard (PTES). PTES merupakan standar metodologis yang dirancang untuk memberikan struktur yang sistematis dalam pelaksanaan pengujian keamanan, mulai dari tahap awal perencanaan hingga pelaporan akhir. Standar ini terdiri dari tujuh tahapan utama, yaitu *Pre-Engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation,* dan *Reporting*. Dengan menggunakan pendekatan ini, pengujian dilakukan secara menyeluruh terhadap sistem untuk mengidentifikasi potensi kerentanan dan mengevaluasi sejauh mana sistem dapat bertahan terhadap skenario serangan yang realistis.

Berdasarkan latar belakang tersebut, penelitian ini difokuskan pada analisis celah kerentanan dan pengujian keamanan terhadap *website* server ujian yang digunakan di SMAN 20 Bandung. Pengujian dilakukan menggunakan pendekatan standar PTES yang disesuaikan dengan kebutuhan sistem pendidikan menengah, dengan tujuan untuk mengidentifikasi titik-titik lemah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Hasil dari penelitian ini diharapkan dapat memberikan gambaran nyata mengenai kondisi keamanan sistem ujian sekolah serta menjadi dasar dalam perbaikan dan peningkatan pengamanan sistem informasi pendidikan di lingkungan SMAN 20 Bandung.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diketahui maka terdapat beberapa permasalahan yang terjadi pada SMAN 20 Bandung terkait dengan keamanan suatu *website* server dimana hal tersebut menjadi fokus utama dilakukannya analisis celah kerentanan pada *website* server. Rumusan masalah yang menjadi fokus penelitian ini adalah sebagai berikut:

1. Bagaimana cara menemukan kerentanan pada *Web Server* ujian SMAN 20 Bandung?
2. Bagaimana cara melakukan eksploitasi dan melakukan mitigasi pada *website* server ujian SMAN 20 Bandung?

I.3 Tujuan Tugas Akhir

Penelitian ini dilakukan dengan tujuan adalah sebagai berikut:

1. Mengetahui kerentanan pada *website* server ujian pada SMAN 20 Bandung.
2. Melakukan eksploitasi dan melakukan mitigasi pada *website* server ujian SMAN 20 Bandung.

I.4 Batasan Tugas Akhir

Ruang lingkup pada penelitian ini akan berfokus pada hal yang berhubungan langsung dengan keamanan web server sebagai berikut:

1. Objek penelitian ini akan terbatas pada *website* server ujian SMAN 20 Bandung.
2. Penelitian ini akan menggunakan *automated tools scanning*, berupa Burpsuite *professional* versi 2025.1.4, OWASP ZAP versi 2.16.1, dan Nessus 10.8.4 dalam melakukan pemindaian kerentanan terhadap *website* target.
3. Parameter diukur meliputi tingkat kerentanan dan solusi mitigasi yang diterapkan berdasarkan hasil pemindaian kerentanan.
4. Penelitian ini terbatas pada tahap *vulnerability analysis,* eksploitasi, dan mitigasi. Jika ditemukan kerentanan pada konfigurasi *server* dan baris kode sistem *website*, langkah mitigasi yang akan diambil dengan memberikan rekomendasi mitigasi.

I.5 Manfaat Tugas Akhir

Hasil yang akan didapatkan pada penelitian ini diharapkan dapat digunakan dan memberikan manfaat sebagai berikut:

1. Bagi SMAN 20 Bandung, penelitian ini bermanfaat dalam meningkatkan pemahaman tentang keamanan *website* server ujian dari mengetahui kerentanan apa saja yang ada pada *website* ujian dan menjadi acuan dalam rekomendasi peningkatan keamanan pada sistem *website.*

2. Bagi peneliti lain yang bergerak dalam Sistem Informasi pendidikan tinggi, penelitian ini bermanfaat untuk memberikan referensi dan acuan guna menyelesaikan karya tulis lain yang menggunakan objek target, maupun *tools* yang digunakan berupa Burpsuite, OWASP ZAP, dan Nessus.
3. Bagi penulis menambahkan wawasan ilmu dari penelitian mengenai permasalahan yang di dapat dan sebagai syarat kelulusan pada program studi Strata 1 Sistem Informasi Universitas Telkom Bandung.