DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Meningkatnya penggunaan internet dari tahun ke tahun seiring dengan perkembangan pesat teknologi informasi dan komunikasi, termasuk website, menjadikan website sebagai salah satu media penting yang digunakan pemerintah untuk menyebarkan dan memperoleh informasi. Namun, perhatian khusus perlu diberikan terhadap keamanan dalam pengembangan website pemerintah, mengingat banyaknya kasus kebocoran data masyarakat yang bersumber dari server milik pemerintah. Hal ini dapat menurunkan kepercayaan masyarakat kepada pemerintah.

Website Desa Sudagaran yang dikelola oleh Kemendikbud menjadi objek penelitian ini untuk mengidentifikasi dan mengevaluasi tingkat keamanannya. Penelitian dilakukan menggunakan metode penetration testing dan mengacu pada OWASP Top 10, dengan langkah-langkah identifikasi kerentanan dan simulasi penyerangan pada kerentanan yang ditemukan.

Hasil implementasi menunjukkan adanya beberapa kerentanan, seperti SQL Injection, Cross-Site Scripting (XSS), dan kelemahan konfigurasi keamanan. Rekomendasi mitigasi mencakup penerapan header keamanan, validasi input, penggunaan HTTPS, dan pembaruan komponen yang usang. Implementasi langkah mitigasi ini diharapkan dapat meningkatkan keamanan website dan memulihkan kepercayaan masyarakat terhadap layanan berbasis digital.

Kata kunci: *owasp*, *penetration testing, website*, pemerintah, Banyumas

ABSTRACT

The increasing use of the internet from year to year along with the rapid development of information and communication technology, including websites, makes websites one of the important media used by the government to disseminate and obtain information. However, special attention needs to be given to security in the development of government websites, given the many cases of leakage of public data sourced from government-owned servers. This can reduce public trust in the government.

The Sudagaran Village website managed by the Ministry of Education and Culture is the object of this research to identify and evaluate its security level. The research was conducted using the penetration testing method and refers to the OWASP Top 10, with the steps of identifying vulnerabilities and simulating attacks on the vulnerabilities found.

The implementation results show the existence of several vulnerabilities, such as SQL Injection, Cross-Site Scripting (XSS), and security configuration weaknesses. Mitigation recommendations include implementing security headers, input validation, using HTTPS, and updating obsolete components. The implementation of these mitigation measures is expected to improve website security and restore public trust in digital-based services.

Keywords: owasp, penetration testing, website, government, Banyumas

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].

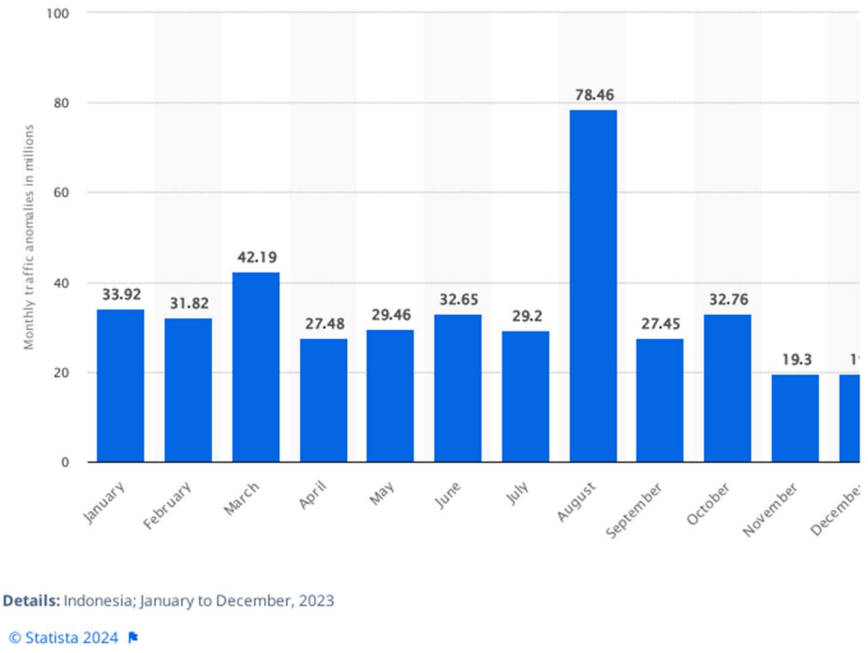
Situs web menjadi alternatif utama bagi perusahaan untuk berkomunikasi, promosi dan berinteraksi dengan khalayak [3]. Tidak hanya perusahaan seperti media berita, instansi pendidikan, sosial media. Pemerintah juga telah menerapkan *website* sebagai media untuk memudahkan penyebaran informasi kepada masyarakat 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.

BAB 2

TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Website pemerintah sewajarnya memiliki keamanan yang baik untuk melindungi data masyarakat yang dikumpulkan dan dikelola oleh pemerintah. Selain dugaan kasus kebocoran data masyarakan dari server pemerintahan, hasil pengujian Mantra dkk tentang tingkat kerentanan situs web dan tingkat kematangan keamanan situs web pada 33 situs web kampus di Jakarta, menunjukkan bahwa sekitar 60% dari total 33 situs web memiliki tingkat kematangan di bawah angka 3, yang menunjukkan bahwa tingkat kerentanan pada situs web di beberapa kampus di Jakarta masih tinggi[10].

Penetration testing yang semakin luas, membuat kebutuhan akan otomatisasi semakin diperlukan. Telah banyak alat yang dapat membantu otomatisasi dalam mengidentifikasi kerentanan web. Penelitian Yazeed Alkhurayif dkk menunjukkan manfaat alat penguji otomatis dalam identifikasi awal kerentanan web sehingga dapat meminimalisir kerugian perusahaan.

Standar keamanan diperlukan untuk menentukan apakah sebuah web dapat dikategorikan aman atau tidak. sehingga dalam penelitian Kiran Gandikota dkk menggunakan OWASP top 10 2021 untuk mengidentifikasi apakah website dikategorikan sebagai rentan atau tidak.

Tabel 2.1Penelitian Terkait

Penulis	**Variabel Penelitian**	**Metode analisis yang digunakan**	**Lokasi/ Objek penelitian**	**Hasil Penelitian**
I. G. N. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman [10]	tingkat kerentanan situs web dan tingkat kematangan keamanan situs web	Cyber security maturity model menggunakan alat uji kerentanan seperti Nessus dan Skipfish	33 situs web kampus di jakarta	Hasil pengujian menunjukkan bahwa sekitar 60% dari total 33 situs web memiliki tingkat kematangan di bawah angka 3, yang menunjukkan bahwa tingkat kerentanan pada situs web masih tinggi
P. S. S. Kiran Gandikota, D. Valluri, S. B. Mundru, G. K. Yanala, and S. Sushaini [11]	berbagai jenis kerentanan web aplikasi, dengan fokus pada kerentanan yang diidentifikasi oleh	evaluasi kerentanan, pengklasifikasian berdasarkan tingkat keparahan dan dampak potensial, serta pelaporan	Kerentanan aplikasi web yang telah diidentifikasi	Hasil penelitian menunjukkan perbandingan hasil alat scanning seperti

Penulis	Variabel Penelitian	Metode analisis yang digunakan	Lokasi/ Objek penelitian	Hasil Penelitian
	Open Web Application Security Project (OWASP).	dan perbaikan kerentanan yang ditemukan selama proses penilaian		burpsuite, nessus, openvas, wapiti.
F. Putri, Y. Utomo, and H. Kurniadi [12]	Keamanan pada website pemerintah kediri	*information gathering*, *vulnerability testing*, dan eksploitasi	website Pemerintah Kabupaten Kediri: kedirikab.go.id	Ditemukan beberapa port terbuka yang memungkinkan akses ke data sensitif (username, password) pada direktori tertentu. CVSS Base Score: 5.5 (level medium).
D. Hariyadi and F. E. Nastiti [13]	Keamanan web sistem informasi	Adopsi *Information Systems Security Assessment Framework*	sistem informasi berbasis web di	Ditemukan celah keamanan pada sub-domain tertentu,

DAFTAR LAMPIRAN

ABSTRAK

Meningkatnya penggunaan internet dari tahun ke tahun seiring dengan perkembangan pesat teknologi informasi dan komunikasi, termasuk website, menjadikan website sebagai salah satu media penting yang digunakan pemerintah untuk menyebarkan dan memperoleh informasi. Namun, perhatian khusus perlu diberikan terhadap keamanan dalam pengembangan website pemerintah, mengingat banyaknya kasus kebocoran data masyarakat yang bersumber dari server milik pemerintah. Hal ini dapat menurunkan kepercayaan masyarakat kepada pemerintah.

Website Desa Sudagaran yang dikelola oleh Kemendikbud menjadi objek penelitian ini untuk mengidentifikasi dan mengevaluasi tingkat keamanannya. Penelitian dilakukan menggunakan metode penetration testing dan mengacu pada OWASP Top 10, dengan langkah-langkah identifikasi kerentanan dan simulasi penyerangan pada kerentanan yang ditemukan.

Hasil implementasi menunjukkan adanya beberapa kerentanan, seperti SQL Injection, Cross-Site Scripting (XSS), dan kelemahan konfigurasi keamanan. Rekomendasi mitigasi mencakup penerapan header keamanan, validasi input, penggunaan HTTPS, dan pembaruan komponen yang usang. Implementasi langkah mitigasi ini diharapkan dapat meningkatkan keamanan website dan memulihkan kepercayaan masyarakat terhadap layanan berbasis digital.

Kata kunci: *owasp*, *penetration testing, website*, pemerintah, Banyumas

ABSTRACT

The increasing use of the internet from year to year along with the rapid development of information and communication technology, including websites, makes websites one of the important media used by the government to disseminate and obtain information. However, special attention needs to be given to security in the development of government websites, given the many cases of leakage of public data sourced from government-owned servers. This can reduce public trust in the government.

The Sudagaran Village website managed by the Ministry of Education and Culture is the object of this research to identify and evaluate its security level. The research was conducted using the penetration testing method and refers to the OWASP Top 10, with the steps of identifying vulnerabilities and simulating attacks on the vulnerabilities found.

The implementation results show the existence of several vulnerabilities, such as SQL Injection, Cross-Site Scripting (XSS), and security configuration weaknesses. Mitigation recommendations include implementing security headers, input validation, using HTTPS, and updating obsolete components. The implementation of these mitigation measures is expected to improve website security and restore public trust in digital-based services.

Keywords: owasp, penetration testing, website, government, Banyumas

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].

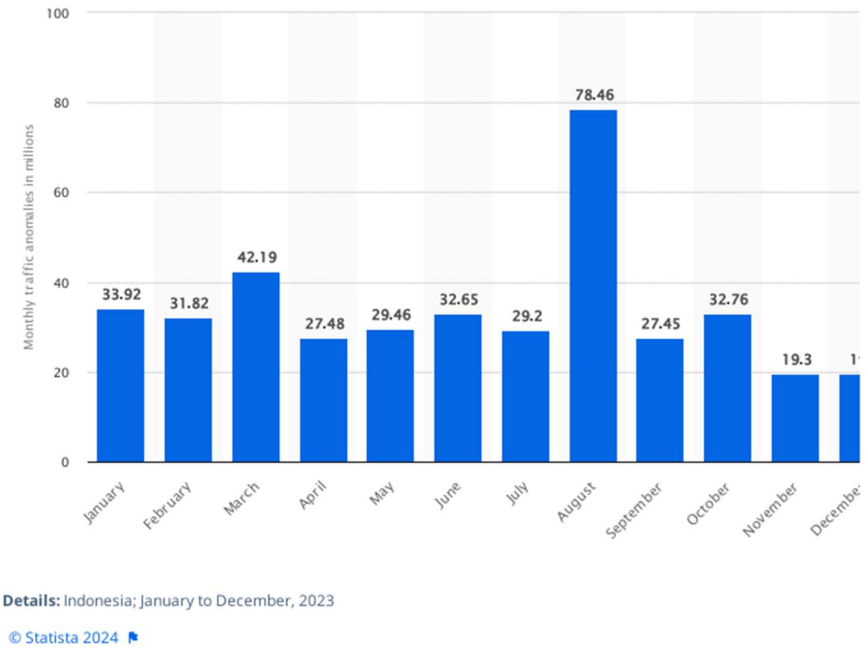
Situs web menjadi alternatif utama bagi perusahaan untuk berkomunikasi, promosi dan berinteraksi dengan khalayak [3]. Tidak hanya perusahaan seperti media berita, instansi pendidikan, sosial media. Pemerintah juga telah menerapkan *website* sebagai media untuk memudahkan penyebaran informasi kepada masyarakat 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.

BAB 2

TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Website pemerintah sewajarnya memiliki keamanan yang baik untuk melindungi data masyarakat yang dikumpulkan dan dikelola oleh pemerintah. Selain dugaan kasus kebocoran data masyarakan dari server pemerintahan, hasil pengujian Mantra dkk tentang tingkat kerentanan situs web dan tingkat kematangan keamanan situs web pada 33 situs web kampus di Jakarta, menunjukkan bahwa sekitar 60% dari total 33 situs web memiliki tingkat kematangan di bawah angka 3, yang menunjukkan bahwa tingkat kerentanan pada situs web di beberapa kampus di Jakarta masih tinggi[10].

Penetration testing yang semakin luas, membuat kebutuhan akan otomatisasi semakin diperlukan. Telah banyak alat yang dapat membantu otomatisasi dalam mengidentifikasi kerentanan web. Penelitian Yazeed Alkhurayif dkk menunjukkan manfaat alat penguji otomatis dalam identifikasi awal kerentanan web sehingga dapat meminimalisir kerugian perusahaan.

Standar keamanan diperlukan untuk menentukan apakah sebuah web dapat dikategorikan aman atau tidak. sehingga dalam penelitian Kiran Gandikota dkk menggunakan OWASP top 10 2021 untuk mengidentifikasi apakah website dikategorikan sebagai rentan atau tidak.

Tabel 2.1Penelitian Terkait

Penulis	**Variabel Penelitian**	**Metode analisis yang digunakan**	**Lokasi/ Objek penelitian**	**Hasil Penelitian**
I. G. N. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman [10]	tingkat kerentanan situs web dan tingkat kematangan keamanan situs web	Cyber security maturity model menggunakan alat uji kerentanan seperti Nessus dan Skipfish	33 situs web kampus di jakarta	Hasil pengujian menunjukkan bahwa sekitar 60% dari total 33 situs web memiliki tingkat kematangan di bawah angka 3, yang menunjukkan bahwa tingkat kerentanan pada situs web masih tinggi
P. S. S. Kiran Gandikota, D. Valluri, S. B. Mundru, G. K. Yanala, and S. Sushaini [11]	berbagai jenis kerentanan web aplikasi, dengan fokus pada kerentanan yang diidentifikasi oleh	evaluasi kerentanan, pengklasifikasian berdasarkan tingkat keparahan dan dampak potensial, serta pelaporan	Kerentanan aplikasi web yang telah diidentifikasi	Hasil penelitian menunjukkan perbandingan hasil alat scanning seperti

Penulis	Variabel Penelitian	Metode analisis yang digunakan	Lokasi/ Objek penelitian	Hasil Penelitian
	Open Web Application Security Project (OWASP).	dan perbaikan kerentanan yang ditemukan selama proses penilaian		burpsuite, nessus, openvas, wapiti.
F. Putri, Y. Utomo, and H. Kurniadi [12]	Keamanan pada website pemerintah kediri	*information gathering*, *vulnerability testing*, dan eksploitasi	website Pemerintah Kabupaten Kediri: kedirikab.go.id	Ditemukan beberapa port terbuka yang memungkinkan akses ke data sensitif (username, password) pada direktori tertentu. CVSS Base Score: 5.5 (level medium).
D. Hariyadi and F. E. Nastiti [13]	Keamanan web sistem informasi	Adopsi *Information Systems Security Assessment Framework*	sistem informasi berbasis web di	Ditemukan celah keamanan pada sub-domain tertentu,

Penulis	Variabel Penelitian	Metode analisis yang digunakan	Lokasi/ Objek penelitian	Hasil Penelitian
		(ISSAF) dengan tahapan *Information Gathering*, *Network Mapping*, dan *Vulnerability Identification*, menggunakan aplikasi Sudomy dan OWASP ZAP	Universitas Duta Bangsa Surakarta	termasuk potensi serangan web defacement dan rekomendasi untuk tindak lanjut dengan penetration testing.
L. F. Burhani and D. Priyawati[14]	Keamanan website pengelolaan internet	Menggunakan *metode Penetration Testing Execution Standard* (PTES), meliputi tahapan *Information Gathering*, *Threat Modelling*, *Vulnerability Scanning*,	internetkragan.com	Ditemukan 14 celah keamanan, beberapa dieksploitasi, seperti *Absence of Anti-CSRF Tokens*, *Clickjacking*, dan *Vulnerable JS Library*. *SQL Injection* tidak dapat dieksploitasi karena