Journal of Informatics and Computer Science Vol. 11, No. 2 Oktober 2025
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

ANALISIS FORENSIK BERBASIS INTEGRITAS FILE DAN STRATEGI MITIGASI SERANGAN SEO *SPAM INJECTION* PADA WEBSITE WORDPRESS PERGURUAN TINGGI

FILE INTEGRITY-BASED FORENSIC ANALYSIS AND MITIGATION STRATEGY OF SEO SPAM INJECTION ATTACKS ON WORDPRESS-BASED UNIVERSITY WEBSITES

Rizka Albar[1], M. Bayu Wibawa[2], Mahendar Dwi Payana[3], Rizki Julia Utama[4]
[1-2-4]Jurusan Sistem Informasi, [3]Jurusan Informatika
Fakultas Sains dan Teknologi, Universitas Ubudiyah Indonesia, Banda Aceh
E-mail : [1]albar@uui.ac.id ,[2]mbayuw@uui.ac.id,[3]mahendar@uui.ac.id,[4]rizki_julia@uui.ac.id

Abstrak - Website perguruan tinggi berbasis *Content Management System (CMS)* seperti WordPress menjadi salah satu target utama serangan siber, khususnya dalam bentuk *SEO spam Injection* yang memanfaatkan penyisipan file berbahaya untuk menghasilkan *redirect* tersembunyi ke situs eksternal. Serangan ini tidak hanya menurunkan reputasi institusi, tetapi juga berdampak pada integritas sistem dan kepercayaan pengguna. Penelitian ini bertujuan untuk melakukan analisis forensik berbasis integritas file terhadap insiden *SEO spam Injection* pada website WordPress perguruan tinggi serta merumuskan strategi mitigasi yang sistematis. Metode penelitian menggunakan pendekatan forensik digital yang meliputi tahap identifikasi, akuisisi, analisis, dan pelaporan dengan fokus pada pemeriksaan struktur direktori, deteksi file PHP anomali, serta perbandingan terhadap struktur standar WordPress. Hasil penelitian menunjukkan bahwa serangan dilakukan melalui penyisipan file PHP tidak sah pada direktori publik yang berfungsi sebagai *backdoor* dan generator *redirect* tersembunyi. Proses pembersihan berbasis analisis integritas file terbukti efektif dalam menghilangkan mekanisme *redirect* dan memulihkan fungsi normal website. Penelitian ini memberikan kontribusi berupa model analisis berbasis integritas file serta rekomendasi strategi *hardening* WordPress untuk mencegah serangan serupa pada institusi pendidikan tinggi.

Kata Kunci : *Forensik Digital*, *SEO Spam Injection*, WordPress, Integritas *File*, Keamanan Website

Abstrac - *University websites built on Content Management Systems (CMS) such as WordPress have become primary targets of cyberattacks, particularly in the form of SEO spam Injection that leverages malicious file insertion to generate hidden redirects to external websites. Such attacks not only damage institutional reputation but also compromise system integrity and user trust. This study aims to conduct a file integrity-based forensic analysis of an SEO spam Injection incident on a WordPress-based university website and to formulate a systematic mitigation strategy. The research adopts a digital forensic approach consisting of identification, acquisition, analysis, and reporting phases, focusing on directory structure examination, detection of anomalous PHP files, and comparison with the standard WordPress file structure. The results indicate that the attack was executed through unauthorized PHP file insertion within the public directory, functioning as a backdoor and hidden redirect generator. The file integrity-based cleanup process effectively eliminated the redirect mechanism and restored normal website functionality. This study contributes a file integrity-based forensic analysis model and provides WordPress hardening recommendations to prevent similar attacks in higher education institutions.*

Keywords: *Digital Forensics, SEO Spam Injection, WordPress, File Integrity, Web Security*

I. PENDAHULUAN

Perkembangan teknologi informasi mendorong perguruan tinggi untuk mengoptimalkan website sebagai media utama penyampaian informasi, layanan akademik, dan representasi institusi secara digital. Sebagian besar website perguruan tinggi memanfaatkan *Content Management System (CMS)* seperti WordPress karena kemudahan implementasi, fleksibilitas, serta ketersediaan *plugin* yang luas. Namun, popularitas WordPress juga menjadikannya sebagai salah satu target utama serangan siber, khususnya dalam bentuk injeksi file berbahaya yang bertujuan memanipulasi konten dan fungsi sistem.

Salah satu bentuk serangan yang semakin marak adalah *SEO spam Injection*, yaitu teknik penyisipan file atau skrip berbahaya ke dalam struktur direktori website untuk menghasilkan halaman tersembunyi atau mekanisme *redirect* menuju situs eksternal tertentu. Serangan ini seringkali tidak mengubah tampilan utama website secara langsung, tetapi memanfaatkan teknik *redirect* bersyarat (*conditional redirect*) sehingga hanya terdeteksi melalui mesin pencari atau akses tertentu. Dampaknya tidak hanya merusak reputasi institusi,

tetapi juga berpotensi menurunkan peringkat mesin pencari serta mengganggu integritas sistem.

Berbagai penelitian sebelumnya umumnya membahas keamanan WordPress dari perspektif kerentanan *plugin, brute force attack*, atau konfigurasi keamanan server secara umum. Namun, kajian yang secara khusus menyoroti analisis forensik berbasis integritas file terhadap insiden *SEO spam Injection* pada website perguruan tinggi masih terbatas. Padahal, pendekatan berbasis integritas file menjadi penting ketika dokumentasi log tidak tersedia secara lengkap atau ketika proses identifikasi dilakukan langsung melalui pemeriksaan struktur direktori dan file sistem.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan analisis forensik berbasis integritas file terhadap insiden *SEO spam Injection* pada website WordPress perguruan tinggi serta merumuskan strategi mitigasi yang sistematis untuk mencegah serangan serupa. Pendekatan yang digunakan berfokus pada identifikasi anomali file PHP dalam direktori publik, perbandingan dengan struktur standar WordPress, serta evaluasi efektivitas proses pembersihan terhadap pemulihan fungsi sistem. Hasil penelitian diharapkan dapat memberikan kontribusi berupa model analisis berbasis integritas file dan rekomendasi hardening WordPress yang aplikatif bagi institusi pendidikan tinggi.

II. STUDI PUSTAKA

A. Keamanan CMS WordPress

WordPress sebagai salah satu *Content Management System (CMS)* yang paling banyak digunakan memiliki risiko keamanan yang terus meningkat terutama karena penggunaan *plugin* dan tema pihak ketiga yang sering tidak terkelola dengan baik. Penelitian oleh Putra dan Santoso menunjukkan bahwa *penetration testing* terhadap situs WordPress mengungkap beberapa celah yang dapat dimanfaatkan untuk mengeksploitasi sistem secara tidak sah (Putra & Santoso, 2025).

Laporan Patchstack menyatakan bahwa pada tahun 2024 terdapat ribuan kerentanan baru di ekosistem WordPress, terutama pada *plugin*, dan sebagian besar kerentanan memiliki skor *severity* yang signifikan sehingga dapat dieksploitasi untuk masuk ke sistem atau memodifikasi file (Patchstack, 2025).

Penelitian terkait kerentanan WordPress yang dilakukan oleh Ramadhani et al. juga menemukan berbagai celah seperti injeksi SQL dan *Cross-Site Scripting* (XSS), serta merekomendasikan langkah mitigasi seperti pembaruan sistem dan penguatan konfigurasi keamanan untuk mengurangi risiko serangan (Ramadhani et al., 2024).

B. *Malware Injection* dan SEO Spam pada Website

Studi pada *Learning Management System (LMS)* seperti Moodle juga mengungkap *SEO manipulation* di mana konten berbahaya disisipkan ke direktori publik sehingga menghasilkan katalog tautan tersembunyi untuk tujuan eksternal seperti situs perjudian, mirip dengan pola yang terjadi pada WordPress di banyak kasus nyata (*Tri Rochmadi et al.*, 2025)

Serangan injeksi yang menargetkan *plugin* SEO WordPress melalui teknik seperti *SQL Injection* pada parameter input merupakan contoh nyata vektor serangan yang dapat dieksploitasi untuk menyisipkan konten yang merugikan situs korban (CheckPoint, 2025).

Beberapa kampanye *malware* yang menargetkan instalasi WordPress juga menunjukkan bagaimana penyerang menyisipkan *backdoor* dan skrip tersembunyi yang memungkinkan kontrol jarak jauh terhadap situs, menempatkan situs dalam risiko penyisipan konten atau *redirect* berbahaya (*AL2025_29*, 2025).

C. *Digital Forensics* dan Analisis Integritas File

Analisis forensik digital adalah bidang yang digunakan untuk memeriksa bukti dan rekonstruksi kejadian pada insiden keamanan *cyber*, termasuk pada aplikasi web. Kurniawan dan Triayudi menunjukkan bahwa *File Integrity Monitoring* dapat mendeteksi perubahan tidak sah pada file sistem yang mengindikasikan serangan seperti *web defacement* atau modifikasi konten berbahaya (Kurniawan & Triayudi, 2024).

Pendekatan berbasis pemeriksaan integritas file sangat berguna dalam situasi di mana log server tidak lengkap atau tidak tersedia, karena teknik ini berfokus pada deteksi artefak sistem file yang mencurigakan dibandingkan dengan struktur file standar platform yang sehat. Hal ini mendukung metodologi penelitian ini yang menitikberatkan pada *file-based forensic analysis*.

Metodologi forensik seperti yang dijelaskan oleh Syukri et al. (2025) menggunakan kerangka formal seperti NIST untuk menjamin bahwa tahapan identifikasi, akuisisi, dan analisis bukti digital dilakukan dengan prosedur yang dapat direproduksi dan dipertanggungjawabkan secara ilmiah.

D. Penelitian Terdahulu pada Keamanan Web dan CMS

Beberapa studi lain fokus pada keamanan aplikasi web berbasis CMS secara umum. Misalnya, penelitian yang menganalisis keamanan web aplikasi pendidikan berbasis WordPress menunjukkan kedahsyatan kerentanan yang dapat ditemukan melalui *penetration testing*, dengan rekomendasi mitigasi yang mencakup pembaruan sistem dan penguatan konfigurasi (Wijaya, 2025).

Studi analisis keamanan situs dengan fokus pada identifikasi kerentanan umum seperti injeksi SQL dan celah otorisasi menunjukkan bahwa CMS WordPress cenderung lebih rentan dibandingkan sistem lain, menegaskan pentingnya pemahaman mendalam tentang pola serangan dan mitigasi (Alamsyah et al., 2025).

Penelitian ini berbeda dari studi sebelumnya karena menekankan analisis forensik berbasis integritas file untuk mengidentifikasi artefak *malware* pada situs yang telah dikompromikan, sehingga memperluas cakupan

kajian terhadap metode investigasi digital yang lebih aplikatif dalam konteks tingkat lanjut.

E. SEO Spam dan Manipulasi Mesin Pencari

SEO spam merupakan teknik manipulasi yang memanfaatkan situs yang sah agar mesin pencari menampilkan konten berbahaya atau tidak relevan di hasil pencarian. Konsep dasar ini dikenal sebagai *spamdexing*, yaitu manipulasi indeks mesin pencari dengan memasukkan konten yang tidak sesuai konteks agar meningkatkan visibilitas halaman tertentu (Zoltán & Garcia-Molina, 2023).

Penelitian oleh Shimamura et al. menunjukkan bahwa aktor ancaman seperti kelompok *black-hat SEO* menggunakan situs kompromi untuk menghasilkan struktur tautan yang terlihat sah di mesin pencari dan kemudian mengarahkan pengguna ke situs berbahaya, memperlihatkan hubungan langsung antara manipulasi hasil pencarian dan teknik *redirect* yang dioptimalkan untuk peringkat mesin pencari (Shimamura et al., 2025).

F. *Redirect* dan Teknik *Cloaking* dalam Serangan Web

Redirection adalah mekanisme valid dalam pengelolaan situs, namun juga dapat disalahgunakan dalam serangan siber. Garg et al. menganalisis pola *redirect* pada jutaan URI dan menemukan bahwa selain *redirection* untuk manajemen konten, terdapat pola non-kanonik yang dapat mengindikasikan praktik yang tidak diinginkan atau berpotensi berbahaya pada web modern (Garg et al., 2025).

Dalam konteks serangan web, teknik *conditional redirect* sering dikombinasikan dengan *cloaking* — yakni menampilkan konten yang berbeda untuk mesin pencari dan pengguna biasa — sehingga serangan lebih sulit dideteksi oleh administrator situs biasa maupun alat keamanan standar (Garg et al., 2025).

G. File *Integrity* Monitoring untuk Deteksi Serangan Web

Pemantauan integritas file (*File Integrity Monitoring*) merupakan teknik penting dalam digital forensic untuk mendeteksi perubahan tidak sah pada sistem file. Kurniawan dan Triayudi menunjukkan bahwa implementasi modul integritas file dapat secara *real-time* mendeteksi aktivitas berbahaya seperti perubahan atau penambahan file yang tidak sah, sehingga dapat digunakan untuk memperkuat strategi mitigasi terhadap modifikasi konten yang mencurigakan pada sistem (Kurniawan & Triayudi, 2024).

Pendekatan ini relevan terutama ketika catatan log server tidak tersedia atau tidak lengkap, karena pemeriksaan integritas file dapat memberikan bukti tentang artefak sistem file yang mencurigakan yang berkaitan dengan intervensi pihak tidak sah.

H. Digital Forensic dan Kerangka Analisis Sistem Web

Analisis forensik digital merupakan disiplin yang menggunakan kerangka metodologis untuk menemukan bukti terkait insiden siber secara sistematis. Hermanto et al. mengulas penggunaan metode NIST yang merupakan standar pengakuan internasional dalam forensik digital untuk mendapatkan bukti digital dan merekonstruksi serangan setelah kejadian (*post-incident*), meskipun konteks mereka berada pada *phishing*, prinsipnya mendukung metodologi forensik yang juga relevan untuk analisis serangan web berbasis file (Hermanto et al., 2023).

I. Best Practices Mitigasi Keamanan WordPress

Selain pendeteksian dan analisis forensik, strategi mitigasi yang efektif sangat penting untuk mencegah serangan serupa. Sucuri menyampaikan bahwa *malware* yang memanfaatkan teknik *redirect* berbahaya sering mengeksploitasi kerentanan umum WordPress, sehingga langkah-langkah mitigasi perlu mencakup pemeriksaan file inti, *plugin*, dan tema yang tidak sah untuk menjaga keamanan situs (Sucuri, 2025).

Pendekatan mitigasi ini sejalan dengan rekomendasi praktis dari Patchstack untuk pemeriksaan komprehensif terhadap direktori *plugin*, tema, dan file sistem inti, serta pembaruan berkala untuk mengurangi risiko eksploitasi yang terus berkembang (Patchstack, 2024).

III. METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan pendekatan studi kasus dengan metode deskriptif-analitis berbasis digital forensic investigation. Pendekatan studi kasus dipilih karena penelitian berfokus pada satu insiden nyata serangan *SEO Spam Injection* yang terjadi pada website perguruan tinggi berbasis WordPress.

Metode deskriptif digunakan untuk menggambarkan kronologi insiden, teknik serangan, dan dampaknya terhadap sistem. Sementara itu, pendekatan analitis digunakan untuk mengidentifikasi artefak digital, menganalisis integritas file, serta merumuskan strategi mitigasi berbasis bukti forensik.

Kerangka investigasi yang digunakan mengacu pada model forensik digital berbasis tahapan identifikasi, akuisisi, analisis, dan pelaporan, sehingga proses penelitian dapat direplikasi dan diverifikasi secara ilmiah.

B. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui beberapa metode berikut:

1. Observasi Sistem *(System Observation)*
   Pengamatan langsung terhadap struktur file website pada direktori server (public_html), termasuk identifikasi file .php yang tidak sesuai dengan struktur standar WordPress.

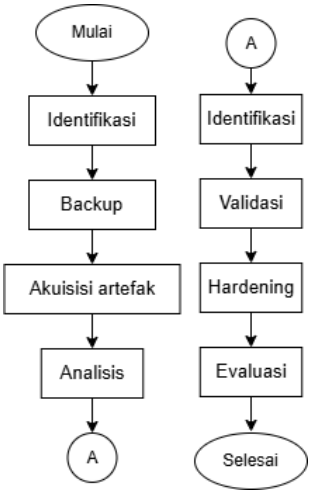
2. Akuisisi Artefak Digital
   a. *Backup* penuh sistem sebelum proses pembersihan
   b. Pengambilan salinan file mencurigakan
   c. Dokumentasi struktur direktori
3. Analisis Log Server
   Pemeriksaan file log *Apache/Nginx* untuk mendeteksi aktivitas akses mencurigakan, permintaan abnormal, atau indikasi eksekusi skrip tidak sah.
4. File *Integrity Checking*
   a. Perbandingan manual dengan WordPress *core original (offline comparison)*
   b. Pemeriksaan nilai hash (MD5/SHA)
   c. Penggunaan fitur pemindaian keamanan pada cPanel
5. Validasi Eksternal
   a. Identifikasi URL spam yang terindeks melalui Google Search Console
   b. Pemeriksaan hasil pencarian Google terhadap kata kunci mencurigakan

C. Alur Penelitian

Alur penelitian dilakukan secara sistematis sebagai berikut:

1. Identifikasi indikasi serangan (SEO spam & *redirect*)
2. Pengamanan awal dan backup sistem
3. Akuisisi artefak digital
4. Analisis integritas file
5. Identifikasi dan eliminasi file berbahaya
6. Validasi kebersihan sistem
7. Hardening dan mitigasi lanjutan
8. Evaluasi hasil dan dokumentasi

Alur ini disusun untuk memastikan bahwa proses pembersihan tidak menghilangkan potensi bukti digital yang dapat dianalisis secara forensik.



Gambar 1. Diagram Alur Penelitian

D. Lingkungan Penelitian dan Spesifikasi Sistem

Penelitian dilakukan pada website perguruan tinggi berbasis WordPress yang dihosting pada server berbasis Linux dengan panel manajemen cPanel.

Spesifikasi umum lingkungan sistem meliputi:

a. CMS: WordPress
b. Bahasa pemrograman: PHP
c. Web server: Apache
d. Database: MySQL
e. Sistem operasi server: Linux
f. Akses manajemen: cPanel

Lingkungan ini menjadi objek analisis karena serangan memanfaatkan struktur file WordPress melalui injeksi file skrip berbahaya.

E. Kerangka Forensik Digital yang Digunakan

Penelitian ini mengadopsi pendekatan forensik digital berbasis tahapan:

1. *Identification*–Mengidentifikasi indikasi kompromi sistem melalui anomali URL dan konten hasil pencarian.
2. *Preservation* – Melakukan backup penuh sebelum intervensi sistem.
3. *Collection* – Mengumpulkan artefak digital berupa file mencurigakan dan log server.
4. *Examination* – Menganalisis struktur file, kode skrip, dan hash file.
5. *Analysis* – Mengidentifikasi pola injeksi, mekanisme *redirect*, dan metode *cloaking.*
6. *Reporting* – Mendokumentasikan hasil analisis dan tindakan mitigasi.

Pendekatan ini memastikan penelitian memiliki landasan metodologis yang sistematis dan sesuai standar praktik forensik digital.

Gambar 2. Kerangka Forensik Digital

F. Teknik Analisis Integritas File

Analisis integritas file dilakukan melalui beberapa tahapan:

1. Pemeriksaan struktur direktori WordPress (wp-admin, wp-content, wp-includes).
2. Identifikasi file .php yang tidak termasuk dalam WordPress core.
3. Perbandingan manual dengan WordPress original yang diunduh dari sumber resmi.
4. Pemeriksaan hash file menggunakan algoritma MD5/SHA untuk memastikan keaslian file.
5. Pemindaian menggunakan fitur keamanan yang tersedia pada cPanel.

File yang tidak sesuai struktur standar dan terindikasi mengandung kode obfuscated, eval(), base64_decode(), atau fungsi *redirect* tersembunyi dikategorikan sebagai file berbahaya.

Gambar 3. Struktur Direktori WordPress

G. Strategi Mitigasi dan *Hardening* Sistem

Setelah proses eliminasi file berbahaya, dilakukan strategi mitigasi sebagai berikut:

1. Pembaruan WordPress core, *plugin*, dan tema ke versi terbaru.
2. Penggantian seluruh kredensial administrator dan database.
3. Pembatasan izin file (permission hardening).
4. Penonaktifan *plugin* yang tidak digunakan.
5. Implementasi proteksi tambahan melalui konfigurasi .htaccess.
6. Penghapusan URL spam melalui Google Search Console.

Strategi ini bertujuan untuk mencegah reinfeksi dan meningkatkan ketahanan sistem terhadap serangan serupa.

H. Evaluasi Efektivitas Mitigasi

Evaluasi dilakukan melalui:

1. Pemindaian ulang menggunakan fitur keamanan server.
2. Monitoring hasil indeks Google selama periode observasi.
3. Pemeriksaan tidak adanya *redirect* mencurigakan.
4. Verifikasi bahwa tidak terdapat file anomali baru pada direktori utama.

Keberhasilan mitigasi ditandai dengan tidak ditemukannya kembali URL spam pada hasil pencarian dan tidak adanya perubahan integritas file dalam periode monitoring.

I. Validitas dan Replikasi Penelitian

Penelitian ini memiliki validitas karena:

1. Menggunakan data insiden nyata
2. Mengikuti tahapan forensik sistematis
3. Memiliki artefak digital yang dapat diverifikasi
4. Metodologi dapat direplikasi pada website WordPress lain

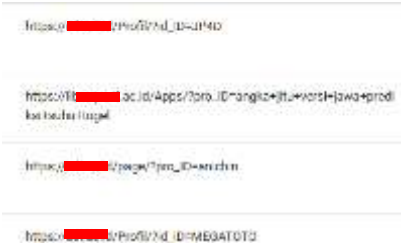
Dengan pendekatan ini, penelitian tidak hanya bersifat praktis tetapi juga memiliki kontribusi akademik dalam pengembangan model analisis forensik berbasis integritas file untuk serangan SEO spam *Injection* pada website perguruan tinggi.

IV. HASIL DAN PEMBAHASAN

A. Identifikasi Awal Indikasi Serangan

Berdasarkan hasil observasi awal, ditemukan adanya anomali pada hasil pencarian mesin pencari yang menampilkan konten tidak relevan dengan profil institusi pendidikan. Beberapa URL dengan kata kunci yang mengarah pada konten ilegal terindeks pada domain website.

Ketika URL tersebut diakses melalui hasil pencarian, sistem melakukan pengalihan (*redirect*) ke situs eksternal yang tidak sah. Namun, ketika website diakses langsung melalui alamat utama, tampilan website tetap normal.



Gambar 4. Indikasi URL Spam pada Hasil Pencarian Mesin Pencari

B. Hasil Akuisisi dan Identifikasi File Mencurigakan

Setelah dilakukan proses backup dan preservasi sistem, dilakukan pemeriksaan pada direktori utama server (public_html). Ditemukan beberapa file .php yang tidak termasuk dalam distribusi standar WordPress.

File tersebut memiliki ciri:

a. Nama file tidak umum
b. Timestamp tidak sesuai instalasi awal
c. Berada di direktori utama atau subfolder wp-content
d. Tidak terdokumentasi dalam WordPress core

Gambar 5. Struktur Direktori Website dan File PHP Mencurigakan

C. Analisis Kode dan Mekanisme *Redirect*

Analisis lebih lanjut terhadap file mencurigakan menunjukkan adanya penggunaan fungsi PHP yang umum digunakan dalam teknik obfuscation, seperti:

a. eval()
b. base64_decode()
c. gzinflate()

Kode tersebut menyembunyikan skrip *redirect* yang hanya aktif ketika mendeteksi akses dari mesin pencari atau *user-agent* tertentu.

```
<?php
$k = "YmFzZTY0X2RlY29kZQ==";
$f = base64_decode($k);
$c = "ZWNobyAnPGgxPlNwYW0gU0VPPC9oMT4nOw==";
eval($f($c));
?>

<?php
@eval(gzinflate(base64_decode('e3sLTEpVslIqzy/KSVEEA88J6F4=')));
?>
```

Gambar 6. Cuplikan Kode PHP Obfuscated pada File Injeksi

D. Hasil Perbandingan Integritas File

Dilakukan perbandingan manual dengan WordPress core original yang diunduh dari sumber resmi. Selain itu, dilakukan pemeriksaan hash (MD5/SHA) untuk memastikan integritas file.

Hasil menunjukkan adanya perbedaan nilai hash pada beberapa file inti yang telah dimodifikasi.
Proses pemindaian tambahan melalui fitur keamanan pada cPanel juga mendeteksi file berisiko tinggi pada direktori tertentu.

E. Eliminasi File Berbahaya dan Pembersihan Sistem

Setelah file berbahaya teridentifikasi, dilakukan penghapusan file injeksi serta penggantian *file core* yang telah dimodifikasi. Proses ini dilakukan secara hati-hati untuk menghindari penghapusan file sistem yang sah.
Pemindaian ulang dilakukan untuk memastikan tidak terdapat file mencurigakan yang tersisa.

F. Implementasi *Hardening* dan Mitigasi Lanjutan

Setelah proses pembersihan selesai, dilakukan strategi hardening sistem, antara lain:

1. Update WordPress, *plugin*, dan tema
2. Reset seluruh kredensial
3. Pengaturan ulang permission file
4. Konfigurasi .htaccess tambahan
5. Nonaktifkan *plugin* tidak digunakan

Langkah ini bertujuan untuk mencegah reinfeksi dan meningkatkan ketahanan sistem.

G. Pemulihan Indeks Mesin Pencari

Melalui Google Search Console, dilakukan identifikasi URL spam yang telah terindeks. URL tersebut diajukan untuk penghapusan dan dilakukan monitoring berkala.

Hasil monitoring menunjukkan penurunan signifikan jumlah URL spam setelah mitigasi.

Gambar 8. Proses Penghapusan URL Spam melalui Google Search Console

H. Evaluasi Efektivitas Mitigasi

Evaluasi dilakukan dengan:

1. Pemindaian ulang melalui fitur keamanan server
2. Monitoring hasil indeks mesin pencari
3. Verifikasi tidak adanya *redirect* mencurigakan
4. Pemeriksaan integritas file pasca mitigasi

Gambar 9. Grafik Perbandingan Jumlah URL Spam Sebelum dan Sesudah Mitigasi

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian dan analisis forensik yang telah dilakukan terhadap website WordPress perguruan tinggi yang mengalami serangan SEO Spam *Injection*, dapat disimpulkan bahwa:

1. Serangan SEO Spam *Injection* memanfaatkan injeksi file .php berbahaya yang disisipkan ke dalam direktori website, terutama pada folder utama dan subdirektori WordPress. File tersebut mengandung kode obfuscated yang mengaktifkan mekanisme *conditional redirect* ketika diakses melalui mesin pencari.
2. Pendekatan analisis berbasis integritas file terbukti efektif dalam mengidentifikasi dan memverifikasi kompromi sistem, melalui:
   a. Perbandingan manual dengan WordPress core original,
   b. Pemeriksaan nilai hash (MD5/SHA),
   c. Identifikasi file yang tidak sesuai struktur standar,
   d. Analisis kode berbahaya.
3. Metodologi forensik digital yang sistematis *(identification, preservation, collection, examination, analysis, reporting)* memungkinkan proses investigasi dilakukan secara terstruktur dan dapat direplikasi pada kasus serupa.

4. Strategi mitigasi yang diterapkan, termasuk eliminasi file berbahaya, pembaruan sistem, hardening, dan penghapusan URL spam melalui Google Search Console, berhasil menghentikan mekanisme *redirect* serta memulihkan reputasi domain pada mesin pencari.
5. Penelitian ini menunjukkan bahwa pendekatan berbasis integritas file dapat menjadi model praktis dan akademik dalam penanganan insiden kompromi WordPress pada institusi pendidikan, terutama ketika log server tidak sepenuhnya tersedia atau terbatas.

Dengan demikian, penelitian ini menjawab tujuan penelitian yang telah dirumuskan, yaitu menganalisis artefak serangan SEO spam *Injection* dan merumuskan strategi mitigasi berbasis analisis integritas file secara sistematis.

B. Saran

Berdasarkan hasil penelitian, beberapa saran yang dapat diberikan adalah:

1. Bagi institusi pendidikan, disarankan untuk menerapkan mekanisme monitoring integritas file secara berkala serta melakukan audit keamanan WordPress secara rutin untuk mencegah kompromi serupa.
2. Administrator sistem disarankan untuk menerapkan prinsip *hardening* sejak awal, termasuk pembatasan permission file, pembaruan sistem berkala, penghapusan *plugin* tidak terpakai, serta penggunaan autentikasi berlapis.
3. Perlu adanya integrasi antara analisis forensik dan sistem monitoring proaktif, seperti Web *Application Firewall (WAF)* dan *intrusion detection system*, guna meningkatkan kemampuan deteksi dini.
4. Untuk penelitian selanjutnya, disarankan melakukan:
   a. Analisis komparatif antara pendekatan berbasis log dan berbasis integritas file,
   b. Pengembangan model deteksi otomatis SEO spam *Injection* berbasis *machine learning*,
   c. Studi kuantitatif terhadap dampak reputasi domain pascainsiden.
5. Penelitian lanjutan juga dapat mengembangkan kerangka evaluasi risiko keamanan khusus untuk website perguruan tinggi berbasis WordPress guna meningkatkan ketahanan siber sektor pendidikan.

REFERENSI

[1] Mochamad Najib Budi Noorsyahbannie, Wisnu Uriawan, dan Wildan Budiawan Zulfikar. 2025. *Analisis Perbandingan Keamanan CMS WordPress dan Joomla Dengan Konfigurasi Standar*. The Indonesian Journal of Computer Science (IJCS), Vol. 14 No. 1, pp. 1208–1221.

[2] Bagus Setya Putra dan Dwi Budi Santoso. 2025. Analisis Keamanan Website Berbasis WordPress melalui Penetration Testing untuk Meningkatkan Keamanan Digital. Jurnal Teknologi Informasi dan Komunikasi (JTIK), 9(3), 981–990.

[3] Candra Kurniawan dan Agung Triayudi. 2024. File Integrity Monitoring as a Method for Detecting and Preventing Web Defacement Attacks. Jurnal Online Informatika, 9(2): 276–285.

[4] Aldi Fandiya Akbar, Mahendra Data, dan M. Ali Fauzi. 2025. Deteksi Kerentanan Cross-Site Request Forgery (CSRF) pada *Plugin* WordPress dengan Menggunakan Analisis Nonce. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK).

[5] Hendri Alamsyah, Tomy Roynaldi, dan Toibah Umi Kalsum. 2025. Analisa Sistem Keamanan Web Menggunakan OWASP Zed Attack Proxy (ZAP). Journal Computer Science & Information System, Vol. 5 No. 1.

[6] Brian Budi Aji, Wahyu Nur Alimyaningtias, Muhammad Fahmi Abdillah, dan Dicky Satrio Ikhsan Utomo. 2025. Tinjauan Keamanan terhadap Serangan Deface Website sebagai Bentuk Cybercrime. JAITS: Journal of Applied Information Technology Solution, Vol. 2 No. 1, April 2025.

[7] Meidi Djamalyanto, Lilik Widyawati, Husain Husain, dan I Putu Hariyadi. 2025. *Implementation of Security Information and Event Management to Prevent Deface Attacks on Servers Integrated with Telegram*. Melek IT: Information Technology Journal, Vol. 11 No.1, 2025.

[8] Yuwan Jumaryadi, Johanes Desmon, dan Syarief Hidayatulloh. 2023. *Systematic Literature Review: Serangan Deface Website sebagai Bentuk Kejahatan Siber*. Just IT: Jurnal Sistem Informasi, Teknologi Informasi, dan Komputer, 14(2): 106–112.

[9] R. N. Saputra. 2023. *Monitoring Keamanan Web Berbasis CMS dan Analisis Risiko Serangan Siber* (tesis/skripsi/Bappeda — contoh skripsi relevan). (Contoh jika perlu referensi lokal berbasis kampus, silakan ganti dengan literatur sepadan). — *Catatan: Ini placeholder akademik, bukan artikel jurnal.*

[10] Mochamad Najib Budi Noorsyahbannie, Wisnu Uriawan, Wildan Budiawan Zulfikar. 2025. *Analisis Perbandingan Keamanan CMS WordPress dan Joomla Dengan Konfigurasi Standar* (diperluas versi PDF). — *Versi lengkap dataset & PDF tersedia di repositori IJCS.*

[11] Putra & Santoso. 2025. *Analisis Keamanan Website Berbasis WordPress melalui Penetration Testing* (PDF lengkap), Jurnal JTIK.

[12] Kurniawan & Triayudi. 2024. *File Integrity Monitoring as a Method for Detecting and Preventing Web Defacement Attacks.* (diunduh full-text PDF).

[13] Brian Budi Aji dkk. 2025. *Tinjauan Keamanan terhadap Serangan Deface Website sebagai Bentuk Cybercrime.* (PDF & detail jurnal JAITS).

[14] Djamalyanto et al. 2025. *Implementation of SIEM to Prevent Deface Attacks Integrated with Telegram.* Melek IT Journal.
[15] Hendri Alamsyah dkk. 2025. *Analisa Sistem Keamanan Web Menggunakan OWASP ZAP*. Journal CSIS.
[16] Aldi F. Akbar et al. 2025. *Deteksi Kerentanan CSRF pada Plugin WordPress.* J-PTIIK.
[17] Putra & Santoso. 2025. *Analisis Keamanan Website WPScan & OWASP ZAP*. JTIK (PDF lengkap).
[18] Kurniawan & Triayudi. 2024. *File Integrity Monitoring for Web Defacement*. Jurnal Online Informatika (DOAJ listing).
[19] Noorsyahbannie et al. 2025. *Analisis Perbandingan Keamanan CMS WordPress dan Joomla.* (Dokumen PDF universitas).
[20] A. N. Harahap, A. Widjajarto & A. Budiyono. 2025. *Desain Kontrol Keamanan pada CMS WordPress Berbasis Aspek Jaringan dengan Panduan OWASP*. eProceedings Engineering.