BAB II
LANDASAN TEORI

2.1 Website Desa

Website Desa adalah platform sistem informasi yang dirancang untuk mendukung pengelolaan data dan administrasi di tingkat desa dan kelurahan, memfasilitasi akses publik terhadap informasi penting dan memperkuat transparansi dalam pelayanan desa. Salah satu program yang terintegrasi dalam Website Desa adalah Program Statistik Desa, sebuah inisiatif pemerintah yang bertujuan meningkatkan kemampuan aparatur desa dalam mengelola dan memanfaatkan data statistik sektoral secara optimal. Melalui Website Desa ini, desa dapat mempromosikan potensi lokal seperti pariwisata dan produk unggulan, serta menyebarluaskan informasi program-program pemerintah, yang pada akhirnya mendorong pelayanan publik yang lebih efektif, pemberdayaan masyarakat, dan peningkatan ekonomi desa (Ansar et al., 2023).

2.2 Keamanan Sistem Informasi

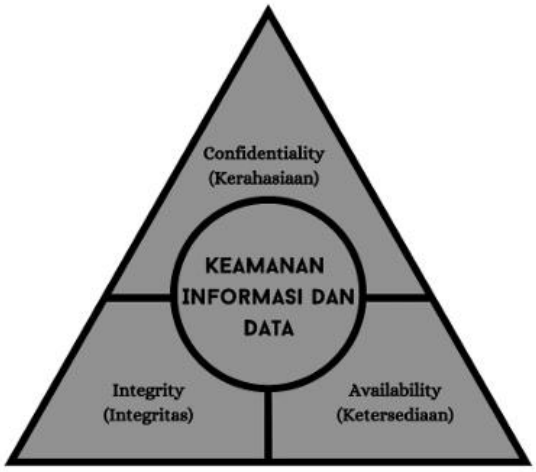
2.2.1 Pentingnya Keamanan Sistem Informasi

Keamanan untuk masuk ke dalam sebuah sistem memiliki peran yang sangat penting karena berfungsi sebagai pintu utama untuk mengakses sumber data. Akses yang tidak aman berpotensi membuka celah bagi pihak tidak sah untuk mendapatkan akses, mengakibatkan risiko kebocoran dan penyalahgunaan data. Sayangnya, aspek keamanan ini sering kali kurang mendapat perhatian dari pemilik dan pengelola sistem informasi. Oleh karena itu, perlu adanya upaya untuk memperkuat mekanisme autentikasi sebagai lapisan perlindungan. Salah satu metode yang sering digunakan adalah *One-Time Password* (OTP), yang membuat kata sandi menjadi dinamis dengan terus berubah-ubah pada waktu tertentu (Permana et al., 2020). Sifat dinamis OTP membantu mempersulit pencurian sandi, sehingga dapat meningkatkan keamanan akses sistem.

Penelitian ini akan membahas metode keamanan yang lebih mendalam untuk memastikan sistem informasi terlindungi dari upaya akses tidak sah, terutama dalam mengamankan data sensitif.

2.2.2 Konsep Keamanan dalam Sistem Informasi: CIA Triad

Ancaman keamanan siber seperti kebocoran data, serangan berbasis web, dan phishing semakin sering terjadi, menuntut penerapan keamanan sistem informasi yang lebih baik. Untuk menghadapi risiko ini, keamanan sistem informasi mengikuti model Cybersecurity yang berfokus pada tiga aspek utama, yaitu CIA Triad: *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan). CIA Triad merupakan landasan penting dalam pengembangan kebijakan keamanan untuk memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang, tetap akurat dan konsisten, serta selalu tersedia saat diperlukan. Penerapan model ini telah terbukti efektif dalam menjaga keamanan sistem informasi dan melindungi data dari ancaman siber yang semakin kompleks (Harahap et al., 2023)



Gambar 2.2.1 CIA Triad Keamanan Informasi dan Data.

(Sumber : (Harahap et al., 2023)**)**

2.3 Autentikasi dalam Sistem Informasi

2.3.1 Email Authentication Multi-Factor Authentication (MFA)

Sebuah langkah pengamanan tambahan, membantu melindungi akun apa pun. Untuk mengaktifkan *multi-factor authentication*, diperlukan perangkat berbeda, seperti ponsel pribadi dan email, untuk mengidentifikasi dan memverifikasi identitas kita. Akibatnya, kemungkinan akun pribadi dikompromikan menjadi lebih kecil, dan data akan selalu tetap terlindungi. Metode ini juga menyediakan lapisan perlindungan tambahan untuk alamat email dan kata sandi. Jika *two-factor authentication* diaktifkan, bahkan jika seseorang mengetahui kata sandi pengguna, mereka tidak dapat mengakses suatu akun tanpa izin penggunanya.

Oleh karena itu, ketika karyawan mendaftar untuk akun menggunakan email mereka, desain antarmuka akan terhubung dengan email tersebut. Sebuah *One-Time Password* (OTP) yang hanya dapat digunakan untuk periode singkat akan dikirimkan ke email untuk mempertahankan tingkat keamanan. *Simple Mail Transfer Protocol* (SMTP) Server akan digunakan untuk mengirimkan *One-Time Password* (OTP) melalui email karyawan dengan menggunakan PHP Mailer (Nur et al., 2024).

2.3.2 Teknologi Pengenalan Wajah dalam Autentikasi

Penggunaan teknologi pengenalan wajah telah menawarkan kemajuan signifikan dalam sistem autentikasi modern, khususnya dalam aplikasi yang memerlukan tingkat keamanan tinggi. Penggabungan pengenalan wajah dengan metode lain, seperti *One-Time Password* (OTP), meningkatkan keamanan dan akurasi autentikasi pengguna. Pengenalan wajah sulit dipalsukan karena karakteristik unik individu, sehingga memungkinkan tingkat keamanan yang lebih tinggi dibandingkan metode berbasis kata sandi. Dengan adanya integrasi teknologi ini, proses autentikasi menjadi lebih efisien dan aman dari risiko

pemalsuan atau duplikasi data, yang pada akhirnya dapat melindungi informasi pribadi yang sensitif (Syahputri et al., 2024).

2.3.3 Time-Based One-Time Password (TOTP)

Time-Based One-Time Passwords (TOTP) mengatasi beberapa kelemahan dari kata sandi konvensional (static passwords). Masalah terbesar yang diselesaikan oleh TOTP adalah menghilangkan kerentanan terhadap serangan replay. Sistem menjadi lebih aman dengan autentikasi berbasis one-time password dibandingkan autentikasi berbasis kata sandi yang dapat digunakan ulang. Sebagai contoh, untuk mendapatkan akses jarak jauh, pengguna biasanya perlu mengirimkan kata sandi atau frasa sandi. Data ini sering kali dikirim melalui jaringan yang tidak aman tanpa enkripsi. Karena nilai kata sandi berkurang setelah digunakan, TOTP mengurangi kemungkinan penyadapan. Ketika diimplementasikan secara efektif, teknik one-time password sulit untuk ditebak oleh sebagian besar penyerang dan memerlukan upaya aktif untuk dieksploitasi (Nur et al., 2024).

2.4 Keamanan Akun

2.4.1 Login Attempt Throttling

Login Attempt Throttling adalah mekanisme yang dirancang untuk mengurangi risiko serangan tebak kata sandi secara online yang semakin meluas dan menjadi ancaman privasi serta keamanan yang persisten bagi pengguna. Salah satu metode umum untuk mengurangi risiko peretasan online adalah dengan mengunci akun pengguna setelah sejumlah (K) percobaan login yang salah secara berturut-turut.

Pemilihan nilai K ini menciptakan trade-off klasik antara keamanan dan kegunaan. Jika K terlalu besar, seorang peretas dapat dengan cepat membobol sejumlah besar akun pengguna. Sebaliknya, jika K terlalu kecil, pengguna yang

jujur akan merasa terganggu karena terkunci setelah beberapa kesalahan login (Blocki & Zhang, 2022).

2.4.2 Password Recovery

Proses pemulihan password merupakan bagian penting dari fungsionalitas sebuah website. Banyak situs web yang menyediakan layanan online bagi pengguna mereka juga perlu menyelesaikan masalah yang berkaitan dengan pengaturan ulang password (misalnya, jika pengguna lupa password mereka). Salah satu teknik yang populer dan telah terbukti untuk memungkinkan pengguna memulihkan akun yang hilang adalah dengan mengizinkan mereka mengirimkan tautan reset ke akun email mereka sendiri (Innocenti Tommasoand Mirheidari, 2021).

2.4.3 Logging

Logging merupakan proses pencatatan yang penting dalam pengujian keamanan website, terutama untuk mengukur adopsi langkah-langkah keamanan web. Dalam konteks pengujian keamanan, pencatatan percobaan login pengguna menjadi krusial karena keragaman yang ada pada alur proses login di berbagai situs web. Setiap situs mungkin memiliki variasi halus dalam cara mereka menangani login, yang dapat memengaruhi efektivitas pengujian.

Upaya saat ini untuk menyelidiki keamanan login sering kali bersifat semi-otomatis, memerlukan intervensi manual yang tidak efisien dan sulit untuk diskalakan. Hal ini mengakibatkan studi komprehensif tentang area pasca-login menjadi tidak mungkin dilakukan. Untuk mengatasi tantangan ini, diperkenalkan sebuah kerangka kerja bernama Shepherd, yang dirancang untuk melakukan pencatatan otomatis pada proses login di situs web (Jonker et al., 2020).

2.4.4 Non Repudiation

Non-repudiation adalah mekanisme yang memberikan perlindungan terhadap penolakan oleh salah satu pihak yang terlibat dalam komunikasi, karena mereka

telah berpartisipasi dalam seluruh atau sebagian dari komunikasi tersebut (Rahmalia Syahputri, 2022). *Non-repudiation* berfungsi memastikan bahwa pengguna tidak dapat menyangkal atau membantah bahwa mereka telah melakukan akses ke dalam sistem atau jaringan tersebut. Hal ini dicapai dengan cara mencatat dan menyimpan informasi yang dapat digunakan untuk membuktikan identitas pengguna dan aktivitas mereka selama mengakses sistem. Pencatatan ini meliputi waktu akses, jenis tindakan yang dilakukan, serta identitas yang terautentikasi (Galang Saputra & Parga Zen, 2023).

2.5 Serangan terhadap sistem informasi

2.5.1 Insider Attack

Insider Attack adalah ancaman signifikan dalam sistem informasi, dilakukan oleh individu dalam organisasi seperti karyawan atau mantan karyawan yang memiliki akses langsung ke sistem. Meskipun berbagai kata sandi atau variasi pola sering digunakan untuk meningkatkan keamanan, sistem tetap rentan terhadap serangan dari pihak yang tidak sah, seperti penyerang yang mengeksploitasi kelemahan keamanan.

Serangan ini bisa aktif, di mana penyerang mengganggu fungsi sistem, atau pasif, di mana penyerang memantau data tanpa gangguan langsung. *Insider attack* dianggap paling berbahaya karena membutuhkan upaya lebih sedikit untuk mengakses sistem. Oleh karena itu, tindakan preventif seperti pengelolaan hak akses dan pembaruan kata sandi sangat penting untuk mengurangi risiko serangan ini (Shamshad et al., 2021).

2.5.2 Dictionary Attack

Dictionary Attack adalah metode untuk membobol komputer atau server yang dilindungi kata sandi dengan cara sistematis memasukkan setiap kata dari kamus sebagai kata sandi. Metode ini juga dapat digunakan untuk mencari kunci yang diperlukan dalam mendekripsi pesan atau dokumen yang telah dienkripsi (Fa'atulo Halawa et al., 2020).

Ciri Password yang lemah terhadap serangan *Dictionary Attack*:

a. Kata sandi dengan menggunakan abjad kecil
b. Kata sandi dengan menggunakan abjad besar
c. Kata sandi dengan menggunakan angka
d. Kombinasi kata sandi abjad besar dan abjad kecil

Contoh Password yang lemah terhadap serangan *Dictionary Attack*:

1. admindesa123
2. 123Aparat
3. Admin123
4. Desapekanbaru
5. BALAIDESA

2.5.3 Brute Force Attack

Brute Force Attack adalah jenis serangan yang mencoba berbagai kombinasi kata sandi dengan menggunakan karakter, huruf, dan angka (Rahmalia Syahputri, 2022).

Contoh serangan Brute Force Attack (Abjad besar, kecil, angka dan karakter):

1. Admin07&D3sa
2. 4dM1n_D354_P3k4n_B4Ru
3. B4l41*DE54

2.5.4 Hybrid Attack

Serangan hibrida umumnya menggabungkan dua atau lebih metode atau alat untuk melancarkan serangan, seperti mengkombinasikan serangan dictionary dan brute force (Rahmalia Syahputri, 2022).

2.6 MockUp

MockUp adalah representasi visual dari antarmuka pengguna yang dirancang untuk memberikan gambaran awal tentang bagaimana sistem atau website akan berfungsi. Dalam konteks pengembangan website profil perusahaan, MockUp berfungsi sebagai alat penting untuk merancang dan menguji konsep sebelum implementasi akhir dilakukan. Dengan kemajuan teknologi digital, keberadaan online suatu instansi atau perusahaan menjadi semakin penting, terutama melalui website profil perusahaan.

Salah satu alasan utama pembuatan MockUp adalah untuk melakukan pengujian keamanan, khususnya dalam menghadapi serangan brute force. Dengan menggunakan MockUp, pengujian dapat dilakukan tanpa risiko merusak website asli. Hal ini memungkinkan pengembang untuk mengidentifikasi dan memperbaiki kerentanan dalam sistem keamanan sebelum implementasi dilakukan. Selain itu, MockUp membantu dalam memvisualisasikan pengembangan sistem keamanan website, sehingga tim pengembang dapat lebih mudah memahami dan merencanakan langkah-langkah yang diperlukan untuk meningkatkan keamanan. Dengan cara ini, MockUp tidak hanya berfungsi sebagai alat desain, tetapi juga sebagai sarana untuk memastikan bahwa aspek keamanan telah dipertimbangkan secara menyeluruh dalam proses pengembangan (Paulina Suri & Yudi Arifin, 2024).

2.7 Alat dan Teknologi Pengembangan Sistem Keamanan WEBSITE DESA

2.7.1 WGET

WGET adalah alat yang umum digunakan untuk mengunduh halaman web dan merupakan mekanisme yang berguna dalam banyak proyek pengukuran. Meskipun tugas dasar ini tampak sederhana dan tidak memerlukan banyak pertimbangan, banyak penelitian sebelumnya cenderung menggunakan alat yang relatif dasar (seperti Selenium atau Puppeteer) dan mengasumsikan bahwa mengunduh sebuah halaman sekali akan menghasilkan semua kontennya. Pendekatan ini mungkin berhasil untuk konten statis, tetapi tidak efektif untuk halaman web dinamis yang memiliki konten pihak ketiga (Indela & Levin, 2021).

2.7.2 VS Code

Visual Studio Code adalah editor kode yang gratis dan sumber terbuka yang dikembangkan secara aktif oleh Microsoft. Sebagai alat pengembangan yang populer, VS Code menawarkan berbagai fitur yang mendukung pengembangan perangkat lunak, termasuk penyorotan sintaks, penyelesaian kode, dan integrasi dengan sistem kontrol versi (Plainer, 2021).

2.7.3 PHP

PHP adalah bahasa pemrograman yang dirancang untuk pengembangan web di sisi server. Selain itu, PHP juga dapat digunakan sebagai bahasa pemrograman umum. Bahasa ini pertama kali diciptakan oleh Rasmus Lerdorf pada tahun 1994. Saat ini, PHP merupakan singkatan dari PHP: Hypertext Preprocessor, yang merupakan contoh dari akronim rekursif, di mana kepanjangannya mencakup singkatan itu sendiri. PHP bersifat gratis dan open source, dirilis di bawah lisensi PHP License, yang sedikit berbeda dari lisensi GNU General Public License (GPL) yang sering digunakan dalam proyek open source (Noviana, 2022).

2.7.4 XAMPP

XAMPP adalah akronim dari (X-platform, Apache, MySQL, PHP, Perl), yang merupakan perangkat lunak server web open source yang mendukung berbagai sistem operasi, termasuk Windows, Linux, dan Mac OS. XAMPP berfungsi sebagai server mandiri (standalone) atau localhost, mempermudah proses pengeditan, desain, dan pengembangan aplikasi. Alat ini penting untuk mengembangkan perangkat lunak atau tampilan website dengan cara yang lebih mudah dan cepat. Terdapat tiga komponen utama dalam XAMPP, yaitu htdocs, Control Panel, dan PhpMyAdmin, yang dapat digunakan sebagai alat bantu untuk belajar pengembangan perangkat lunak sesuai kebutuhan atau proyek bisnis (Noviana, 2022).

2.7.5 MySQL

MySQL adalah sistem manajemen basis data (DBMS) open source yang mendukung banyak pengguna dan multi-threaded, serta terkenal dan gratis. Berdasarkan definisi tersebut, SQL adalah bahasa yang digunakan untuk berinteraksi dengan basis data, di mana subbahasa ini memungkinkan pengguna untuk membuat dan memanipulasi data di dalam basis data. SQL digunakan untuk melakukan berbagai tugas, termasuk memperbarui basis data, yang merujuk pada konsep Relational Database Management System (RDBMS) (Noviana, 2022).

2.7.6 PHP Mailer

PHPMailer adalah teknologi yang memungkinkan pengiriman informasi kepada pengguna yang terhubung dengan web secara otomatis tanpa memerlukan pengirim langsung. Dengan menggunakan fungsi mail dari PHP, PHPMailer dapat mengirimkan email secara cepat dan efisien, sehingga mengurangi waktu untuk pengiriman email manual. Teknologi ini juga mempermudah proses pengiriman email melalui integrasi dengan koneksi internet. Namun, kecepatan internet yang lambat dapat memengaruhi waktu pengiriman email kepada

pengguna. Penggunaan PHPMailer memastikan kemudahan dan efisiensi dalam komunikasi berbasis email (Pahrizal et al., 2022).

2.7.7 Twilio

Twilio adalah platform komunikasi berbasis cloud yang terkenal secara global, dirancang untuk memfasilitasi interaksi pengguna melalui berbagai saluran komunikasi. Dengan Twilio, pengembang dapat mengintegrasikan kemampuan komunikasi seperti SMS, panggilan suara, video, WhatsApp, dan email ke dalam aplikasi mereka dengan mudah (Twilio Team, 2025).

2.8 Perlindungan Data Pribadi

Perlindungan Data Pribadi (PDP) di Indonesia, sebagaimana diatur dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, mencakup prinsip-prinsip dasar untuk melindungi data pribadi individu dalam berbagai sektor, baik publik maupun privat. Undang-undang ini memberikan hak kepada pemilik data untuk mengakses, mengubah, menghapus, serta memperoleh informasi terkait penggunaan data mereka, sekaligus menetapkan kewajiban bagi pengendali data untuk menjaga keamanan dan privasi data pribadi yang dikelola. Dalam pasal-pasalnya, UU ini menekankan pentingnya transparansi, keadilan, serta penggunaan data untuk tujuan spesifik guna mencegah kebocoran dan penyalahgunaan data. Sanksi administratif dan pidana pun diterapkan pada pelanggaran yang terjadi, memberikan jaminan hukum terhadap privasi warga negara dalam ekosistem digital yang semakin kompleks (Kementerian Komunikasi dan Informatika Republik Indonesia, 2022).

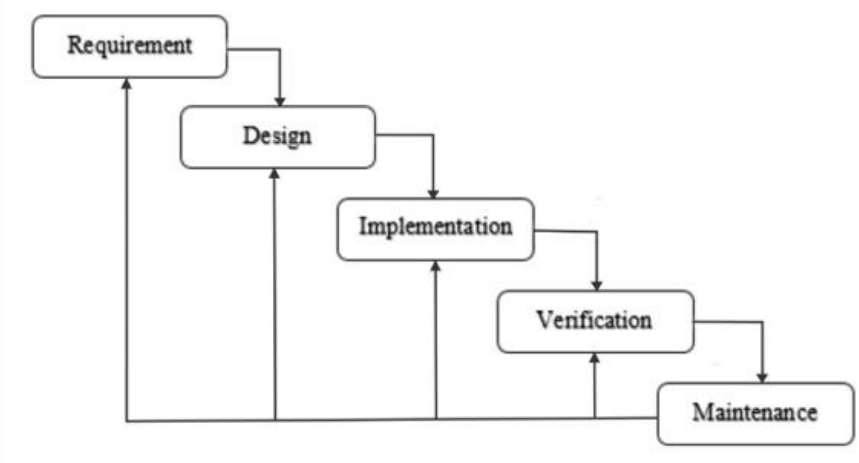
2.9 Metodologi Penelitian

Penelitian ini menggunakan waterfall untuk pengembangan perangkat lunak dan Penetration Testing Execution Standard (PTES) untuk pengujian sistem keamanan. Tiap tahap pada PTES akan diintegrasikan kedalam metode *waterfall*

2.9.1 Waterfall

Metode waterfall, yang juga dikenal sebagai siklus hidup klasik (classic life cycle), sebenarnya memiliki nama asli “Linear Sequential Model.” Model ini menggambarkan pendekatan sistematis dan berurutan dalam pengembangan perangkat lunak, dimulai dari perumusan kebutuhan pengguna, kemudian berlanjut ke tahap perencanaan, perancangan, pembangunan, implementasi, hingga penyebaran sistem kepada pengguna. Setelah sistem digunakan, dilakukan pemeliharaan terhadap perangkat lunak yang telah dikembangkan (Pressman, 2019).

Konsep waterfall pertama kali diperkenalkan oleh Winston Royce pada tahun 1970, sehingga sering dianggap sebagai metode lama. Namun, hingga saat ini, model ini masih banyak digunakan dalam bidang rekayasa perangkat lunak. Model waterfall mengikuti pendekatan yang terstruktur dan berurutan, di mana setiap tahap harus diselesaikan sebelum melanjutkan ke tahap berikutnya. Dinamakan "waterfall" karena alur pengembangannya menyerupai air terjun, di mana setiap tahapan berjalan secara linear dari awal hingga akhir tanpa memungkinkan kembali ke tahap sebelumnya. Tahapan metode waterfall dapat dilihat pada gambar 2.9.1 berikut.



Gambar 2.9.1 Metode *Waterfall*

1. ***Requirement***

   Pada tahap ini, pengembang berinteraksi dengan pengguna untuk memahami kebutuhan dan batasan sistem yang akan dibangun. Informasi dikumpulkan melalui wawancara, diskusi, atau survei, kemudian dianalisis untuk merancang sistem sesuai dengan kebutuhan pengguna.

2. ***Design***

   Tahap ini berfokus pada pembuatan desain sistem yang mencakup pemilihan perangkat keras, spesifikasi sistem, serta arsitektur perangkat lunak secara keseluruhan. Tujuannya adalah memberikan gambaran teknis mengenai bagaimana sistem akan dikembangkan.

3. ***Implementation***

   Setelah desain selesai, sistem mulai dikembangkan dalam bentuk unit-unit kecil yang nantinya akan diintegrasikan. Setiap unit diuji secara individual dalam proses yang disebut unit testing guna memastikan bahwa setiap bagian berfungsi dengan baik sebelum diintegrasikan ke dalam sistem utama.

4. ***Verification***

   Pada tahap ini, dilakukan pengujian menyeluruh untuk memastikan bahwa sistem memenuhi spesifikasi yang telah ditentukan. Pengujian dapat

dilakukan dalam beberapa kategori, seperti unit testing (pengujian modul tertentu), sistem testing (mengamati interaksi antar modul dalam sistem), serta acceptance testing (pengujian oleh pengguna untuk memastikan bahwa sistem telah sesuai dengan kebutuhan mereka).

5. ***Maintenance***

   Tahap terakhir dalam metode waterfall adalah pemeliharaan perangkat lunak setelah diterapkan. Proses ini mencakup perbaikan kesalahan yang mungkin tidak terdeteksi sebelumnya, peningkatan performa, serta penyesuaian dengan kebutuhan baru pengguna.

2.9.2 Penetration Testing

Penetration Testing atau pengujian penetrasi adalah proses eksploitasi sistem secara terotorisasi untuk mengidentifikasi kemungkinan eksploitasi dalam sistem. Dalam proses ini, penguji memiliki otorisasi untuk melakukan pengujian dan dengan sengaja mencoba mengeksploitasi sistem guna menemukan kelemahan-kelemahan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Tujuan dari penetration testing adalah untuk mensimulasikan serangan yang mungkin terjadi pada sistem dalam kondisi nyata. Dengan demikian, langkah ini membantu mengungkap celah keamanan yang sebelumnya tidak teridentifikasi serta memberikan rekomendasi untuk memperbaiki kelemahan tersebut, sehingga sistem dapat menjadi lebih tangguh terhadap serangan (Vegesna & Varma Vegesna, 2022).

Penetration Testing Execution Standard (PTES) adalah kerangka kerja yang dirancang untuk memberikan panduan dalam pelaksanaan pengujian penetrasi terhadap sistem informasi. PTES menawarkan pendekatan terstruktur untuk mengidentifikasi, mengeksploitasi, dan melaporkan kerentanan keamanan, serta memberikan rekomendasi mitigasi. Tujuannya adalah untuk memastikan

keamanan sistem informasi dari berbagai ancaman siber yang berpotensi membahayakan data dan operasi organisasi.

Gambar 2.9.2 menjelaskan tahapan-tahapan PTES (Penetration Testing Execution Standard). PTES mencakup tujuh tahapan utama yang memberikan panduan menyeluruh dari awal hingga akhir pengujian (The PTES Team, 2024).

1. **Pre-Engagement Interactions**

   Tahap ini melibatkan diskusi awal antara penguji dan pihak terkait (pemilik atau pengelola sistem). Lingkup kerja, tujuan, dan batasan pengujian ditentukan di sini. Kesepakatan formal, seperti kontrak atau dokumen izin, dibuat untuk memastikan pengujian dilakukan sesuai dengan aturan yang berlaku dan tidak melanggar hukum.

2. **Intelligence Gathering**

   Pada tahap ini, penguji mengumpulkan informasi tentang sistem atau infrastruktur yang akan diuji. Informasi ini meliputi konfigurasi sistem, data publik yang tersedia, atau potensi titik lemah yang dapat dieksploitasi. Proses ini mencakup teknik open-source intelligence (OSINT) untuk mendapatkan pemahaman mendalam tentang target.

3. **Threat Modeling**

   Penguji menganalisis informasi yang telah dikumpulkan untuk mengidentifikasi potensi ancaman dan kelemahan yang relevan. Tahap ini bertujuan untuk memodelkan ancaman dengan mempertimbangkan dampaknya terhadap data, sistem, atau pengguna. Hasil threat modeling membantu penguji menentukan prioritas pengujian.

4. **Vulnerability Analysis**

   Pada tahap ini, penguji mengidentifikasi kerentanan spesifik dalam sistem berdasarkan data yang diperoleh. Proses ini bisa melibatkan penggunaan alat otomatis, seperti pemindai kerentanan dan/atau pemeriksaan manual untuk memastikan hasil yang akurat. Kerentanan yang ditemukan dicatat untuk diuji lebih lanjut pada tahap berikutnya.

5. **Exploitation**

   Tahap ini bertujuan untuk mengeksploitasi kerentanan yang ditemukan dalam tahap sebelumnya. Penguji mencoba mendapatkan akses ke sistem dengan memanfaatkan kelemahan yang ada untuk memahami dampaknya. Eksploitasi dilakukan dengan hati-hati untuk meminimalkan risiko kerusakan pada sistem.

6. **Post-Exploitation**

   Setelah berhasil mengeksploitasi sistem, penguji menganalisis tingkat akses yang diperoleh dan potensi risiko yang dihadapi. Tahap ini juga mencakup pengumpulan informasi tambahan yang dapat digunakan untuk menilai lebih lanjut dampak dari serangan dan untuk membantu dalam mitigasi.

7. **Reporting**

   Tahap terakhir adalah penyusunan laporan yang berisi temuan pengujian, dampak potensial dari kerentanan, serta rekomendasi untuk mitigasi. Laporan ini disusun secara jelas dan dapat dimengerti oleh pihak terkait, termasuk manajemen dan tim teknis.

Gambar 2.9.2 Methodology Penetration Testing Execution Standard (PTES)

(Sumber : (Abu-Dabaseh & Alshammari, 2018)**)**

2.9.3 Alat Penetration Testing

Hydra adalah salah satu alat yang disertakan dalam distribusi Linux Kali, yang terkenal sebagai platform untuk pengujian penetrasi dan ethical hacking. Alat ini sangat populer di kalangan profesional keamanan siber karena kemampuannya untuk menguji keamanan sistem, khususnya dalam konteks pengujian kekuatan kata sandi. Hydra dirancang untuk melakukan serangan brute force, di mana alat ini secara otomatis mencoba semua kemungkinan kombinasi kata sandi untuk mendapatkan akses ke sistem yang dilindungi.

Dengan menggunakan Hydra, penguji keamanan dapat mengevaluasi seberapa kuat kata sandi yang digunakan dalam sistem target. Alat ini mendukung berbagai protokol dan layanan, termasuk HTTP, FTP, SSH, dan banyak lagi, sehingga memberikan fleksibilitas dalam pengujian berbagai jenis aplikasi dan layanan (Az Zahra et al., 2024).

2.10 Penelitian Terkait

Tabel 2.10.1 Penelitian Terkait

No	Nama	Judul	Sumber	Uraian
1	Yusuf Heriyanto, Anas Azhimi Qalban, Iif Alfiatul Mukaromah	Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik	ejournal.pnc.ac.id	Penelitian ini berfokus pada peningkatan keamanan sistem informasi akademik melalui autentikasi dua faktor (2FA) berbasis OTP dan Telegram untuk mengurangi risiko akses tidak sah akibat kelalaian pengguna dalam mengamankan kata sandi(Yusuf Heriyanto et al., 2022)
2	Iman Permana, Mardi	Securing the Website Login System with the	journal.uniska.ac.id	Penelitian ini menerapkan OTP berbasis SHA256 dan TOTP pada perangkat

	Hardjianto, Kiki Ahmad Baihaqi	SHA256 Generating Method and Time-based One-time Password (TOTP)		mobile untuk meningkatkan keamanan sistem login dan mengurangi risiko pencurian password pengguna(Permana et al., 2020)
3	Rahmalia Syahputri, Berkat Fa'atulo Halawa, Sherli Trisnawati, Nurfiana, Taufik	FaceVoting: e-voting Berbasiskan Pengenalan Wajah	ejournal.bsi.ac.id	Penelitian ini mengembangkan FaceVoting, sistem e-voting berbasis pengenalan wajah menggunakan algoritma Haar Cascade untuk meningkatkan keamanan dan efisiensi. Hasil uji coba menunjukkan efektivitas dalam mengenali wajah di berbagai kondisi, dengan tingkat kepuasan 96.5% dari partisipan, mendukung keandalan dan potensi sistem untuk pemilihan yang lebih aman dan transparan(Syahputri et al., 2024)
4	Fahmi Fachri	Optimasi Keamanan Web Server terhadap Serangan Brute-Force Menggunakan Penetration Testing	pdfs.semanticscholar.org	Penelitian ini mengoptimalkan keamanan web server dengan uji penetrasi, mengidentifikasi tiga kategori kelemahan serta kerentanan pada level tinggi, medium, dan rendah. Optimalisasi menggunakan konfigurasi Fail2ban berhasil menolak akses penyusup (Fachri, 2023)

5	Tomoyud S. Waruwu, Suhendri Nasution	Pengembangan Keamanan Web Login Portal Dosen Menggunakan Unified Modelling Language (UML)	e-journal.sari-mutiara.ac.id	Penelitian ini mengembangkan keamanan portal dosen berbasis web di STMIK Methodist Binjai menggunakan UML dan algoritma MD5 untuk pengacakan sandi(Tomoyud S. Waruwu & Suhendri Nasution, 2018)
6	Adnan Buyung Nasution, Ahir Yugo Nugroho Hrp, Yudi, Muhammad Fauzi	Implementation of OTP Code as Application Login Verification Via Whatsapp	journal.formosapublisher.org	Penelitian ini mengimplementasikan verifikasi login menggunakan OTP yang dikirim melalui WhatsApp, meningkatkan keamanan dan kenyamanan pengguna (Nasution et al., 2024).
7	Chairil Anwar, Sriani	Implementasi Algoritma OTP dan HMAC untuk Two Factor Authentication Sistem Login Relawan Pemilu	jurnal.polsri.ac.id	Penelitian ini menerapkan 2FA pada Sistem Informasi Relawan Pemilu (SIRP) dengan algoritma OTP dan HMAC untuk meningkatkan keamanan login, menghasilkan kode OTP 6 digit yang berubah setiap 15 detik, guna melawan serangan siber (Teknika & Anwar, 2024).
8	Laila Qadriah, Sayed Achmady, Husaini	Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor	jsi.politala.ac.id	Penelitian ini merancang sistem pengamanan dokumen dengan 2FA menggunakan TOTP untuk menghasilkan kata sandi sekali pakai yang dikirim ke email, dilengkapi dengan QR Code melalui Google Authenticator, guna meningkatkan

		Authentication (2FA)		keamanan dokumen (Qadriah et al., 2023)
9	Angga Eko Bayu Arieska, Fransiska Sisilia Mukti	Pemanfaatan One-Time Password dan Algoritma Advanced Encryption Standard dalam Sistem Login Internet Kampus	ejournal.uniramalang.ac.id	Penelitian ini menggabungkan OTP dan algoritma AES dalam sistem login internet kampus untuk meningkatkan keamanan autentikasi, menjaga integritas dan kerahasiaan informasi login, serta memastikan akses hanya bagi pengguna berwenang (Arieska & Mukti, 2023).
10	Zuhar Musliyana, Teuku Yuliar Arif, Rizal Munadi	Peningkatan Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password	jurnal.unsyiah.ac.id	Penelitian ini meningkatkan keamanan otentikasi SSO di Universitas Ubudiyah Indonesia dengan algoritma AES dan OTP berbasis sinkronisasi waktu, mengamankan autentikasi dari serangan seperti dictionary attack dan rainbow table (Musliyana et al., 2016).
11	Nosiel, Isnandar Agus	E-Commerce Pada UMKM Desa Wiralaga Di Mesuji	jurnal.darmajaya.ac.id	Penelitian ini bertujuan untuk membantu Usaha Mikro, Kecil, dan Menengah (UMKM) dalam meningkatkan pemasaran produk-produk UMKM di Desa Wiralaga II. Pengembangan perangkat lunak e-commerce dibangun dengan menggunakan model pengembangan perangkat lunak prototype, sehingga para pelaku usaha dapat

				mempromosikan hasil usaha dengan mudah (Nosiel & Isnandar Agus, 2020).
12	Riyandini Riyan Utami, Muhammad Saputra, Muhammad Fauzan Azima, Siti Nur Laila	Inovasi Limbah Kemasan Plastik Dan Pelatihan Pembuatan Web Pekon Mulyorejo Kecamatan Banyumas Kabupaten Pringsewu	jurnal.darmajaya.ac.id	Penelitian ini menghasilkan inovasi produk limbah kemasan plastik dan Web Pekon Mulyorejo sebagai situs resmi dan sarana informasi desa. Kegiatan ini melibatkan pelatihan, penyuluhan, dan pendampingan langsung untuk mengoptimalkan pengembangan UKM di pekon Mulyorejo (Saputra et al., 2020).
13	Viola De Yusa, Betty Magdalena	Pemanfaatan Dan Pengembangan Desa Berbasis Web Dan Pengembangan Bisnis Budidaya Jamur Tiram Menjadi Bakso Jamur Di Pekon Tambah Rejo Kec Gading Rejo Kab Pringsewu	jurnal.darmajaya.ac.id	Penelitian ini membahas penerapan e-commerce untuk mempublikasikan produk dan jasa, termasuk pengembangan web SIDesa dan pelatihan teknologi untuk UKM. Fokus pada UKM jamur tiram untuk meningkatkan penjualan melalui media online menggunakan aplikasi Freewebstore (Viola De Yusa & Betty Magdalena, 2015).
14	Arman Suryadi Karim, Melda Agarina, Sutedi	Pembangunan Sistem Informasi Manajemen Seminar (Nasional dan Internasional) pada IBI Darmajaya	jurnal.darmajaya.ac.id	Penelitian ini membangun Sistem Informasi Manajemen Seminar untuk memfasilitasi pendaftaran dan dokumentasi kegiatan seminar. Sistem ini menggunakan metodologi Prototyping-Based Methodology untuk

				memenuhi kebutuhan peserta dan manajemen dalam pengelolaan data seminar (Suryadi Karim & Agarina, 2019).
15	Sulyono, Fitria, Lia Indriyati	Rancang Bangun Teknologi Informasi E-Complaint pada Perguruan Tinggi	jurnal.darmajaya.ac.id	Penelitian ini merancang dan membangun aplikasi E-Complaint untuk menampung keluhan, kritik, dan saran dari mahasiswa terhadap operasional kampus dan dosen di IBI Darmajaya. Aplikasi ini menggunakan model SDLC air terjun dan framework bootstrap untuk tampilan responsif, mendukung fungsi Quality Assurance Center (QAC) (Sulyono et al., 2018).

Penelitian ini bertujuan untuk menguji keamanan sistem Website Desa, dengan fokus pada identifikasi kelemahan yang terdapat pada autentikasi satu faktor yang saat ini diterapkan. Setelah kelemahan tersebut teridentifikasi, penelitian ini akan mengembangkan sistem informasi dengan menerapkan *Two-Factor Authentication* (2FA) berbasis *One-Time Password* (OTP), serta membatasi jumlah percobaan login. Langkah-langkah ini diharapkan dapat meningkatkan perlindungan data pribadi masyarakat desa dan mengurangi risiko kebocoran data akibat akses tidak sah.

Penelitian ini juga akan menambahkan fitur aktivasi akun yang mewajibkan operator desa mengganti kata sandi dan menambahkan email setelah pembuatan akun baru. Selain itu, fitur log aktivitas login akan diterapkan untuk memblokir alamat IP setelah lima kali percobaan login gagal dan memblokir akun setelah sepuluh kali percobaan gagal. Tujuan penelitian ini adalah meningkatkan keamanan sistem dan melindungi data masyarakat dari potensi penyalahgunaan.