JAITS: JOURNAL OF APPLIED INFORMATION TECHNOLOGY SOLUTION
Journal homepage: https://journal.universitasmulia.ac.id/index.php/jaits
ISSN:
Vol. 2 No.1 April 2025, Pg. 7 - 11

Tinjauan Keamanan terhadap Serangan Deface Website sebagai Bentuk Cybercrime

Brian Budi Aji[1*], Wahyu Nur Alimyaningtias[2], Muhammad Fahmi Abdillah[3], Dicky Satrio Ikhsan Utomo[4]
[1,2, 3,4] Teknologi Informasi, Universitas Mulia

Info Artikel
Kata Kunci:
Deface website
Cybercrime
SQL injection
Digital forensics
Keamanan web

Histori Artikel
Received 19 Desember 2023
Revised 27 April 2025
Accepted 30 April 2025
Available online 15 November 2025

*Corresponding Author
Brian Budi Aji
Email Address:
brianbudi@students.universitasmulia.ac.id

Abstrak
Perkembangan teknologi informasi yang pesat telah memberikan dampak besar terhadap kemudahan akses informasi dan komunikasi. Namun, kemajuan ini juga menimbulkan berbagai ancaman keamanan, salah satunya berupa kejahatan siber dalam bentuk website defacement. Tindakan deface website dilakukan oleh peretas dengan tujuan merusak atau mengubah tampilan halaman utama situs web untuk menodai reputasi organisasi, mengeksploitasi celah keamanan, atau menyampaikan pesan politik tertentu. Penelitian ini bertujuan untuk mengkaji bentuk dan teknik serangan deface website serta dampaknya terhadap keamanan sistem informasi. Metode yang digunakan adalah tinjauan sistematis terhadap berbagai literatur dan hasil penelitian sebelumnya terkait cybercrime dan keamanan web. Berdasarkan hasil kajian, ditemukan bahwa teknik serangan yang paling sering digunakan adalah SQL Injection, Remote File Inclusion (RFI), Local File Inclusion (LFI), dan Cross-Site Scripting (XSS). Serangan ini umumnya terjadi karena lemahnya validasi input, kesalahan konfigurasi server, serta kurangnya pembaruan sistem keamanan. Kasus deface pada situs resmi DPR RI tahun 2020 menjadi contoh nyata bahwa lemahnya keamanan situs dapat dimanfaatkan oleh pelaku untuk menyampaikan aspirasi maupun melakukan tindakan ilegal. Hasil penelitian ini menegaskan pentingnya penerapan sistem keamanan berlapis dan peningkatan kesadaran keamanan siber guna mencegah serangan serupa di masa mendatang.

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mengubah cara manusia berinteraksi, bertransaksi, dan mengelola informasi di berbagai bidang, mulai dari pemerintahan, bisnis, hingga Pendidikan [1], [2]. Kemudahan akses digital dan keterhubungan sistem informasi memberikan efisiensi tinggi, tetapi di sisi lain juga memunculkan ancaman serius berupa kejahatan siber (cybercrime) yang terus berevolusi dari waktu ke waktu [3]. Cybercrime mencakup berbagai bentuk pelanggaran hukum berbasis teknologi seperti peretasan, pencurian data, penipuan digital, hingga serangan terhadap situs web organisasi publik dan swasta [4].

Salah satu bentuk kejahatan siber yang sering terjadi adalah serangan deface website — tindakan ilegal yang dilakukan oleh peretas untuk mengubah tampilan antarmuka situs web tanpa izin dari pemilik atau administratornya [5]. Umumnya, pelaku defacement melakukan modifikasi pada halaman utama dengan menambahkan pesan tertentu, simbol, atau gambar yang berisi provokasi, protes politik, maupun klaim identitas kelompok peretas [6]. Meski sering dianggap sebagai serangan ringan, defacement dapat menimbulkan dampak yang serius terhadap reputasi organisasi, kepercayaan publik, serta keamanan data di balik sistem web [7].

Secara teknis, web defacement merupakan hasil dari eksploitasi terhadap kerentanan keamanan aplikasi web, seperti SQL Injection, Cross-Site Scripting (XSS), Remote File Inclusion (RFI), dan Local File Inclusion (LFI) [8], [9]. Serangan ini memanfaatkan kelemahan pada mekanisme validasi input, kesalahan konfigurasi server, dan kurangnya pembaruan sistem keamanan [10]. Studi yang dilakukan oleh [11] menunjukkan bahwa serangan defacement terhadap situs sebagian besar disebabkan oleh lemahnya sistem autentikasi dan pengelolaan server.

Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, lebih dari 361 juta anomali trafik yang berpotensi sebagai serangan siber terdeteksi di Indonesia, di mana sebagian besar berupa serangan web-based dan application-layer attack. Serangan defacement bahkan menjadi salah satu insiden paling umum di domain pemerintah (.go.id) dan institusi pendidikan, dengan ratusan kasus setiap tahun. Misalnya, pada tahun 2020 situs web resmi Dewan Perwakilan Rakyat Republik Indonesia (DPR RI) sempat diretas oleh pihak tak dikenal yang mengganti tampilan halaman utama dengan pesan politik. Kasus serupa juga menimpa situs pemerintah daerah dan lembaga pendidikan, menandakan bahwa keamanan siber di Indonesia masih lemah pada tingkat aplikasi web.

Selain aspek teknis, terdapat pula dimensi hukum dan sosial dalam fenomena web defacement. Dari sisi hukum, tindakan ini termasuk pelanggaran terhadap Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), khususnya pasal 32 dan 48, yang melarang perubahan, perusakan, atau penghapusan informasi elektronik milik orang lain tanpa

hak. Dari sisi sosial, defacement sering kali digunakan sebagai media hacktivism — bentuk protes digital untuk menyuarakan ketidakpuasan terhadap kebijakan atau isu tertentu, sebagaimana ditemukan dalam kasus peretasan situs-situs pemerintah pada masa pandemi.

Oleh karena itu, perlu dilakukan tinjauan keamanan (security review) yang komprehensif untuk memahami pola, teknik, dan dampak dari serangan deface website sebagai salah satu bentuk cybercrime yang paling sering terjadi di Indonesia [12], [13]. Tinjauan ini tidak hanya bertujuan mengidentifikasi kerentanan teknis, tetapi juga memberikan pandangan tentang bagaimana organisasi dapat membangun strategi pertahanan yang efektif melalui penerapan layered security, vulnerability assessment, serta peningkatan kesadaran keamanan siber di kalangan pengembang dan administrator web [14].

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada tinjauan keamanan terhadap serangan deface website sebagai bentuk cybercrime, dengan tujuan untuk mengidentifikasi pola dan teknik serangan yang umum digunakan pelaku, menganalisis faktor-faktor penyebab utama kerentanan situs web, dan memberikan rekomendasi langkah preventif untuk memperkuat keamanan web di lingkungan digital yang semakin kompleks..

2. Metode

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode tinjauan literatur (literature review) dan analisis komparatif terhadap berbagai sumber terkait keamanan siber dan serangan deface website. Pendekatan ini dipilih karena topik penelitian berfokus pada pemetaan konsep, pola serangan, serta strategi mitigasi yang digunakan untuk mencegah kejahatan siber dalam bentuk web defacement. Langkah-langkah penelitian dilakukan melalui beberapa tahapan berikut:

2.1 Identifikasi dan Pengumpulan Literatur

Mengumpulkan sumber pustaka terkait cybercrime, keamanan web, serta studi kasus defacement dengan kriteria relevansi terhadap topik penelitian.

2.2 Klasifikasi dan Seleksi Data

Menyeleksi literatur berdasarkan jenis serangan, teknik eksploitasi (misalnya SQL Injection, RFI, XSS), dan konteks kejadian (nasional/internasional).

2.3 Analisis Komparatif

Melakukan analisis terhadap hasil temuan dari berbagai literatur untuk menemukan pola serangan dan celah keamanan yang umum dimanfaatkan pelaku defacement:

2.4 Tinjauan Keamanan (Security Review)

Mengkaji langkah mitigasi yang diterapkan dalam studi terdahulu, serta membandingkannya dengan standar keamanan web modern seperti OWASP Top 10, ISO/IEC 27001, dan rekomendasi BSSN mengenai tata kelola keamanan siber nasional:

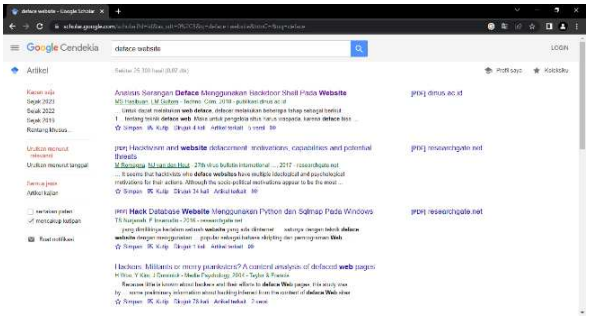
2.5 Sintesis dan Rekomendasi

Menyusun hasil analisis menjadi kesimpulan konseptual yang memuat pola serangan, penyebab utama, dan langkah strategis dalam mencegah serangan defacement di masa depan

3. Hasil dan Pembahasan

3.1 Analisis Kasus Serangan Deface Website

Hasil pengamatan terhadap kasus deface website menunjukkan bahwa serangan ini umumnya diawali dengan eksploitasi terhadap celah keamanan aplikasi web yang tidak diperbarui secara berkala (unpatched vulnerabilities). Berdasarkan hasil tangkapan layar (Gambar 1), tampilan utama situs yang telah diserang menampilkan pesan yang dimodifikasi oleh pelaku, sering kali memuat simbol atau teks yang menunjukkan identitas kelompok peretas (hacker signature).



Gambar 1. Pencarian Jurnal di Google Schoolar

JAITS: JOURNAL OF APPLIED INFORMATION TECHNOLOGY SOLUTION
Journal homepage: https://journal.universitasmulia.ac.id/index.php/jaits
ISSN:
Vol. 2 No.1 April 2025, Pg. 7 - 11

Fenomena ini sejalan dengan penelitian [4], [7] yang menyatakan bahwa defacement sering dilakukan sebagai bentuk unjuk eksistensi atau protes digital terhadap institusi tertentu. Dalam konteks kasus di Indonesia, situs pemerintah, lembaga pendidikan, dan organisasi publik menjadi sasaran utama karena infrastruktur keamanannya cenderung tidak diperkuat oleh sistem Web Application Firewall (WAF) atau Intrusion Detection System (IDS) yang memadai [9], [11]..

3.2 Teknik dan Mekanisme Serangan

Berdasarkan hasil penelusuran, pelaku deface website umumnya memanfaatkan beberapa teknik umum, antara lain:

- SQL Injection (SQLi) — memanfaatkan kesalahan validasi input pada parameter query basis data untuk memperoleh akses administratif dan mengubah konten web.
- Cross-Site Scripting (XSS) — menyisipkan skrip berbahaya pada halaman web untuk mengubah tampilan atau mengeksekusi perintah tertentu di sisi pengguna.
- Remote File Inclusion (RFI) — menyisipkan file eksternal berisi malicious script agar server mengeksekusi kode secara tidak sah.

Hasil eksploitasi yang dilakukan pada direktori file web, di mana pelaku berhasil menanamkan file index.html baru berisi tampilan hasil defacement. Pola ini menunjukkan bahwa akses pelaku umumnya diperoleh melalui kesalahan konfigurasi izin (file permission) atau penggunaan kredensial lemah pada panel cPanel atau CMS WordPress.

3.3 Dampak terhadap Keamanan dan Reputasi

Dampak utama dari serangan deface website tidak hanya berupa perubahan tampilan visual, tetapi juga mencakup:

- Kerugian Reputasi: Situs resmi yang diretas kehilangan kredibilitas di mata publik, terutama bagi lembaga pemerintahan dan akademik.
- Gangguan Operasional: Dalam beberapa kasus, sistem web yang diserang mengalami downtime cukup lama karena proses pemulihan membutuhkan waktu verifikasi integritas data.
- Potensi Kebocoran Data: Pelaku sering kali meninggalkan backdoor untuk melakukan serangan lanjutan seperti pencurian data atau penyebaran malware.

Hasil pengamatan ini yang mencatat peningkatan signifikan pada serangan berbasis aplikasi web di Indonesia, dengan defacement menempati posisi tiga besar insiden yang paling banyak terjadi.

3.4 Analisis Forensik Digital terhadap Serangan Deface

Analisis digital forensik yang dilakukan terhadap kasus defacement (Gambar 3 dan Gambar 4 dalam artikel) menunjukkan adanya pola umum pada file log server:

- Aktivitas anomali pada access.log sekitar waktu kejadian.
- Akses berulang dari IP address asing (non-lokal).
- Pengunggahan file berformat .php, .html, dan .js yang tidak sesuai dengan struktur awal situs.

Hasil analisis log memperkuat dugaan bahwa serangan dilakukan melalui eksploitasi remote inclusion dan kemudian pelaku menanamkan file tampilan baru untuk mengganti halaman utama situs. Data log juga digunakan untuk menelusuri jejak waktu (timestamp) dan metode akses (GET/POST), sehingga dapat menjadi dasar identifikasi digital sesuai dengan prosedur Computer Forensic Investigation.

3.5 Strategi Mitigasi dan Pencegahan

Berdasarkan hasil studi dan temuan lapangan, beberapa langkah mitigasi disarankan untuk mencegah serangan serupa, yaitu:

- Penerapan Patch Management secara rutin terhadap CMS, plugin, dan server web.
- Penguatan Autentikasi dengan menerapkan multi-factor authentication (MFA) bagi administrator.
- Implementasi Web Application Firewall (WAF) untuk mendeteksi dan memblokir pola serangan berbasis injeksi.
- Audit Keamanan Berkala melalui vulnerability assessment dan penetration testing sesuai rekomendasi OWASP Top 10.
- Peningkatan Kesadaran Keamanan (Security Awareness) di kalangan pengelola situs agar tidak menggunakan kredensial lemah dan rutin melakukan pencadangan data.

Strategi ini menekankan pentingnya pendekatan berlapis (defense in depth) dalam sistem keamanan siber modern. Dengan penerapan langkah-langkah tersebut, risiko terjadinya web defacement dapat diminimalkan, sekaligus meningkatkan ketahanan digital lembaga terhadap ancaman siber..

4. Kesimpulan

Serangan deface website merupakan salah satu bentuk kejahatan siber yang paling sering terjadi di Indonesia dan memberikan dampak serius terhadap reputasi, keamanan data, serta kepercayaan publik terhadap sistem informasi daring. Berdasarkan hasil kajian dan analisis pada beberapa kasus nyata, termasuk pengamatan terhadap tampilan situs yang telah

diserang, dapat disimpulkan bahwa pola utama serangan defacement terjadi karena kerentanan pada konfigurasi sistem, kelemahan autentikasi, dan tidak diterapkannya pembaruan keamanan secara berkala pada server maupun aplikasi web. Secara teknis, pelaku umumnya memanfaatkan teknik seperti SQL Injection, Cross-Site Scripting (XSS), dan Remote File Inclusion (RFI) untuk memperoleh akses tidak sah dan mengganti tampilan halaman utama situs. Analisis terhadap log server menunjukkan adanya pola aktivitas mencurigakan berupa unggahan file asing, akses berulang dari alamat IP luar negeri, dan perubahan file sistem yang tidak terotorisasi. Hal ini menegaskan bahwa lemahnya vulnerability management dan absennya sistem deteksi dini menjadi penyebab utama keberhasilan serangan. Dari sisi forensik digital, hasil investigasi memperlihatkan bahwa bukti digital yang terekam pada log file dan direktori server sangat penting untuk menelusuri jejak pelaku dan membuktikan tindak pidana siber. Oleh karena itu, penerapan standar digital evidence handling menjadi kunci untuk mendukung proses hukum yang sah dan valid. Untuk mencegah terulangnya insiden serupa, diperlukan strategi pertahanan siber yang menyeluruh melalui penerapan konsep keamanan berlapis (defense in depth), mencakup patch management, Web Application Firewall (WAF), multi-factor authentication (MFA), serta audit keamanan berkala mengacu pada standar OWASP Top 10 dan ISO/IEC 27001. Selain itu, peningkatan kesadaran keamanan bagi pengelola situs dan pelatihan teknis bagi administrator menjadi langkah strategis dalam membangun ketahanan digital organisasi. Dengan demikian, dapat disimpulkan bahwa penanganan deface website tidak hanya membutuhkan pendekatan teknis, tetapi juga kebijakan keamanan yang terintegrasi antara aspek teknologi, prosedur operasional, dan kesiapan sumber daya manusia. Penelitian ini diharapkan dapat menjadi referensi bagi institusi pendidikan, lembaga pemerintah, maupun penegak hukum dalam memperkuat keamanan siber nasional dan mengurangi risiko serangan serupa di masa mendatang.

Referensi

[1] G. Guntoro, L. Costaner, and M. Musfawati, “ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING),” *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, Jun. 2020, doi: 10.29100/jipi.v5i1.1565.

[2] A. Wijayanto, “Mengenal Cybersecurity: Perlindungan Data Pribadi Dan Privasi Di Sma Negeri 1 Samboja,” *J. Mulia*, vol. 3, no. 2, pp. 165–172, 2024, doi: 10.47002/jpm.v3i2.867.

[3] A. Djenna, S. Harous, and D. E. Saidouni, “Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure,” *Appl. Sci.*, vol. 11, no. 10, p. 4580, May 2021, doi: 10.3390/app11104580.

[4] D. Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, D. N. Akhtar, and A. Kumar Jaiswal, “A Systematic Literature Review on the Cyber Security,” *Int. J. Sci. Res. Manag.*, vol. 9, no. 12, pp. 669–710, Dec. 2021, doi: 10.18535/ijsrm/v9i12.ec04.

[5] F. Putra Utama and R. M. Hilmi Nurhadi, “Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method,” *CommIT (Communication Inf. Technol. J.*, vol. 18, no. 1, pp. 39–51, Apr. 2024, doi: 10.21512/commit.v18i1.9384.

[6] A. Wijayanto, I. Riadi, and Y. Prayudi, “TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 7, no. 2, pp. 208–217, Mar. 2023, doi: 10.29207/resti.v7i2.4589.

[7] T. Widodo and A. S. Aji, “Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS),” *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, Jan. 2022, doi: 10.14421/jiska.2022.7.1.46-55.

[8] E. Riana, “Implementasi Cloud Computing Technology dan Dampaknya Terhadap Kelangsungan Bisnis Perusahaan Dengan Menggunakan Metode Agile dan Studi Literatur,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 3, p. 439, Jun. 2020, doi: 10.30865/jurikom.v7i3.2192.

[9] S. Utoro *et al.*, “Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard.”

[10] M. F. Abdillah, A. Wijayanto, and W. H. Pamungkas, “Virtual Local Area Network for Optimizing Network Performance using Simplified Form of Action Research,” *J. Appl. Informatics Comput.*, vol. 9, no. 4, pp. 1897–1905, 2025, doi: 10.30871/jaic.v9i4.10141.

[11] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, “PENGUJIAN PENETRASI PADA WEBSITE ELEARNING2.BINADARMA.AC.ID DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD),” *J. Komput. dan Inform.*, vol. 11, no. 1, pp. 91–95, Mar. 2023, doi: 10.35508/jicon.v11i1.9809.

[12] W. A. Purnama, Y. Servanda, Djumhadi, and A. Wijayanto, “Analisis Kasus Kehilangan Data Akibat Format dan Pemulihan Data Menggunakan Aplikasi Wondershare Recoverit,” *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 8, no. 4, pp. 1042–1050, Oct. 2024, doi: 10.35870/jtik.v8i4.2367.

[13] M. N. Hafizh, I. Riadi, and A. Fadlil, “Forensik Jaringan Terhadap Serangan ARP Spoofing Menggunakan Metode Live Forensic,” *J. Telekomun. Dan Komput.*, vol. 10, no. 2, p. 111, 2020, doi: 10.22441/incomtech.v10i2.8757.

[14] L. Galchynsky and A. Murtazina, “Vulnerability detection in the network traffic flow of the RADIUS protocol based

on the object-oriented model," *Theor. Appl. Cybersecurity*, vol. 4, no. 1, Feb. 2023, doi: 10.20535/tacs.2664-29132022.1.274119.