BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Penerapan teknologi informasi dalam pengelolaan data desa telah memungkinkan proses pengolahan informasi menjadi lebih cepat dan efisien. Salah satu inisiatif pemerintah yang mendukung pembangunan berbasis data di desa adalah adanya sistem informasi untuk mengelola data masyarakat dan Program Statistik Desa. Program ini bertujuan untuk meningkatkan kesadaran dan kemampuan aparatur desa dalam memanfaatkan data statistik sektoral secara optimal guna pengambilan keputusan yang lebih tepat terkait pembangunan desa. Melalui pemanfaatan data yang lebih akurat, diharapkan pembangunan desa dapat berjalan lebih efektif dan efisien, sehingga kesejahteraan masyarakat desa meningkat.

Keamanan siber telah menjadi isu yang sangat krusial di era digital, khususnya dalam melindungi data pribadi yang bersifat sensitif. Jika sistem keamanan tidak diperkuat, hal ini bisa membuka peluang bagi pihak yang tidak berwenang, atau pihak eksternal lainnya, untuk mengakses, mencuri, atau menyalahgunakan data tersebut. Dalam kasus sistem informasi desa ini, kelemahan dalam sistem login berpotensi menimbulkan risiko serius terhadap perlindungan data masyarakat.

Permasalahan keamanan data semakin diperhatikan seiring dengan beberapa insiden kebocoran data yang terjadi di tingkat nasional. Salah satu kasus yang menyoroti pentingnya perlindungan data adalah serangan ransomare pada Pusat Data Nasional (PDN) bulan Juni 2024 (Simorangkir et al., 2024). Serangan ini mengakibatkan sebagian data digital terkunci *(encrypted)* sehingga tidak dapat diakses oleh pengguna maupun pengelola layanan imigrasi. Selain itu, data penerima beasiswa di Kemendikbud juga terkena dampaknya, yang mengakibatkan kerugian mencapai nilai setara dengan 6,3 triliun rupiah (MetroTV, 2024). Penyebab utama serangan ini adalah rendahnya kepatuhan dan adanya kelalaian dalam menjaga password seperti

meminjamkan password ke pengguna lain (KumparanNews, 2024). Kejadian ini menunjukkan betapa pentingnya penerapan langkah-langkah keamanan yang lebih ketat, seperti pengelolaan password yang lebih ketat dan autentikasi berlapis untuk melindungi data sensitif dari akses yang tidak sah.

Berdasarkan hal kasus PDN tersebut, maka salah satu solusi untuk mengatasi kelemahan dalam sistem autentikasi satu faktor di sistem informasi ini adalah penerapan *Two-Factor Authentication* (2FA**)**. 2FA memberikan lapisan keamanan tambahan dengan mewajibkan pengguna untuk melakukan dua langkah verifikasi, sehingga meskipun password seseorang diketahui oleh pihak yang tidak berwenang, mereka tetap memerlukan verifikasi tambahan. Salah satu bentuk 2FA yang umum digunakan adalah melalui *One-Time Password* (OTP), yaitu kode verifikasi unik yang hanya berlaku untuk satu kali penggunaan dan dikirimkan melalui pesan singkat (SMS), email, atau platform pesan instan seperti WhatsApp. Pengiriman OTP melalui WhatsApp memberikan keuntungan karena infrastruktur yang andal dan pengalaman pengguna yang lebih nyaman, memungkinkan pengguna untuk menerima kode verifikasi secara cepat dan aman.

Selain itu, sistem keamanan yang kuat juga harus mencakup pembatasan waktu dan jumlah percobaan login yang salah. Hal ini penting untuk mencegah serangan *brute force*, di mana penyerang mencoba berbagai kombinasi password hingga menemukan yang benar. Dengan membatasi jumlah percobaan login yang salah dan menerapkan waktu tunggu setelah sejumlah percobaan yang gagal, risiko serangan dapat diminimalkan.

Untuk itu telah dilaksanakan penelitian dengan judul **"PENGEMBANGAN SISTEM KEAMANAN UNTUK MENINGKATKAN PERLINDUNGAN DATA PRIBADI PADA WEBSITE DESA"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, terdapat beberapa permasalahan yang diidentifikasi dalam penelitian ini, yaitu:

a. Bagaimana sistem keamanan login pada website saat ini.

b. Bagaimana kelemahan sistem keamanan login berkontribusi terhadap potensi serangan.

c. Bagaimana pengembangan sistem keamanan login berbasis *Two-Factor Authentication* (2FA) dengan penerapan *One-Time Password* (OTP) dapat meningkatkan keamanan website desa.

1.3 Batasan Masalah

Batasan atau Ruang Lingkup penelitian ini meliputi:

1. Penelitian ini dilakukan pada website desa versi V2.0.6.24.
2. Pengujian tidak di lakukan dengan menggunakan website aslinya melainkan hanya dengan menggunakan mockup.
3. Penelitian tidak ditujukan untuk membuat ulang website, melainkan ditujukan untuk memberikan rekomendasi pengembangan sistem keamanan yang ada.
4. Implementasi sistem keamanan yang direkomendasikan dilakukan pada mockup website aslinya karena website asli desa saat ini masih dalam masa penggunaan.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengidentifikasi kelemahan pada sistem login website desa yang saat ini hanya menggunakan autentikasi satu faktor (password), serta mengevaluasi risiko yang terkait dengan perlindungan data pribadi masyarakat.
2. Merancang dan mengembangkan sistem keamanan login yang dapat diterapkan pada website desa ini untuk meningkatkan keamanan akses dan melindungi data masyarakat dari potensi penyalahgunaan.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Adanya hasil analisa atas kerentanan yang dapat mengancam keamanan data pribadi masyarakat yang dikelola melalui sistem website desa.
2. Adanya usulan perbaikan dari celah keamanan pada sistem website desa tersebut.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penelitian ini sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang masalah, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian dan sistematika penulisan penelitian.

BAB II LANDASAN TEORI

Bab ini menjelaskan mengenai teori-teori pendukung penelitian yang akan dilakukan oleh penulis. Seperti teori mengenai keamanan sistem informasi, serangan terhadap sistem informasi, alat serta teknologi pengembangan mockup sistem keamanan website desa.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metode pendekatan yang digunakan untuk menyelesaikan permasalahan yang dirumuskan dalam analisis dan perancangan. Bab ini juga menguraikan tahapan yang diterapkan dalam membangun mockup sistem keamanan website desa, yaitu *Pre-Engagement, Intelligence Gathering, Threat Modeling,* dan *Vulnerability Analysis.*

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menyajikan hasil penelitian yang meliputi analisis dan pembahasan berdasarkan landasan teori yang relevan. Selain itu, bab ini juga memberikan gambaran mengenai pembangunan mockup sistem keamanan pada website desa, yang mencakup tahapan *Exploitation, Post-Exploitation,* dan *Reporting.*

BAB V KESIMPULAN DAN SARAN

Berisi suatu rangkuman dari keseluruhan hasil penelitian. Selain itu, penulis juga memberikan saran yang dapat digunakan oleh pengembang dalam melakukan mitigasi yang direkomendasikan sebelumnya yang berguna untuk perkembangan website desa ini kedepannya.