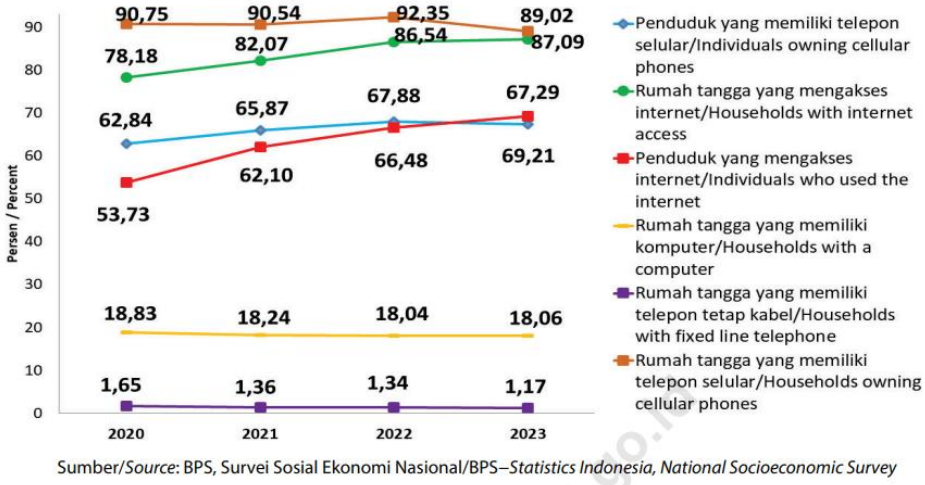
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi di abad ke-21 terus bertumbuh hingga menjangkau hampir seluruh masyarakat secara global. Peningkatan penggunaan alat komunikasi elektronik mendorong perusahaan teknologi untuk mengembangkan berbagai inovasi yang memberikan kemudahan pada pengguna. Jumlah penggunaan perangkat Teknologi Informasi dan Komunikasi (TIK) di Indonesia untuk perangkat yang tersambung internet meningkat dari 2020 hingga 2023 berdasarkan data yang dihimpun dari Badan Pusat Statistik.



Sumber/*Source*: BPS, Survei Sosial Ekonomi Nasional/BPS–*Statistics Indonesia, National Socioeconomic Survey*

Gambar 1.1 Data Pengguna TIK di Indonesia 2020 – 2023 (Badan Pusat Statistik, 2024)

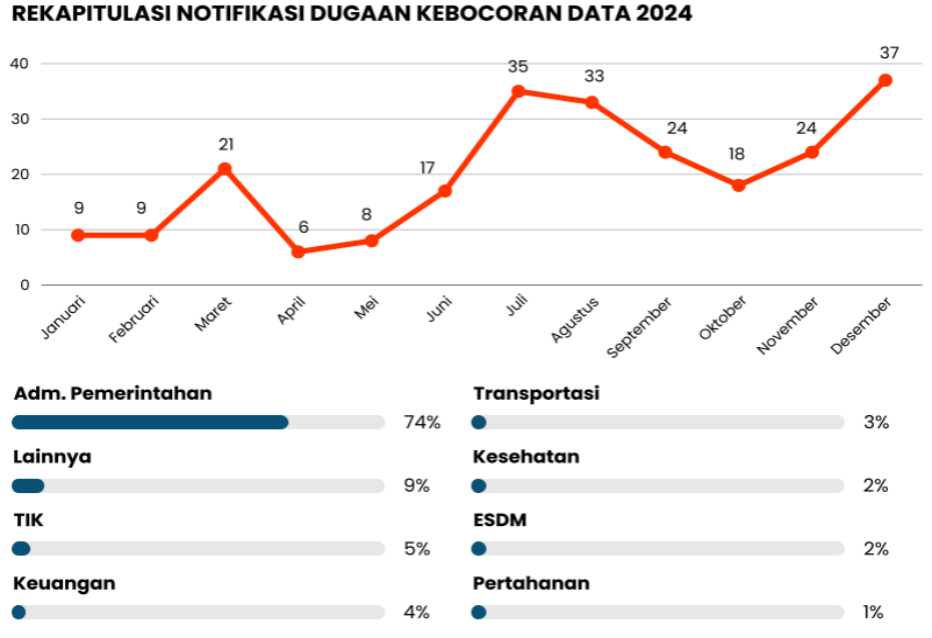
Meskipun penggunaan telepon seluler meningkat, namun penggunaan komputer oleh rumah tangga stabil. Berdasarkan hasil survey dari didapatkan jawaban bahwa kemudahan akses internet dengan berbagai media komunikasi khususnya perangkat seluler menyebabkan peralihan teknologi (Badan Pusat Statistik, 2024). Namun, komputer tetap memiliki peran penting dalam berbagai sektor, terutama sebagai media utama dalam produksi, penyebaran, dan konsumsi informasi digital.

Komputer tidak hanya digunakan sebagai alat pengolah data, tetapi juga sebagai jembatan utama dalam infrastruktur teknologi informasi pada berbagai sektor. Dalam konteks komunikasi dan akses informasi, komputer telah bertransformasi menjadi pusat kendali digital yang memungkinkan masyarakat mengakses sumber daya pengetahuan secara lebih luas. Berdasarkan penelitian mengenai dampak perkembangan teknologi informasi pada masyarakat oleh (Lubis & Nasution, 2023), kesenjangan digital dapat menjadi masalah dalam perkembangan pemanfaatan teknologi yang disebabkan oleh faktor ekonomi, infrastruktur, atau keterampilan digital terhadap pemanfaatan akses masyarakat terhadap komputer dan internet.

Penggunaan komputer tidak terbatas sebagai alat pengolah informasi, namun memiliki peran strategis dalam mendukung infrastruktur jaringan global yang menghubungkan miliaran pengguna ke internet. Sejak perkembangan internet di akhir abad ke-20, komputer menjadi *gateway* utama dalam ekosistem digital yang memungkinkan pengguna untuk mengakses berbagai platform informasi, seperti website, media sosial, dan layanan berbasis *cloud*. Dalam laporan yang diterbitkan oleh (Badan Pusat Statistik, 2024), diperkirakan selama periode 2022 – 2023 terdapat peningkatan pengguna internet dalam tiga bulan terakhir dari 66,48% dan naik menjadi 69,21%. Masyarakat Indonesia telah beradaptasi dalam menggunakan internet dengan peningkatan akses yang sebagian besar didorong oleh integrasi komputer dalam kehidupan sehari-hari.

Penyebaran informasi jauh lebih cepat berkembang dengan adanya media digital yang mendukung efisiensi dan layanan interaktif pada pengguna internet. Jika dahulu orang memerlukan koran atau tabloid dalam mencari informasi, sekarang dengan adanya website pengguna internet akan lebih mudah mencari berita dengan membaca di laman portal *blog* yang telah disediakan oleh *blogger*. Penggunaan website sebagai sarana dalam menyebarkan informasi dapat diadopsi oleh berbagai pihak, baik secara pribadi maupun organisasi atau badan lembaga tertentu.

Masifnya perkembangan teknologi juga perlu didukung dengan kesadaran akan pentingnya menjaga data pribadi. Akses kemudahan internet yang dapat menghubungkan satu sama lain memiliki risiko terhadap pencurian data. Data yang berasal dari jurnal mendapati hasil bahwa peningkatakan serangan siber dunia cukup masif. Sedangkan di Indonesia sendiri berdasarkan data yang dihimpun dari (BSSN, 2025)**,** korban kejahatan pencurian data ada dalam berbagai sektor seperti pemerintahan, ekonomi, kesehatan dan berbagai sektor lainnya dengan dugaan kebocoran data sebanyak 241 insiden.



Gambar 1.2 Rekapitulasi dugaan kebocoran data 2024 (BSSN, 2025)

Meskipun perkembangan teknologi membantu manusia dalam menyelesaikan pekerjaan, namun tidak dapat dipungkiri bahwa kesempatan celah yang ada pada website publik menjadi kesempatan bagi para *hacker* untuk melakukan kejahatan internet. Beberapa contoh kejahatan siber yang banyak menyerang di Indonesia berdasarkan data yang dihimpun dari Parulian dkk. (2021) adalah *Denial of Service attack, phishing ,* dan pencurian data.

Menurut laporan dari *Open Web Application Security Project* (OWASP, 2021) dengan mengumpulkan data dari berbagai sumber seperti laporan dari praktisi, survey langsung, dan organisasai mitra serangan terhadap aplikasi web masih menjadi salah satu ancaman utama dalam dunia keamanan siber.

Dihimpun dari laporan (OWASP, 2021) yang menganalisis lebih dari 500.000 aplikasi website, beberapa serangan yang terjadi seperti kerentanan *Broken Access Control* 3,81%, dengan 318.000 kasus dan *Injection* 3,37%, 274.000 kasus. Serangan yang terjadi dalam website dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mencuri data, memodifikasi informasi, atau bahkan mengambil alih kendali sistem. Maka pengujian keamanan website menjadi aspek yang sangat penting guna memastikan bahwa website yang digunakan oleh institusi pendidikan aman dari eksploitasi dan penyalahgunaan.

Penggunaan teknologi telah digunakan menyeluruh dalam berbagai bidang. Salah satu bidang terdepan yang memanfaatkan perkembangan teknologi dengan baik adalah pendidikan. Berdasarkan penelitian dari (Cholik, 2021), perkembangan teknologi pada pendidikan dapat berguna sebagai infrastruktur pembelajaran, sumber bahan ajar, alat bantu dan fasilitas pembelajaran, sumber informasi penelitian, media komunikasi, dan sumber belajar daring. Pemanfaatan penggunaan website sebagai media penyalur informasi dapat memberikan manfaat pada institusi pendidikan. Sekolah mengintegrasikan website untuk menyampaikan informasi mengenai berbagai aktivitas akademik. Website dapat digunakan sebagai sarana utama bagi sekolah dalam menyampaikan informasi pada pengunjung sehingga iformasi dapat diperoleh maksimal.

Penggunaan website publik memiliki risiko keamanan dari serangan siber. Perkembangan teknologi informasi yang begitu pesat telah mendorong sistem berbasis website tetapi juga meningkatkan potensi serangan keamanan pada situs web (Widya Ningsih Nasir dkk., 2021). Beberapa contoh serangan siber pada website adalah *SQL Injection, Cross-site scripting (XSS),* dan *Cross-Site Request Forgery (CSRF)* menjadi perhatian sendiri bagi pengembang website dan lembaga terkait dalam menjaga keamanan sistem informasi. Tanpa pengujian keamanan yang memadai, celah pada sistem dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mencuri data, mengubah informasi, atau bahkan mengambil alih kendali website. Adopsi penggunaan website sebagai sistem informasi telah digunakan oleh SMKN 1 Jakarta. Website SMKN 1 Jakarta berisi informasi mengenai kegiatan belajar mengajar,

ekstrakurikuler, berita akademik, dan informasi data profil sekolah. Berdasarkan hasil observasi berupa wawancara dari tim pengembang website profil SMKN 1 Jakarta didapati hasil bahwa selama website berjalan memang belum terdapat audit pada keamanan website. Lalu secara historis terdapat penyerangan yang mengakibatkan website *down* sehingga mengharuskan *administrator* website melakukan migrasi dengan membuat website baru. Menurut (Rais dkk., 2024) dikatakan bahwa audit teknologi informasi merupakan proses pemeriksaan dan evaluasi sistem informasi perusahaan yang dilakukan dengan cara mengumpulkan data melalui analisis risiko berdasarkan prosedur tertentu. Melakukan audit secara berkala pada sistem infrastruktur TI akan meminimalisir kemungkinan adanya kerusakan sistem di masa depan.

Dalam upaya menjaga keamanan sistem informasi, keberadaan standar pengujian yang terarah dan sistematis penting sebagai acuan utama dalam melakukan evaluasi. Beragam pedoman audit dan pengujian keamanan telah dikembangkan oleh beberapa badan organisasi *international*, mulai dari yang menekankan pada tata kelola menyeluruh hingga yang berfokus pada aspek teknis sistem. Beberapa standar seperti ISO/IEC 27001 memang banyak diterapkan pada institusi dengan struktur manajemen keamanan informasi yang sudah mapan. Namun, di lingkungan pendidikan seperti sekolah yang masih dalam tahap awal penerapan pengamanan sistem digital, pendekatan yang lebih fleksibel dan praktis menjadi pertimbangan utama. Dalam konteks ini, pedoman teknis seperti NIST Special Publication 800-115 memberikan panduan yang lebih aplikatif dalam melakukan pengujian terhadap komponen sistem tertentu, termasuk website melalui metode tertentu seperti *white-box* dan *black-box testing*. Dengan fokus langsung pada pengujian keamanan sistem tanpa menuntut adanya struktur tata kelola IT yang kompleks, pendekatan NIST dinilai relevan untuk diterapkan pada objek penelitian seperti website profil sekolah.

Meskipun banyak manfaat dari penggunaan website, namun jika tidak dijaga dengan baik, maka dapat mengakibatkan kerugian pada SMKN 1 Jakarta terutama dalam distribusi informasi. *Hacker* dapat memanfaatkan celah untuk kepentingan pribadi dengan melakukan berbagai macam jenis kejahatan siber.

Celah keamanan yang berhasil diretas berpotensi mencuri data yang bersifat rahasia dan sensitif. Secara khusus pemerintah melakukan upaya untuk memperkuat regulasi dengan mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam UU PDP disebutkan bahwa setiap penyelenggara sistem elektronik, termasuk institusi pendidikan wajib melindungi data pribadi yang dikumpulkan, disimpan, dan diproses. Website sekolah yang menyimpan atau menampilkan data siswa, guru, dan informasi internal sekolah berpotensi mengandung data pribadi yang wajib dilindungi. Ketiadaan pengujian keamanan berisiko mengakibatkan kebocoran data dan melanggar prinsip-prinsip perlindungan data sebagaimana diatur dalam UU PDP. Untuk meminimalisir risiko terhadap serangan siber, maka diperlukan sebuah langkah pengujian dari perspektif luar sistem website smkn1jkt.sch.id. Hasil dari penelitian ini akan berupa laporan, dokumentasi hasil pengujian, dan saran mitigasi sebagai referensi bagi pengelola IT dalam meningkatkan keamanan website SMKN 1 Jakarta.

1.2 Identifikasi Masalah

Berdasarkan penjelasan dari latar belakang penelitian, maka identifikasi masalah dapat ditulis sebagai berikut :

1. Risiko kejahatan siber seperti *Injection, Cross-site scripting (XSS)*, dan *clickjacking* meningkatkan risiko eksploitasi pada website publik seperti xxx.jkt.xxx.id .
2. Belum dilakukan pengujian keamanan pada website profil SMK Negeri 1 Jakarta untuk mengidentifikasi potensi celah keamanan yang dapat mengancam integritas informasi akademik.
3. Ketiadaan dokumentasi tertulis terhadap kondisi keamanan website profil SMK Negeri 1 Jakarta seperti laporan kerentanan atau riwayat serangan yang diperlukan sebagai acuan dalam perbaikan sistem dan mitigasi risiko siber.
4. Belum tersedia mekanisme evaluasi keamanan yang dapat mendukung penerapan prinsip-prinsip perlindungan data pribadi sesuai ketentuan UU PDP.

1.3 Pembatasan masalah

1. Objek penelitian terbatas pada domain xxx.jkt.xxx.id .
2. Fokus penelitian pada identifikasi celah keamanan dan validasi kerentanan tanpa melakukan eksploitasi lebih lanjut yang dapat menyebabkan kerusakan pada sistem atau upaya mengambil alih akses sistem.
3. Penelitian berfokus pada identifikasi celah keamanan tanpa menyajikan mitigasi mendalam, mengingat ruang lingkup penelitian ini lebih mengarah pada dokumentasi hasil pengujian sehingga hasil yang diharapkan sebatas rekomendasi mitigasi.

1.4 Perumusan masalah

Berdasarkan penjabaran dari latar belakang, maka rumusan masalah yang akan dikembangkan adalah "bagaimana cara melakukan pengujian keamanan pada website profil SMKN 1 Jakarta dengan menggunakan *blackbox – testing* dengan menggunakan standar NIST SP 800-115?"

1.5 Tujuan penelitian

Tujuan dari penelitian ini adalah melakukan pengujian keamanan guna mengidentifikasi potensi kerentanan serta mendokumentasikan proses dan hasil temuan terhadap website SMKN 1 Jakarta sebagai acuan dalam memperkuat sistem keamanan.

1.6 Manfaat penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

Bagi Pengembang Website:

1. Memberikan gambaran mengenai teknik pengujian keamanan dari perspektif luar sistem.
2. Menunjukkan potensi celah keamanan yang harus diperhatikan *web developer* dalam mengembangkan website.

Bagi Sekolah:

1. Memanfaatkan laporan dokumentasi hasil pengujian untuk bahan evaluasi dan perbaikan.

2. Meningkatkan kesadaran akan bahaya kejahatan internet sehingga dapat mencegah kebocoran data.

Bagi Universitas

1. Menyediakan referensi akademik mengenai *cyber security* dengan topik pengujian keamanan website.
2. Memberikan wawasan bagi akademisi untuk mengembangkan metode pembelajaran terkait *ethical hacking* dan *penetration testing* di lingkungan pendidikan.

Bagi Peneliti:

1. Mendapatkan ilmu dan pemahaman pada bidang *cyber security* dari pengalaman menguji website .
2. Mendapatkan gelar sarjana dengan menyelesaikan tugas akhir.