Just IT : Jurnal Sistem Informasi, Teknologi Informasi dan Komputer
Vol. 14, No. 2, Januari 2024, pp. 80-149
P-ISSN: 2089 – 0256, e-ISSN: 2598 – 3016

SYSTEMATIC LITERATURE REVIEW: SERANGAN DEFACE *WEBSITE* SEBAGAI BENTUK KEJAHATAN SIBER

Johanes Desmon[1], Syarief Hidayatulloh[2], Yuwan Jumaryadi[3]
[1]Program Studi Teknik Informatika, Fakultas Teknik dan Informatika,
Universitas Dian Nusantara.

411202088@mahahsiswa.undira.ac.id

Abstrak

Serangan terhadap keamanan website, khususnya dalam bentuk deface, merupakan tindakan yang dilakukan oleh peretas dengan tujuan merusak atau mengubah tampilan homepage sebuah situs. Serangan ini dapat merugikan reputasi organisasi atau individu, mengeksploitasi kerentanan sistem keamanan, atau menyampaikan pesan tertentu. Untuk mengkaji evolusi kejahatan siber dalam bentuk deface website, artikel ini melakukan tinjauan sistematis dengan memilih dan menentukan daftar jurnal yang relevan dengan cybercrime. Kajian sistematis ini melibatkan analisis terhadap hasil penelitian tentang serangan deface web di beberapa situs, menyajikan gambaran komprehensif mengenai perubahan dan tren dalam dunia keamanan siber.Tujuan dari penelitian ini adalah untuk memahami dan menggambarkan evolusi serangan deface website, serta mengidentifikasi faktor-faktor yang memengaruhi keberhasilan atau kegagalan upaya perlindungan terhadap serangan semacam itu. Selain itu, penelitian ini bertujuan untuk memberikan wawasan mendalam terkait strategi pencegahan dan deteksi serangan deface di lingkungan digital. Hasil analisis menunjukkan bahwa serangan deface website terus berkembang dan menjadi tantangan yang signifikan dalam keamanan siber. Oleh karena itu, perlindungan terhadap website perlu diperkuat melalui penerapan langkah-langkah keamanan yang lebih canggih.
Kata kunci: deface website, hacker, kejahatan siber, tinjauan sistematis.

Abstract

Attacks on website security, especially in the form of defacing, are actions carried out by hackers with the aim of damaging or changing the appearance of a site's homepage. These attacks can harm an organization's or individual's reputation, exploit security system vulnerabilities, or convey certain messages. To examine the evolution of cybercrime in the form of website defacement, this article carries out a systematic review by selecting and determining a list of journals that are relevant to cybercrime. This systematic review involves the analysis of research results on web deface attacks on several sites, presenting a comprehensive picture of changes and trends in the world of cybersecurity. The aim of this research is to understand and describe the evolution of website deface attacks, as well as identify the factors that influence success or failure of safeguards against such attacks. In addition, this research aims to provide in-depth insight into strategies for preventing and detecting deface attacks in digital environments. The analysis results show that website deface attacks continue to grow and become a significant challenge in cyber security. Therefore, website protection needs to be strengthened through the implementation of more sophisticated security measures.
Keywords: *website deface, hackers, cybercrime, systematic review.*

1. Pendahuluan

Dalam era digital yang semakin maju, perkembangan teknologi informasi dan komunikasi telah memberikan dampak positif yang signifikan bagi masyarakat global (Indah Septiani et al., 2022). Namun, tidak dapat dipungkiri bahwa seiring dengan kemajuan tersebut, muncul pula ancaman baru dalam bentuk kejahatan dunia maya. Salah satu kejahatan yang cukup umum dalam ranah cybercrime adalah deface website (Siddik Hasibuan & Mashur Gultom, 2018). Deface website merupakan tindakan yang dilakukan oleh seorang hacker atau peretas dengan maksud merusak atau mengubah tampilan halaman depan sebuah website. Tindakan ini seringkali bertujuan untuk mencemarkan reputasi organisasi atau individu, mengeksploitasi kerentanan dalam sistem keamanan, atau bahkan untuk menyampaikan pesan politik atau ideologis tertentu. Kejahatan seperti ini memiliki konsekuensi serius, baik bagi pemilik situs web maupun bagi pengguna yang mengandalkan informasi atau layanan yang terdapat di dalamnya. Selain itu, deface website juga dapat menjadi titik awal bagi serangan yang lebih berbahaya, seperti pencurian data pribadi atau serangan penolakan layanan (DdoS Attack). Oleh karena itu, penting bagi kita untuk memahami dan mengambil langkah-langkah yang tepat dalam menjaga keamanan dan integritas situs web demi melindungi diri kita dari ancaman-ancaman kejahatan siber yang ada.

Dalam konteks ini, kajian tentang kejahatan dunia maya yang melibatkan penurunan situs web menjadi sangat penting. Memahami metode dan motif di balik tindakan ini dapat memberikan kontribusi yang signifikan dalam meningkatkan keamanan sistem informasi dan mengembangkan strategi perlindungan yang efektif. Selain itu, penelitian juga dapat memberikan wawasan yang lebih mendalam tentang pelaku kejahatan dunia maya serta faktor-faktor yang mendorong mereka untuk melakukan tindakan tersebut. Dalam jurnal ini, kami melakukan tinjauan secara komprehensif terhadap fenomena kejahatan dunia maya yang melibatkan penurunan situs web. Kami akan menganalisis secara mendalam teknik-teknik yang digunakan oleh pelaku, motif di balik tindakan tersebut, dan dampaknya terhadap korban.

Tujuan dari penelitian ini adalah untuk menyajikan pemahaman yang komprehensif tentang serangan deface website sebagai bentuk kejahatan siber. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pemahaman tentang serangan deface website serta memberikan dasar untuk pengembangan kebijakan dan tindakan keamanan siber yang lebih efektif.

2. Metodologi

Dalam upaya mencapai tujuan penelitian, artikel ilmiah ini menggunakan pendekatan review literatur sistematis. Pada Gambar 1 merupakan langkah-langkah penelitian yang dilakukan.

Gambar 1. Tahapan Penelitian

3.1 Strategi Pencarian

Strategi pencarian dilakukan untuk mengidentifikasi literatur yang relevan tentang deface website sebagai bentuk kejahatan siber. Pencarian literatur yang dilakukan di berbagai basis data, seperti Google Scholar, IEEE Access, ScienceDirect dan MDPI dengan menggunakan kata kunci seperti "deface website", "website defacement" “cyber-attacks”, “cybercrime”, dan "attack techniques". dan memasukan filter

p-ISSN 2089-0265
e-ISSN 2598-3016

tahun 2018-2023.

3.2 Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi ditetapkan untuk pemilihan studi yang relevan. Studi-studi yang termasuk dalam review ini adalah artikel jurnal ilmiah, laporan penelitian, dan studi kasus yang berkaitan dengan deface website. Studi yang tidak memenuhi kriteria inklusi atau terindikasi duplikasi akan dikecualikan dari review.

3.3 Seleksi Studi

Seleksi studi dilakukan berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan. Studi-studi yang memenuhi kriteria inklusi akan dipertimbangkan untuk disertakan dalam review literatur sistematis ini. Proses seleksi studi dilakukan secara independen oleh dua peneliti untuk memastikan konsistensi.

3.4 Evaluasi Kualitas

Kualitas dan validitas setiap studi yang diikutsertakan dalam review ini akan dievaluasi. Evaluasi kualitas mencakup pertimbangan terhadap desain penelitian, metodologi, dan tingkat kepercayaan dalam temuan studi. Pada Gambar 2 merupakan Teknik pencarian artikel mengenai kejahatan siber.

Hasil evaluasi dapat memberikan kontribusi penting dalam menghadapi tantangan keamanan siber, memberikan solusi praktis untuk meningkatkan keamanan situs web dari serangan jahat serta memitigasi dampak yang mungkin terjadi.

Gambar 2. Teknik pencarian

3. Hasil dan pembahasan

Dalam penelitian yang telah dilakukan, para peneliti memberikan informasi terperinci mengenai teknik penipuan situs web, tindakan pencegahan, dan kontrol yang dapat diimplementasikan guna melindungi situs web dari serangan deface. Mereka menjelaskan beberapa teknik umum yang digunakan dalam deface situs web, seperti serangan injeksi SQL, Remote File Inclusion (RFI), Local File Inclusion (LFI), dan Cross-Site Scripting (XSS). Penjelasan diberikan mengenai bagaimana teknik-teknik tersebut bekerja dan bagaimana para pelaku serangan dapat memperoleh keuntungan dari serangan tersebut. Selain itu, jurnal tersebut juga membahas berbagai langkah pencegahan yang dapat diambil untuk mengurangi risiko serangan deface.

Beberapa langkah yang disebutkan termasuk dalam penelitian ini antara lain menerapkan kebijakan keamanan yang kuat, melakukan pembaruan dan pemeriksaan sistem secara teratur, menggunakan mekanisme autentikasi yang kuat, serta melindungi dari kerentanan yang umum ditemukan pada aplikasi web. Selain itu, juga dibahas langkah-langkah pengendalian yang dapat diambil jika sebuah website mengalami serangan deface. Langkah-langkah tersebut meliputi isolasi dan pemisahan sistem yang terkena dampak, pemulihan data dari cadangan yang aman, serta melakukan analisis forensik untuk mengidentifikasi pelaku dan sumber serangan. Secara keseluruhan, jurnal ini memberikan tinjauan komprehensif tentang teknik modifikasi situs web, tindakan pencegahan, dan pengendalian yang dapat digunakan untuk melindungi situs web dari serangan jahat. Jurnal ini dapat menjadi sumber yang bermanfaat bagi para profesional keamanan informasi dan administrator sistem yang ingin memahami dan melindungi situs web mereka dari ancaman deface website.

Teknik pencemaran nama baik situs web melibatkan penyusupan ilegal ke dalam sistem situs web dengan tujuan memodifikasi konten atau mengubah tampilan halaman depan. Serangan ini dilakukan oleh individu atau kelompok yang memiliki pengetahuan teknis di bidang keamanan komputer dan memiliki niat jahat. Ada beberapa teknik yang umum digunakan oleh para peretas situs web, salah satunya adalah serangan injeksi SQL. Dalam serangan ini, penyerang memanfaatkan kerentanan pada aplikasi web yang

p-ISSN 2089-0265
e-ISSN 2598-3016

menggunakan database SQL. Dengan memasukkan kode SQL yang berbahaya melalui input yang tidak diverifikasi, penyerang dapat mengambil kendali atas database dan melakukan modifikasi terhadap konten situs web.

SQL injection merupakan teknik yang sering digunakan oleh para hacker karena masih banyak website yang kurang memperhatikan keamanan sistemnya, sehingga celah ini dapat dimanfaatkan oleh pengguna yang tidak bertanggung jawab. Serangan SQL injection dapat terjadi ketika penyerang yang memiliki pengetahuan tentang query SQL dapat melewati kelemahan keamanan di lapisan basis data aplikasi. Kerentanan ini terjadi ketika input dari pengguna tidak difilter dengan benar, terutama untuk karakter meta saat menggunakan formulir input. Oleh karena itu, serangan SQL injection masih menjadi salah satu pilihan favorit para penyerang untuk mengakses dan memanipulasi data pada website. Terlebih lagi, dengan kemajuan teknologi saat ini, hacking melalui internet tidak sekompleks seperti sebelumnya. Sekali lagi, serangan SQL injection sering terjadi akibat kelalaian dari para programmer atau pengembang aplikasi yang tidak mengimplementasikan pembatasan filter untuk karakter metadata yang digunakan dalam sintaks SQL pada formulir input aplikasi. Hal ini memungkinkan penyerang untuk mengirimkan kombinasi kueri yang berbahaya melalui formulir input, sehingga mereka dapat melakukan tindakan yang tidak sah dengan mengeksploitasi kelemahan dalam autentikasi sistem. Jika aplikasi web tidak menerapkan filter pada formulir input, penyerang dapat meluncurkan serangan dengan memasukkan nama pengguna dan menambahkan karakter '#', misalnya 'rudz#'. Hal ini membuat karakter selanjutnya tidak diperlakukan sebagai kode SQL, sehingga pengguna "rudz" tidak perlu memasukkan kata sandi untuk masuk ke dalam sistem.

Dalam dunia keamanan web, terdapat dua teknik yang umum digunakan oleh para penyerang, yaitu Remote File Inclusion (RFI) dan Local File Inclusion (LFI). Teknik RFI melibatkan eksploitasi celah keamanan pada aplikasi web untuk mengimpor dan menjalankan kode berbahaya dari sumber eksternal. Di sisi lain, teknik LFI melibatkan pemanggilan file lokal yang seharusnya tidak dapat diakses oleh pengguna biasa.

Inklusi file jarak jauh (Remote File Inclusion) adalah sebuah celah keamanan yang memungkinkan penyerang untuk menyisipkan file berbahaya dari luar server dan menjalankannya. File yang disisipkan ini biasanya mengandung kode berbahaya yang dapat digunakan untuk mengontrol komputer atau server korban. Keberadaan celah ini seringkali disebabkan oleh kesalahan konfigurasi pada server serta kurangnya validasi dan verifikasi pada proses pengkodean. Dampak dari kerentanan ini sangat serius, karena penyerang dapat mengakses file sensitif, memanipulasi file secara langsung, menampilkan isi database, mengubah izin, bahkan dalam kasus terburuk, mengambil alih kendali atas server tersebut..

Inklusi file lokal (Local File Inclusion/LFI) merupakan sebuah celah keamanan yang memungkinkan penyerang untuk membaca atau mengakses file di server, termasuk file-file yang bersifat sensitif. Keberadaan LFI seringkali disebabkan oleh kesalahan dalam proses pengkodean, di mana fungsi seperti `include()` tidak diautentikasi dan difilter dengan benar. Fungsi `include()` sendiri adalah sebuah fitur dalam bahasa pemrograman PHP yang digunakan untuk menyisipkan string atau file ke dalam halaman situs web. Jika fungsi ini tidak diautentikasi dengan benar, serangan LFI dapat dieksekusi pada halaman yang rentan. Dampak dari serangan LFI ini adalah kemampuan untuk membaca file sensitif yang ada di server, seperti file-file sensitif pada server Linux, contohnya adalah file `/etc/passwd`. Di dalam file tersebut terdapat informasi sensitif seperti nama pengguna, kata sandi terenkripsi, ID pengguna, ID grup, dan sebagainya. Informasi seperti ini seharusnya tidak boleh diketahui oleh pihak yang tidak memiliki izin atau akses ke server.

Selain itu, terdapat juga serangan yang dikenal dengan nama Cross-Site Scripting (XSS) yang sering digunakan untuk melakukan perubahan pada suatu situs web. Dalam serangan ini, penyerang menyisipkan kode skrip berbahaya ke dalam halaman web, yang nantinya akan dieksekusi oleh browser pengguna. Dengan demikian, penyerang dapat mencuri informasi sensitif, mengarahkan

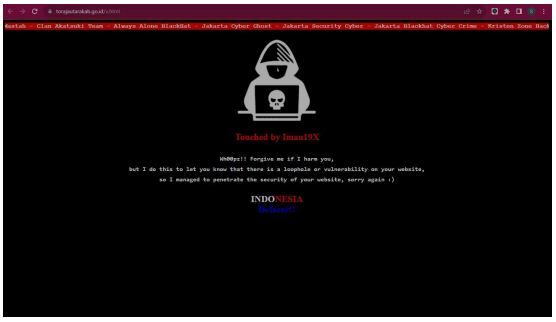
p-ISSN 2089-0265
e-ISSN 2598-3016

pengguna ke halaman palsu, atau mengubah tampilan dan nuansa situs tersebut.

Kejahatan dunia maya dalam bentuk deface website seringkali terjadi di platform website pemerintahan. Website pemerintah dan komersial menjadi target utama bagi para peretas karena memiliki jumlah pengguna yang banyak dan menjadi sasaran yang menarik untuk menyampaikan aspirasi atau melakukan pemerasan terhadap perusahaan atau pemerintah. Kekurangan pemahaman tentang keamanan website juga menjadi faktor yang memudahkan para peretas dalam melakukan penetrasi ke server website. Mayoritas website yang sering menjadi sasaran utama adalah website pemerintahan, yang digunakan sebagai sarana bagi peretas untuk menyampaikan keluhan terhadap tindakan pemerintah terhadap masyarakat. Para peretas memanfaatkan tampilan website untuk berkreasi sesuai dengan keinginan mereka. Ketika seorang pengguna mengakses suatu website yang telah diretas, mereka akan secara otomatis diarahkan ke halaman website yang telah mengalami perubahan dalam tampilannya.

Berdasarkan hasil penelitian yang dilakukan mengenai studi deface web di beberapa website, ditemukan bahwa deface website yang dilakukan oleh para peretas dapat berupa penambahan atau perubahan keseluruhan tampilan website. Hal ini menjadi bukti nyata terjadinya tindak kriminal dalam bentuk deface website.

Pemahaman yang mendalam mengenai teknik deface website merupakan hal yang sangat penting dalam upaya pencegahan serangan dan menjaga keamanan sistem informasi. Dengan mengetahui cara kerja dan kerentanan yang sering dimanfaatkan oleh para penyerang, kita dapat menerapkan perlindungan yang lebih efektif guna mengurangi risiko terjadinya deface pada situs. Pada Gambar 3 merupakan bukti bahwa deface website dapat mengubah halaman website.



Gambar 3. Contoh Bukti Kasus Deface Website.

Selain digunakan untuk menyampaikan aspirasi, website juga menjadi target para peretas untuk mencuri berbagai data pelanggan suatu perusahaan komersial. Dengan memanfaatkan kelemahan dan celah dalam keamanan web yang dapat dieksploitasi, para peretas akan melakukan serangan terhadap server perusahaan tersebut guna melakukan pencurian data. Banyak kasus seperti ini terjadi terutama di website pemerintah dan komersial.

4. Kesimpulan

Dalam pengumpulan dan analisis literatur, penelitian ini berhasil menggali informasi tentang teknik-teknik serangan, motif di balik serangan, serta dampak yang mungkin dialami oleh organisasi atau individu yang menjadi korban. Beberapa temuan kunci yang dapat diungkap melalui review ini melibatkan pemahaman mendalam tentang kerentanan sistem, metode penetrasi yang digunakan, dan berbagai tujuan yang mungkin menjadi motivasi pelaku serangan.

Pemahaman terhadap teknik-teknik serangan dapat membantu pihak keamanan siber untuk lebih efektif mendeteksi dan merespons ancaman. Selain itu, pemahaman terhadap motif dan tujuan serangan dapat memberikan wawasan yang lebih baik tentang cara menanggapi dan melindungi diri dari serangan yang mungkin lebih spesifik.

Rekomendasi perlindungan dan pencegahan yang dihasilkan dari review ini menjadi kontribusi penting dalam menghadapi tantangan keamanan siber. Implementasi strategi keamanan yang disarankan dapat membantu organisasi dan individu untuk meningkatkan ketahanan mereka terhadap serangan deface website. Oleh karena itu,

p-ISSN 2089-0265
e-ISSN 2598-3016

temuan dan rekomendasi dari review literatur sistematis ini diharapkan dapat menjadi panduan berharga dalam upaya melindungi situs web dari serangan jahat serta memitigasi dampak yang mungkin terjadi. Dengan demikian, penelitian ini bukan hanya memberikan pemahaman yang lebih mendalam, tetapi juga menyumbangkan solusi praktis untuk meningkatkan keamanan siber di dunia digital yang terus berkembang.

Daftar Pustaka

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Xplore*, *8*, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259

Ali, A. B. M., Shakhatreh, A. Y. I., Abdullah, M. S., & Alostad, J. (2011). SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks. *Procedia Computer Science*, *3*, 453–458. https://doi.org/10.1016/j.procs.2010.12.076

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers and Security*, *105*(2021), 102258. https://doi.org/10.1016/j.cose.2021.102258

Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify Cyber Crime offenses using machine learning. *Sustainability (Switzerland)*, *12*(10). https://doi.org/10.3390/SU12104087

Devalla, V., Srinivasa Raghavan, S., Maste, S., Kotian, J. D., & Annapurna, D. (2022). MURLi: A Tool for Detection of Malicious URLs and Injection Attacks. *Procedia Computer Science*, *215*,662–676.https://doi.org/10.1016/j.procs.2022.12.068

Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers and Security*, *124*, 102954. https://doi.org/10.1016/j.cose.2022.102954

Golchha, R., Joshi, A., & Gupta, G. P. (2022). Voting-based Ensemble Learning approach for Cyber Attacks Detection in Industrial Internet of Things. *Procedia Computer Science*, *218*, 1752–1759. https://doi.org/10.1016/j.procs.2023.01.153

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 210. https://doi.org/10.30998/string.v6i2.11477

Indah Septiani, N., Sediyono, A., & Rochman, A. (2022). Perancangan Web Defacement Monitoring Dengan Menggunakan Metode Komparasi Nilai Hash1. *JIKO (Jurnal Informatika Dan Komputer)*, *5*(2), 150–155. https://doi.org/10.33387/jiko.v5i2.4852

Kharisma Putra, I. K. O., Darmawan, I. M. A., Juliana, I. P. G., & Indriyani. (2023). Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phising. *Cyber Security Dan Forensik Digital*, *5*(2), 77–82. https://doi.org/10.14421/csecurity.2022.5.2.3797

Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G. A., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, *126*(July 2021). https://doi.org/10.1016/j.chb.2021.106984

Sharma, K., Yadav, A. K., & Sharma, B. B. (2023). Kharitonov theorem-based robust control approach for sustainable

p-ISSN 2089-0265
e-ISSN 2598-3016

microgrid against DoS cyber-attack. *Digital Chemical Engineering*, *7*(March), 100099. https://doi.org/10.1016/j.dche.2023.100099

Siddik Hasibuan, M., & Mashur Gultom, L. (2018). Analisis Serangan Deface Menggunakan Backdoor Shell Pada Website Analysis of Deface Attacks Using Backdoor Shell On Websites. (*Jurnal Techno.Com)* https://doi.org/10.33633/tc.v17i4.187

van de Weijer, S. G. A., Holt, T. J., & Leukfeldt, E. R. (2021). Heterogeneity in trajectories of cybercriminals: A longitudinal analyses of web defacements. *Computers in Human Behavior Reports*, *4*(June), 100113. https://doi.org/10.1016/j.chbr.2021.100113

van de Weijer, S. G. A., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, *8*(November), 100249. https://doi.org/10.1016/j.chbr.2022.100249