BAB III
METODOLOGI PENELITIAN

3.1 Kerangka Kerja Pengujian dan Analisis Resiko

Jenis penelitian yang digunakan adalah penelitian eksploratif dengan metode *penetration testing* dan analisis keamanan berbasis *vulnerability assessment*. Metode ini bertujuan untuk menemukan celah keamanan yang dapat dieksploitasi serta memberikan solusi mitigasi yang efektif guna meningkatkan keamanan website *SAMBANG*. Dengan pendekatan ini, penelitian dapat memberikan pemahaman mendalam mengenai risiko keamanan serta merumuskan strategi mitigasi yang lebih tepat guna.

Untuk memastikan proses analisis keamanan berjalan secara sistematis dan sesuai dengan standar industri, penelitian ini mengadopsi dua kerangka kerja utama: OWASP untuk metodologi pengujian kerentanan dan NIST untuk proses penilaian risiko.

3.1.1 Penerapan Kerangka OWASP (Open Web Application Security Project)

OWASP menyediakan sumber daya dan panduan praktik terbaik untuk keamanan aplikasi web. Dalam penelitian ini, kerangka OWASP digunakan dalam dua aspek utama:

1. Sebagai Dasar Identifikasi Kerentanan (OWASP Top 10): Penelitian ini memfokuskan analisis pada jenis ancaman siber yang paling umum dan kritis sebagaimana diidentifikasi dalam daftar OWASP Top 10. Fokus pengujian pada serangan seperti *SQL Injection*, *Cross-Site Scripting* (XSS), dan kelemahan autentikasi pengguna didasarkan pada relevansi dan dampak tinggi dari ancaman-ancaman ini terhadap aplikasi web modern .
2. Sebagai Panduan Prosedur Pengujian (OWASP Web Security Testing Guide - WSTG): Mekanisme pengujian yang dijelaskan dalam sub-bab "3.5 Prosedur Penelitian" secara langsung mengacu pada

metodologi yang diuraikan dalam WSTG. Contoh penerapan konkretnya adalah:

a Pengujian SQL Injection: Langkah-langkah seperti memasukkan *payload* ' OR '1'='1'; -- ke dalam form input merupakan teknik standar yang direkomendasikan WSTG untuk menguji validasi input dan celah pada *query* database.
b Pengujian Cross-Site Scripting (XSS): Penyuntikan skrip seperti <script>alert('XSS Test')</script> ke dalam parameter yang dapat diinput oleh pengguna adalah prosedur fundamental dari WSTG untuk memeriksa apakah aplikasi melakukan sanitasi dan *encoding output* dengan benar.
c Pengujian Keamanan Autentikasi: Simulasi serangan *brute force* pada halaman login untuk menguji ada atau tidaknya mekanisme pembatasan percobaan login adalah salah satu skenario pengujian utama yang diuraikan dalam WSTG untuk kategori kelemahan autentikasi.

3.1.2 Penerapan Kerangka NIST (National Institute of Standards and Technology)

Setelah kerentanan diidentifikasi menggunakan panduan OWASP, kerangka NIST digunakan untuk menganalisis dan mengukur tingkat risikonya. Penelitian ini secara spesifik mengacu pada NIST Special Publication 800-30, "Guide for Conducting Risk Assessments".

1. Sebagai Dasar Analisis dan Penilaian Risiko: Proses analisis risiko yang dilakukan pada BAB IV mengadopsi pendekatan NIST. Kerangka ini membantu menerjemahkan temuan teknis (kerentanan) menjadi risiko bisnis yang dapat dipahami dan diprioritaskan.

a Penentuan *Likelihood* dan *Impact*: Konsep penentuan risiko berdasarkan dua parameter utama, yaitu tingkat kemungkinan terjadinya eksploitasi (*likelihood*) dan besarnya dampak

terhadap sistem (*impact*), diadopsi langsung dari metodologi NIST 800-30.

b Pembuatan Matriks Risiko: Penyusunan rangkuman risiko dan prioritas mitigasi dalam bentuk matriks pada Tabel 4.7 adalah implementasi dari tahap evaluasi risiko dalam kerangka NIST. Matriks ini secara visual memetakan setiap kerentanan berdasarkan tingkat kemungkinan dan dampaknya, sehingga menghasilkan kategori risiko (Kritis, Tinggi, Sedang) yang menjadi dasar untuk menentukan tindakan prioritas.

Dengan mengintegrasikan kedua kerangka ini, penelitian tidak hanya mengidentifikasi celah keamanan secara teknis, tetapi juga memberikan penilaian risiko yang terukur dan rekomendasi mitigasi yang dapat ditindaklanjuti sesuai dengan tingkat urgensinya.

3.2 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif eksploratif dalam mengidentifikasi serta menganalisis bug keamanan pada website *SAMBANG*. Metode kualitatif eksploratif digunakan untuk memahami fenomena yang sedang terjadi serta mencari korelasi baru yang berkaitan dengan ancaman keamanan siber pada sistem pemerintahan digital. Penelitian eksploratif bersifat terbuka sehingga banyak informasi yang dikumpulkan, sehingga peneliti perlu memahami teori lebih baik untuk mendapatkan hasil yang maksimal [14].

Jenis penelitian yang digunakan adalah penelitian eksploratif dengan metode *penetration testing* dan analisis keamanan berbasis *vulnerability assessment*. Metode ini bertujuan untuk menemukan celah keamanan yang dapat dieksploitasi serta memberikan solusi mitigasi yang efektif guna meningkatkan keamanan website *SAMBANG*. Dengan pendekatan ini, penelitian dapat memberikan pemahaman mendalam mengenai risiko keamanan serta merumuskan strategi mitigasi yang lebih tepat guna.

3.3 Objek Penelitian

Objek penelitian ini adalah website SAMBANG (Sistem Administrasi Berbasis Digital Jombang), yang merupakan platform layanan digital milik Pemerintah Kabupaten Jombang. Website ini digunakan untuk berbagai keperluan administratif dan pelayanan publik, sehingga memerlukan sistem keamanan yang optimal guna melindungi data pengguna.

3.4 Teknik Pengumpulan Data

1. Observasi

   Langkah ini di lakukan penulis sebagai salah satu langkah agar penulis mendapatkan data yang diperlukan untuk pengembangan Applikasi ini, penulis melakukan penelitian langsung ke website "SAMBANG". Langkah tersebut penulis lakukan bertujuan untuk mendapatkan informasi berupa data serta keterangan yang di butuhkan dan untuk menganalisis rancangan sistem untuk memenuhi kebutuhan website "SAMBANG".

2. Dokumentasi

   Salah satu cara pengumpulan data adalah melalui prosedur dokumentasi, yang melibatkan penelaahan atau evaluasi dokumen yang telah dihasilkan oleh subjek atau orang lain. Teknik dokumentasi adalah metode pengumpulan data yang memanfaatkan sumber tertulis yang diterbitkan oleh lembaga penelitian. Bahan-bahan ini dapat mencakup laporan kerja, peraturan, dan prosedur yang diterbitkan oleh lembaga penelitian. Dokumentasi dalam penelitian ini berupa bukti penelitian di website "SAMBANG".

3. Studi Literatur

   Studi pustaka merupakan serangkaian kegiatan yang berkaitan dengan metode pengumpulan data pustaka, pembacaan dan pencatatan, serta pengolahan bahan penelitian. Menurut Danial dan Warsiah (2009:80), studi pustaka adalah penelitian yang dilakukan oleh peneliti dengan mengumpulkan sejumlah buku dan majalah yang berkaitan dengan permasalahan dan tujuan penelitian.

Teknik ini dilakukan dengan tujuan mengungkap berbagai teori yang relevan dengan permasalahan yang sedang dibahas/diteliti sebagai bahan rujukan dalam membahas hasil penelitian. Definisi lain dari studi pustaka adalah pencarian referensi teoritis yang relevan dengan kasus atau permasalahan yang diteliti.

Tinjauan pustaka, secara umum, adalah metode pemecahan masalah yang melibatkan penelusuran materi yang telah dipublikasikan sebelumnya. Dalam aspek lain, istilah "tinjauan pustaka" dan "studi kepustakaan" juga agak mirip. Seorang peneliti harus menguasai topik yang ditelitinya agar dapat melakukan penelitian. Risiko kegagalan penelitian akan sangat meningkat jika hal ini tidak dilakukan.

3.5 Prosedur Penelitian

Prosedur penelitian ini bertujuan untuk mengidentifikasi dan mengeksplorasi bug keamanan pada website "SAMBANG" serta menerapkan strategi mitigasi yang sesuai. Fokus utama pengujian adalah serangan berbasis SQL Injection, Cross-Site Scripting (XSS), dan kelemahan autentikasi pengguna.

A. SQL Injection

Metode Pengujian:

- Memasukkan kode SQL berbahaya pada input formulir login dan pencarian.
- Menggunakan tool seperti SQLmap untuk mengidentifikasi kerentanan pada database.

Langkah-langkah:

1. Mengakses halaman login dan input pengguna lainnya.

2. Memasukkan payload SQL Injection seperti:

' OR '1'='1'; --

" OR "1"="1"; --

admin' –

3. Mengamati respon sistem terhadap input yang diberikan.

Parameter Evaluasi:

- Apakah sistem mengizinkan akses tidak sah?
- Apakah terjadi kebocoran data dari database?

Hasil:

- Jika sistem menampilkan data atau mengizinkan login tanpa kredensial yang valid, maka terdapat celah SQL Injection.
- Jika sistem memberikan pesan error terkait database, maka input tidak disanitasi dengan baik.

Mitigasi:

- Menggunakan parameterized query atau prepared statements.
- Menerapkan validasi input yang ketat.

B. Cross-Site Scripting (XSS)

Metode Pengujian:

- Menyuntikkan skrip berbahaya ke dalam formulir input.
- Menggunakan tool seperti OWASP ZAP untuk mendeteksi XSS.

Langkah-langkah:

1. Menginput skrip berbahaya pada form komentar atau pencarian:

<script>alert('XSS Test')</script>

"><script>alert('XSS')</script>

2. Mengamati apakah sistem mengeksekusi skrip berbahaya tersebut.

Parameter Evaluasi:

- Apakah skrip berjalan di browser pengguna?
- Apakah terdapat indikasi pencurian cookie atau data pengguna?

Hasil:

- Jika skrip dijalankan tanpa sanitasi, maka sistem rentan terhadap serangan XSS.

Mitigasi:

- Menggunakan Content Security Policy (CSP).
- Melakukan sanitasi dan validasi input.
- Encoding output sebelum ditampilkan ke pengguna.

C. Keamanan Autentifikasi

Metode Pengujian:

- Melakukan serangan brute force menggunakan daftar kata sandi umum.
- Menguji kelemahan dalam manajemen sesi pengguna.

Langkah-langkah:

1. Mencoba login dengan berbagai kombinasi kata sandi umum menggunakan tool seperti Hydra atau Burp Suite.

2. Mengamati apakah sistem mengunci akun setelah beberapa percobaan gagal.
3. Menguji apakah cookie sesi dapat dicuri atau digunakan kembali.

Parameter Evaluasi:

- Apakah sistem membatasi percobaan login?
- Apakah sesi pengguna tetap aktif setelah logout?

Hasil:

- Jika sistem mengizinkan percobaan login tanpa batas, maka rentan terhadap serangan brute force.
- Jika sesi tetap aktif setelah logout, maka ada celah keamanan sesi.

Mitigasi:

- Menerapkan autentikasi multi-faktor (MFA).
- Mengenkripsi cookie sesi dan membatasi waktu kedaluwarsa.

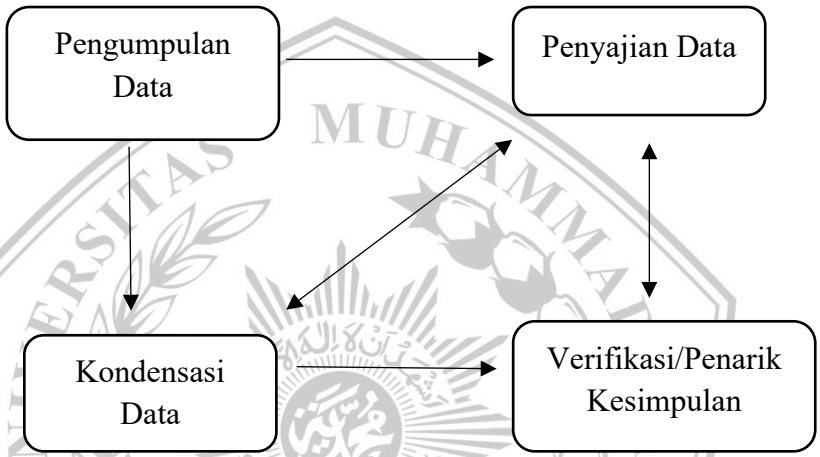
Dengan melakukan pengujian terhadap berbagai bug keamanan pada website "SAMBANG," penelitian ini berhasil mengidentifikasi celah keamanan yang dapat dieksploitasi. Implementasi strategi mitigasi yang efektif sangat penting untuk meningkatkan keamanan sistem dan mencegah serangan siber di masa mendatang. Penelitian ini memberikan rekomendasi praktis bagi pengelola website untuk meningkatkan perlindungan terhadap ancaman siber.

3.6 Teknik Analisis Data

Analisis penelitian ini bersifat kualitatif dan melibatkan tulisan dalam bentuk kumpulan kata, alih-alih angka. Data dikumpulkan melalui berbagai metode, seperti observasi, wawancara, dokumentasi, serta rekaman audio dan video. Teknik analisis data merupakan studi yang menantang karena membutuhkan pengetahuan tingkat tinggi,

usaha keras, dan kemampuan berpikir kreatif. Selain itu, teknik analisis data bervariasi antar peneliti, terutama dalam hal metodologi yang digunakan (Sugiyono, 2010).

Oleh karena itu, analisis data yang digunakan dalam penelitian ini menggunakan model interaktif, sebagaimana disarankan oleh Miles dan Huberman, yang melibatkan reduksi data dan penyusunan kesimpulan atau verifikasi yang dilakukan secara bersamaan. Model analisis yang digunakan dijelaskan sebagai berikut:



Gambar 3. 1 Model Analisis Interaktif Miles dan Huberman

Sumber : Matthew B. Miles, A. Michael Huberman, (2014): Analisis Data Kualitatif

Adapun langkah-langkah dalam melakukan analisis data adalah sebagai berikut:

1. Pengumpulan Data

   Proses pengumpulan data untuk mendapatkan berbagai jenis data yang dibutuhkan untuk penelitian ini dikenal sebagai pengumpulan data. Wawancara dan pencatatan data yang dibutuhkan merupakan beberapa metode yang digunakan. Informasi ini dikumpulkan melalui informan dan peneliti yang menemukan celah keamanan pada situs web "SAMBANG" di Kabupaten Jombang. Serta pengamat sebagai pemeran peneliti

dan dokumentasi yang dihimpun oleh peneliti selama melakukan pengamatan di lokasi penelitian.

2. Kondensasi Data

   Kondensasi data adalah proses di mana peneliti memilih, menyederhanakan, dan mengabstraksikan data dari berbagai sumber seperti catatan lapangan, observasi, dokumen, dan materi empiris lainnya. Tujuan dari kondensasi ini adalah untuk menyusun data menjadi bentuk yang lebih fokus dan relevan dengan kebutuhan penelitian. Ini melibatkan pengumpulan data dari observasi yang telah dilakukan untuk memastikan bahwa informasi yang diperoleh sesuai dengan topik penelitian.

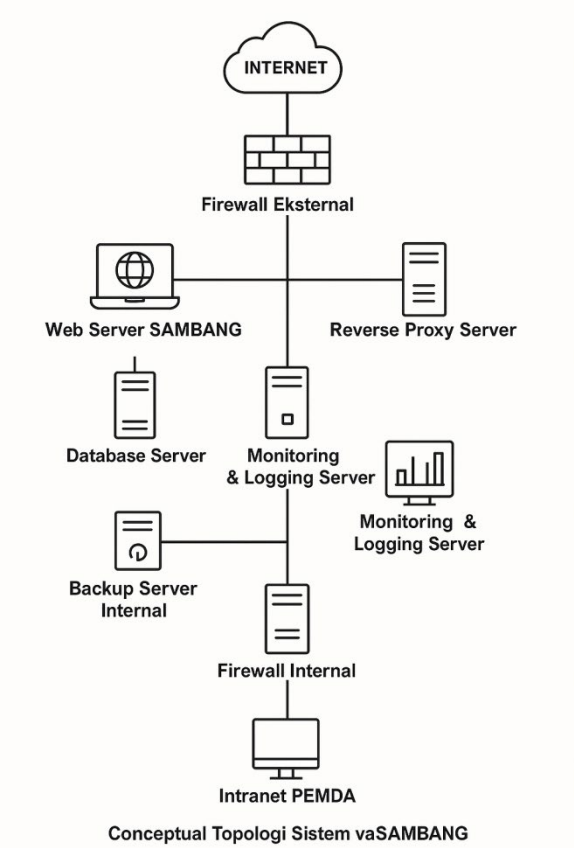
3. Penyajian Data

   Sebagai langkah awal dalam pengelolaan data, penyajian data mencakup pengumpulan dan penyajian hasil penelitian dalam format eksploratif, termasuk foto-foto penelitian yang dilakukan di situs web "SAMBANG" dan analisis awal berbagai temuan data di lapangan.

4. Penarikan Kesimpulan dan Verifikasi

   Untuk menarik kesimpulan, diskusi berdasarkan hasil reduksi dan penyajian data perlu dilakukan. Peneliti akan mendasarkan hasil penelitiannya pada observasi yang dilakukan di situs web "SAMBANG" saat melakukan penelitian. Peneliti akan mengeksplor dan menarik kesimpulan mengenai bug pada celah keamanan di *website* “SAMBANG” Kabupaten Jombang. Setelah menarik kesimpulan, kemudian di verifikasi yang bertujuan untuk mencari data baru yang lebih mendalam dengan persetujuan yang sama.

3.6 Desain Topologi



Conceptual Topologi Sistem vaSAMBANG

Ketereangan:

1. Internet

   Akses publik oleh pengguna (warga Jombang) untuk membuka website *SAMBANG*.

2. Firewall Eksternal

   Menyaring lalu lintas dari internet ke DMZ. Hanya memperbolehkan trafik HTTP/HTTPS ke Web Server atau Reverse Proxy.

3. Web Server (Public-Facing)

   Server utama yang melayani permintaan pengguna terhadap website *SAMBANG*. Terletak di zona DMZ untuk mengisolasi dari sistem internal.

4. Reverse Proxy Server (Opsional)

   Bertugas menyaring, men-cache, dan memvalidasi permintaan sebelum

diteruskan ke Web Server. Bisa mengurangi risiko serangan langsung dan membantu mitigasi DDoS.

5. Application Server

   Tempat dijalankannya logika aplikasi dari sistem SAMBANG (pengelolaan form, verifikasi input, pemrosesan data, dll). Terhubung ke database dan sistem backend.

6. Database Server

   Menyimpan semua data penting, termasuk data pengguna. Diberi proteksi khusus dan tidak langsung terhubung dengan internet.

7. Monitoring & Logging Server

   Merekam aktivitas sistem, termasuk anomali, serangan siber, atau kegagalan akses. Diperlukan untuk analisis forensik jika terjadi insiden.

8. Backup Server Internal

   Menyimpan cadangan data secara berkala, diisolasi dari koneksi langsung ke publik agar tidak mudah disusupi ransomware.

9. Firewall Internal

   Mengatur lalu lintas antara DMZ dan jaringan internal pemerintah (intranet PEMDA) untuk mencegah akses tidak sah.

10. Intranet PEMDA (Internal Network)

    Sistem yang hanya bisa diakses oleh pegawai Pemkab Jombang. Memiliki aplikasi admin, manajemen pengguna, dan dashboard internal.

3.7 Teknik Analisis Resiko

Untuk mengubah temuan teknis mengenai kerentanan menjadi metrik risiko yang terukur, penelitian ini menggunakan pendekatan sistematis yang diadopsi dari kerangka kerja NIST SP 800-30. Proses ini melibatkan pendefinisian dua parameter utama—kemungkinan (likelihood) dan dampak (impact)—serta penggunaan matriks risiko untuk mengkategorikan tingkat keparahan setiap ancaman.

1. Definisi Parameter Risiko

Untuk memastikan penilaian yang konsisten, setiap parameter didefinisikan secara operasional sebagai berikut:

a Likelihood (Tingkat Kemungkinan) Parameter ini mengukur seberapa mudah sebuah kerentanan dapat dieksploitasi oleh penyerang.

1) Tinggi: Kerentanan sangat mudah ditemukan dan dieksploitasi, bahkan oleh penyerang dengan keahlian terbatas dan tanpa memerlukan alat khusus. Contoh: *Stored XSS* pada kolom komentar publik.
2) Sedang: Proses eksploitasi memerlukan kondisi tertentu, alat bantu khusus, atau tingkat keahlian menengah. Contoh: *Reflected XSS* yang memerlukan interaksi dari korban (misalnya, mengklik tautan).
3) Rendah: Eksploitasi sangat sulit dilakukan, memerlukan keahlian teknis yang sangat tinggi, akses internal, atau kondisi yang sangat spesifik yang jarang terpenuhi.

b Impact (Tingkat Dampak) Parameter ini mengukur besarnya kerugian atau konsekuensi negatif jika sebuah kerentanan berhasil dieksploitasi.

1) Tinggi: Eksploitasi dapat menyebabkan kerugian yang masif, seperti kebocoran seluruh data pengguna di database, pengambilalihan sistem sepenuhnya (*full system compromise*), atau terhentinya layanan publik secara total. Dampaknya mencakup kerugian finansial, reputasi, dan hukum yang signifikan.
2) Sedang: Menyebabkan kerugian yang terbatas, seperti kebocoran sebagian data non-kritis, manipulasi tampilan (defacement) pada halaman tertentu, atau penurunan kualitas layanan.

3) Rendah: Dampaknya minimal dan cenderung bersifat teknis, seperti kebocoran informasi konfigurasi server yang tidak sensitif atau gangguan minor yang tidak memengaruhi fungsionalitas utama sistem.

2. Perhitungan Risiko Menggunakan Matriks

Setelah setiap kerentanan dinilai berdasarkan tingkat likelihood dan impact-nya, tingkat risiko keseluruhan dihitung menggunakan matriks risiko. Matriks ini menggabungkan kedua parameter untuk menghasilkan kategori risiko yang menjadi dasar prioritas mitigasi, sebagaimana disajikan pada Tabel 4.7.

	Dampak Rendah	Dampak Sedang	Dampak Tinggi
Likelihood Tinggi	Sedang	Tinggi	Kritis
Likelihood Sedang	Rendah	Sedang	Tinggi
Likelihood Rendah	Rendah	Rendah	Sedang

Tabel 3. 1 Matriks Penilaian Resiko

Berdasarkan matriks ini, sebuah kerentanan seperti *Stored* XSS—yang memiliki *likelihood* Tinggi (mudah dilakukan) dan *impact* Tinggi (dapat mencuri data sesi admin)—akan dikategorikan sebagai risiko Kritis dan harus menjadi prioritas utama untuk diperbaiki. Pendekatan ini memastikan bahwa upaya perbaikan difokuskan pada celah keamanan yang paling berbahaya terlebih dahulu.