BAB 1

PENDAHULUAN

1.1 Latar Belakang

Penggunaan internet mengambil tempat yang penting dalam kehidupan sehari hari. Di era digitalisasi dan informasi saat ini, aplikasi web menjadi sesuatu yang penting [1]. Pada tahun 2018, Asosiasi Penyelenggara Jasa Internet Indonesia menyebutkan jumlah pengguna internet di Indonesia tahun 2018 adalah 64,8% dari jumlah penduduk Indonesia. Jumlah tersebut mengalami peningkatan dibandingkan tahun 2017 yakni 54,68%[2]. Sebuah laporan digital dari *We Are Social* menyoroti bahwa pengguna internet Indonesia mencapai 212,0 juta pada tahun 2023, yaitu setara dengan 77% total populasi di Indonesia[3].

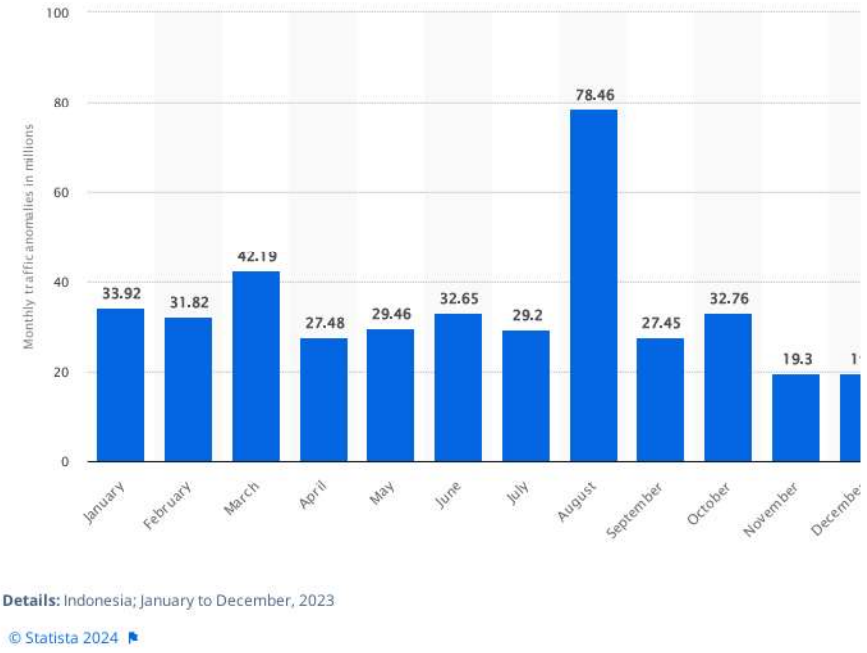
Situs web menjadi alternatif utama bagi perusahaan untuk berkomunikasi, promosi dan berinteraksi dengan khalayak [3]. Tidak hanya perusahaan seperti media berita, instansi pendidikan, sosial media. Pemerintah juga telah menerapkan *website* sebagai media untuk memudahkan penyebaran informasi kepada masyarakat luas. Dengan adanya *website* maka kualitas layanan dapat meningkat serta menyediakan peluang yang bagus agar masyarakat dapat berpartisipasi dalam proses demokrasi [4]

Mempertimbangkan data masyarakat yang dikumpulkan dan dikelola oleh pemerintah. Oleh karena itu keamanan data masyarakat perlu dijadikan perhatian lebih oleh pemerintah. Memastikan keamanan penggunaan internet dan sumber dayanya menjadi sangat penting melihat meningkatnya pengguna teknologi ini. Kebocoran data dapat mempengaruhi seseorang dalam hal reputasi, uang dan peluang kehilangan data [5]. Terkait dengan perlindungan data pribadi, Indonesia belum memiliki aturan khusus mengenai perlindungan data pribadi pada level undang-undang. Meskipun demikian, setidaknya terdapat 30 ketentuan perundang-undangan yang mengatur mengenai kewajiban untuk memberikan perlindungan data pribadi diindonesia[2].

Sayangnya masih banyak dugaan kasus kebocoran data yang bersumber dari *server* pemerintahan. Bocornya ratusan juta data pribadi warga Indonesia yang

dipegang oleh BPJS kesehatan[6], 337 juta data masyarakat yang diduga dikelola Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri bocor[7], 6 juta data pasien diduga bocor dan dijual di forum *online*[8].

Selain itu Badan Siber dan Sandi Negara atau dapat di singkat BSSN merangkum trafik anomali serangan siber di Indonesia pada 2023 dengan total 403.990.813 trafik. Hal ini membuktikan besarnya kemungkinan untuk terjadinya penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi[9].



Gambar 1.1 Grafik Anomali trafik yang terkait dengan serangan siber di Indonesia dari Januari hingga Desember 2023 https://www.statista.com/statistics/1423738/indonesia-monthly-traffic-anomalies-cyber-attacks/

Melihat banyaknya kasus kebocoran data dari server pemerintah dimana data masyarakan menjadi korban, maka perlu dilakukan analisis keamanan pada *website* agar dapat menjadi langkah awal pemerintah sebelum terjadinya eksploitasi celah keamanan *website* dari orang-orang yang tidak bertanggung jawab.

Sudagaran merupakan salah satu desa yang berlokasi di Kabupaten Banyumas, Provinsi Jawa Tengah, Indonesia. Desa Sudagaran menjadi salah satu desa yang menerapkan teknologi *website*. *Website* desa Sudagaran berlokasi di *internet* dengan domain sudagaran.desa.id. *Website* desa Sudagaran dikelola langsung oleh Dinas Komunikasi dan Informatika kabupaten Banyumas. *Website* desa Sudagaran lah yang akan menjadi objek penelitian ini.

Penelitian ini bertujuan untuk menguji serta menganalisis apakah *website* pemerintah yang dikelola Dinas Komunikasi dan Informatika kabupaten Banyumas yang secara spesifik ber*domain* sudagaran.desa.id, memiliki keamanan yang sesuai standar owasp top 10.

Penelitian dilakukan dengan metode penetration testing dan berusaha mengidentifikasi apa saja dari daftar OWASP top 10 2021 yang dimiliki oleh website sudagaran.desa.id, domain ini dipilih karena telah mendapat izin secara lisan dari dinas komunikasi dan informatika kabupaten banyumas. Pendekatan penetration testing yang digunakan adalah pendekatan black box.10 Daftar celah keamanan yang dirilis oleh *OWASP* akan dijadikan acuan sejauh mana *penetration testing* yang akan dilakukan.

1.2 Rumusan Masalah

Berdasarkan latar belakang. Penulis menetapkan beberapa masalah yang diidentifikasi dengan beberapa pertanyaan berikut:

1. Apakah sistem keamanan aplikasi web sudah sesuai dengan standar OWASP Top 10?
2. Apakah ada solusi mitigasi untuk setiap kerentanan yang ditemukan?

1.3 Tujuan Penelitian

Mempertimbangkan masalah kebocoran data dan besarnya tingkat trafik anomali di Indonesia. Perlu dipastikan apakah sistem web yang digunakan mampu menjaga keamanan data masyarakat. Maka tujuan dari adanya penelitian ini adalah untuk mengetahui seberapa jauh keamanan website desa Sudagaran yang dikelola oleh Dinas Komunikasi dan Informatika kabupaten Banyumas.

1.4 Batasan Masalah

agar penelitian dapat terfokus serta tidak melebar maka penulis menetapkan beberapa batasan dalam penelitian ini:

1. *Website* pemerintah yang diteliti adalah dari domain sudagaran.desa.id.
2. *Website* pemerintah yang diteliti merupakan *website* yang telah diberikan izin oleh pengelola *website.*
3. Kerentanan yang akan dianalisis adalah 10 kerentanan umum berdasarkan *OWASP Top 10* yang dapat di identifikasi melalui pendekatan blackbox..
4. Pengujian hanya menggunakan pendekatan black-box sehingga tidak mengidentifikasi ancaman internal.
5. Dalam melakukan *penetration testing,* penulis tidak melakukan *exploitasi* secara memaksa yang dapat berdampak terhadap penurunan kinerja *website* atau kehilangan data

1.5 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan dapat membantu pemerintah khususnya Dinas Komunikasi dan Informatika kabupaten Banyumas untuk mengetahui seberapa baik keamanan situs web yang dikelola dan dapat dijadikan acuan dalam pengembangan keamanan situs web yang dikelola oleh Dinas Komunikasi dan Informatika kabupaten Banyumas.