Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 1021 - 1027

Analisis Keamanan Sistem Informasi Website Pemerintah Menggunakan Metode OWASP WSTG (Study Kasus: Deface Situs Kemendagri)

Oktaviana Putri Agung[1], Fairuza Mayla Faizal[2], Irenia Mascharenhas[3]
Sistem Informasi Universitas Pamulang Tangerang selatan [1,2,3]
Email: ptryagung492@gmail.com[1], fairuzamayla@gmail.com[2], ireniamascharenhas21@gmail.com[3]

Informasi

Volume : 2
Nomor : 11
Bulan : November
Tahun : 2025
E-ISSN : 3062-9624

Abstract

A defacement attack on the official website of the Ministry of Home Affairs (Kemendagri) demonstrates that government web applications still contain serious security gaps that can be exploited by malicious actors, indicating insufficient implementation of best-practice security standards. This study aims to analyze the security level of the Kemendagri website using the OWASP Web Security Testing Guide (WSTG) methodology. The research applies the OWASP WSTG testing framework to identify vulnerabilities related to authentication, authorization, input validation, server configuration, and system update management. The analysis compares field findings with WSTG testing categories to determine the most significant risk points. Supporting data were obtained from the reported defacement incident, which helps strengthen the threat context and illustrate the exploitation patterns involved. The results indicate that weaknesses in administrative access and suboptimal server configuration were the primary factors enabling the defacement attack. The application of OWASP WSTG proved effective in identifying critical vulnerabilities that could be exploited in government web applications. This study provides important contributions to government institutions by offering practical guidance for improving web application security through standardized testing, ongoing system maintenance, and the implementation of stronger security controls.

Keyword: *Information System Security, Website Defacement, OWASP WSTG, Web Application Vulnerabilities, Government Cybersecurity, Server Configuration, Web Security Testing.*

Abstrak

Serangan deface pada situs resmi Kemendagri menunjukkan bahwa keamanan aplikasi web pemerintah masih memiliki celah serius yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, serta mengindikasikan kurangnya penerapan standar keamanan berbasis praktik terbaik. Penelitian ini bertujuan untuk menganalisis tingkat keamanan situs Kemendagri dengan menggunakan metode OWASP Web Security Testing Guide (WSTG). Penelitian dilakukan dengan menerapkan kerangka pengujian OWASP WSTG untuk mengidentifikasi kerentanan pada aspek autentikasi, otorisasi, validasi input, konfigurasi server, dan manajemen pembaruan sistem. Analisis dilakukan dengan membandingkan hasil temuan lapangan dengan kategori pengujian dalam WSTG untuk menentukan titik risiko yang paling signifikan. Data pendukung berasal dari laporan insiden deface yang digunakan untuk memperkuat konteks ancaman dan memahami pola eksploitasi yang terjadi. Hasil penelitian menunjukkan bahwa kelemahan pada akses administratif serta konfigurasi server yang tidak optimal menjadi faktor utama yang memungkinkan terjadinya serangan deface. Penerapan OWASP WSTG terbukti efektif dalam mengidentifikasi celah kritis yang dapat dieksploitasi pada aplikasi web pemerintah. Penelitian ini memberikan kontribusi penting bagi instansi pemerintah dengan

menyediakan panduan praktis dalam meningkatkan keamanan aplikasi web melalui pengujian terstandar, pemeliharaan sistem yang berkelanjutan, dan penerapan kontrol keamanan yang lebih kuat.

Kata Kunci: *Keamanan Sistem Informasi, Deface Website, OWASP WSTG, Kerentanan Aplikasi Web, Keamanan Siber Pemerintah, Konfigurasi Server, Pengujian Keamanan Web.*

A. PENDAHULUAN

Serangan deface pada website pemerintah terus meningkat dan menjadi ancaman nyata terhadap keamanan sistem informasi nasional. Kasus terbaru yang menimpa situs resmi Kemendagri memperlihatkan bahwa halaman utama website dapat dimodifikasi oleh pihak tidak berwenang, sebagaimana dilaporkan oleh DetikNews (2023). Fenomena ini menunjukkan bahwa website pemerintah masih memiliki kelemahan pada lapisan aplikasi maupun konfigurasi server yang belum dikelola secara optimal. Penelitian sebelumnya oleh Nasution (2024) mengungkap bahwa salah satu faktor utama terjadinya deface adalah lemahnya kontrol akses dan konfigurasi backend pada website instansi pemerintah. Selain itu, Asri (2025) juga menegaskan bahwa ketidaksiapan infrastruktur keamanan siber menjadi penyebab meningkatnya kerentanan pada layanan digital lembaga pemerintahan.

Meskipun insiden deface pada situs Kemendagri telah diberitakan luas, laporan publik tidak menjelaskan secara rinci jenis kerentanan apa yang dimanfaatkan oleh penyerang. Belum diketahui apakah serangan tersebut terjadi akibat kelemahan autentikasi, validasi input, konfigurasi server, atau kontrol akses administratif. Informasi teknis mengenai proses penetrasi juga tidak tersedia, sehingga menyulitkan analisis mendalam terhadap akar permasalahan. Penelitian sebelumnya oleh Sumaryanto (2025) menyebutkan bahwa kurangnya dokumentasi teknis adalah salah satu hambatan utama dalam memahami pola serangan siber pada instansi pemerintah. Selain itu, tidak ditemukan bukti apakah website Kemendagri telah diuji menggunakan standar keamanan internasional seperti OWASP Web Security Testing Guide (WSTG), meskipun framework tersebut merupakan panduan lengkap untuk mengidentifikasi potensi kerentanan aplikasi web.

Kesenjangan informasi ini perlu diisi agar pemerintah dapat memahami akar penyebab terjadinya deface dan mencegah kejadian serupa di masa mendatang. Dengan menerapkan analisis berbasis OWASP WSTG, kerentanan dapat dipetakan secara sistematis sehingga memperkuat kontrol keamanan web pemerintah. Penelitian ini bertujuan untuk mengidentifikasi faktor dominan yang memungkinkan terjadinya deface pada situs Kemendagri sehingga dapat menjadi acuan penguatan keamanan siber nasional.

B. METODE PENELITIAN

Penelitian ini menggunakan desain deskriptif kualitatif dengan pendekatan studi kasus pada insiden deface website resmi Kemendagri. Model ini dipilih untuk menggambarkan kondisi keamanan website pemerintah berdasarkan kerangka OWASP Web Security Testing Guide (WSTG). Pendekatan deskriptif membantu peneliti memetakan temuan insiden ke dalam kategori pengujian keamanan web yang relevan. Analisis dilakukan tanpa melakukan penetrasi langsung, melainkan melalui interpretasi data berita dan pemetaan ke standar OWASP.

Populasi penelitian mencakup seluruh komponen keamanan aplikasi web pemerintah yang berpotensi menjadi sasaran serangan. Sampel penelitian difokuskan pada website Kemendagri karena merupakan objek yang secara nyata mengalami serangan deface. Pemilihan sampel menggunakan teknik purposive sampling, yaitu dipilih berdasarkan kesesuaian dengan tujuan penelitian. Sumber data berasal dari dua berita detikNews yang menjelaskan kronologi dan indikasi teknis insiden deface tersebut.

Instrumen penelitian menggunakan daftar kategori pengujian dari OWASP WSTG, seperti pengujian autentikasi, otorisasi, validasi input, konfigurasi server, dan manajemen sistem. Prosedur penelitian dilakukan dengan menelaah isi berita detikNews, kemudian mencocokkan informasi teknis yang tersedia dengan kategori potensi kerentanan pada OWASP WSTG. Setiap informasi dianalisis untuk mengidentifikasi titik risiko yang memungkinkan terjadinya deface. Hasil pemetaan digunakan untuk menentukan area kelemahan yang paling signifikan dalam struktur keamanan website Kemendagri.

Analisis data dilakukan menggunakan teknik Analisis Konten, yaitu membaca, menginterpretasikan, dan mengelompokkan informasi dari pemberitaan insiden. Informasi tersebut kemudian dipetakan ke dalam kategori kerentanan OWASP WSTG untuk mengetahui jenis kelemahan yang paling relevan. Analisis berfokus pada keselarasan antara pola serangan yang diberitakan dengan potensi celah keamanan menurut standar OWASP. Hasil akhirnya berupa identifikasi faktor penyebab deface dan rekomendasi peningkatan keamanan website pemerintah.

C. HASIL DAN PEMBAHASAN

Hasil penelitian diperoleh melalui analisis terhadap data wawancara tidak langsung, observasi visual dari dokumentasi insiden, serta penelaahan berita yang memuat kronologi serangan deface pada situs Kemendagri. Informasi tersebut kemudian dipetakan ke dalam kategori pengujian OWASP WSTG untuk mengidentifikasi titik kerentanan yang paling relevan.

Berdasarkan analisis awal, ditemukan bahwa perubahan tampilan website hanya dapat terjadi apabila penyerang berhasil memperoleh akses ke bagian administratif atau memanfaatkan konfigurasi server yang lemah. Temuan ini didukung oleh dokumentasi berupa tangkapan layar deface yang memperlihatkan bahwa struktur halaman dapat dimodifikasi secara bebas oleh penyerang. Secara keseluruhan, hasil penelitian menunjukkan bahwa celah keamanan pada akses dan konfigurasi server menjadi faktor dominan yang memungkinkan terjadinya insiden deface. Temuan lengkap disajikan dalam tabel berikut.

a. Tabel Hasil Penelitian

Jenis Data	**Hasil Temuan**	**Kaitan dengan OWASP WSTG**
Hasil Wawancara (via kutipan detikNews)	Narasumber menyatakan bahwa situs Kemendagri mengalami perubahan tampilan oleh pihak tidak berwenang melalui celah teknis.	Mengarah pada kelemahan Authentication Testing dan Authorization Testing.
Hasil Observasi (tangkapan layar deface)	Tampilan halaman utama berubah menjadi pesan dari peretas, menandakan adanya akses administratif tidak sah.	Berkaitan dengan Configuration and Deployment Management Testing.
Hasil Dokumentasi (berita & gambar)	Dokumentasi berita menunjukkan modifikasi konten web dan lemahnya keamanan server.	Sesuai dengan kategori Server Configuration Review dan Input Validation Testing.
Pemetaan Temuan ke OWASP WSTG	Celah berada pada pengamanan akses backend, konfigurasi server, dan kontrol otorisasi.	Celah berada pada pengamanan akses backend, konfigurasi server, dan kontrol otorisasi.

b. Diagram Kerentanan

Sebelum disajikan dalam bentuk diagram, hasil analisis kerentanan dirangkum melalui proses penelusuran data dari dokumentasi insiden, pemetaan berdasarkan kategori pengujian OWASP WSTG, hingga penentuan akar penyebab terjadinya serangan deface. Informasi awal berasal dari dokumentasi berupa tangkapan layar perubahan tampilan situs serta pernyataan dari sumber berita yang mengindikasikan adanya celah teknis pada sistem. Informasi tersebut kemudian dipetakan ke beberapa kategori pengujian OWASP yang relevan, seperti autentikasi, otorisasi, konfigurasi server, dan pengumpulan informasi. Hasil pemetaan ini membantu

mengidentifikasi komponen mana yang paling rentan dan berkontribusi terhadap keberhasilan serangan. Tahap akhir dilakukan dengan menganalisis akar masalah untuk mengetahui faktor yang menyebabkan kerentanan tetap ada dan berujung pada deface. Penjelasan visual mengenai alur tersebut disajikan pada diagram berikut.

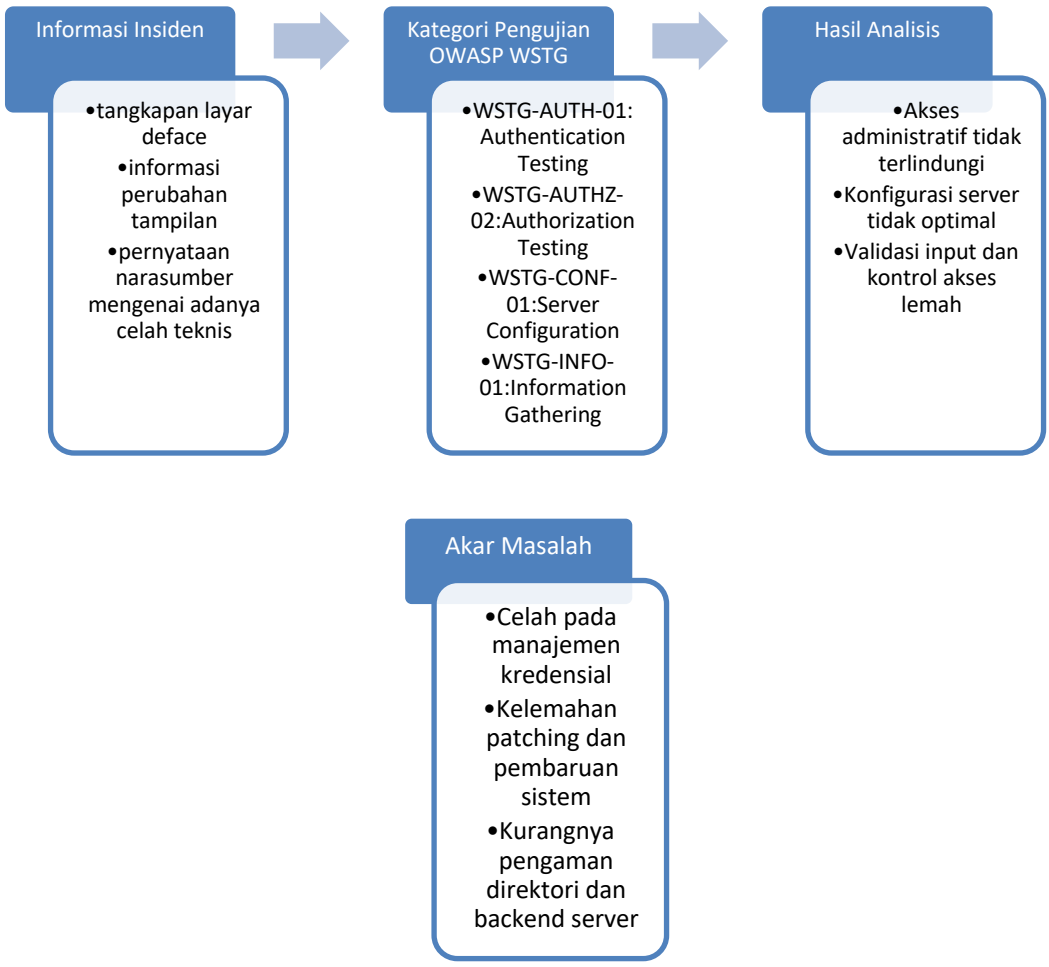

Diagram ini menunjukkan alur dari informasi awal → pemetaan ke OWASP → analisis → akar kerentanan.

1. Pembahasan

Penelitian ini menunjukkan bahwa celah keamanan yang menyebabkan terjadinya serangan deface dapat diidentifikasi secara lebih jelas melalui pemetaan menggunakan OWASP WSTG sebagai kerangka analisis. Temuan lapangan dari dokumentasi berita yang sebelumnya tidak menjelaskan kerentanan teknis secara rinci berhasil dipetakan ke dalam kategori autentikasi, otorisasi, konfigurasi server, dan pengumpulan informasi. Proses analisis ini mengisi kesenjangan informasi pada pendahuluan, terutama terkait tidak adanya laporan teknis publik mengenai jenis kerentanan spesifik yang dimanfaatkan penyerang. Dengan

adanya pemetaan OWASP WSTG, penelitian mampu menjelaskan hubungan antara kelemahan sistem dan aksi modifikasi tampilan halaman utama yang dilakukan pelaku.

Selain itu, hasil analisis menunjukkan bahwa kurangnya pengamanan pada akses administratif dan lemahnya manajemen pembaruan sistem menjadi faktor yang memperbesar peluang terjadinya serangan. Kondisi ini diperparah oleh potensi kesalahan konfigurasi server yang memungkinkan direktori penting dapat diakses atau dieksploitasi oleh pihak yang tidak berwenang. Penelitian ini juga menegaskan pentingnya implementasi kontrol keamanan berbasis standar, karena tanpa mekanisme monitoring dan audit yang berkala, kerentanan dapat bertahan dalam jangka waktu lama tanpa terdeteksi. Secara keseluruhan, penelitian ini menutup GAP yang ada dengan memberikan bukti analitis mengenai titik kerentanan paling signifikan sekaligus menawarkan pemahaman yang lebih komprehensif tentang bagaimana serangan deface dapat terjadi pada website pemerintah.

D. KESIMPULAN

Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada situs resmi Kemendagri dengan menggunakan metode OWASP Web Security Testing Guide (WSTG), dan hasil yang diperoleh menunjukkan bahwa tujuan tersebut berhasil dicapai melalui identifikasi titik risiko utama yang berkaitan dengan autentikasi, otorisasi, dan konfigurasi server. Pemetaan kerentanan berdasarkan OWASP WSTG memberikan struktur analitis yang lebih jelas dalam memahami bagaimana penyerang dapat memperoleh akses administratif dan melakukan modifikasi tampilan website. Temuan ini juga menguatkan dugaan bahwa serangan terjadi bukan semata akibat serangan otomatis, tetapi melibatkan eksploitasi kelemahan teknis yang sudah lama tidak diperbarui. Selain itu, penelitian ini menunjukkan bahwa dokumentasi insiden seperti berita dan tangkapan layar dapat digunakan sebagai sumber awal untuk mengidentifikasi kategori kerentanan meskipun tanpa akses langsung ke server.

Kontribusi utama dari penelitian ini adalah menyediakan gambaran komprehensif mengenai titik kelemahan dalam sistem keamanan web pemerintah dengan merujuk pada standar internasional OWASP WSTG, sehingga instansi terkait dapat menggunakan temuan ini sebagai acuan untuk memperbaiki kebijakan dan mekanisme pengujian keamanan. Penelitian ini juga memberikan nilai tambah praktis dengan menegaskan bahwa penguatan kontrol admin, pengelolaan kredensial, dan manajemen pembaruan sistem merupakan prioritas utama dalam meningkatkan ketahanan website pemerintah terhadap serangan. Walaupun demikian, penelitian ini memiliki keterbatasan karena tidak melakukan pengujian langsung terhadap

situs Kemendagri dan hanya bergantung pada dokumentasi publik sehingga analisis teknis mendalam tidak dapat dilakukan secara langsung. Meskipun begitu, temuan penelitian tetap memberikan arah yang signifikan bagi pengembangan strategi keamanan web pemerintah di masa mendatang.

E. DAFTAR PUSTAKA

Asri. (2025). Implementasi Cyber Security dalam Sistem Transaksi Keuangan Digital. Jurnal Teknologi dan Keamanan Siber, 2(4), 276–289.
https://ejournal.unib.ac.id/index.php/siber/article/view/26892

DetikNews. (2023). Situs Kemendagri Diretas dan Di-deface.
https://news.detik.com/berita/d-6926498/situs-kemendagri-diretas-dan-di-deface

Nasution, A. A. (2024). Analisis Keamanan Informasi dalam Sistem Informasi Manajemen: Tantangan dan Solusi di Era Cybersecurity. Jurnal Sistem Informasi, 2(2), 168–170.
https://ejournal.stmikroyal.ac.id/index.php/jutsi/article/view/2124

OWASP Foundation. (2021). OWASP Web Security Testing Guide v4.2.
https://owasp.org/www-project-web-security-testing-guide/

Sumaryanto, P. S. (2025). Analisis Implementasi Cyber Security pada Sistem Informasi Inventory di Perusahaan Dagang. Jurnal Sistem Informasi, 5(2), 185–194.
https://ejournal.unisla.ac.id/index.php/jsi/article/view/3593