BAB III

METODE PENELITIAN

3.1 Metode Pengumpulan Data

Penelitian ini menggunakan data dan informasi yang diperoleh dari berbagai sumber yang relevan dengan objek penelitian. Oleh karena itu, diperlukan beberapa metode untuk memperoleh informasi yang akurat mengenai kerentanan keamanan pada Sistem Payroll PT. Vidira Eshan Abadi, baik melalui pengamatan langsung terhadap sistem, wawancara dengan pihak terkait maupun kajian literatur.

Data yang dikumpulkan mencakup informasi mengenai aplikasi Payroll yang digunakan, arsitektur sistem, serta mekanisme keamanan yang diterapkan. Adapun metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut:

3.1.1 Observasi

Metode observasi dilakukan dengan cara mengamati secara langsung objek penelitian, yaitu Sistem Payroll milik PT. Vidira Eshan Abadi. Tujuan dari kegiatan ini adalah untuk memahami struktur aplikasi, fitur utama, serta mekanisme autentikasi dan otorisasi yang digunakan dalam sistem. Selain itu, observasi juga dilakukan terhadap konfigurasi jaringan dan basis data yang terhubung dengan sistem Payroll untuk mengidentifikasi potensi kerentanan keamanan yang mungkin terjadi.

Tempat : PT VIDIRA ESHAN ABADI

Alamat : Grand Wisata, Tambun Selatan, Bekasi, Jawa Barat

Website : https://194.233.89.138

Waktu : Oktober 2025 – Desember 2025

Dari hasil observasi, peneliti memperoleh gambaran umum mengenai alur kerja sistem Payroll, termasuk modul login, dashboard dan form pengelolaan data karyawan. Observasi ini juga menjadi dasar dalam tahap *Intelligence Gathering* pada metodologi Penetration Testing Execution Standard (PTES) untuk menentukan target pengujian yang relevan.

3.1.2 Wawancara

Untuk memperkuat hasil observasi, peneliti melakukan wawancara dengan tim pengembang dan pengelola sistem IT PT. Vidira Eshan Abadi guna memperoleh pemahaman yang lebih mendalam mengenai kebijakan keamanan aplikasi, proses pemeliharaan sistem, serta langkah mitigasi terhadap ancaman siber. Wawancara yang dilaksanakan pada 01 Oktober 2025 ini membahas beberapa topik utama, meliputi proses pengembangan dan pengujian keamanan sistem payroll, kebijakan keamanan data dan kontrol akses pengguna, penerapan metode Penetration Testing Execution Standard (PTES), serta upaya perusahaan dalam menjaga Confidentiality, Integrity dan Availability (CIA) data karyawan. Selain itu, dibahas pula langkah pencegahan terhadap ancaman yang umum terjadi berdasarkan OWASP Top 10, seperti *SQL Injection*, *Cross-Site Scripting (XSS)* dan *Broken Authentication*. Hasil wawancara ini menjadi dasar penting dalam penyusunan rencana dan pelaksanaan pengujian penetrasi (penetration testing) pada tahap penelitian berikutnya.

3.1.3 Studi Literatur

Data-data dan informasi yang digunakan sebagai studi literatur yang dilakukan dengan mempelajari dan mengumpulkan meteri-meteri yang berkaitan dengan keamanan sistem informasi yang berupa 4 dokumen junal

lokal, sebagai acuan pengujian keamanan istem Payroll PT. Vidira Eshan Abadi. Berikut ini adalah penjabaran dari literatur-leteratur sejenis dengan penelitian yang dilakukan. Dapat terelihat pada Tabel 3.1.

No	Nama Penilitian	Judul	Tahun	Masalah	Hasil Penilitian
1	Madya, A., Purnomo, R., & Nurfiyah, S.	Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta	2024	Sistem informasi universitas memiliki potensi kerentanan keamanan yang belum teridentifikasi secara menyeluruh.	Menggunakan ISSAF dengan alat Sudomy dan OWASP ZAP untuk mendeteksi kelemahan system:relevan dengan penelitian ini karena menggunakan OWASP ZAP namun belum menilai tingkat keparahan dengan CVSS v3.1.
2	Rahmawati, N., & Suryanto, A.	Implementasi Penetration Testing pada Website Menggunakan Metode PTES	2023	Pengujian keamanan website belum mengikuti metodologi yang sistematis.	PTES memberikan alur pengujian terstruktur dari *Pre-Engagement* hingga *Reporting*; menjadi dasar metodologis bagi penelitian ini meskipun belum dikombinasikan dengan OWASP Top 10.
3	Nurhadi	Penetration Testing Website dengan Metode Black Box Testing untuk Meningkatkan Keamanan	2023	Sistem belum diuji secara menyeluruh terhadap serangan eksternal yang realistis.	Menggunakan pendekatan *Black Box Testing* berbasis PTES; efektif untuk simulasi serangan namun belum mencakup klasifikasi tingkat risiko

		Website pada Instansi			seperti CVSS v3.1.
4	Sari, L., & Nugraha, D.	Evaluasi Keamanan Aplikasi E-Government Menggunakan OWASP Top 10 dan CVSS v3.1	2024	Aplikasi e-Government masih memiliki kerentanan berdasarkan OWASP Top 10 yang belum dikategorikan risikonya.	Menggabungkan OWASP Top 10 dan CVSS v3.1 untuk penilaian keamanan; relevan dengan penelitian ini karena menggunakan pendekatan serupa namun belum mengintegrasikan metodologi PTES.

Tabel 3. 1 Studi Literatur

3.1.4 Pengujian dan Analisis

Kerangka kerja yang dirancang untuk melakukan pengujian penetrasi dengan cara yang konsisten, terstruktur, dan efektif. PTES memastikan bahwa setiap langkah dalam uji penetrasi mengikuti standar yang jelas sehingga memberikan hasil yang dapat diandalkan pada saat pengujian berlangsung. Dapat dilihat road map penelitian pada Tabel 3.2.

No	Tahapan	Aktivitas	Tools	Tujuan
1	Pre -Engagement Interactions	Penentuan lingkup (scope)	Wawancara, Zoommetting	Memastikan semua pihak mengerti tujuan dan runag lingkup pengujian.
2	Reconnaissance	Crawling Direktori	Dirsearch, Gobuster	Menemukan direktori dan file tersembunyi atau sensitif di server web yang mungkin tidak terlihat oleh pengguna biasa
3	Scanning	Pemindaian kerentanan otomatis,	Nuclei	Melakukan pemindaian kerentanan dan

		analisis parameter aplikasi web.		analisis parameter aplikasi web untuk menemukan potensi celah keamanan.
4	Enumeration	Mengidentifikasi endpoint sensitif, menganalisis struktur URL dan parameter.	Gobuster	Mengidentifikasi endpoint sensitif dan memahami struktur URL serta parameter yang digunakan aplikasi.
5	Exploitation	Sql Injection, pengujian CrossSite Scripting XSS	Sqlmap	Menguji celah keamanan seperti SQL Injection dan XSS untuk membuktikan adanya kerentanan.
6	Post Exploitation	Mengevaluasi akses yang diperoleh, mengekstraksi data sensitif.	Sqlmap,Manual testing	Mengevaluasi akses yang didapatkan dan Mengumpulkan data sensitif dari sistem
7	Reporting	Membuat laporan kerentanan lengkap, Memberikan rekomendasi mitigasi	Manual	Membuat laporan yang komprehensif, termasuk rekomendasi mitigasi terhadap kerentanan yang ditemukan.

Tabel 3.2 Road Map Penelitian

3.1.5 Pre-Engagement Interactions

Tahapan ini bertujuan untuk memastikan semua pihak memahami ruang lingkup, tujuan, dan ekspektasi uji penetrasi dengan mendefinisikan batasan pengujian, jenis pengujian (black-box, white-box atau gray-box) dan tujuan utama seperti identifikasi celah keamanan aplikasi PT. Vidira Eshan Abadi.

3.1.6 Reconnaissance (Pengintaian)

Tahap *reconnaissance* atau pengintaian merupakan langkah awal dalam pengujian penetrasi yang bertujuan mengumpulkan sebanyak mungkin informasi tentang Sistem Payroll PT. Vidira Eshan Abadi untuk memahami struktur aplikasi, mengidentifikasi potensi titik lemah dan merancang skenario eksploitasi yang terfokus. Kegiatan utama pada tahap ini meliputi:

1. Directory crawling menggunakan gobuster dan dirsearch untuk menemukan direktori tersembunyi, endpoint sensitif, serta file yang tidak seharusnya dapat diakses publik;
2. Pemindaian port dan layanan menggunakan *Nmap* untuk mengidentifikasi port terbuka, layanan yang berjalan, serta versi perangkat lunak yang dapat menjadi vektor serangan.

3.1.7 Scanning

Tahap *scanning* bertujuan mengidentifikasi kerentanan pada Sistem Payroll PT. Vidira Eshan Abadi dengan memanfaatkan informasi hasil *reconnaissance*. Kegiatan ini difokuskan untuk mengetahui layanan, port, serta teknologi yang berpotensi memiliki kelemahan dan menghasilkan daftar temuan awal yang akan diverifikasi pada tahap selanjutnya. Aktivitas utama dalam tahapan *scanning* meliputi:

1. Pemindaian otomatis kerentanan aplikasi menggunakan *Nuclei* untuk mendeteksi kerentanan umum seperti SQL Injection, Cross-Site Scripting (XSS) dan Cross-Site Request Forgery (CSRF).

2. Analisis lalu lintas HTTP/HTTPS menggunakan BurpSuite untuk mengintersep, memodifikasi dan menganalisis parameter pada *request* dan *response* aplikasi web sehingga dapat mengidentifikasi celah yang tidak selalu terdeteksi oleh scanner otomatis.
3. Verifikasi temuan mempalidasi hasil pemindaian otomatis untuk mengeliminasi false positive dan menentukan temuan yang memang dapat dieksploitasi.
4. Pemeriksaan konfigurasi server menilai pengaturan web server dan keamanan header HTTP (mis. HSTS, CSP, X-Frame-Options) serta konfigurasi lain yang dapat memengaruhi kerentanan aplikasi.

3.1.8 Enumeration

Tahap *enumeration* merupakan proses pendalaman terhadap aset-aset yang telah teridentifikasi pada tahap *reconnaissance* dan *scanning* dengan tujuan memperoleh informasi teknis yang lebih rinci mengenai endpoint layanan dan fitur pada Sistem Payroll PT. Vidira Eshan Abadi yang berpotensi dieksploitasi. Kegiatan pada tahapan ini meliputi:

1. Identifikasi endpoint sensitive menggunakan *gobuster* untuk menemukan endpoint direktori dan file tersembunyi yang belum terdeteksi pada tahap sebelumnya.
2. Analisis struktur URL dan parameter memanfaatkan Burp Suite untuk memetakan pola URL, parameter GET/POST dan header HTTP yang dipakai aplikasi sehingga memudahkan penyusunan payload pengujian.

3. Pengecekan mekanisme autentikasi menguji endpoint login serta melakukan pengujian *brute force* terkontrol untuk melihat potensi kelemahan pengelolaan kredensial.

3.1.9 Exploitation

Tahap *exploitation* bertujuan memverifikasi dan membuktikan keberadaan kerentanan yang teridentifikasi pada Sistem Payroll PT. Vidira Eshan Abadi dengan melakukan eksploitasi terkendali tanpa menyebabkan kerusakan pada sistem. Kegiatan pada tahap ini difokuskan pada *proof-of-concept* (PoC) untuk menilai dampak nyata setiap kelemahan serta mengumpulkan bukti yang diperlukan untuk pelaporan dan penentuan prioritas perbaikan. Prinsip yang dianut adalah etika pengujian untuk minimalisasi gangguan dan dokumentasi lengkap. Aktivitas utama pada tahapan *exploitation* meliputi:

1. SQL Injection melakukan uji injeksi ke parameter yang rentan menggunakan *sqlmap* atau teknik manual untuk membuktikan kemungkinan ekstraksi data sensitif (mis. nama pengguna, hash password) dalam skenario PoC yang aman.
2. Cross-Site Scripting menyuntikkan payload skrip melalui input/parameter teridentifikasi dan memverifikasi eksekusi di sisi klien menggunakan *Burp Suite* atau pengujian manual untuk menilai risiko pencurian sesi atau manipulasi tampilan.
3. Directory Traversal mencoba memanipulasi path file untuk mengakses berkas yang seharusnya tidak dapat diakses dengan tetap membatasi tindakan hanya pada pembacaan file non-sensitif sebagai bukti eksploitasi.

4. Command Injection menguji kemungkinan eksekusi perintah pada server melalui input yang tidak tervalidasi dilakukan secara terkendali dan hanya sampai level PoC tanpa menjalankan perintah berisiko.
5. Authentication Bypass menguji kelemahan mekanisme autentikasi (mis. brute-force terkontrol manipulasi parameter atau pengujian logika otentikasi) untuk menilai potensi pengambilalihan akun dengan memperhatikan pengamanan rate limiting dan lockout.

3.1.10 Post Exploitation

Tahapan post exploitation bertujuan mengevaluasi dampak nyata dari eksploitasi yang berhasil dilakukan. Kegiatan ini fokus pada penentuan sejauh mana akses yang diperoleh dapat membahayakan kerahasiaan integritas dan ketersediaan data serta system sekaligus menyediakan bukti dan rekomendasi perbaikan yang terukur. Prinsip pelaksanaan adalah bersifat non-destruktif terdokumentasi dengan rinci dan memprioritaskan pemulihan kondisi sistem setelah pengujian.

Aktivitas utama pada tahap post exploitation meliputi:

1. Pengumpulan data yang di peroleh selama eksploitasi untuk membuktikan eksposur tanpa menyalin atau mengubah data sensitif kecuali yang diperlukan untuk *proof-of-concept* yang direkam.
2. Evaluasi dampak menilai konsekuensi akses terhadap *Confidentiality*, *Integrity* dan *Availability* (CIA) dengan menguraikan skenario serangan potensial, skala data yang terpengaruh, kemungkinan eskalasi hak akses serta dampak operasional terhadap layanan payroll.

3. Dokumentasi aktivitas dan menyusun langkah reproduksi (step-by-step) bukti pendukung (screenshot, log, request/response) serta penilaian keparahan yang dapat diverifikasi oleh tim teknis perusahaan.

3.1.11 Reporting

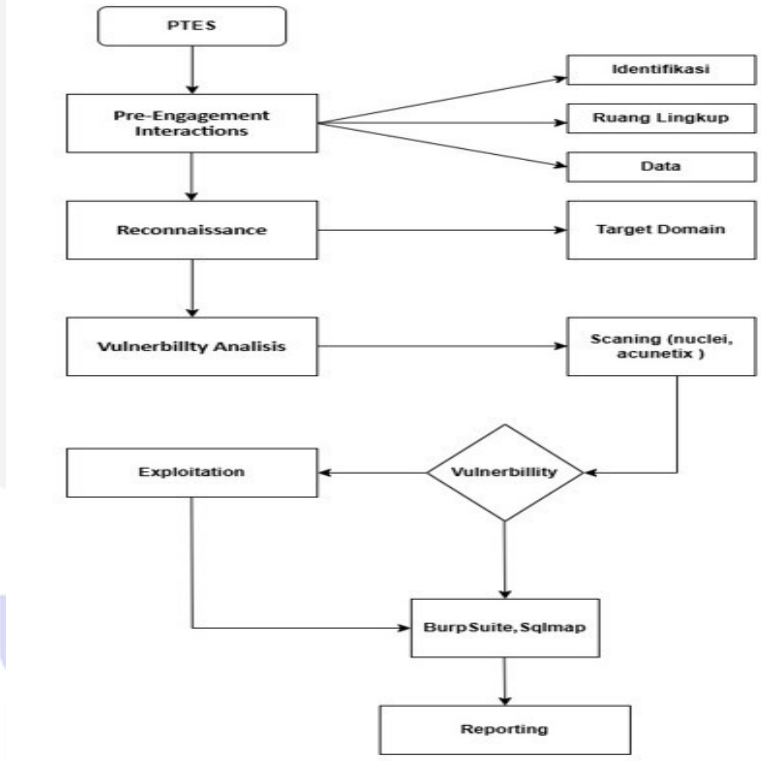
Tahap Reporting merupakan proses akhir dalam kegiatan pengujian penetrasi yang berfokus pada penyusunan dokumentasi hasil pengujian secara lengkap dan sistematis. Tujuan utama dari tahap ini adalah agar hasil pengujian dapat dipahami dengan baik oleh pihak teknis maupun non-teknis serta menjadi dasar dalam pengambilan keputusan terkait peningkatan keamanan sistem.

Adapun langkah-langkah yang dilakukan pada tahap ini meliputi:

1. Penyusunan Laporan Teknis yang berisi hasil pengujian secara detail mencakup jenis kerentanan yang ditemukan, bukti eksploitasi serta potensi dampak terhadap sistem.
2. Penyusunan Rekomendasi Mitigasi yaitu pemberian saran perbaikan terhadap setiap kerentanan yang ditemukan seperti penerapan patch keamanan perbaikan konfigurasi system atau penambahan kontrol keamanan yang relevan.
3. Penyampaian Hasil Pengujian dilakukan melalui presentasi kepada pihak terkait (stakeholder) agar seluruh pihak memahami temuan yang ada serta langkah tindak lanjut yang perlu dilakukan untuk memperkuat keamanan sistem.

3.2 Kerangka Penelitian

Kerangka penelitian ini menjelaskan alur pelaksanaan penetration test yang dilakukan secara terstruktur dimulai dari tahap perencanaan pengumpulan informasi, pemindaian dan analisis kerentanan eksploitasi serta verifikasi hasil hingga tahap mitigasi dan pelaporan. Alur lengkap kegiatan penilitian ini di tampilkan pada Gambar 3.1.



Sumber : Hasil Penelitian, 2025

Gambar 3. 1 Tahapan Pelaksanaan Pengujian