BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi memungkinkan organisasi untuk menghasilkan data *output* yang lebih baik dan mengambil langkah-langkah yang tepat dan efektif. Salah satu contoh perkembangan teknologi saat ini adalah *website*. Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023). Teknologi informasi tidak hanya media komunikasi saja, tapi sebagai media bertukar informasi. Karena informasi sangat dibutuhkan oleh semua orang, misalnya dalam bidang sistem informasi, informasi akan membantu perusahaan untuk menyusun rencana, sistem pendukung keputusan yang memungkinkan akses data bersifat penting untuk perusahaan dan mengidentifikasi peluang baru guna membawa bisnis berada di langkah yang tepat. Teknologi Informasi bisa menjadi fondasi dalam pengembangan suatu *website*. *Website* berfungsi sebagai wadah untuk komunikasi, media promosi, dan kumpulan informasi penting bagi pengguna. Selain itu, *website* merupakan alat alternatif yang dapat digunakan oleh banyak orang dari mana pun dan kapan pun.

Informasi merupakan salah satu aspek penting dalam sistem informasi suatu organisasi. Hal ini dikarenakan informasi memiliki peran strategis dalam meningkatkan nilai perusahaan. Salah satu aspek dalam menjaga nilai suatu perusahaan adalah dengan meningkatkan keamanan Informasi. Penting untuk menjaga keamanan informasi agar terhindar dari potensi ancaman dan risiko dari pihak luar. Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023). Dalam menjaga keamanan sistem informasi juga ada ancaman serius yang tidak bisa dilupakan. Penelitian oleh Fitri Nur Latifahi, Imron Mawardi, Bayu Wardhana yang berjudul "Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid – 19 (Study Phishing di Indonesia") mengatakan bahwa pencurian data merupakan masalah terbesar pertama yang menjadi ancaman serius bagi data pengguna. Latifah, F. N., Mawardi, I., & Wardhana, B. (2022).

Tindakan yang dilakukan untuk tujuan pribadi dengan menyebarkan pesan palsu kepada pengguna melalui media komunikasi. Husna, F. F., & Mustaqim, M. (2020). Tidak hanya itu ancaman *cyber* di Indonesia juga sangat tinggi. Hal ini menjadi faktor kejahatan pencurian data atau phising kerap terjadi. Badan Siber dan Sandi Negara

Republik Indonesia memaparkan bahwa pada kurun waktu Oktober 2023 telah terjadi serangan cyber sebesar 88 juta serangan *cyber* (B. S. dan S. N. R. Indonesia, 2020), oleh karena itu penting bagi semua orang untuk memahami dan waspada tindak kejahatan *phising* agar data pengguna tidak dicuri oleh pihak yang tidak bertanggung jawab. Sutarli, A. F., & Kurniawan, S. (2023).

Dalam perkembangannya, saat ini serangan *cyber* dan pencurian data semakin tinggi terjadi, menurut perusahaan saluran berita *Cable News Network* (CNN), pada tahun 2023 terjadi kasus kebocoran data yang berjumlah 35 kasus di Indonesia. Pada bulan Juni 2023 tercatat 15 kasus yang merupakan kasus tertinggi selama per bulannya. Kemudian kasus seorang *hacker* yang sempat menggemparkan Indonesia, kasus bjorka tentang dugaan peretasan data sensitif, diantaranya: 3,2 Miliar data Peduli Lindungi; 44,2 juta data dari aplikasi *My Pertamina*; 1,3 Miliar, dan 1,3 Miliar data registrasi SIM Card Kementerian Komunikasi dan Informatika (KOMINFO). (CNN Indonesia, 2023) Setelah itu, tidak lama terjadi lagi kasus pada Juni 2024 yaitu tentang pencurian data dengan cara menyerang sebuah situs milik Kominfo, yaitu kasus penyerangan siber terhadap *Server* Pusat Data Nasional (PDN) yang menyebabkan *server down* dan mengganggu layanan publik dari berbagai instansi serta imigrasi. Kejadian itu berlangsung selama 4 hari tanpa solusi untuk menangani kasus tersebut, sampai peretas meminta biaya tebusan sebesar 131 Miliar Rupiah untuk mengembalikan data PDN tersebut. Berdasarkan saluran berita dari CNBC Indonesia, peretas menggunakan virus *ransomware* versi update yaitu 3.0 dan sering disebut dengan *Lock bit*. *Ransomeware* sendiri merupakan *tools* yang dapat mengunci seluruh data dan mengubah data hingga tidak bisa di baca dan dimengerti oleh orang lain, kecuali peretas yang membuat enkripsi tersebut. (Bestari, 2024).

Dalam upaya meningkatkan keamanan sistem informasi harus diperlukan perhatian khusus, dengan tujuan mencegah ancaman terhadap sistem dan mendeteksi potensi kerusakan. Keamanan informasi mencakup beberapa aspek yang perlu dipahami dan dijaga. Aspek keamanan sistem informasi antara lain kerahasiaan *(Confidentiality),* yaitu memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki izin dan menjaga kerahasiaan data. Selain itu, integritas *(Integrity)* juga penting, yaitu memastikan akurasi informasi melalui pengolahan data yang terpercaya. Terakhir, ketersediaan *(Availability)* adalah memastikan bahwa informasi dapat diakses sesuai dengan kebutuhan.

Dinas Bupati M merupakan kantor yang bergerak pada bidang pemerintahan dalam tingkat kabupaten yang menjadi pusat administrasi dan tempat kerja Bupati dan jajaranya. Dinas Bupati M juga terintegrasi dengan Dinas Komunikasi dan Informatika M (DISKOMINFO) untuk pengelolaan semua informasi, komunikasi, serta teknologi informasi yang ada di Kabupaten M. Dari semua tugas Diskominfo ada salah satu pengelolaan yang bergerak pada bidang Teknologi Informasi, yaitu informasi berbasis modern yang berbasis *website*. Dinas komunikasi dan informatika Kabupaten M memiliki *website* sebagai situs yang dapat dikunjungi oleh semua kalangan masyarakat. *Website* tersebut adalah Sistem Informasi Kerjasama Media (XYZ) yang merupakan inovasi dari Dinas Komunikasi Dan Informatika Kabupaten M dalam rangka menjalankan tugas kerjasama media Pemerintah Kabupaten M dengan media *partner*, secara transparan, efektif dan efisien. Pada *website* XYZ terdapat beberapa fitur, yaitu daftar, masuk, verifikasi akun, upload kontrak. Selain itu, XYZ ini sudah terintegerasi dengan *database* milik Diskominfo Kabupaten M.

Database atau sering kita kenal sebagai basis data merupakan kumpulan semua data seperti angka, gambar, video maupun foto yang dikelola secara teratur dan mudah dikelola, diperbarui, diakses, oleh pihak Diskominfo Kabupaten M dengan cara yang efisien. Data seperti angka, gambar, video maupun foto merupakan data sensitif bagi para masyarakat dan sangat rentan untuk terjadinya pencurian data oleh pihak yang tidak bertanggung jawab. Dikarenakan krusialnya isi dari *database*, penting untuk dilakukan pengecekan keamanan *website* secara berkala. Berdasarkan hasil wawancara dari peneliti dengan Bapak Diding Adi selaku Kepala Bagian Divisi Teknologi Informasi Bupati Kabupaten M, diketahui bahwa tidak pernah dilakukan tindakan keamanan dari pihak Kominfo Kabupaten M dan pengecekan secara berkala serta permintaan dari objek sehingga perlu dilakukan analisis keamanan pada *website* XYZ. Hal ini dapat dilihat pada **Lampiran 6** Pertanyaan wawancara. Saat ini *website* XYZ belum pernah dilakukan uji keamanan, untuk meminimalisir terjadinya hal hal seperti serangan *cyber, exploit* sistem dan pencurian data. Maka peneliti akan melakukan pengujian terhadap keamanan *website* XYZ. Oleh karena itu peneliti menggunakan metode guna melakukan analisis keamanan *website* XYZ. Berdasarkan lampiran wawancara XYZ, dampak jika terjadi serangan *hacker* pada *website* XYZ adalah pencurian data sensitif yang mencakup data pada *database* milik DISKOMINFO,

kerugian pada sisi finansial serta adanya gangguan layanan yang sedang dijalankan oleh XYZ.

Pengujian keamanan *website* XYZ dilakukan dengan menggunakan metode *Web Penetration testing*. *Web Penetration testing* juga dikenal sebagai *pentest*, adalah tindakan di mana seseorang berupaya untuk melakukan serangan terhadap jaringan suatu organisasi atau perusahaan dengan tujuan mengidentifikasi potensi kelemahan dalam sistem tersebut. Hal ini merupakan praktik umum yang dilakukan oleh *ethical hacker* untuk memperkuat tingkat keamanan suatu sistem. Dalam konteks penelitian ini, akan dilakukan pengujian penetrasi terhadap aplikasi berbasis *web* dengan tujuan menemukan potensi kerentanan sebelum dapat dieksploitasi oleh pihak - pihak yang tidak bertanggung jawab, dan juga untuk membantu meningkatkan keamanan sistem. Pendekatan pentest dalam penelitian ini juga akan mengadopsi lima tahapan dari *ethical hacking*, yakni *Reconnaissance, Scanning & Enumeration, Gaining Access (Exploitation), Maintaining Access, Dan Covering Tracks*. Dalam melakukan *Penetration testing* peneliti membutuhkan sebuah *Framework* yang dapat membantu analisis keamanan *website* XYZ. *Framework* tersebut yaitu *ISSAF (Information Systems Security Assessment Framework).* Umar, R., Riadi, I., & Elfatiha, M. I. A. (2023)

Framework ISSAF merupakan sebuah kerangka kerja terstruktur yang memisahkan aspek keamanan sistem informasi ke dalam berbagai kategori dan penilaian yang khusus. Hal ini bertujuan untuk memberikan rekomendasi dan umpan balik berdasarkan alur kerja yang sesungguhnya, serta dapat digunakan sebagai panduan untuk memastikan keamanan sistem informasi. *Framework ISSAF* sendiri memiliki sembilan tahapan pengujian diantaranya *Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access, dan Covering Tracks*. Alasan peneliti memilih *Framework ISSAF* yaitu dikarenakan *Framework ISSAF* lebih sesuai dari pada *Framework OWASP* dalam sisi keamanan *website* XYZ. Oleh karena itu, peneliti memutuskan untuk melakukan uji keamanan keamanan *website* XYZ dengan menggunakan *Framework ISSAF* yang telah didukung dengan perbandingan *Framework* pada **Tabel 2.6** dan **Tabel 2.7.** Sutarli, A. F., & Kurniawan, S. (2023).

Dalam mengatasi masalah tersebut maka analisis keamanan dirasa sangat penting untuk dilakukan. Langkah yang dapat dilakukan adalah analisis keamanan pada *website* XYZ menggunakan metode *Penetration testing*. Hasil akhir dari penelitian ini diharapkan dapat mengetahui celah keamanan dan kelemahan dari *website* XYZ. Pemberian rekomendasi perbaikan teknis yang akan diberikan kepada Teknologi Informasi Kominfo Kabupaten M sebagai acuan dalam pengembangan atau peningkatan terhadap keamanan *website* XYZ sehingga dapat meminimalisir terjadinya pencurian data dan kejahatan *cyber*.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan permasalahan untuk penelitian ini adalah: Bagaimana keamanan sistem informasi pada *website* XYZ dapat dilakukan dengan baik. Rumusan permasalahan ini diturunkan ke sub-permasalahan yaitu:

a. Bagaimana proses layanan kerjasama media yang krusial untuk dilakukan pengetesan keamanan?
b. Apa saja kerentanan yang ditemukan dalam *website* XYZ serta apa saja penyebabnya?
c. Apa saja rekomendasi perbaikan agar dapat meningkatkan keamanan website XYZ?

1.3. Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mengetahui apa saja celah kerentanan dan apa penyebabnya dari *website* XYZ berdasarkan *Framework ISSAF*.

b. Memberikan rekomendasi perbaikan kerentanan pada *website* XYZ terhadap kejahatan *cyber*, pencurian data dari pihak yang tidak bertanggung jawab.

c. Menyusun re*port* kondisi keamanan yang berisikan hasil pengetesan keamanan, temuan kerentanan dan hasil evaluasi.

1.4. Batasan dan Asumsi Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan di atas, maka perlu adanya batasan - batasan masalah sebagai berikut:

a. Tingkat kerentanan *website* XYZ: penelitian ini akan difokuskan untuk menilai dan menentukan tingkat keamanan *website* XYZ terhadap potensi serangan cyber atau pencurian data.
b. Evaluasi serangan cyber dan upaya pencurian data: Penelitian ini akan berfokus menilai potensi serangan cyber dan upaya pencurian data dari pihak - pihak yang tidak bertanggung jawab.
c. Keamanan *website* XYZ: Hasil dari analisis ini dapat membantu memberikan rekomendasi perbaikan kepada pihak Teknologi Informasi Kominfo Kabupaten M dalam hal keamanan *website* XYZ,

Berikut adalah beberapa contoh asumsi penelitian terkait topik keamanan *website* XYZ:

a. Asumsi Keamanan Teknis: *Website* XYZ memiliki potensi kerentanan keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Database XYZ menyimpan data sensitif yang rentan terhadap ancaman pencurian jika tidak dilindungi dengan mekanisme keamanan yang memadai.
b. Asumsi Penggunaan *Framework ISSAF*: *Framework ISSAF* mampu memberikan panduan yang terstruktur dalam pengujian keamanan *website* untuk mengidentifikasi celah keamanan secara menyeluruh. Metode penetration testing berbasis *ISSAF* dapat mendeteksi berbagai jenis kerentanan dalam sistem informasi *website* XYZ.
c. Asumsi Manajemen Keamanan: Tidak adanya pengujian keamanan rutin meningkatkan risiko serangan siber terhadap *website* XYZ. Pihak pengelola *website* XYZ bersedia menerima rekomendasi hasil penelitian untuk meningkatkan keamanan sistem.
d. Asumsi Pengguna dan Data: Data yang dikelola oleh XYZ bersifat sensitif dan penting untuk operasional Pemerintah Kabupaten M serta harus dijaga kerahasiaannya. Pengguna *website* XYZ, termasuk media partner, mempercayai bahwa data yang mereka unggah akan aman dari ancaman kebocoran.

Asumsi ini menjadi landasan dalam proses penelitian untuk memastikan fokus dan relevansi pengujian keamanan yang dilakukan.

1.5. Manfaat Penelitian

Manfaat penelitian ini:

1. Peneliti mendapatkan wawasan serta pengetahuan lebih tentang pengujian keamanan menggunakan *penetration testing* dan *Framework ISSAF*.
2. Pembaca dapat menjadikan sebagai referensi pada penelitian selanjutnya mengenai pengujian keamanan sistem informasi dengan menggunakan *Framework ISSAF*.
3. Memberikan pemahaman mendalam tentang kondisi keamanan *website* XYZ sehingga dapat melakukan perbaikan sesuai dengan saran yang diberikan oleh peneliti.

1.6. Sistematika Penulisan

Dalam menyusun karya tulis ilmiah ini, agar dalam pembahasan terfokus pada pokok permasalahan dan tidak melebar ke masalah yang lain, maka penulis membuat sistematika penulisan karya tulis ilmiah sebagai berikut:

Bab I Pendahuluan

1.1 Latar Belakang

Menjelaskan pentingnya menjaga keamanan *website* XYZ sebagai sistem informasi strategis dan risiko yang dihadapi jika tidak dilakukan pengujian keamanan secara rutin.

1.2 Rumusan Masalah

Merumuskan masalah utama terkait potensi kerentanan dan keamanan *website* XYZ.

1.3 Tujuan Penelitian

Menjelaskan tujuan penelitian, seperti mengidentifikasi celah keamanan dan memberikan rekomendasi perbaikan.

1.4 Manfaat Penelitian

Menguraikan manfaat penelitian bagi Dinas Kominfo Kabupaten M dan sektor pemerintah lainnya.

Bab II Tinjauan Pustaka

2.1 *Website* dan Sistem Informasi

Membahas konsep dasar *website* dan sistem informasi serta penggunaannya di sektor pemerintahan.

2.2 Keamanan Sistem Informasi

Menjelaskan kenapa harus menjaga keamanan sistem informasi, termasuk ancaman yang mungkin terjadi.

2.3 *Framework ISSAF*

Menjelaskan *Framework ISSAF* sebagai metode pengujian keamanan *website*, mencakup tahapannya.

2.4 Penelitian Terkait

Membahas penelitian sebelumnya yang relevan dengan topik ini sebagai referensi

Bab III Metodologi Penelitian

3.1 Desain Penelitian

Menjelaskan pendekatan dan metode penelitian yang digunakan.

3.2 Objek Penelitian

Menguraikan objek penelitian, yaitu *website* XYZ.

3.3 Tahapan Pengujian Keamanan

Menguraikan langkah-langkah pengujian menggunakan *Framework ISSAF*, dari tahap awal hingga akhir.

Bab IV Hasil dan Evaluasi

4.1 Pengumpulan Data

Menyajikan pengumpilan data pengumpulan informasi yang bertujuan untuk memudahkan peneliti melakukan pengetesan keamanan pada *website* XYZ.

4.2 Pengolahan Data

Peneliti ini juga menyusun pengelolaan data dalam melakukan pengetesan keamanan sistem informasi dengan menggunakan *Framework ISSAF* dalam *website* XYZ.

Bab V Analisis dan Pembahasan

5.1 Verifikasi dan Validasi

Dalam penelitian ini juga dilakukan pengumpulan informasi yang bertujuan untuk memudahkan peneliti melakukan pengetesan keamanan *website* XYZ.

5.2 *Assessment*

Pada tahap Assestment ini adalah tahap ke 2 dari pelaksanaan 9 langkah pengujian keamanan *website* yang berdasarkan *Framework ISSAF*

5.3 *Reporting, Clean Up and Destroy Artefacts*

Merupakan tahap ketiga dalam *Framework ISSAF* yang dilakukan dalam penelitian ini.

Bab VI Kesimpulan dan Saran

5.1 Kesimpulan

Merangkum temuan utama penelitian, termasuk tingkat kerentanan keamanan *website* XYZ.

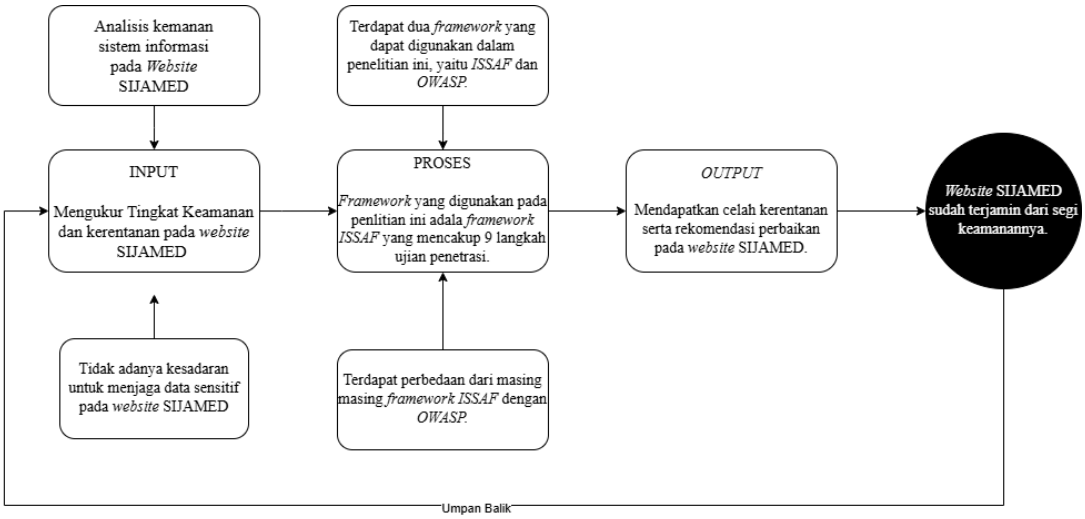
5.2 Saran

Memberikan saran untuk pengelola *website* XYZ dan pengembangan penelitian di masa depan.

1.7. Kerangka Berpikir

Kerangka berpikir merupakan pemikiran dasar peneliti yang disintesiskan dari tinjauan pustaka dan hasil penelitian yang relevan, observasi, kajian perpustakaan, atau narasi tentang kerangka bagaimana pemecahan masalah yang telah dirumuskan. Peirisal, T., & Hidayat, S. (2021, October). Pada penelitian ini terdapat *flowchart* kerangka berpikir, yaitu dimulai dengan menentukan topik, pada tahapan ini akan mencari masalah yang terjadi serta menghasilkan output sebuah pemberian saran perbaikan kepada objek. Kemudian ada batasan dan rumusan masalah, pada tahap ini akan dilakukan studi literatur pada jurnal, *website*, tugas akhir, buku. Setelah menentukan batasan dan rumusan masalah maka langkah selanjutnya yaitu pemilihan *Framework ISSAF* yang telah dipilih oleh peneliti dari perbandingan tabel *Framework* yang terdapat pada **Tabel 2.1** dan **Tabel 2.2**. Setelah dilakukan pemilihan *Framework*

serta dilakukannya uji penetrasi maka langkah selanjutnya adalah analisis serta kesimpulan dari penelitian ini.



Gambar 1. 1 *Flowchart Alur Kerangka Berpikir*