Journal of Informatics and Computer Science Vol.12 No. 1 April 2026
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

ANALISIS DAN PENANGANAN INSIDEN KEAMANAN SIBER: SERANGAN SINDIKAT JUDI ONLINE PADA WEBSITE UNIVERSITAS UBUDIYAH INDONESIA

ANALYSIS AND MITIGATION OF CYBERSECURITY INCIDENTS: ONLINE GAMBLING SYNDICATE ATTACKS ON THE UNIVERSITY OF UBUDIYAH INDONESIA WEBSITE

Mahendar Dwi Payana[1], Rifki Sani[1], Zuhar Musliyana[2], Rizka Albar[2], M. Bayu Wibawa[1]
[1]Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas, Ubudiyah Indonesia
[2]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas, Ubudiyah Indonesia
Jl. Alue Naga Desa Tibang Kecamatan Syiah Kuala Banda Aceh
Koresponden E-mail: mahendar@uui.ac.id[1]

Abstrak— Kasus peretasan situs web akademik oleh sindikat judi *online* telah menjadi ancaman serius bagi institusi Pendidikan di Indonesia. Penelitian ini mendokumentasikan dan menganalisis insiden keamanan siber yang terjadi pada infrastruktur digital Universitas Ubudiyah Indonesia (UUI) pada periode tahun 2025. Hasil investigasi menunjukkan serangan bersifat masif dengan mengeksploitasi 18 subdomain aktif melalui kerentanan platform CMS WordPress yang sudah usang, penggunaan tema bajakan (*nulled*), dan celah *file upload* pada Open Journal System (OJS) versi 2.x. Penyerang menanamkan puluhan *backdoor shell* (seperti kobe.php, sc.php, jago.php, dan varian *script* ALFA/Rimuru) yang terobfuskasi menggunakan fungsi dinamis PHP seperti base_64_decode dan eval()[1][3]. Lebih lanjut, penyerang melakukan pembajakan hak kepemilikan pada Google Search Console (GSC) menggunakan akun luar (ilhamhidayat2522@gmail.com) untuk memanipulasi indeks pencarian melalui teknik *Blackhat SEO*, menghasilkan 123.000 klik ilegal dan 6.83 juta impresi untuk kueri-kueri tidak senonoh. Sebagai langkah remediasi, diimplementasikan isolasi subdomain, pembersihan massal otomatis, pemutakhiran sistem, dan penerapan Web Application Firewall(WAF).

Kata kunci: *Keamanan Siber, Peretasan, Judi Online, Malware, Blackat SEO*

Abstract—*Cases of academic website hacking by online gambling syndicates have become a serious threat to educational institutions in Indonesia. This study documents and analyzes a cyber security incident that occurred on the digital infrastructure of Universitas Ubudiyah Indonesia (UUI) in the 2025 period. The investigation results show a massive attack exploiting 18 active subdomains by leveraging outdated WordPress CMS applications, pirated (nulled) themes, and file upload vulnerability in Open Journal Systems (OJS) version 2.x. Attackers planted dozens of obfuscated backdoor shells (such as kobe.php, sc.php, jago.php, and ALFA/Rimuru script variants) utilizing dynamic PHP functions like base64_decode and eval(). Furthermore, attackers hijacked Google Search Console (GSC) property ownership using an unauthorized account (ilhamhidayat2522@gmail.com) to manipulate search indexing through Blackhat SEO techniques, yielding 123,000 illicit clicks and 6.83 million impressions for inappropriate queries. As mitigation steps, subdomain isolation, automated mass malware removal, system upgrades, and the implementation of Web Application Firewall (WAF) were carried out*

Keywords: *Cyber Security, Hacking, Online Gambling, Malware, Blackhat SEO*

I. PENDAHULUAN

Perkembangan teknologi informasi memberikan kemudahan akses data secara global, namun di sisi lain membuka celah bagi kejahatan dunia maya (*cybercrime*). Belakang ini, ancaman siber yang sangat marak di Indonesia adalah peretasan sites web institusi pemeriintah (.go.id) dan pendidikan (.ac.id) oleh sindikat judi online. Sindikat ini meretas laman lembaga pendidikan yang memiliki sistem keamanan yang lemah, lalu memanfaatkannya sebagai ladang promosi menggunakan teknik manipulasi mesin pencari [1].

Pada periode Januari hingga September 2025, *Direktorat Cyber Development Center* (DCDC) Universitas Ubudiyah Indonesia (UUI) mengindentifikasi anomali tingkat tinggi pada aset digital website universitas. Sejumlah website disusupi konten berbahaya yang terafiliasi dengan judi online dan konten ilegal lainnya. Srangan ini mencakup *deface* (perubahan tampilan), injeksi *blackhat SEO*, serta penanaman *backdoor rootkit* [2]. Naskah ini bertujuan untuk memberikan gambaran kronologis, analisis celah keamanan, dan langkah mitigasi yang diimplementasikan di UUI agar dapat menjadi acuan serta dasar evaluasi bagi institusi akademik lainnya dalam menghadapi ancaman serupa.

II. STUDI PUSTAKA

Peretasan (*hacking*) merupakan tindakan intrusi yang berkaitan dengan pemanfaatan sistem komputer atau jaringan tanpa izin yang sah. Dalam konteks hukum di Indonesia, peretasan yang dilakukan oleh sindikat judi online secara nyata telah melanggar Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

(UU ITE) yang telah diubah terakhir dengan Undang-undang Nomor 1 Tahun 2024. Tindakan ini dapat dijerat dengan sanksi pidana berdasarkan Pasal 30 dan Pasal 46 UUI ITE mengenai akses ilegal, serta Pasal 303 KUHP terkait perjudian [1].

Kejahatan ini sangat bermotif ekonomi, Pelaku mencari keuntungan finansial dengan meretas laman web yang memiliki reputasi tinggi (*High Domain Authority*) seperti domain akademik *(ac.id)*. Mereka menggunakan teknik *Search Engine optimization* (SEO) *Spamming* atau *Blackhat SEO* untuk memanipulasi algoritma Google, menaikkan peringkat situs judi di halaman pertama pencarian, dan menyewakan *backlink* tersebut kepada operator judi di luar negeri.

III. METODE

Metode penanganan dan penelitian insiden ini dilakukan melalui kerangka kerja respons insiden keamanan siber (*incident Response Framework*) yang mencakup empat tahapan utama :

1. **Identifikasi dan Verifikasi**: Melakukan pemindaian otomatis menggunakan malware scanner server dan menganalisis surel peringatan otomatis sistem GSC terkait pendaftaran pemilik properti (*property owner*) yang tidak sah.
2. **Isolasi:** Membatasi akses jaringan ke sistem dan 18 subdomain yang terdampak guna mencegah penyebaran infeksi secara lateral (*lateral movement*).
3. **Investigasi dan analisis Log:** Melakukan forensik digital melalui peninjauan *access log*, *server*, basis data, dasbor Google Search Console, serta penelusuran struktur direktori menggunakan utilitas baris perintah (*command-line utility*) berbasis Linux seperti grep untuk memetakan fungsi-fungsi obfuskasi kode tersembunyi.
4. **Pembersihan dan Pemulihan (Remediasi):** Penghapusan skrip berbahaya secara massal, penutupan akun administrasi ilegal pada dasbor Google, *patching* celah keamanan, migrasi CMS OJS ke versi 3.x dan pemulihan data dari cadangan bersih (*clean backup*).

IV. HASIL DAN PEMBAHASAN

A. Skala dan Dampak Insiden

Investigasi menyeluruh terhadap infrastruktur server UUI menunjukkan bahwa serangan ini tidak hanya berdampak pada subdomain utama, melainkan menyebar secara lateral ke 18 subdomain yang dikelola oleh universitas. Berdasarkan laporan otomatisasi *Malware Scanner* dan audit akses server, tabel berikut merangkum subdomain terdampak beserta berkas berbahaya (*backdoor*) yang berhasil diidentifikasi dan dibersihkan.

Tabel 1. Daftar Subdomain dan Pemetaan Subdomain Terdampak

No	Subdomain Terdampak	Plaffor m Utama	Berkas Berbahaya (Malware) yang ditemukan	Status Tndakan
1	Sipenmaru.uui .ac.id	Aplikas i Kustom	Kobe.php	Di hapus Kredensi al di-reset
2	Library.uui.ac. id	OJS 2.x	kobe.php, daa-bsdk.pdf.php, jago.php, cats	Dihapus & Migrasi Platform
3	siakad.uui.ac.i d	Aplikas i Kustom	kobe.php,	Dihapus
4	digilib.uui.ac.i d	PHP Kustom	sc.php,	Dihapus
5	simtakp.uui.ac .id	PHP Kustom	kom.php,	Dihapus
6	tuomaru.uui.ac .id	Custom MVC	Kobe.php, header.php(compre mised)	Remedias i Kode & dihapus
7	fikes.uui.ac.id	Wordpr ess	Varian skrip ALFA (perl.alfa), index.php(compro mised)	Pembersi han massal
8	Farmasi.uui.ac .id	Wordpr ess	Bash.alfa, py.alfa, 403.php	Pembersi han massal
9	Ubnews.uui.ac .id	Wordpr ess	Varian rimuru, (bash.rimuru, py.rimuru, perl.rimuru), mo.php, cache.php	Pembersi han massal
10	Fst.uui.ac.id	Wordpr ess	Injeksi direktori ./wp-admin/images/ post/php	Tambah code (*patching*)
11	Akuntansi.uui. ac.id	Wordpr ess	Injeksi direktori upload	Dihapus
12	Psikologi.uui.a c.id	Wordpr ess	Injeksi halaman spam	Eksklusi Google Index
13	Informatika.uu i.ac.id	Wordpr ess	Injeksi halaman spam	Eksklusi Google Index
14	Daa.uui.ac.id	Wordpr ess	Injeksi halaman spam	Eksklusi Google Index
15	Demosite.uui. ac.id	Wordpr ess	Injeksi halaman spam	Eksklusi Google Index
16	Evaluasi.uui.a c..id	Custom PHP	Index.php(compro mised), 403.php	Ganti dan dihapus
17	Dsdms.uui.ac.i d	Wordpr ess	/wp-content/ uploads/ sucuri/index.php	Dihapus
18	Elearning.uui. ac.id	Moodle	Berkas temporer pada /tmp	Pembersi han berkas temp

Insiden peretasan ini berdampak masih pada berbagai domain dan layanan penting di lingkungan UUI, di antaranya sistem Penerimaan Mahasiswa Baru (sipenmaru.uui.ac.id), perpustakaan (library.uui.ac.id), portal akademik (siakad.uui.ac.id), hingga situs jurnal ilmiah (jurnal.uui.ac.id).

Dampak kerugian reputasi sangat terlihat dari data *Google Search Console*. URL situr yang disusupi menghasilkan puluhan ribu impresi dan klik di mesin pencarian untuk kueri-kueri yang tidak pantas, seperti konten pornografi video jepang, dan istilah-istilah judi *slot.* Peratasan jenis *Blackhat SEO* ini menciptakan ribuan halaman fiktif berisikan kata kunci terlarang yang menumpang pada otoritas domain UUI.

B. Vektor Eksploitasi Google Search Console (GSC) dan Performa Blackhat Seo

Salah satu temuan paling krusial dalam insiden ini adalah keberhasilan penyerang melakukan **Injeksi Kepemilikan (Ownership Hijacking)** pada Google Search Console (GSC) milik UUI. Pada tanggal 22 Agustus 2025, surel peringatan keamanan dari Google mendeteksi adanya penambahan akun luar secara massal, yaitu ilhamhidayat2522@gmail.com, sebagai pemilik sah baru (*new owner*) untuk properti domain utama uui.ac.id beserta seluruh subdomain terkait.

Dengan status kepemilikan tersebut, sindikat judi online mendapatkan akses penuh terhadap kontrol pengindeksan situs di mesin pencari Google. Mereka memanfaatkan akses ini untuk:

1. Mengunggah berkas sitemap.xml fiktif yang berisi ribuan URL promosi judi slot dan pornografi.
2. Memantau efektivitas kata kunci pencarian terlarang yang mereka tanamkan.
3. Melakukan manipulasi indeks agar algoritma perayap Google memprioritaskan situs ilegal tersebut di halaman pertama.

Analisis performa riwayat dasbor GSC UUI pada periode Juni hingga September 2025 mendeteksi anomali trafik berskala masif akibat teknik *Blackhat SEO* ini. Sistem mencatat akumulasi performa sebagai berikut:

- **Total Clicks:** 123.000 (123K) klik masuk ke situs-situs subdomain UUI.
- **Total Impressions:** 6,83 Juta (6.83M) kali halaman fiktif berbau judi/lendir tampil di halaman pencarian pengguna.
- **Average Position:** Berada pada posisi rata-rata 9,8 (Halaman pertama hasil pencarian Google).

Sindikat ini secara sengaja membidik domain bertipe .ac.id karena memiliki *Domain Authority* (DA) yang sangat tinggi di mata algoritma Google, sehingga kueri-kueri mesin pencari yang tidak pantas dapat dengan mudah menduduki peringkat teratas pencarian global. Berdasarkan analisis kueri terpopuler di dasbor GSC, berikut adalah daftar kueri *spamming* teratas yang mengarah ke website UUI:

Tabel 2. Kueri Penelusuran Teratas Akibat Blackhat SEO

No	Kueri Penelusuran Terpopuler (Spam)	Jumlah Klik Ilegal	Jumlah Impresi
1	~~“Video Bokeh Japanese word origin full”~~	61	594
2	~~“proxy video barat”~~	58	3.326
3	~~“Yandex Japan”~~	28	1.261
4	~~“video bokep”~~	23	329
5	~~“bokepindo”~~	17	759
6	~~“bocil sd colmek”~~	16	115

Berdasarkan hasil audit dan investigasi mendalam, celah intrusi bermula dari tiga vektor kelemahan utama:

1. **Validasi File Upload yang Lemah:** Misalkan pada aplikasi jurnal ilmiah menggunakan Framework CMS OJS versi 2.x yang berstatus *End-of-Life* (usang). Penyerang mendaftarkan diri sebagai pengguna biasa (seperti *author*), kemudian mengeksploitasi celah *file uplaod vulnerability* untuk mengunggah berkas PHP (*Backdoor shell*) yang disamarkan dengan ekstensi ganda, misalnya daa.bsdk.pdf.php [2]. Atau menggunakan file PDF tetapi terdapat *backdoor shell* di dalam file tersebut. Hal ini bisa terjadi ketika aplikasi tidak melaukan validasi *file* sampai ke mimetype.
2. **Kelemahan Kredensial dan Manajemen Server:** Penggunaan kata sandi administrator yang lemah (mudah ditebah) atau kata sandi yang sudah ter-*record* pada *password leak.* Hal ini menyebabkan aplikasi mudah dimasuki penyusup seperti contoh aplikasi *wordpress* sehingga penyusup melakukan rencananya untuk melakukan peretasan. Lebih lanjut, hak akses direktori (*file permission*) pada server khususnya di wp-content/uploads diatur menjadi 777 (dapat dibaca, ditulis, dan dieksekusi oleh siapa saja), yang memberikan kebebasan mutlak bagi *malware* untuk bersarang.
3. **Penggunaan Tema/Plugin Bacakan:** Ditemukan indikasi penggunaan tema premium yang dimodifikasi secara ilegal (*nulled theme*). Skrip jahat umumnya telah ditanamkan ke dalam tema tersebut sejak awal proses instalasi.

C. Analisis Forensik Malware dan Obfuskasi PHP

Forensik digital tingkat lanjut dilakukan pada sisi *back-end* server menggunakan baris perintah pencarian pola (grep) untuk melacak muatan berbahaya (*malicious payload*). Penyerang menggunakan metode pengelabuan berlapis untuk menghindari deteksi sistem antivirus dan administrator jaringan melalui teknik obfuskasi berbasis string dinamis.

Temuan paling cerdas terdapat pada berkas bawaan resmi WordPress [4][5][6] di subdomain fst.uui.ac.id, tepatnya pada lokasi jalur ./wp-admin/images/post.php baris ke-203782. Berkas post-image yang seharusnya hanya memuat data media telah disusupi oleh baris kode dinamis PHP berikut:

```
$a = "base";
$b = "64_decode";
$c = $a.$b;
$string = $c($z);
$string = $c($string);
eval($string);
```

Penyerang mendefinisikan string pecahan $a dan $b untuk menghindari deteksi pemindaian statis (*static signature scanning*) terhadap fungsi sensitif base64_decode. Variabel $c menggabungkan string tersebut sehingga memanggil fungsi base64_decode secara dinamis.

Kode berbahaya yang terenkripsi di dalam variabel $z kemudian didekode secara berlapis (*nested decoding*) dan dieksekusi langsung di memori menggunakan pemanggilan eval($string). Teknik ini memungkinkan penyerang menjalankan perintah *remote code execution* (RCE) secara arbitrer tanpa memicu peringatan (*alert*) pada sistem keamanan standar.

Selain itu, pemindaian menyeluruh di tingkat sistem server berbasis CloudLinux (.cagefs/tmp/) menemukan ratusan berkas sementara dengan pola penamaan acak terenkripsi, seperti temp_e56514bbf46772346984395ff75cbaea.php. Berkas-berkas temporer ini dimanfaatkan oleh sindikat untuk menyimpan hasil generasi halaman fiktif *Blackhat SEO* sebelum dikirimkan ke mesin perayap (*crawler*) Google.

Pemindaian (scanning) server mengidentifikasi ratusan berkas injeksi di berbagai titik. Berkas utama pengontrol akses, atau *Backdoor Shell*, terdeteksi dengan nama-nama konvensi penyerang seperti *kobe.php, sc.php,* dan *kom.php.* Analisis *source code* menggunakan perintah *"grep"* mengungkapkan bahwa *malware* secara intensif menggunakan teknik obfuskasi tingkat lanjut untuk mengelabui administrator maupun sistem *antivirus.*

1. Penggunaan *base64_decode* dan fungsi *eval()* untuk mendekripsi dan mengeksekusi langsung sekumpulan *string* jahat secara *real-time.*
2. Pemanggilan fungsi *gzinflate* guna mendekompresi muatan program berbaya secara otomatis ketika *file* diakses.
3. Penggunaan pemanggilan *shell_exec* dan *passthru* untuk menjalankan perintah terminal sistem operasi (Seperti *id, whoami, netstat*) yang memfasilitasi pengambilalihan kontrol server secara menyeluruh.

D. Tingkat Mitigasi

Tim DCDC UUI telah menetapkan protokol penanganan darurat yang meliputi:

1. **Penanganan Jangka Pendek:** Isolasi *website,* pembersihan *file malcious* (seperti *kobe.php*) dan penghapusan *cache* berbahaya di tingkat server (misal direktori .cagefs/tmp). Seluruh akses akun di-reset secara paksa. *Request* penghapusan URL massal (URL *removals*) juga dikirimkan melalui *Google Search Console* untuk membersihkan indeks pencarian serta melalukan reindeks ulang.
2. **Mitigasi Jangka Panjang:** Pemutakhiran sistem secara total, termasuk migrasi jurnal dari OJS 2.x ke versi terbaru 3.x, penghapusan *plugin* bajakan, serta penerapan *web application firewall* (WAF). Kebijakan penggunaan kata sandi kompleks (*strong password policy*) diwajibkan bagi seluruh sivitas pengelola web.

V. KESIMPULAN

Insiden keamanan siber berskala masif yang menargetkan infrastruktur digital Universitas Ubudiyah Indonesia menegaskan besarnya ancaman dari sindikat judi online internasional yang secara agresif mengeksploitasi reputasi domain institusi akademik berotoritas tinggi (.ac.id). Berdasarkan investigasi forensik, akar masalah dari keberhasilan intrusi ini bertumpu pada kelemahan administrasi keamanan dasar atau *security hygiene* [7][8], seperti penggunaan platform CMS WordPress dan OJS 2.x yang telah usang, manajemen kredensial administratif yang lemah, kelalaian penggunaan komponen bajakan (*nulled themes/plugins*), serta longgarnya pengaturan hak akses berkas direktori server. Kerentanan teknis tersebut dimanfaatkan oleh penyerang untuk menanamkan puluhan *backdoor* terobfuskasi menggunakan fungsi dinamis PHP dan melakukan pembajakan hak kepemilikan Google Search Console guna melancarkan kampanye promosi ilegal bermotif ekonomi melalui manipulasi mesin pencari. Sebagai langkah mitigasi masa depan, institusi akademik wajib menerapkan sistem keamanan berlapis melalui pemutakhiran perangkat lunak secara berkala, migrasi platform usang, penghapusan komponen ilegal, implementasi Web Application Firewall secara ketat, serta pemantauan berkelanjutan terhadap hak akses administratif aset digital universitas guna meminimalisir celah eksploitasi di masa mendatang.

REFERENSI

[1] H. M. Mansur and L. Sumanto, "Analisis Penegakan Hukum Peretasan Situs Website Oleh Sindikat Judi Online," *Ensiklopedia Education Review*, vol. 6, no. 3, pp. 132-138, 2024.

[2] Direktorat Cyber Development Center (CDC), *Laporan Insiden Keamanan Siber: Laporan Penanganan Insiden Peretasan Website oleh Konten Judi Online* (Dokumen No: ICT-UUI/IS-REP/2025/IX/001), Universitas Ubudiyah Indonesia, Banda Aceh, 2025.

[3] Pan, Z., Chen, Y., Chen, Y., Shen, Y., & Guo, X. (2021). Webshell Detection Based on Executable Data Characteristics of PHP Code. *Wirel. Commun. Mob. Comput., 2021*, 5533963:1-5533963:12. https://doi.org/10.1155/2021/5533963

[4] Mesa, O., Vieira, R., Viana, M. L., Durelli, V. H. S., Cirilo, E., Kalinowski, M., & Lucena, C. (2018). Understanding vulnerabilities in plugin-based web systems: an exploratory study of wordpress. *Proceedings of the 22nd International Systems and Software Product Line Conference - Volume 1*.

[5] Kabata, P. (2025). Analysis of vulnerabilities and consequences of missing hardening in WordPress-based CMS environments. *Computer Science and Mathematical Modelling*.

[6] Riadi, I., Yudhana, A., & Yunanri, W. (2020). *Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment*

[7] Laksmiati, D. (2023). *Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security*

[8] Petrica, G. (2022). *Cybersecurity of WordPress Platforms*

[9] Nurseno, M., et al. (2024). *Detecting Hidden Illegal Online Gambling on .go.id Domains Using Web Scraping Algorithms*