JURNAL SISTEM INFORMASI BISNIS (JUNSIBI)
OPEN ACCES
p-ISSN: 2774-3446
e-ISSN: 2774-3454
diterbitkan oleh:
Program Studi Sistem Informasi
Institut Bisnis dan Informatika (IBI) Kosgoro 1957
Vol.7 No.1, April, Tahun 2026, pp. 70-79
DOI: https://doi.org/10.55122/junsibi.v7i1.2081

DIGITAL FORENSIC DAN PENGANGGULANAN MALWARE JUDI ONLINE PADA WORDPRESS

PENULIS [1)]Egi Adithia Pradana, [2)]Taruna Nasution, [3)]Teten Sutendi

ABSTRAK

Pemanfaatan WordPress sebagai platform pengelolaan website terus meningkat seiring dengan kemudahan dan fleksibilitas yang ditawarkan. Namun, popularitas tersebut juga menjadikannya sasaran utama berbagai serangan siber, termasuk penyebaran malware yang berkaitan dengan aktivitas judi online. Ancaman ini tidak hanya berdampak pada keamanan data, tetapi juga menurunkan reputasi situs yang terinfeksi.Penelitian ini bertujuan untuk mengidentifikasi karakteristik serangan malware pada WordPress serta merumuskan langkah penanggulangan berbasis pendekatan digital forensik. Metode yang digunakan meliputi identifikasi insiden, akuisisi bukti digital, analisis log server, serta pemeriksaan kode berbahaya melalui teknik reverse engineering.Hasil penelitian menunjukkan bahwa serangan umumnya memanfaatkan celah keamanan pada plugin dan tema yang tidak diperbarui, serta menggunakan teknik obfuscation untuk menghindari deteksi. Proses forensik berhasil mengungkap pola serangan, mekanisme injeksi konten ilegal, serta aktivitas backdoor pada sistem.Penanganan dilakukan melalui isolasi sistem, pembersihan file terinfeksi, serta penguatan keamanan dengan konfigurasi ulang dan monitoring berkelanjutan. Temuan ini menegaskan bahwa penerapan digital forensik tidak hanya efektif dalam investigasi, tetapi juga berperan penting dalam meningkatkan ketahanan sistem terhadap serangan berulang.

Kata Kunci *Digital Forensik, Malware, WordPress, Judi Online, Keamanan Website*

AFILIASI

Program Studi
[1)]Informatika, Fakultas Sains dan Bisnis
[2)]Sistem Informasi, Fakultas Sains dan Bisnis
[3)]Program Studi Teknik Informatika

Nama Institusi
[1-2)]Universitas LIA
[3)]Sekolah Tinggi Teknologi Informasi NIIT (I-Tech)

Alamat Institusi
[1-2)]Jl. Pengadegan Timur Raya No.3, Pengadegan, Pancoran, Jakarta Selatan, DKI Jakarta
[3)]Jl. Asem 2 No.22, Cipete, Jakarta Selatan, DKI Jakarta

KORESPONDENSI

Penulis Egi Adithia
Email egiadithia@universitaslia.ac.id

I. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong penggunaan Content Management System (CMS), khususnya WordPress, sebagai solusi utama dalam pengelolaan website. Tingginya tingkat adopsi WordPress menjadikannya target potensial bagi pelaku kejahatan siber, terutama karena ketergantungannya pada plugin dan tema pihak ketiga. Dalam beberapa tahun terakhir, kerentanan pada komponen tersebut terus meningkat secara signifikan. Laporan keamanan menunjukkan bahwa lebih dari 90% kerentanan pada ekosistem WordPress berasal dari plugin, sementara sisanya berasal dari tema dan core system [3].

Seiring meningkatnya kompleksitas serangan, diperlukan pendekatan yang sistematis untuk mengidentifikasi dan menganalisis insiden keamanan. Digital forensik hadir sebagai metode yang mampu mengungkap jejak aktivitas penyerang melalui analisis bukti digital, baik dari file sistem, log server, maupun database. [2]. Sebagian besar celah keamanan pada WordPress berasal dari komponen tambahan yang tidak diperbarui secara berkala.

Kondisi ini membuka peluang bagi penyerang untuk mengeksploitasi kerentanan seperti Remote Code Execution (RCE), SQL Injection, dan Cross-Site Scripting (XSS). Dalam praktiknya, banyak situs yang disusupi malware untuk menyisipkan konten ilegal, termasuk promosi judi online secara tersembunyi. Penelitian menunjukkan bahwa banyak situs WordPress telah disusupi malware yang digunakan untuk berbagai aktivitas ilegal, termasuk distribusi konten judi online secara tersembunyi [1]. Kondisi ini diperparah oleh rendahnya tingkat pembaruan sistem, di mana sebagian besar serangan memanfaatkan kerentanan lama yang belum ditambal [10].

Dalam menghadapi ancaman tersebut, digital forensik menjadi pendekatan penting dalam proses investigasi keamanan siber. Digital forensik memungkinkan identifikasi, pengumpulan, analisis, dan interpretasi bukti digital untuk mengungkap pola serangan, sumber ancaman, serta teknik yang digunakan oleh pelaku. Pendekatan ini juga dapat digunakan untuk menganalisis teknik obfuscation dan backdoor yang sering digunakan dalam malware berbasis WordPress [7]. Selain itu, digital forensik berperan dalam mendukung proses pemulihan sistem dan perumusan strategi mitigasi yang efektif [13].

Perkembangan teknologi informasi telah mendorong penggunaan Content Management System (CMS) seperti WordPress sebagai platform utama dalam pengelolaan situs web. Popularitas WordPress yang tinggi menjadikannya target utama serangan siber, terutama karena fleksibilitasnya yang bergantung pada plugin dan tema pihak ketiga. Dalam beberapa tahun terakhir, kerentanan pada komponen tersebut terus meningkat secara signifikan. Laporan keamanan menunjukkan bahwa lebih dari 90% kerentanan pada ekosistem WordPress berasal dari plugin, sementara sisanya berasal dari tema dan core system [3]. Selain itu, tren peningkatan serangan terhadap website berbasis WordPress juga menunjukkan eskalasi ancaman yang semakin kompleks dan masif [2].

Serangan terhadap WordPress umumnya memanfaatkan plugin atau tema yang tidak diperbarui, serta celah keamanan seperti Remote Code Execution (RCE), SQL Injection, dan Cross-Site Scripting (XSS). Penelitian menunjukkan bahwa banyak situs WordPress telah disusupi malware yang digunakan untuk berbagai aktivitas ilegal, termasuk distribusi konten judi online secara tersembunyi [1]. Kondisi ini diperparah oleh rendahnya tingkat pembaruan sistem, di mana sebagian besar serangan memanfaatkan kerentanan lama yang belum ditambal [10].

Dalam menghadapi ancaman tersebut, digital forensik menjadi pendekatan penting dalam proses investigasi keamanan siber. Digital forensik memungkinkan identifikasi, pengumpulan, analisis, dan interpretasi bukti digital untuk mengungkap pola serangan, sumber ancaman, serta teknik yang digunakan oleh pelaku. Pendekatan ini juga dapat digunakan untuk menganalisis teknik obfuscation dan backdoor yang sering digunakan dalam malware berbasis WordPress [7]. Selain itu, digital forensik berperan dalam mendukung proses pemulihan sistem dan perumusan strategi mitigasi yang efektif [13].

Penelitian ini berfokus pada analisis serangan malware yang berkaitan dengan praktik judi online pada platform WordPress dengan menggunakan pendekatan digital forensik. Tujuan penelitian adalah untuk mengidentifikasi karakteristik serangan, menganalisis pola distribusi malware, serta merumuskan strategi penanggulangan yang efektif. Hasil penelitian diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan website berbasis WordPress serta menjadi referensi dalam pengembangan sistem deteksi dan pencegahan serangan siber yang lebih adaptif dan berkelanjutan.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode digital forensik untuk mengkaji serangan malware pada website berbasis WordPress. Proses penelitian dilakukan secara bertahap mulai dari pengumpulan data hingga implementasi solusi keamanan.

2.1 Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui beberapa metode, yaitu :

1) **Observasi**
   Observasi dilakukan terhadap file system pada hosting berbasis cPanel untuk mengidentifikasi file yang terindikasi terinfeksi malware maupun file mencurigakan. Pada tahapan ini, dilakukan observasi terhadap berkas-berkas pada file manager di CPANEL secara mendalam, untuk melakukan pencarian pada berkas-berkas yang dianggap sudah diinfeksi atau berkas yang memang bawaan dari malware.
2) **Studi Pustaka**
   Studi pustaka digunakan untuk memperoleh referensi terkait keamanan WordPress, teknik serangan malware, serta metode digital forensik sebagai dasar analisis penelitian. Studi pustaka dilakukan untuk melengkapi informasi-informasi yang dibutuhkan dalam melakukan penelitian ini. Informasi yang berkaitan dengan topik atau masalah yang dapat mendukung penyelesaian masalah yang dibahas.

2.2 Tahapan Digital Forensik

Penelitian ini mengadopsi tahapan digital forensik yang meliputi :

1) **Identifikasi (Identification)**
   Menentukan indikasi awal adanya serangan malware pada sistem. Untuk mendukung penelitian ini dilakukan analisa mendalam pada berkas-berkas yang dianggap bermasalah serta pada log sistem, web server, ftp dan lain-lain ilakukan dengan metode digital forensic.
2) **Akuisisi (Collection)**
   Mengumpulkan data berupa file website, log server (web server, FTP), serta database.
3) **Pemeriksaan (Examination)**
   Melakukan scanning file menggunakan teknik berbasis command line seperti grep dan find untuk mendeteksi kode berbahaya.
4) **Analisis (Analysis)**
   Menganalisis pola serangan, teknik obfuscation, serta keberadaan backdoor pada sistem.
5) **Pelaporan (Reporting)**
   Menyusun hasil analisis sebagai dasar penanggulangan malware.

Adapun bentuk dari Analisis Forensik Malware pada WordPress dapat dilihat pada tabel 1 dibawah ini:

Tabel 1. Analisis Analisis Forensik Malware pada WordPress

No	Indikator Forensik	Artefak Digital	Teknik Malware	Dampak	Metode Deteksi	Tindakan Penanganan
1	Fungsi eval()	File PHP	Code Execution	Eksekusi kode berbahaya	grep scanning	Hapus file
2	base64_decode	Script terenkripsi	Obfuscation	Menyembunyikan payload	Analisis string	Decode & hapus
3	gzinflate	Kompresi script	Obfuscation	Menyulitkan analisis	Pattern detection	Deobfuscate
4	$_GET / $_POST	Input user	Remote Command	Akses ilegal	Log analysis	Validasi input
5	curl_exec	Koneksi eksternal	Remote Loader	Ambil script luar	Network log	Blok domain
6	fsockopen	Socket connection	Backdoor	Akses jarak jauh	Traffic monitoring	Disable fungsi
7	Script judi	HTML / DB	SEO Spam	Redirect ke situs judi	Keyword scan	Bersihkan DB
8	auto_prepend_file	Config PHP	Persistence	Malware auto load	Config audit	Reset config
9	File baru (-mtime)	File system	Dropper	Tambah file malware	find command	Hapus file
10	wp_options inject	Database	Data Injection	Script tersembunyi	SQL query	Bersihkan DB

2.3 Implementasi Penanganan Malware

Tahapan implementasi dilakukan melalui:

1) Isolasi Sistem

Melakukan lockdown pada cPanel untuk mencegah penyebaran malware pada lingkungan hosting.Diperlukan isolasi atau *lockdown* pada cpanel untuk mencegah penyebaran *malware* ke akun-akun lain yang menggunakan *shared hosting* yang sama serta untuk memudahkan tahapan selanjutnya.

2) Identifikasi File Terinfeksi

Mendeteksi file berbahaya menggunakan teknik pencarian berbasis signature dan pola script mencurigakan.

3) Pembersihan Sistem

Menghapus atau memperbaiki file yang terinfeksi serta membersihkan database dari script injeksi.

4) Hardening Sistem

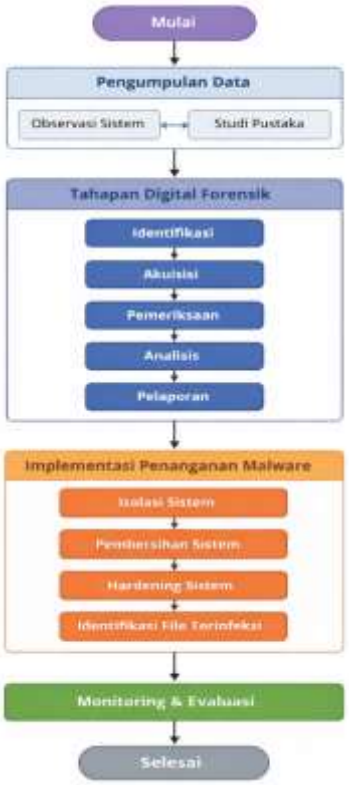
Melakukan penguatan keamanan melalui pembaruan WordPress, plugin, tema, serta penggantian kredensial.

Setelah beberapa tahapan-tahapan sebelumnya sudah dilakukan, berikutnya adalah implementasi yaitu perbaikan berkas-berkas yang sudah diinfeksi dan juga pembersihan berkas malware.

5) Monitoring

Melakukan pemantauan secara berkala terhadap aktivitas sistem dan trafik jaringan untuk mencegah serangan ulang. Pengawasan atau monitoring dilakukan untuk mencegah terjadi masalah yang sama serta mengawasi trafik jaringan yang tidak aman atau dari pihak lain yang dianggap bermasalah.

Dengan metode ini, penelitian diharapkan mampu memberikan pendekatan yang sistematis dalam mendeteksi, menganalisis, serta menanggulangi serangan malware pada platform WordPress.Adapun alur dari penelitian dapat dilihat pada flowchart dibawah ini :



Gambar 1. Alur Tahapan Penelitian

Adapun bentuk tabel penelitian dapat dilihat pada tabel 1 dibawah ini :

Tabel 2. Tahapan Penelitian dan Output yang diHasilkan

No	Tahapan Penelitian	Aktivitas Utama	Output yang Dihasilkan
1	Pengumpulan Data	Observasi sistem (file manager cPanel) dan studi pustaka	Data awal sistem dan referensi penelitian
2	Identifikasi	Menentukan indikasi adanya serangan malware	Indikasi awal sistem terinfeksi
3	Akuisisi	Mengumpulkan file website, log server, dan database	Bukti digital (file, log, database)
4	Pemeriksaan	Scanning file menggunakan grep, find, dan teknik deteksi malware	Daftar file mencurigakan
5	Analisis	Analisis pola serangan, obfuscation, dan backdoor	Pola serangan dan teknik malware
6	Pelaporan	Dokumentasi hasil analisis forensik	Laporan hasil investigasi
7	Isolasi Sistem	Lockdown hosting untuk mencegah penyebaran malware	Sistem terisolasi
8	Identifikasi File Terinfeksi	Deteksi file berbahaya berbasis signature dan script mencurigakan	File terinfeksi teridentifikasi
9	Pembersihan Sistem	Penghapusan dan perbaikan file serta database yang terinfeksi	Sistem bersih dari malware
10	Hardening Sistem	Update WordPress, plugin, tema, serta penggantian kredensial	Sistem lebih aman
11	Monitoring & Evaluasi	Pemantauan aktivitas sistem dan trafik jaringan secara berkala	Pencegahan serangan ulang
12	Selesai	Sistem berjalan normal dan aman	Website kembali optimal

III. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

1) Isolasi Website

Aktifkan maintenance mode Backup file & database (untuk forensik)

2) Identifikasi File Terinfeksi berikut comand untuk mencari file yang terinfeksi pada website :

grep -R "base64_decode" public_html
grep -R "eval(" public_html
grep -R "gzinflate" public_html
grep -R "__callStatic" public_html
bisa di buatkan dalam satu baris perintah dan disimpan pada file txt
Jalankan via Terminal cPanel atau SSH user cPanel
grep -RIl --binary-files=without-match -E
"eval\(|assert\(|base64_decode|gzinflate|str_rot13|__callStatic|metaphone|str_shuffle|preg_replace\s*\(.*/e" ~/public_html >> hasil.txt

Berikut adalah hasil yang ditemukan oleh command tersebut :

Gambar 2. Hasil Pencarian Syntax tertentu pada Berkas Malicious

Isi File Malicious yang berhasil di temukan yaitu sebagai berikut :

Gambar 3. Pencarian Backdoor pada Server menggunakan Command Find

Selain menggunakan command mencari langsung bisa dengan menacri file terbaru pada server menggunakan perintah :

find public_html -type f -mtime -7 -print
perintah tersebut akan mencari file yang di buat 7 hari dari pencarian.

3.2 Pembahasan

Script untuk mencari backdoor/malware :

berikut perintah yang bisa di coba untuk mencari malware atau backdoor pada website terutama di wordpress :

a. BACKDOOR :

```
grep -RInE --color=auto \
"(eval|assert|system|exec|shell_exec|passthru|popen|proc_open)[[:space:]]*\(" .
REGEX WEB-SHELL (GET / POST → EXEC)
grep -RInE --color=auto \
"\$_(GET|POST|REQUEST)\s*\[[^]]+\].*(eval|assert|system|exec|shell_exec)" .
REGEX OBFUSCATION
grep -RInE --color=auto \
"(eval|assert)[[:space:]]*\([[:space:]]*(base64_decode|gzinflate|gzuncompress|str_rot13|convert_uudecod
e)" .
```

b. BREGEX REMOTE LOADER (FILE/CURL/SOCKET) :

```
grep -RInE --color=auto \
"(file_get_contents|curl_exec|fopen|fsockopen)[[:space:]]*\([^)]*https?://" .
REGEX VARIABLE FUNCTION / DYNAMIC CALL
grep -RInE --color=auto \
"\$[a-zA-Z_][a-zA-Z0-9_]*\s*\(\s*\$_(GET|POST|REQUEST)" .
REGEX HEX / XOR OBFUSCATION
grep -RInE --color=auto \
"(\\\\x[0-9a-fA-F]{2}|chr\s*\(|ord\s*\(|\^)" .
```

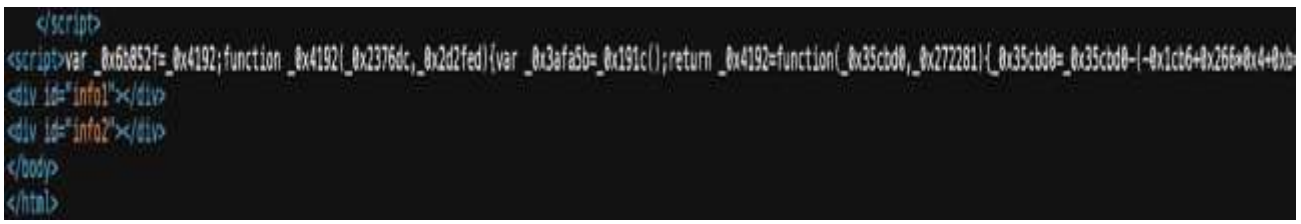
c. REGEX SEO SPAM/JUDI ONLINE :

```
grep -RInE --color=auto \
"(judi|slot|casino|togel|betting|poker|jackpot|sbobet|maxwin)" .
```

d. REGEX AUTO-INCLUDE/PERSISTENCE :

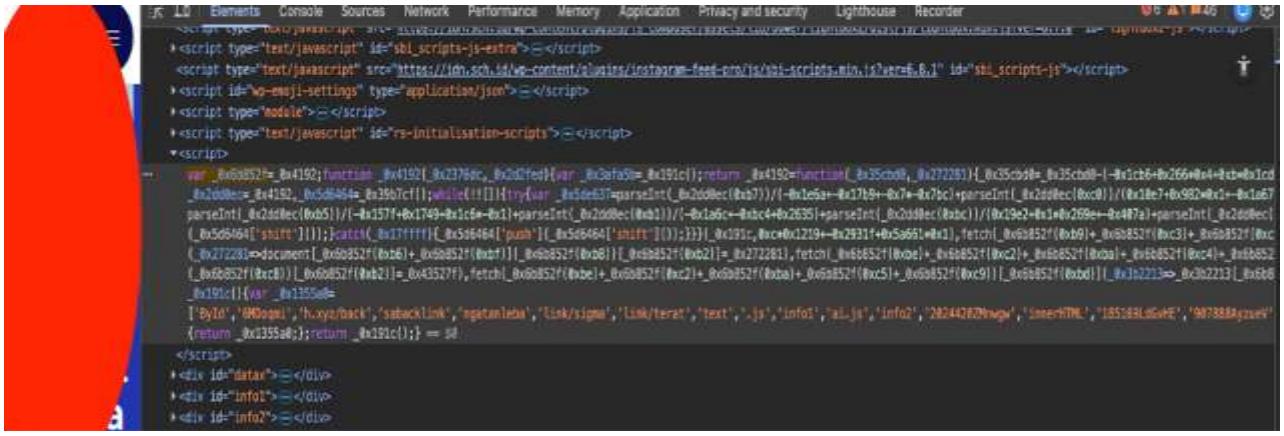
```
grep -RInE --color=auto \
"(auto_prepend_file|auto_append_file|register_shutdown_function)" .
ALL-IN-ONE BACKDOOR & MALWARE SCAN
grep -RInE --color=auto \
--exclude-dir={vendor,node_modules,.git,logs} \
--exclude=*.min.php \
"(eval|assert|system|exec|shell_exec|passthru|popen|proc_open)[[:space:]]*\(|\
\$_(GET|POST|REQUEST)\s*\[[^]]+\]|\
(base64_decode|gzinflate|gzuncompress|str_rot13|convert_uudecode)[[:space:]]*\(|\
(file_get_contents|curl_exec|fopen|fsockopen)[[:space:]]*\([^)]*https?://|\
\$[a-zA-Z_][a-zA-Z0-9_]*\s*\(\s*\$_(GET|POST|REQUEST)|\
\\\\x[0-9a-fA-F]{2}|chr\s*\(|ord\s*\(|\^|\
auto_prepend_file|auto_append_file|register_shutdown_function|\judi|slot|casino|togel|sbobet|maxwin|bett
ing|poker|jackpot" .
```

Adapun script untuk mencari content judol (judi online) pada database yang harus dilakukan adalah backup database terlebih dahulu, dan salah satu contoh content judol yang telah di inject pada website dapat dilihat pada gambar 4 dibawah ini :



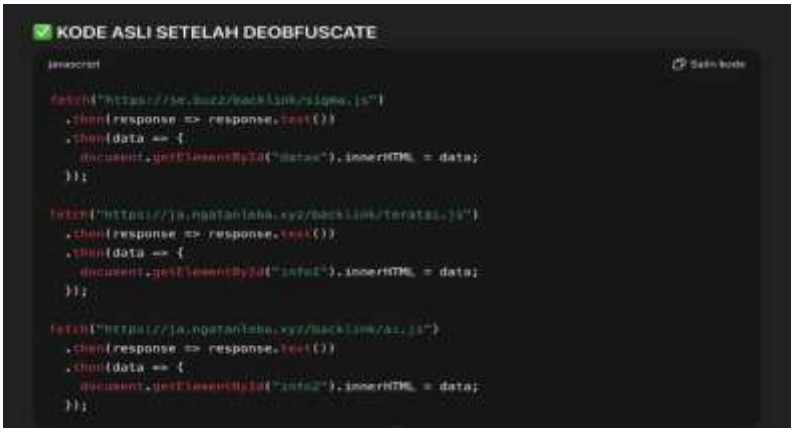
Gambar 4. script pencarian konten judol pada berkas html

Pada gambar tersebut terdapat script malicious yang di inject pada halaman web, maka langkah selanjutnya adalah melakukan inspect halaman tersebut dan cari script nya dapat dilihat pada gambar 5 dibawah ini :



Gambar 5. inspeksi sintaks *malicious* pada berkas html

setelah dapat scriptnya, maka langkah selanjutnya dapat dilakukan deobfuscator pakai chat gpt open AI :



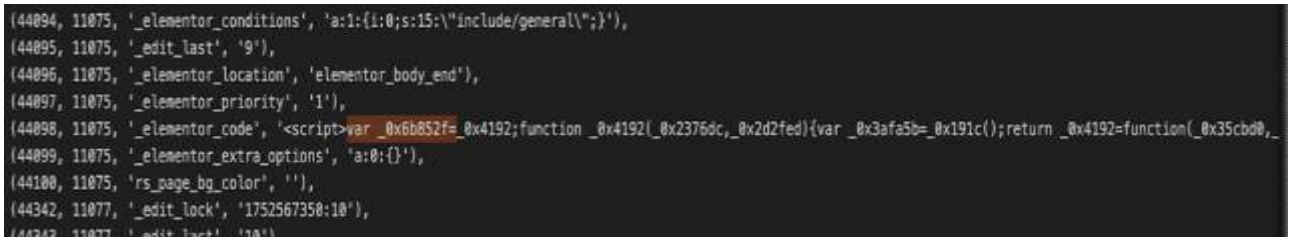
Gambar 6. hasil *deobfuscate* berkas html

Hasil dari deobfuscate Remote JavaScript Injection script ini :

a. Mengambil konten JS dari domain luar
b. Memasukkan hasilnya langsung ke DOM via innerHTML

Teknik klasik malware/SEO spam/backdoor frontend :

Langkah yang dilakukan yaitu mencari database script tersebut tidak menempel pada script php atau lain nya. pencarian pada hasil dump sql/backup database script tersebut di inject pada function columt _elementor_code, dalam case ini pencarian hasil dump di buka via visual code.



Gambar 7. sintak backdoor pada berkas html di frontend website

Pada umumnya malware JS seperti ini disimpan di :

1. wp_options (PALING SERING)
2. wp_posts (post/page tersembunyi)
3. wp_postmeta
4. wp_widgets (via option)
5. wp_usermeta (jarang tapi ada)

Adapun Script untuk mencari Malicious pada database adalah sebagai berikut :

```
SELECT option_name FROM wp_options
WHERE option_value LIKE '%ngatanleba%'
OR option_value LIKE '%se.buzz%';
```

IV. KESIMPULAN

4.1 Simpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa :

1) Platform WordPress memiliki tingkat kerentanan yang cukup tinggi terhadap serangan malware, terutama yang dimanfaatkan untuk penyebaran konten judi online. Serangan umumnya terjadi melalui eksploitasi plugin dan tema yang tidak diperbarui, serta penggunaan teknik obfuscation yang bertujuan untuk menyembunyikan kode berbahaya dari deteksi sistem keamanan.
2) Penerapan metode digital forensik terbukti efektif dalam mengidentifikasi, menganalisis, dan mengungkap pola serangan malware, baik melalui analisis file sistem, log server, maupun database. Teknik pencarian berbasis command line dan analisis signature malware mampu mendeteksi keberadaan backdoor, script injeksi, serta aktivitas mencurigakan lainnya.
3) Selain itu, proses penanggulangan melalui isolasi sistem, pembersihan file terinfeksi, serta penguatan keamanan menunjukkan hasil yang signifikan dalam mengurangi potensi serangan ulang. Implementasi monitoring berkelanjutan juga menjadi faktor penting dalam menjaga stabilitas dan keamanan sistem. Dengan demikian, digital forensik tidak hanya berperan dalam investigasi, tetapi juga sebagai pendekatan strategis dalam meningkatkan ketahanan keamanan website berbasis WordPress.

4.2 Saran

Adapun saran yang dapat diberikan berdasarkan penelitian ini adalah sebagai berikut :

1) Administrator website disarankan untuk selalu melakukan pembaruan (update) secara berkala terhadap WordPress core, plugin, dan tema guna menutup celah keamanan.
2) Perlu diterapkan kebijakan keamanan yang ketat seperti penggunaan password yang kuat, pembatasan hak akses pengguna, serta aktivasi firewall aplikasi web (WAF).
3) Disarankan untuk melakukan backup data secara rutin serta audit keamanan secara berkala guna mengantisipasi kemungkinan serangan di masa depan.
4) Penggunaan tools monitoring dan intrusion detection system (IDS) perlu dioptimalkan untuk mendeteksi aktivitas mencurigakan secara real-time.
5) Penelitian selanjutnya diharapkan dapat mengembangkan sistem deteksi otomatis berbasis kecerdasan buatan (AI) untuk meningkatkan efektivitas identifikasi malware pada WordPress.
6) Edukasi terhadap pengguna dan pengelola website perlu ditingkatkan agar memiliki kesadaran terhadap pentingnya keamanan siber dan praktik penggunaan sistem yang aman.

REFERENSI

[1] Kaspersky Lab, 2023, *Vulnerable WordPress Plugins and Themes as Cybersecurity Threats*, Kaspersky Research Report, Moscow.
[2] Sucuri, 2024, *Website Threat Research Report: WordPress Malware Analysis*, Sucuri Inc., California.
[3] Wordfence, 2023, *WordPress Security Report: Vulnerabilities and Attack Trends*, Wordfence Inc., Seattle.
[4] Zhang, Y., Liu, H., and Chen, X., 2022, "Detection of Web Malware Based on Behavior Analysis," *Journal of Cyber Security Technology*, vol. 6, no. 2, hal. 85–102.
[5] Alazab, M., Venkatraman, S., and Watters, P., 2021, "Zero-day Malware Detection Based on Supervised Learning Algorithms of API Call Signatures," *IEEE Access*, vol. 9, hal. 12807–12817.
[6] Behl, A., Behl, K., and Behl, K., 2022, "Cybersecurity and Cyberwar: What Everyone Needs to Know," *Oxford University Press*, New York.
[7] Casey, E., 2020, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed., Academic Press, London.

[8] Choo, K. K. R., 2021, "The Cyber Threat Landscape: Challenges and Future Research Directions," *Computers & Security*, vol. 102, hal. 102206.

[9] Sharma, R., and Gupta, A., 2023, "Web Application Security: Attacks and Prevention Techniques," *International Journal of Information Security Science*, vol. 12, no. 1, hal. 45–60.

[10] Rahman, M. A., et al., 2024, "Analysis of WordPress Security Vulnerabilities and Mitigation Strategies," *Journal of Information Security and Applications*, vol. 75, hal. 103456.

[11] Singh, J., and Singh, J., 2022, "Malware Analysis and Detection Techniques: A Survey," *International Journal of Computer Applications*, vol. 184, no. 12, hal. 1–10.

[12] OWASP Foundation, 2023, *OWASP Top 10: The Ten Most Critical Web Application Security Risks*, OWASP, USA.

[13] NIST, 2021, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86, USA.

[14] Krombholz, K., et al., 2020, "Advanced Obfuscation Techniques in Malware: Analysis and Detection," *Proceedings of IEEE Security Symposium*, San Francisco, May 2020.

[15] Sarker, I. H., 2021, "Cybersecurity Data Science: An Overview from Machine Learning Perspective," *Journal of Big Data*, vol. 8, no. 1, hal. 1–29.