BAB II
TINJAUAN PUSTAKA

Pada tahap ini peneliti akan menjabarkan penelitian terdahulu sebagai penunjang pengerjaan tugas akhir yang diperoleh dari skripsi dan jurnal yang berkaitan dengan penelitian

2.1 Penelitian Terdahulu

Beberapa penelitian yang menggunakan metode PTES dan NIST untuk melakukan penilaian keamanan website telah dilakukan dan diterapkan. Oleh karena itu, pada tahap ini peneliti akan menjabarkan penelitian terdahulu sebagai penunjang pengerjaan tugas akhir yang diperoleh dari skripsi dan jurnal yang berkaitan dengan penelitian. Literature Review dapat dilihat pada Tabel 1.

Table 1. Literature Review

No	Nama Peneliti	Judul	Kekurangan Penelitian	Hasil Penelitian
1	Muhammad Nur Fikri, Bita Parga Zen, Rifki Adhitama, Eryan Ahmad Firdaus, 2023	Analisis Keamanan Sistem Informasi Website SMA Negeri 1 Sokaraja Menggunakan Metode Penetration Testing Execution Standard (PTES)	PTES diterapkan sebagai metode standar dalam penelitian ini, namun, penelitian ini tidak mencakup metode lain yang dapat digunakan untuk membandingkan hasilnya. Selain itu, tidak terdapat pembahasan mendalam mengenai mitigasi risiko setelah eksploitasi berhasil dilakukan.	Melalui metode Penetration Testing Execution Standard (PTES), telah teridentifikasi kerentanan terkait SQL Injection pada database smansoka_webcms , yang terdiri dari 25 tabel. Kerentanan ini memungkinkan data untuk diakses oleh pihak-pihak yang tidak berwenang. Dalam proses pengujian

				keamanan, peneliti berhasil mendapatkan akses ke sistem dengan menerapkan teknik serangan SQL Injection, sehingga dapat mengakses data-data penting yang dimiliki oleh SMA Negeri 1 Sokaraja. Selain itu, selama sesi pemindaian, ditemukan 11 celah lain yang juga bisa dieksploitasi untuk mengakses data tanpa harus melalui tahap SQL Injection.
2	Setyo Utoro, Bayu Andi Nugroho, Meinawati, Septian Rheno Widianto, 2020	Analisis Keamanan WebsiteE-Learning SMKN1 Cibatu Menggunakan Metode PenetrationTesting Execution Standard	PTES digunakan sebagai metode utama dalam penelitian ini, meskipun tidak ada perbandingan yang dilakukan dengan metode lain, seperti NIST SP 800-115. Selain itu, tidak ada pengujian yang dilakukan untuk	Analisis Kerentanan aplikasi website SMKN 1 Cibatu Menggunakan metode PTES (Penetration Testing Execution Standard) dapat membantu menemukan tingkat kelemahan

			mengukur dampak serangan setelah eksploitasi terjadi.	sistem informasi. Melalui pemeriksaan ini, ancaman yang paling signifikan seperti Cross Site Scripting, Cross Site Request Forgery, dan Eavesdropping dapat teridentifikasi, yang berpotensi menyebabkan kebocoran data penting.
3	Syania Aulia Maherza, Bayu Hananto, Wayan Widi Pradnyana, 2023	Penetration Testing Terhadap Website Sekolah Menengah Atas ABC dengan Metode NIST SP 800-115	Metodologi yang diterapkan,yaitu NIST SP 800-115, cukup efektif. Namun, penelitian ini hanya berfokus pada pengujian satu situs dan tidak melakukan perbandingan dengan metode lain. Selain itu, tidak terdapat pembahasan mengenai mitigasi risiko setelah proses eksploitasi dilakukan.	Setelah melakukan penetration testing, telah teridentifikasi tiga kerentanan yang telah tervalidasi. Pertama, terdapat kerentanan Brute Force yang ditemui melalui proses intersepsi menggunakan alat Burp Suite pada situs SMA ABC, serta melalui penggunaan XML-RPC. Kerentanan kedua adalah

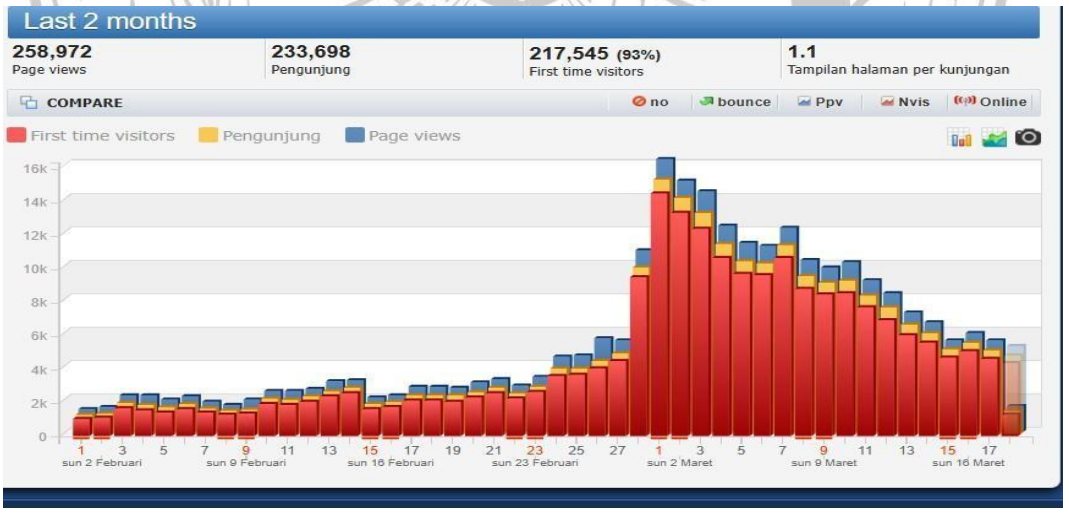
				Information Disclosure, sementara kerentanan ketiga adalah Wordpress User Enumeration yang terdeteksi menggunakan WPScan.
4	Finka Mambo, Dwi Yuniarto, David Setiadi, 2024	Evaluasi Keamanan Website dengan Menggunakan Metode NIST SP 800-115	Pengujian dilakukan hanya dengan menggunakan NIST SP 800-115 tanpa membandingkannya dengan metode lain. Hasil pengujian belum menunjukkan adanya kerentanan yang signifikan, sehingga penelitian ini merekomendasikan untuk melakukan pengujian ulang	Hasil penelitian ini hanya menunjukkan sejumlah kerentanan yang dikategorikan sebagai berikut : 6 kategori medium, 3 rendah, dan 2 informasi. Namin, belum ditemukan kerentanan dengan tingkat tinggi.

Berdasarkan evaluasi terhadap empat studi sebelumnya, dapat disimpulkan bahwa penelitian yang dilakukan oleh Fikri et al. (2023) adalah yang paling unggul karena mampu mengidentifikasi dan memanfaatkan kerentanan yang nyata seperti SQL Injection dengan pendekatan PTES yang sistematis, meskipun analisis mitigasi belum ada. Sebaliknya, studi oleh Mambo et al. (2024) dianggap sebagai yang paling kurang baik karena hanya

mengandalkan satu metode (NIST SP 800-115) tanpa melakukan perbandingan, dan tidak berhasil menemukan kerentanan yang signifikan, sehingga saran yang diberikan pun hanya berupa pengulangan dari pengujian sebelumnya.

2.2 Website Pemerintah Kota Tarakan

Website resmi Kota Tarakan, yang dikenal sebagai Portal Pemerintahan Kota Tarakan, menawarkan berbagai fitur utama, termasuk dashboard yang menampilkan berita terbaru, pengumuman resmi, dan informasi kebijakan pemerintah, serta layanan online untuk konsultasi publik, pembayaran pajak, dan pengajuan izin. Selain itu, ada menu profil pemerintah yang menampilkan struktur pemerintahan, visi, dan misi. Portal ini diharapkan membuat layanan publik lebih mudah diakses, lebih transparan, dan membuat warga lebih terlibat dalam pembangunan kota. karena itu, sistem web harus diuji untuk memastikan keamanannya. Berdasarkan data pada bulan januari 2025, website Portal Pemerintah Kota Tarakan ini dukunjungi oleh 258,972 pengguna aktif, menunjukkan pentingnya keamanan untuk melindungi data yang sensitive pada website tersebut. Dengan jumlah pengguna aktif mencapai 233. 698, risiko serangan siber mengalami peningkatan yang signifikan, mengingat lebih banyak data sensitif yang terkumpul. Untuk statistiknya dapat dilihat pada Gambar 1.



***Gambar 1**. Statistik pengguna website tarakankota.go.id pada januari 2025*

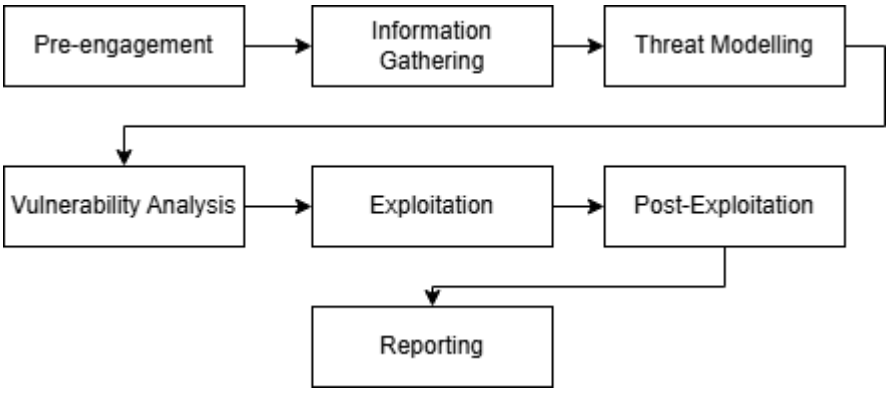
2.3 Keamanan Website

Keamanan sebuah website adalah salah satu prioritas utama bagi pengelola atau

pengguna situs. Seringkali, pengguna lebih fokus pada tampilan desain dan konten yang menarik untuk meningkatkan jumlah pengunjung. Namun, jika pengelola atau pengguna mengabaikan aspek keamanan, mereka akan menanggung risiko serius, karena orang lain dapat mencuri data penting dari situs tersebut dan bahkan merusak tampilan website. Oleh karena itu, perlindungan terhadap komputer, aplikasi, dan jaringan menjadi hal yang paling penting, yang bertujuan untuk mengamankan informasi yang terdapat di dalamnya [11]. Evaluasi keamanan dilakukan untuk mengidentifikasi celah-celah kerentanan pada website dan menyediakan solusi atas masalah yang ditemukan. Proses evaluasi ini bertujuan untuk mencegah risiko kehilangan data penting serta menghindari pengeluaran anggaran tambahan yang mungkin timbul akibat malfungsi atau kerusakan pada website [12]. Beberapa contoh serangan yang pernah terjadi pada website Portal Pemerintah Kota Tarkan antara lain, *Cross- Site Scripting* (XSS), Serangan DDos (*Distributed Deniel of Service*), *Defacement*, dan *SQL Injection*. Setelah memahami risiko keamanan situs web, langkah selanjutnya adalah menerapkan pendekatan sistematis, seperti PTES, untuk mengidentifikasi dan mengatasi kerentanan yang ada.

2.4 PTES (Penetration Testing Execution Standard)

Framework Penetration Testing Execution Standards (PTES) adalah salah satu kerangka kerja untuk pengujian penetrasi yang dikembangkan pada tahun 2010. PTES menyediakan petunjuk pengujian yang sistematis dan mendalam, sehingga dapat memberikan arahan yang terang bagi penggunanya dalam mengevaluasi mutu setiap pengujian yang dilakukan. [13]. PTES berisi sebuah kerangka kerja yang mencakup metode uji penetrasi dengan tujuh tahap utama. Tahap- tahap tersebut meliputi: pra interaksi (*pre-engagement interactions*), pengumpulan informasi *(intelligence gathering*), pemodelan ancaman (*threat modelling*), analisis kerawanan (*vulnerability analysis/VA*), eksploitasi (*exploitation*), pasca eksploitasi (*Post Exploitation)*, dan pelaporan (*reporting*). Berikut adalah penjelasan mengenai setiap langkah dalam uji penetrasi yang sesuai dengan pedoman PTES [14]. Tahapan PTES dapat dilihat pada Gambar 2.



***Gambar 2**. PTES Methodology*

2.4.1 Pre-engagement Insteractions

Tahap ini adalah langkah awal yang harus dilakukan sebelum melaksanakan pengujian penetrasi. Dalam fase ini, perusahaan atau organisasi yang akan menjalani pengujian perlu memberikan persetujuan tertulis sekaligus pemahaman mengenai tujuan dan ruang lingkup dari pengujian tersebut [15]. Tahap ini bertujuan untuk menghindari munculnya permasalahan hukum dan kebijakan yang mungkin muncul akibat tindakan penetrasi yang dilakukan oleh penguji. Pada fase ini, terdapat kerja sama antara pentester atau penguji penetrasi dan klien atau pemilik layanan. Aktivitas yang dilakukan dalam tahap ini meliputi Penentuan lingkup, Penetapan tujuan pengujian penetrasi, Analisis kesiapan organisasi, Penyusunan ROE (Roles Of Engagement), dan Rapat untuk memperdalam lingkup. [14].

2.4.2 Intelligence Gathering

Pada tahap ini, dilakukan pengumpulan informasi yang diperlukan untuk menghasilkan representasi yang jelas dan mudah dipahami. Semua data yang diperoleh selama tahap ini akan memberikan kontribusi penting dalam mengarahkan evaluasi terhadap potensi kerentanan[16].

2.4.3 Threat Modelling

Tahapan ini bertujuan untuk mengidentifikasi pendekatan pemodelan ancaman yang diperlukan dalam pelaksanaan pentesting. Fokus dari standar ini didasarkan pada proses bisnis serta aset-aset yang dimiliki oleh perusahaan. Fase pemodelan ancaman menjadi sangat krusial bagi penguji maupun perusahaan, karena melalui pemodelan ini, kejelasan mengenai risiko dan prioritas target dapat diperoleh [17].

2.4.4 Vulnerabilty Analysis

Analisis Kerentanan, atau yang lebih dikenal dengan *Vulnerabilty Analysis*, berfungsi untuk mendeteksi dan menilai risiko keamanan yang ditimbulkan oleh berbagai komponen yang mengandung kerentanan. Proses analisis ini terbagi menjadi dua tahap: pengenalan dan verifikasi. Tahap pengenalan berfokus pada usaha menemukan kerentanan, sementara tujuan dari verifikasi adalah untuk menyaring jumlah kerentanan yang ditemukan menjadi hanya yang benar-benar valid. [18].

2.4.5 Exploitation

Fase eksploitasi dalam pengujian penetrasi berfokus pada pembuatan akses ke sistem atau sumber daya dengan cara melewati lapisan-lapisan keamanan yang ada. Jika fase sebelumnya, yaitu fase analisis kerentanan, tidak dilaksanakan dengan baik, maka pada fase ini diperlukan tindakan yang terencana dan sangat tepat. Tujuan utama dari fase ini adalah untuk menemukan pintu masuk utama ke dalam organisasi serta mengidentifikasi aset-aset penting yang dimiliki [18].

2.4.6 Post-Expoitation

Post Exploitation mengutamakan penilaian terhadap nilai sistem yang telah dieksploitasi dengan tetap menjaga kendali atas sistem tersebut. Penilaian terhadap nilai sistem dilakukan dengan mempertimbangkan tingkat sensitivitas data yang terdapat di dalamnya serta fungsi sistem dalam jaringan yang menjadi target. Sasaran utamanya adalah untuk mempertahankan akses yang sudah diperoleh dan menggunakan kendali tersebut untuk keperluan lebih lanjut, seperti mengumpulkan

informasi atau merencanakan serangan yang lebih jauh [19].

2.4.7 Reporting

Pada tahap ini, penulis melakukan dokumentasi hasil pengujian keamanan dan eksploitasi, yang nantinya akan digunakan untuk menyusun laporan. Laporan ini disusun dengan cara yang mudah dipahami oleh manajemen. Isi laporan mencakup penjelasan tentang pengertian pengujian penetrasi (pentest), metode yang digunakan, skala risiko keamanan, penjelasan mengenai kerentanan yang berhasil ditemukan, dampak dari kerentanan tersebut, serta *Proof of Concept (POC*) atau langkah- langkah untuk mengidentifikasi kerentanan tersebut.

Skala risiko keamanan terdiri dari beberapa kategori:

a. Tinggi: Komponen dengan indikator tinggi harus segera diperbaiki karena sangat rentan terhadap serangan dan bisa mengganggu performa aplikasi.

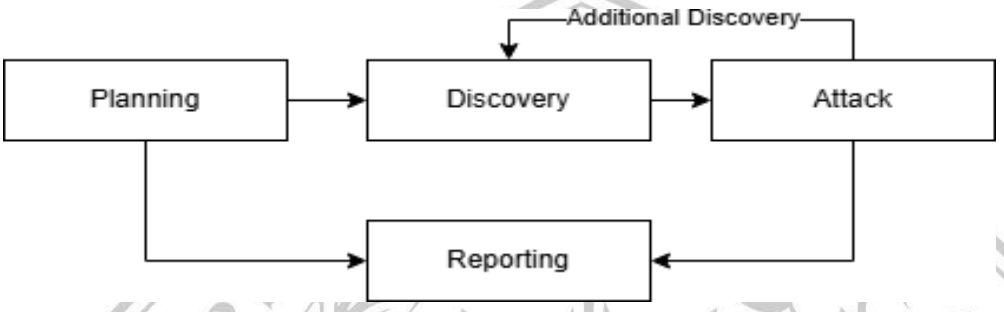
b. Sedang: Komponen dengan indikator sedang menunjukkan adanya masalah pada internal web, seperti kerusakan pada sektor data.

c. Rendah: Komponen dengan indikator rendah menandakan bahwa tindakan yang perlu diambil adalah memperbarui penyimpanan dan melakukan perbaikan di sektor-sektor tertentu [20].

2.5 NIST Special Publication (SP) 800-115

Institut Nasional Standar dan Teknologi, yang lebih dikenal dengan sebutan NIST, adalah sebuah lembaga yang berkonsentrasi pada keamanan informasi yang dikembangkan oleh pemerintah Amerika Serikat. Misi lembaga ini adalah untuk merancang dan mendorong pengukuran, standar, dan teknologi. Dalam kajian ini, peneliti menggunakan NIST SP 800-115 sebagai panduan metodologis. NIST SP 800-115 adalah dokumen yang merinci metode dan teknik yang diterapkan dalam pengujian kerentanan situs melalui penetration testing, serta memberikan saran untuk mengatasi kerentanan yang teridentifikasi [21]. Framework ini menyajikan informasi yang efektif dan mudah dipahami mengenai strukturnya, yang terdiri dari tiga komponen utama: Core, Tiers, dan Profil. Core dalam Framework NIST

memberikan rekomendasi praktik terbaik terkait *cybersecurity*, yang mencakup aspek teknis, hasil, operasional, dan manajemen kontrol. Sementara itu, Tiers berperan sebagai alat penilaian terhadap manajemen *cybersecurity* yang telah diterapkan di dalam organisasi. Adapun Profil digunakan untuk mengevaluasi kondisi *cybersecurity saat ini serta menetapkan target cybersecurity yang ingin dicapai oleh organisasi [22]. Institut Standar dan Teknologi Nasional (NIST) melalui dokumen NIST SP 800-115 memiliki tahapan yang meliputi planning, Discovery, attack, dan reporting [23]. Tahapan NIST dapat dilihat pada Gambar 3.*



***Gambar 3**. Tahapan Nist*

2.5.1 Planning

Pada fase perencanaan, aturan dan hasil yang ingin dicapai akan dibicarakan dan disetujui oleh kedua belah pihak, yaitu peneliti dan sasaran. Beberapa contoh aturan yang akan diperhatikan terdiri dari tujuan dari pelaksanaan pengujian penetrasi, area yang akan diuji, waktu pelaksanaan pengujian, serta hasil yang diharapkan. Penting untuk dicatat bahwa tidak ada pengujian yang dilakukan pada tahap ini [21].

2.5.2 Discovery

Tahapan ini terbagi menjadi dua jenis. Pertama, ada informasi gathering, yaitu pengumpulan informasi terkait website yang akan diuji. Informasi ini meliputi alamat IP, teknologi yang digunakan, dan sistem yang ada, yang dapat diperoleh melalui proses pemindaian. Kedua, terdapat *vulnerability scanning*, yakni tahap di mana dilakukan pemindaian untuk mengidentifikasi kerentanan pada website. Hasil dari tahap ini dapat digunakan sebagai dasar untuk analisis lebih lanjut [24].

Dalam konteks penelitian ini, sangat penting untuk membandingkan

pendekatan yang digunakan oleh NIST SP 800-115 dengan PTES (*Penetration Testing execuittion Standard*). Tujuan utama PTES adalah memberikan panduan dan prosedur yang sistematis serta terstruktur dalam pelaksanaan uji penetrasi, sehingga hasil yang diperoleh dapat diandalkan dan memberikan manfaat bagi para pelanggan [25]. Hasil dari penelitian ini akan merekomendasikan perbaikan untuk meningkatkan keamanan website dengan mengimplementasikan metode NIST SP 800-115 [24].

2.5.3 Attack

Tahap Attack adalah bagian penting dari metode NIST SP 800-115, yang digunakan untuk melakukan penetrasi terhadap situs web yang sedang diuji. Tujuannya adalah untuk menentukan apakah kerentanan yang teridentifikasi pada tahap *Discovery* dapat dieksploitasi, serta untuk mengetahui apakah penguji dapat memperoleh hak akses ke situs web tersebut melalui hasil uji penetrasi yang dilakukan [9].

2.5.4 Reporting

Pada tahap ini, kami akan menjelaskan secara rinci hasil laporan uji penetrasi yang telah dilakukan. Laporan ini dapat dijadikan sebagai panduan untuk perbaikan website di masa mendatang [26].