**INFORMATIKA**
Fakultas Sains dan Teknologi
UniversitasLabuhanbatu
Vol. 12 No.2 / Mei/2024
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

# Analisis Keamanan Website Kecamatan Cibodas Tangerang Dengan Metode *Open Web Application Security Project*

**Janstipen Roy Mansen Sagala[1], Yusnia Budiarti[2], Rosi Kusuma Serli[3]**

Sistem Informasi, Fakultas Teknologi Informasi, Universitas Nusa Mandiri[1]
Informatika, Fakultas Teknologi Informasi, Universitas Nusa Mandiri[2,3]

Email: janstipenroy@gmail.com[1], yusnia.ybi@nusamandiri.ac.id[2], rosi.rsk@nusamandiri.ac.id[3]

*Corresponding Author*: yusnia.ybi@nusamandiri.ac.id

***Abstract***

*This research aims to conduct a security analysis on the website kec-cibodas.tangerangkota.go.id usingthe Open Web Application Security Project (OWASP) methodology. The findings indicate that the OWASP methodology is effective in identifying security vulnerabilities in the web-based application. Several significant results have been uncovered, revealing potential vulnerabilities that could be exploited by malicious actors.The primary findings of this research indicate that OWASP tools remain relevant and reliable as a foundation for website security testing, given the detection of several vulnerabilities. However, it is noted that the domain kec-cibodas.tangerang-kota.go.id is considered relatively secure from potential security threats.This research contributes significantly to understanding and enhancing website security by highlighting existing vulnerabilities and providing recommendations for necessary improvement measures. The results of this study are expected to serve as a basis for developing security policies and more effective preventive measures against potential attacks on the kec.cibodas.go.id website.*

***Keywords: website security, penetration testing, OWASP, security risk, analysis conclusion***

## I. Pendahuluan

Perkembangan cepat dalam ilmu teknologi, komunikasi, dan sistem pertahanan saat ini memberikan dampak signifikan terhadap perkembangan suatu negara. Seiring dengan kemajuan teknologi dan informasi, kita menyaksikan munculnya berbagai jenis konflik yang memanfaatkan jaringan dan informasi, membuka peluang untuk pertempuran dalam domain digital dan perang cyber, yang memiliki potensi untuk memengaruhi stabilitas sistem server(Zen et al., 2020).

Dalam era Internet dan World Wide Web, masalah keamanan sistem telah menjadi sangat penting dalam kerangka sistem informasi global yang menggunakan basis web. Hal ini tercermin dari tingginya komitmen para pakar keamanan sistem, komunitas riset, dan penyedia perangkat lunak(Hidayatulloh & Saptadiaji, 2021).

INFORMATIKA
Fakultas Sains dan Teknologi
UniversitasLabuhanbatu
Vol. 12 No.2 / Mei/2024
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

Keamanan dalam konteks era modern menjadi isu yang sangat krusial. Dengan meningkatnya kompleksitas ancaman siber dan potensi kerentanannya, keamanan menjadi prioritas utama bagi pemerintah, organisasi, dan individu. Kecamatan Cibodas, sebagai entitas pemerintahan, tidak terkecuali dari risiko ini. Dengan tugas dan fungsi untuk mengelola urusan pemerintah, ketertiban umum, ekonomi, dan pembangunan, website Kecamatan Cibodas memiliki peran penting untuk mendukung keberlanjutan tugas dalam konteks pemerintahan(Andriyani et al., 2023). Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi keamanan website Kecamatan Cibodas menggunakan Metode Open Web Application Security Project (OWASP) dengan metode selt test yaitu Penetration Testing(Fauzan & Syukhri, 2021).

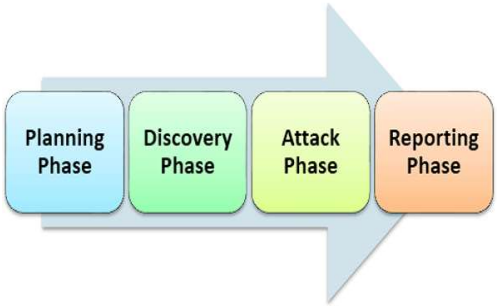
## II. Landasan Teori

OWASP (*Open Web Application Security Project*) adalah komunitas terbuka yang mendedikasikan untuk membuat sebuah organisasi yang bertujuan untuk mengembangkan, membeli, dan memelihara aplikasi yang terpercaya. Di OWASP pengunjung akan menemukan semua gratis dan terbuka. Seluruh *tools*, dokumen, forum, dan cabang OWASP bebas dan terbuka bagi semua orang yang tertarik memperbaiki aplikasi keamanan(Guntoro et al., 2020).

Metode *Penetration Testing* pada OWASP versi 4 Untuk Uji Kerentanan *Web Server* untuk mengamankan *web server* dari serangan *hacker* maka sebaiknya para pemilik *web server* melakukan *self test* terhadap *server* mereka sendiri. Melalui *self test* ini, para pemilik *web server* akan mengetahui letak kerentanan dari sistem yang ada. Salah satu metode *self test* ini adalah *penetration test*(Pohan, 2021). Metode ini sama dengan aktivitas *hacking* namun dilakukan secara legal.

### *Penetration Testing*

Uji penetrasi adalah serangkaian proses yang mencakup berbagai prosedur atau teknik evaluasi terhadap keamanan sistem website(Eko Prasetyo & Hassanah, 2021). Dengan melakukan percobaan serangan, tujuannya adalah untuk mengidentifikasi tempat-tempat yang rentan dalam sistem sehingga dapat segera ditutup atau diperbaiki. Uji penetrasi diterapkan sebagai langkah preventif untuk secara proaktif mengatasi potensi risiko peretasan pada suatu sistem.

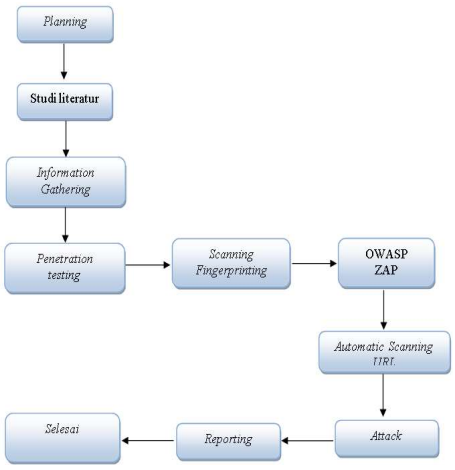



**Gambar 1. *Penetration Testing* Proses**

## III. Metode Penelitian

Metode yang digunakan dalam melaksanakan penelitian ini pada domain kec-cibodas.tangerangkota.go.id adalah dengan menggunakan metode kualitatif deskriptif dengan uji penetrasi. Proses ini melibatkan beberapa langkah, termasuk penilaian kerentanan dengan mengacu pada standarisasi OWASP pada uji penetrasi

INFORMATIKA
Fakultas Sains dan Teknologi
UniversitasLabuhanbatu
Vol. 12 No.2 / Mei/2024
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)




**Gambar 2. Tahapan Penelitian**

***Planning***

Pada fase perencanaan, ruang lingkup Penetration Testing akan didefinisikan. Hal ini mencakup menetapkan batasan dan tujuan pengujian, termasuk sistem yang akan diuji dan metode *self test* yang akan diterapkan.

**Studi Literatur**

Pada tahap ini, dilakukan evaluasi literatur dengan maksud untuk menyajikan review pustaka berdasarkan teori-teori yang mendukung, yang menjadi dasar dari penelitian ini. Data untuk analisis literatur diperoleh dari berbagai sumber, seperti buku, jurnal, artikel, dan sumber-sumber internet. Tujuan utama adalah memberikan gambaran yang komprehensif berdasarkan literatur yang ada untuk mendukung landasan penelitian.

Pada penelitian yang dilakukan oleh(Prasetyo & Lee, 2021) menyatakan bahwa pengujian keamanan terhadap website bertujuan untuk mengetahui serta menentukan serangan yang mungkin terjadi dan dilakukan terhadap kelemahan maupun celah pada sistem tersebut, dan mengetahui dampak bagi bidang bisnis yang diakibatkan oleh hasil eksploitasi data yang dilakukan oleh penyerang.

Berbeda dengan (Madani, 2024) yang menyatakan bahwasannya melakukan analisis celah keamanan merupakan salah satu bentuk deteksi dini terhadap ancaman di masa mendatang serta untuk menjamin confidentiality (kerahasiaan), integrity (konsistensi, akurasi, dan validitas data), availability (ketersediaan) atau biasa disebut dengan CIA Triad yang merupakan komponen dasar keamanan informasi. Celah keamanan dapat dijumpai dalam sebuah sistem maupun jaringan, salah satunya sistem aplikasi berbasis web.

Menurut(Armadhani et al., 2022) Pengujian penetrasi bukan hanya tentang menggunakan alat acak untuk memindai target untuk kerentanan, tetapi proses berorientasi detail yang melibatkan beberapa fase. Penetration testing membantu mengkonfirmasi efektivitas atau ketidak efektifan langkah-langkah keamanan yang telah dilaksanakan, sehingga sangat membantu developer agar tidak memberikan code yang berbahaya atau yang berpotensi untuk disusupi.

**Information Gathering**

Pada tahapan ini peneliti melakukan pengumpulan data dengan cara mengumpulkan informasi domain website, alamat email, kapan domain di daftarkan dan kapan domain kadaluarsa ,dengan cara ketik *who.is* digoogle lalu salin link dari website tersebut dan *paste* pada pencarian *who.is*.

**Penetration Testing**

Tahapan pengujian website menggunakan tools OWASP (*Open Web*

INFORMATIKA
Fakultas Sains dan Teknologi
UniversitasLabuhanbatu
Vol. 12 No.2 / Mei/2024
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

*Application Security Project). Website* yang diuji adalah website www.kec-cibodas.tangerangkota.go.id dimana hasil disesuaikan dengan menunjukan jenis, peringkat resiko, ancaman serta jumlah alert.

***Scanning Finger Printing***

Sebelum melakukan uji keamanan pada aplikasi OWASP maka terlebih dahulu dilakukan scanning fingerprinting untuk memverifikasi akses terhadap user yang berhak melakukan pengujian tersebut.

**OWASP ZAP**

Owasp zap merupakan software yang akan digunakan untuk menguji url website www.kec-cibodas.tangerangkota.go.id .

***Automatic Scanning URL***

Setelah memasukkan url website www.kec-cibodas.tangerangkota.go.id maka akan dilakukan self test terhadap url menggunakan penetration testing secara menyeluruh terhadap system.

***Attack***

Sistem akan menampilkan hasil scanning terhadap serangan yang diterima oleh system, serta menampilkan seluruh dampak resiko terhadap system yang dibagi dalam 4 kategori, yaitu : high, medium, low and informational.

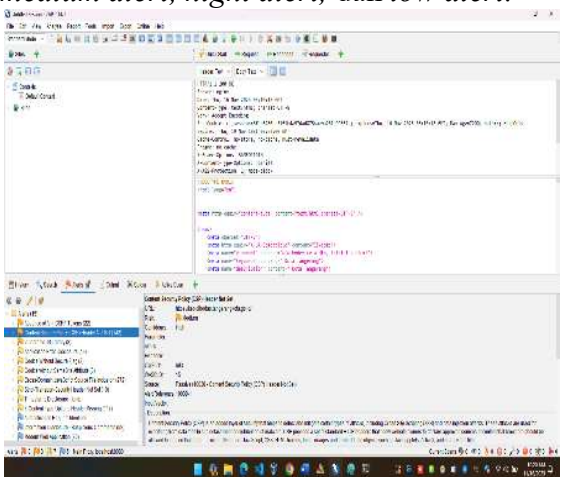
***Reporting***

Pada tahap akhir akan dibuat laporan, laporan tersebut mencakup langkah-langkah yang diambil, kerentanan keamanan yang terdeteksi dengan menggunakan parameter keamanan OWASP.

## IV. Hasil Dan Pembahasan

**Hasil Pengujian**

Setelah proses pemindaian pada website kec-cibodas.tangerangkota.go.id selesai dilakukan menggunakan *OWASP* terdapat beberapa alert yang dimana ada beberapa level kategori diantaranya : *medium alert, hight alert,* dan *low alert.*



**Gambar 3 . Hasil Pengujian Kerentanan**

Berikut adalah analisis hasil pengujian kerentanan terhadap website kec-cibodas.tangerangkota.go.id :

**Tabel 1. Hasil Uji Kerentanan Website**

| No | Alert | Risk | | Keterangan |
|---|---|---|---|---|
| | | Medium | Low | |
| 1 | *Absence of Anti-CSRF Tokens* | ✓ | | Untuk Keterangan *Medium Risk* pada Website Kecamatan Cibodas Tangerang, adalah tahap menghawatirkan dan harus segera untuk di perbaiki oleh pengelola Website Tersebut. |
| 2 | *Content Security Policy* | ✓ | | |
| 3 | *Vulnerable Js Library* | ✓ | | |
| 4 | *Application Error Disclosure* | | ✓ | Sementara pada Keterangan *Low Risk* pada Website Kecamatan Cibodas Tangerang masih cukup tergolong keadan rusak ringan |
| 5 | *Cookie Without Secure Flag* | | ✓ | |
| 6 | *Cookie Without Samesite Attribute* | | ✓ | |
| 7 | *Cross-Domain JS* | | ✓ | |
| 8 | *Strict-Transport Security* | | ✓ | |
| 9 | *Timestamp Disclosure Unix* | | ✓ | |

INFORMATIKA
Fakultas Sains dan Teknologi
UniversitasLabuhanbatu
Vol. 12 No.2 / Mei/2024
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

***Absence Of Anti CSRF Tokens***

Terdeteksi melalui aplikasi owasp zap, dapat terjadi disebabkan karena tidak adanya mekainsme perlindungan terhadap token keamanan, sehingga penyerang dapat mengirim suatu request secara ilegal.

***Content Security Policy***

Header atau meta tag untuk mengatur resource dari sumber mana saja yang diperbolehkan untuk dieksekusi oleh web browser, yang dimaksud resource seperti *javascript, css, font image, video, audio,* dan sebagainya. Penerapan content Security policy dapat dituliskan pada response header, berikut format penulisan header *content security Policy*.


**Gambar 4 . Perintah *Policy Directive***

***Vulnerable Java Script Library***

Menggunakan Java Script *Library* yang mengandung kerentanan dan berdampak terjadinya penyerangan.

***Application Error Disclosure***

Pada situasi ini dimana apliaksi atau website mengungkapkan informasi yang seharusnya tidak terlihat atau diakses oleh pengguna atau pihak yang tidak berwenang, Informasi yang bisa didapatkan mungkin mencakup pesan kesalahan sistem, stack trace,variable internal atau detail teknis lainya.

***Cookie Without Secure Flag***

Jika sebuah cookie tidak memiliki secure flag yang diatur, berarti cookie dapat dikirimkan melalui koneksi HTTP , ini berpotensi menimbulkan resiko keamanan, umumnya disarakan untuk mengatur secure flag pada cookie.

***Cookie Withput Samesite attribute***

Dalam hal ini, tidak adanya atribut *samesite* yang diatur, yang berarti browser akan memperlakukanya seperti "*Samesite=None"* secara default, oleh karena itu, cookie tersebut akan dikirimkan dengan permintaan dari situs yang sama dan situs lintas.

***Cross-Domain Java Script***

Dalam Hal ini berarti terdapat kerentanan pada javascript seperti pada html web dan css layout website.

***Script-Transport Security***

Dengan mengatur header pada *HSTS* pada server, situs web memberi informasi browser untuk selalu terhubung melalui protokol HTTPS selama jangka waktu tertentu.

***Timestamp Disclosure Unix***

Merupakan kerentanan yang disebabkan oleh tampilnya ifnromasi timestamp uni pada browser. Kerentanan ini dapat dimanfaatkan oleh penyerang sebagai sarana pengumpulan informasi untuk melakukan penyerangan.

**Hasil Rekomendasi**

Berikut adalah Beberapa Hasil Rekomendasi yang ada Pada Tabel dibawah ini :

INFORMATIKA
Fakultas Sains dan Teknologi
UniversitasLabuhanbatu
Vol. 12 No.2 / Mei/2024
2615-1855 (E-ISSN)
2303-2863 (P-ISSN)

**Tabel 2. Hasil Rekomendasi**

| No | Nama Sub File Sistem *Vulnerability* | Jumlah *Vulnerability* | Rekomendasi Perbaikan (*Countermeasure*) |
|---|---|---|---|
| 1 | *Absence Of-Anti CSRF Tokens* | 27 | Gunakan Anti CSRF Pada Form Login |
| 2 | *Content Security Policy* | 150 | Menyetel Kebijakan Keamanan Content |
| 3 | *Vulnerable Js Library* | 11 | Melakukanan Pembaharuan Versi *Bootstrap Versi 5.2* |
| 4 | *Application Error Disclosure* | 19 | Pertimbangkan untuk menerapkan mekanisme memberikan referensi / Pengenal |
| 5 | *Cookie Without Secure Flag* | 3 | Tambahkan Secure Flag ke dalam HTTP Header Response, sehingga cookie tidak akan dikirimkan oleh browser melalui permintaan HTTP yang tidak terenkripsi. |
| 6 | *Cross-Domain JS* | 326 | Pastikan bahwa file JavaScript asli berasal hanya dari sumber yang dapat dipercayai. dan tidak dapat dikontrol oleh aplikasi pengguna akhir. |
| 7 | *Strict-Transport Security* | 19 | Pastikan bahwa server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi Untuk menerapkan Strict Transport-Security |
| 8 | *Cookie Without Samesite Attribute* | 5 | Manfaatkan atribut Samesite agar browser dapat memberikan informasi mengenai kapan dan bagaimana cookie dari pihak kedua atau pihak ketiga diaktifkan. |
| 9 | *Timestamp Disclosure Unix* | 1 | Lakukan verifikasi secara manual untuk memastikan bahwa informasi waktu tidak bersifat sensitif, dan bahwa data tersebut tidak dapat digabungkan untuk mengidentifikasi pola yang dapat dimanfaatkan secara merugikan. |

## V. Kesimpulan Dan Saran

### Kesimpulan

Penelitian analisis keamanan website pada website www.kec-cibodas.tangerangkota.go.id telah dilakukan, hasil dari penelitian ini dapat diambil kesimpulan bahwa analisis keamanan pada aplikasi berbasi website dengan menggunakan metode OWASP telah terbukti mampu mengetahui kerentanan keamanan yang berada pada website tersebut, dan didapatkan hasil yang bisa mengacu pada kerentanan yang dapat diserang oleh orang yang tidak bertanggung jawab.

1. *OWASP* masih sangat cocok digunakan sebagai dasar dalam pengujian suatu website, karena masih bisa ditemukan beberapa kerentanan.
2. Kerentanan terhadap domain kec-cibodas.tangerang-kota.go.id masih tergolong cukup aman meskipun ada beberapa yang masuk dalam kategori *medium alert*

### Saran

Dan Berdasarkan penelitian yang sudah dilakukan, terdapat beberapa saran yang bisa diterapkan oleh tim *IT* kecamatan cibodas antara lain :

1. Perlunya dilakukan pengecekan secara berkala pada sistem keamanan *website*
2. Perlunya dilakukan pengecekan update secara berkala terhadap *javascript* dan *plugin* yang terdapat di web tersebut.
3. Perlunya dilakukan sistem *encryption* terhadap data yang penting.

## VI. Daftar Pustaka

Andriyani, S., Fajar Sidiq, M., & Parga Zen, B. (2023). Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar. *Journal*

*Informatic and Information Technology*, *2*(1), 1–13.

Armadhani, A. P., Nofriansyah, D., & Ibnutama, K. (2022). Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab esting Menggunakan Penetration Testing Standart OWASP. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *21*(2), 80. https://doi.org/10.53513/jis.v21i2.6119

Eko Prasetyo, S., & Hassanah, N. (2021). Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf. *Jurnal Ilmiah Informatika*, *9*(02), 82–86. https://doi.org/10.33884/jif.v9i02.3758

Fauzan, F. Y., & Syukhri. (2021). Analisis Metode Web Security PTES ( Penetration Testing Execution And Standart ) Pada Aplikasi E-Learning Universitas Negeri Padang dari keamanan web adalah sebanyak 96 dengan disimpulkan Acunetix Threat Level 2 yaitu pada level Medium yang artinya tidak. *Jurnal Vocational Teknik Elektronika Dan Informatika*, *9*(2).

Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(1), 45. https://doi.org/10.29100/jipi.v5i1.1565

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, *18*(1), 77–86. https://doi.org/10.33364/algoritma/v.18-1.827

Madani, M. A. (2024). Penetration Testing untuk Menguji Sistem Keamanan pada Website. *Jeitech (Journal of Electrical …*, *2*(1), 33–45.

Pohan, Y. A. (2021). Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar. *Jurnal Sistim Informasi Dan Teknologi*, *3*, 1–6. https://doi.org/10.37034/jsisfotek.v3i1.36

Prasetyo, S. E., & Lee, R. C. (2021). Analisis Keamanan Jaringan Pada Pay2home Menggunakan Metode Penetration Testing. *Teknik Informatika*, *1*(1), 710–718.

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. *Jurnal Teknologi Penginderaan*, *2*(1), 105–122.