CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 1, Mei 2023, hlm. 25 of 29

TINDAKAN KEJAHATAN *CYBER CRIME* DALAM BENTUK *DEFACE WEBSITE*

Brian Budi Aji[1]

[1]Universitas Mulia
Email: [1]brianbudi00@gmail.com

Abstrak

Deface website merupakan tindakan yang dilakukan oleh seorang *hacker* atau peretas dengan tujuan untuk merusak atau mengubah tampilan homepage sebuah *website*. Tindakan ini sering dilakukan untuk menodai reputasi organisasi atau individu, mengeksploitasi kerentanan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologis. Mempertimbangkan permasalahan tersebut, artikel ini mengkaji evolusi kejahatan dunia maya dalam bentuk *website* yang terdegradasi dengan menggunakan metode tinjauan sistematis. Dalam diskusi ini dilakukan kajian sistematis dengan terlebih dahulu memilih dan menentukan daftar jurnal yang relevan dengan *cybercrime*. Berdasarkan hasil penelitian yang dilakukan tentang studi deface web di beberapa *website*. *deface website* yang dilakukan peretas berupa menambahkan ataupun merubah keseluruhan tampilan *website*, *Deface website* merupakan tindakan yang dilakukan oleh seorang *hacker* atau peretas dengan tujuan untuk merusak atau mengubah tampilan homepage sebuah *website*. Tindakan ini sering dilakukan untuk menodai reputasi organisasi atau individu, mengeksploitasi kerentanan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologis salah satu contohnya yang terjadi pada tahun 2020 di *website* DPR RI.

Kata kunci: *deface website, cyber crime, hacker*

CYBER CRIME ACTIONS IN THE FORM OF WEBSITE DEFACE

Abstract

Website defacement is an action taken by a hacker or hackers with the aim of destroying or changing the appearance of a website's homepage. These actions are often carried out to tarnish the reputation of organizations or individuals, exploit vulnerabilities in security systems, or convey political or ideological messages. Considering these problems, this article examines the evolution of cybercrimes in the form of degraded websites using a systematic review method. In this discussion, a systematic review is carried out by first selecting and determining a list of journals that are relevant to cybercrime. Based on the results of research conducted on web deface studies on several websites. website defacement by hackers in the form of adding or changing the overall appearance of a website Deface website is an action taken by a hacker or hackers with the aim of damaging or changing the appearance of a website's homepage. These actions are often carried out to tarnish the reputation of organizations or individuals, exploit vulnerabilities in security systems, or convey political or ideological messages, one example that occurred in 2020 on the DPR RI website.

Keywords*: deface website, cyber crime, hacker*

1. PENDAHULUAN

D Di era digital yang semakin maju, kemajuan teknologi informasi dan komunikasi telah memberikan dampak positif bagi masyarakat global. Namun, pada saat yang sama, muncul ancaman baru berupa kejahatan dunia maya. Kejahatan yang cukup umum di dunia *cybercrime* adalah *deface website*. *Deface website* merupakan tindakan yang dilakukan oleh seorang hacker atau peretas dengan tujuan untuk merusak atau mengubah tampilan homepage sebuah *website*. Tindakan ini sering dilakukan untuk menodai reputasi organisasi atau individu, mengeksploitasi kerentanan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologis. Kejahatan dunia maya berupa perusakan situs web memiliki konsekuensi serius, baik bagi pemilik situs web maupun bagi pengguna yang mengandalkan informasi atau layanan yang dikandungnya. Selain itu, degradasi situs web juga dapat menjadi titik awal serangan yang lebih berbahaya, seperti pencurian data pribadi atau serangan penolakan layanan (DdoS *Attack*).

Dalam konteks ini, kajian *cybercrime* berupa *website* yang terdegradasi menjadi sangat penting. Memahami metode dan motif tindakan ini dapat membantu meningkatkan keamanan sistem informasi dan mengembangkan strategi perlindungan yang efektif. Selain itu, penelitian juga dapat memberikan wawasan yang lebih dalam tentang pelaku kejahatan dunia maya dan faktor yang mendorong mereka melakukannya. Dalam

jurnal ini, kami mengulas secara mendalam fenomena kejahatan dunia maya dalam bentuk *website* yang terdegradasi. Kami akan menganalisis teknik yang digunakan pelaku, motif tindakan tersebut dan dampaknya terhadap korban.

Teknik pencemaran nama baik situs web melibatkan penyusupan ilegal ke dalam sistem situs web untuk tujuan memodifikasi konten atau mengubah tampilan beranda. Serangan ini dilakukan oleh individu atau kelompok yang memiliki pengetahuan teknis di bidang keamanan komputer dan memiliki niat jahat. Ada beberapa teknik yang biasa digunakan oleh para debugger situs web. Salah satunya adalah serangan injeksi SQL, dimana penulis memanfaatkan kerentanan pada aplikasi web yang menggunakan database SQL. Dengan memasukkan kode SQL berbahaya melalui input yang tidak diverifikasi, penyerang dapat mengambil kendali database dan memodifikasi konten situs web.

SQL *injection* merupakan teknik yang disukai oleh para hacker karena selama ini masih banyak *website* yang kurang memperhatikan celah keamanan pada sistemnya yang dapat dimanfaatkan oleh pengguna yang tidak bertanggung jawab. Injeksi SQL dapat terjadi karena penyerang yang menguasai teknik *query* SQL dapat mem-*bypass* lubang keamanan di SQL pada lapisan basis data aplikasi. Kerentanan terjadi karena input formulir pengguna tidak difilter dengan benar untuk karakter meta saat menulis menggunakan input formulir. Jadi, selama ini sql injector masih menjadi tool favorit para attacker untuk melakukan penyerangan pada *website*. Apalagi sekarang hacking melalui internet sudah tidak sesulit dulu lagi. Sekali lagi, serangan injeksi SQL sering terjadi karena kelalaian programmer (pengembang aplikasi) yang tidak mengimplementasikan pembatas filter untuk karakter metadata *(&, ;, ', ', \, " , |, *, ?, ~, < ;, >, ^, (,) , [,], {, }, $, \n, \r*) digunakan dalam sintaks SQL aplikasi input formulir, sehingga penyerang dapat memasukkan *wildcard* ini menggunakan kombinasi kueri skrip sehingga tindakan liar dapat dilakukan dengan mengautentikasi penetrasi Jika aplikasi web tidak menerapkan filter pada input formulir, penyerang dapat meluncurkan serangan dengan memasukkan nama pengguna dengan menambahkan '#', misalnya 'rudz#' Hal ini menyebabkan karakter selanjutnya tidak diperlakukan sebagai kode SQL, sehingga username "rudz" tidak perlu memasukkan password untuk masuk ke sistem

Teknik lain yang umum digunakan adalah inklusi file jarak jauh (RFI) dan *inklusi* file lokal (LFI). RFI melibatkan penggunaan lubang keamanan dalam aplikasi web untuk mengimpor dan mengeksekusi kode berbahaya dari sumber eksternal. Padahal, LFI melibatkan pemanggilan file lokal yang tidak dapat diakses oleh pengguna biasa.

Inklusi file jarak jauh adalah lubang keamanan memungkinkan penyerang untuk memasukkan file berbahaya dari luar server dan menjalankannya, file ini biasanya mengandung kesalahan kode berbahaya atau kode yang dapat digunakan untuk mengontrol komputer atau server korban. Jarak ini tampaknya salah satu karena konfigurasi di server salah dan pengkodean tidak divalidasi dan benar. Dampak Kerentanan seperti itu dapat diakses oleh penyerang file sensitif bahkan dapat memanipulasi file secara langsung file, tampilkan database, ubah izin dan itu kasus terburuk mengambil kendali server.

Inklusi file lokal adalah lubang keamanan memungkinkan penyerang untuk membaca atau melihat file di server termasuk file sensitif. LFI biasanya muncul karena kesalahan coding, salah satunya disebabkan oleh fungsi seperti fungsi *include()* itu tidak diautesntikasi dan difilter dengan benar. Fungsi *include()* adalah fungsi dari bahasa pemrograman PHP masukkan fungsi atau string sesuatu seperti file dalam halaman di situs web. Kapan fungsi ini tidak diautentikasi dengan benar, serangan LFI bisa berjalan di halaman tertentu. Dampak serangan LFI adalah kemampuan untuk membaca file sensitif yang ada di server, misalnya file sensitif di server Linux. Contohnya adalah file /etc/passwd, dalam file ini berisi informasi sensitif seperti nama pengguna, kata sandi terenkripsi, ID pengguna, ID grup, dll. Informasi ini tidak boleh diketahui oleh siapa pun yang tidak memiliki izin atau akses ke server.

Selain itu, serangan *Cross-Site Scripting* (XSS) juga biasa digunakan untuk mengubah situs web. Dalam serangan ini, pelaku menyisipkan kode skrip berbahaya ke dalam halaman web, yang kemudian dijalankan oleh browser pengguna. Ini memungkinkan penulis mencuri informasi sensitif, mengarahkan pengguna ke halaman palsu, atau mengubah tampilan dan nuansa situs.

Pemahaman yang mendalam tentang teknik deface *website* sangat penting dalam upaya pencegahan serangan dan menjaga keamanan sistem informasi. Dengan mengetahui cara kerjanya dan kerentanan yang digunakan oleh penulis, perlindungan yang lebih efektif dapat diterapkan untuk mengurangi risiko degradasi situs.

Jurnal Kumar, V., & Shukla, A. K. (2019). Techniques, prevention and countermeasures of *website* defacement attacks: A review. International Journal of Computer Science and Information Security, 17(6), 128-137, didalam penelitian yang telah dilakukan, para peneliti tersebut memberikan informasi terperinci tentang teknik penipuan situs web, tindakan pencegahan, dan kontrol yang dapat diambil untuk melindungi situs web dari serangan *deface website*. menjelaskan beberapa teknik yang umum digunakan dalam *deface* situs web, seperti serangan injeksi SQL, *Remote File Inclusio* (RFI), *Local File Inclusion* (LFI), dan *Cross-Site Scripting* (XSS). Mereka menjelaskan bagaimana teknik ini bekerja dan bagaimana para pelaku bisa mendapatkan keuntungan darinya. Jurnal tersebut

juga membahas berbagai tindakan pencegahan yang dapat diambil untuk mengurangi risiko serangan *Deface*.

Beberapa langkah yang disebutkan termasuk menerapkan kebijakan keamanan yang kuat, memperbarui dan memeriksa sistem secara teratur, menggunakan mekanisme autentikasi yang kuat, dan melindungi dari kerentanan yang biasa ditemukan di aplikasi web. Selain itu, juga dibahas langkah-langkah pengendalian yang dapat dilakukan jika sebuah *website* diserang. Ini termasuk mengisolasi dan memisahkan sistem yang terpengaruh, memulihkan data dari cadangan yang aman, dan melakukan analisis forensik untuk mengidentifikasi pelaku dan sumber serangan. Secara keseluruhan, jurnal ini memberikan tinjauan komprehensif tentang teknik modifikasi situs web, tindakan pencegahan, dan kontrol yang dapat digunakan untuk melindungi situs web dari serangan jahat. Ini dapat menjadi sumber yang berguna bagi para profesional keamanan informasi dan administrator sistem yang ingin memahami dan melindungi situs web mereka dari ancaman *deface website*.

2. METODOLOGI

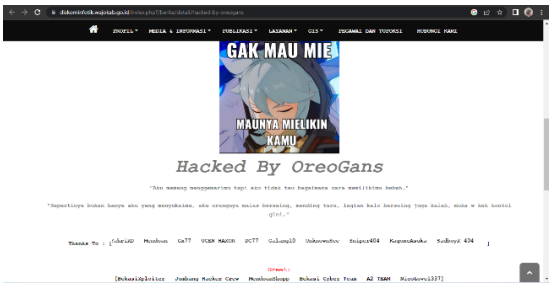
Mempertimbangkan permasalahan tersebut, didalam artikel ilmiah ini mengkaji evolusi kejahatan dunia maya dalam bentuk *website* yang terdegradasi dengan menggunakan metode tinjauan sistematis. Dalam diskusi ini dilakukan kajian sistematis dengan terlebih dahulu memilih dan menentukan daftar jurnal yang relevan dengan *cybercrime*. Berawal dari mencari jurnal yang berhubungan dengan dunia digital, perkembangan teknologi dan berlanjut ke arah kejahatan dunia maya atau *cybercrime*, akhirnya penulis mendapatkan jurnal terkait tindakan kriminal di dunia digital berupa deface *website*.

3. HASIL DAN PEMBAHASAN

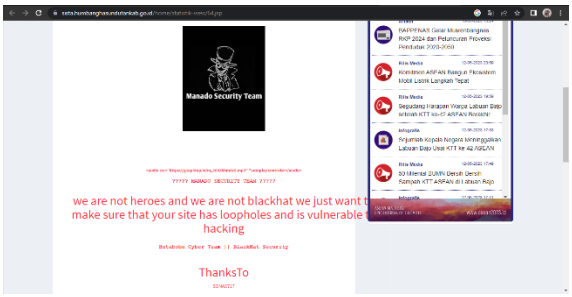
Cybercrime dengan cara *deface website* banyak ditemukan di platform *website* pemerintahan. *website* pemerintah dan commercial adalah target utama para peretas Ambil tindakan karena *website* tersebut memiliki banyak pengguna dan menjadi sasaran yang bagus untuk melakukan aspirasi dan pemerasan terhadap suatu perusahaan atau pemerintah. Kurangnya pendidikan tentang keamanan *website*, sehingga memudahkan para peretas melakukan penyusupan terhadap server *website*. Kebanyakan *website* yang sering di jadikan sasaran utama adalah *website* pemerintahan. *website* pemerintahan digunakan untuk menyampaikan keluh kesah para peretas terhadap tindakan yang dilakukan pemerintah untuk masyarakat. Peretas manfaatkan tampilan *website* untuk berkreasi sesuai dengan keinginan mereka. Ketika seorang pengguna ingin memasuki suatu *website* yang telah di retas maka mereka akan otomatis di arah kan ke halaman *website* yang telah dilakukan perubahan terhadap tampilan halaman tersebut.

Selain untuk menyampaikan aspirasi, *website* menjadi sasaran para hacker Mencuri berbagai data pelanggan suatu perusahaan commercial. Mengandalkan kelemahan dan celah pada keamanan web yang dapat di gunakan peretas, maka peretas akan melakukan tindakan terhadapat server perusahaan tersebut untuk pencurian data. Banyak kasus seperti ini khususnya di *website* pemerintah dan commercial. deface *website* yang pernah terjadi pada tahun 2020 yang sempat menghebohkan yaitu perubahan nama terhadap situs DPR RI. Kasus ini digunakan oleh peretas untj untuk menyuarakan sesuatu atas tindakan pemerintah.

Berdasarkan hasil penelitian yang dilakukan tentang studi deface web di beberapa *website*. deface *website* yang dilakukan peretas berupa menambahkan ataupun merubah keseluruhan tampilan *website*. Ini adalah bukti nyata terjadinya tindak kriminal dalam bentuk deface *website*.



Gambar 1. Bukti Kasus Deface *Website*



Gambar 2. Bukti Kasus Deface *Website*

Pelaku tindakan deface web seringkali mengincar *website* yang memiliki celah dan kelemahan dalam keamanan nya, peretas akan menggunakan berbagai teknik penyerangan untuk melakukan eksploitasi kelemahan ataupun celah dalah keamanan *website* target sehingga peretas dapat memiliki akses kedalam server target untuk melakukan berbagai macam tindakan kejahatan seperti deface *website* untuk berbagai macam hal seperti menunjukkan kelemahan keamanan, melakukan propaganda politik dan agama, menjual produk, untuk kesenangan pribadi,dll. ada berbagai macam tindakan yang dapat di lakukan peretas ketika telah masuk kedalam server target melalui kelemanan keamanan nya tidak jarang para peretas mengambil data yang sangat penting dari target untuk

keuntungan pribadi. dengan pemaparan diatas penulis menyarankan agar para pemilik *website* danpara ahli dalam bidang keamanan *cyber* dapat selalu meningkatkan keamanan *cyber* untuk menghindari berbagai tindak kriminal dalam dunia *cyber*.

4. KESIMPULAN DAN SARAN

Cybercrime adalah kasus pelanggaran berkaitan dengan komputer atau alat komunikasi sebagai target dan komisi atau alat terkait dengan dominasi komputer. Bentuk kejahatan mereka sangat beragam sehingga peretas dapat memilih metode yang ingin mereka gunakan kejahatan di dunia maya.

Deface *website* merupakan tindakan yang dilakukan oleh seorang hacker atau peretas dengan tujuan untuk merusak atau mengubah tampilan homepage sebuah *website*. Tindakan ini sering dilakukan untuk menodai reputasi organisasi atau individu, mengeksploitasi kerentanan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologis salah satu contohnya yang terjadi pada tahun 2020 di *website* DPR RI.

Ada beberapa teknik yang biasa digunakan oleh para debugger situs web. Salah satunya adalah serangan injeksi SQL, dimana penulis memanfaatkan kerentanan pada aplikasi web yang menggunakan database SQL. Teknik lain yang umum digunakan adalah inklusi file jarak jauh (RFI) dan inklusi file lokal (LFI). RFI melibatkan penggunaan lubang keamanan dalam aplikasi web untuk mengimpor dan mengeksekusi kode berbahaya dari sumber eksternal. Selain itu, serangan *Cross-Site Scripting* (XSS) juga biasa digunakan untuk mengubah situs web. Dalam serangan ini, pelaku menyisipkan kode skrip berbahaya ke dalam halaman web, yang kemudian dijalankan oleh browser pengguna.

DAFTAR PUSTAKA

ALI, A.B.M., SHAKHATREH, A.Y.I., ABDULLAH, M.S. AND ALOSTAD, J., 2011. SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks. In: *Procedia Computer Science*. pp.453–458. https://doi.org/10.1016/j.procs.2010.12.076.

AL-KHATER, W.A., AL-MAADEED, S., AHMED, A.A., SADIQ, A.S. AND KHAN, M.K., 2020. Comprehensive review of cybercrime detection techniques. IEEE Access, 8, pp.137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259.

CASCAVILLA, G., TAMBURRI, D.A. AND VAN DEN HEUVEL, W.J., 2021. *Cybercrime threat intelligence: A systematic multi-vocal literature review*. *Computers and Security*, https://doi.org/10.1016/j.cose.2021.102258.

CH, R., GADEKALLU, T.R., ABIDI, M.H. AND 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. AND ANNAPURNA, Dr.D., 2022. URLi: A Tool for Detection of Malicious URLs and Injection Attacks. *Procedia Computer Science*, 215, pp.662–676. https://doi.org/10.1016/j.procs.2022.12.068.

ARROYABE, M.F. AND FERNANDEZ DE ARROYABE, J.C., 2023. *Cyber*security capabilities and *cyber*-attacks as drivers of investment in *cyber*security systems: A UK survey for 2018 and 2019. *Computers and Security*, 124. https://doi.org/10.1016/j.cose.2022.102954.

GOLCHHA, R., JOSHI, A. AND GUPTA, G.P., 2023. Voting-based Ensemble Learning approach for *Cyber* Attacks Detection in Industrial Internet of Things. *Procedia Computer Science*, 218, pp.1752–1759. https://doi.org/10.1016/j.procs.2023.01.153.

HERMAWAN, R., 2021. *STRING (Satuan Tulisan Riset dan Inovasi Teknologi) TEKNIK UJI PENETRASI WEB SERVER MENGGUNAKAN SQL INJECTION DENGAN SQLMAP DI KALILINUX*. Jakarta.

KADEK ODIE KHARISMA PUTRA, I., MADE ADI DARMAWAN, I., PUTU GEDE JULIANA, I., Kunci, K. and Crime, C., 2022. *TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING CRIMINAL ACTS IN THE DIGITAL WORLD WITH A FORM OF PHISHING*. Bali .

KOPRAWI, M., 2020. InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan. *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, [online] 4(2). https://doi.org/10.30743/infotekjar.v4i2.2332.

MONEVA, A., LEUKFELDT, E.R., VAN DE WEIJER, S.G.A. AND MIRÓ-LLINARES, F., 2022. Repeat victimization by *website* defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, 126. https://doi.org/10.1016/j.chb.2021.106984.

SEPTIANI, N.I., SEDIYONO, A. AND ROCHMAN, A., 2022. Perancangan Web Defacement Monitoring Dengan Menggunakan Metode Komparasi Nilai

Hash1. *Jurnal Informatika dan Komputer) Akreditasi KEMENRISTEKDIKTI*, 5(2). https://doi.org/10.33387/jiko.

SHARMA, K., YADAV, A.K. AND SHARMA, B.B., 2023. Kharitonov theorem-based robust control approach for sustainable microgrid against DoS *cyber*-attack. *Digital Chemical Engineering*, 7. https://doi.org/10.1016/j.dche.2023.100099.

VAN DE WEIJER, S.G.A., HOLT, T.J. AND LEUKFELDT, E.R., 2021. Heterogeneity in trajectories of *cyber*criminals: A longitudinal analyses of web defacements. *Computers in Human Behavior Reports*, 4. https://doi.org/10.1016/j.chbr.2021.100113.

VAN DE WEIJER, S.G.A. AND 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. https://doi.org/10.1016/j.chbr.2022.100249.