Journal of Internet and Software Engineering Vol: 1, No 4, 2024, Page: 1-15

Analisis Kerentanan WordPress dengan WPScan dan Teknik Mitigasi

Ghani Trie Aqeela Ramadhani*, Muhammad Hafizh Maulidan, Muhammad Raihan Ramadhan Steyer, Aep Setiawan

Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: WordPress adalah platform yang dikenal sebagai sistem manajemen konten (CMS). Karena banyaknya kerentanan yang dapat dieksploitasi, meskipun populer di seluruh dunia, sering menjadi sasaran serangan siber. Penelitian ini bertujuan untuk menganalisis kerentanan WordPress menggunakan alat pemindaian keamanan WPScan dan mengevaluasi teknik pertahanan yang efektif untuk memitigasi risiko ini. WPScan digunakan untuk mengidentifikasi kerentanan umum dalam instalasi WordPress, seperti plugin dan tema yang rentan, melalui serangkaian pengujian. Analisis tersebut mengungkapkan sejumlah kerentanan kritis, termasuk kerentanan injeksi SQL, XSS (skrip lintas situs), dan kerentanan otentikasi. Berdasarkan temuan ini, berbagai langkah mitigasi direkomendasikan, termasuk pembaruan sistem secara berkala, pengaturan konfigurasi keamanan yang lebih ketat, dan penggunaan *plugin* keamanan tambahan. Menerapkan teknik mitigasi ini diharapkan dapat meningkatkan keamanan situs WordPress Anda secara signifikan, mengurangi kemungkinan serangan, dan melindungi data pengguna Anda. Penelitian ini memberikan wawasan yang dapat ditindaklanjuti bagi administrator situs WordPress agar dapat mengidentifikasi dan memulihkan kerentanan keamanan secara lebih efektif.

Kata kunci: Serangan Siber, WordPress, WPScan

DOI: https://doi.org/10.47134/pjise.v1i4.2613
*Correspondence: Ghani Trie Aqeela Ramadhani
Email: ghanitrieaqeela@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *WordPress is a platform known as a content management system (CMS). Due to the large number of exploitable vulnerabilities, despite being popular worldwide, it is often the target of cyberattacks. This research aims to analyze WordPress vulnerabilities using the WPScan security scanning tool and evaluate effective defense techniques to mitigate these risks. WPScan is used to identify common vulnerabilities in WordPress installations, such as vulnerable plugins and themes, through a series of tests. The analysis revealed a number of critical vulnerabilities, including SQL injection vulnerabilities, XSS (cross-site scripting), and authentication vulnerabilities. Based on these findings, various mitigation measures are recommended, including regular system updates, more stringent security configuration settings, and the use of additional security plugins. Implementing these mitigation techniques is expected to significantly improve the security of your WordPress site, reduce the likelihood of attacks, and protect your users' data. This research provides actionable insights for WordPress site administrators to more effectively identify and remediate security vulnerabilities..*

Keywords: *Cyber Attack, WordPress, WPScan*

Pendahuluan

Cyberspace menjadi sumber berbagai ancaman terhadap kedaulatan suatu negara, yang dapat berasal dari pemerintah, individu, atau pengusaha yang ingin memperoleh keuntungan sendiri. Ancaman ini mencakup ancaman militer dan non-militer. *Cyberspace* dapat digunakan untuk melakukan pencurian data, menyebarkan propaganda, mengganggu, dan menyerang sistem penting seperti jaringan militer, sistem pertahanan negara, dan data perbankan. Ancaman dari *cyberspace* dapat mengganggu stabilitas keamanan dan pertahanan suatu negara jika tidak ada pengawasan yang memadai (Setiyawan et al., 2020).

Sudut pandang Raden Mas Jerry Indrawan dan Efriza dalam menyikapi bahaya abad ke-21 harus diperhatikan, karena beberapa ancaman tersebut bersifat intelektual dan tidak mudah terlihat, seperti terorisme dan radikalisme. Keamanan dan pertahanan negara terkena dampak bahaya tersebut, khususnya di Indonesia.(Arianto, Adi Rio & Anggraini, 2019).

Kejahatan siber, sebagai ancaman perang modern atau non-militer, dapat menyebabkan disintegrasi bangsa melalui motif kepentingan individu atau kelompok tertentu. Perkembangan teknologi informasi dan komunikasi telah mengubah perilaku masyarakat secara global, menciptakan perubahan sosial yang cepat dan tak terbatas. Namun, teknologi informasi juga menjadi sarana efektif bagi kegiatan ilegal. Oleh karena itu, penelitian mengenai penggunaan alat bukti digital dalam undang-undang informasi dan perdagangan elektronik menjadi penting. Di Indonesia, kebutuhan untuk mengatasi kejahatan siber seiring dengan percepatan digitalisasi regional menjadi fokus. (Ariyaningsih et al., 2023).

Kejahatan siber telah berkembang menjadi ancaman global yang merugikan tidak hanya individu, tetapi juga entitas bisnis dan infrastruktur kritis suatu negara. Dengan meningkatnya serangan siber yang terorganisir dan canggih, seperti pencurian data besar-besaran, serangan *ransomware*, dan sabotase sistem informasi, keberadaan sanksi pidana menjadi sangat penting untuk memberikan respons yang tegas terhadap para pelaku kejahatan (Sanksi et al., 2024).

Ancaman yang semakin mengancam keamanan nasional adalah serangan siber. Menjamin keamanan suatu negara secara keseluruhan dan memungkinkan orang untuk tinggal di sana dikenal sebagai keamanan nasional. Perubahan lingkungan yang dihadapi semua negara dalam sistem internasional saat ini dapat menjadi sumber ancaman terhadap keamanan nasional (Vimy et al., 2022).

Di era teknologi komunikasi dan informasi yang modern telah mengubah wajah masyarakat global secara fundamental, tantangan keamanan siber menjadi semakin kompleks dan mendesak. Indonesia, sebagai negara dengan populasi internet yang

berkembang pesat, tidak terkecuali dari ancaman kejahatan siber yang semakin meningkat. Untuk menghadapi tantangan ini, Indonesia telah mengandalkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sebagai landasan hukum utama untuk meminimalisir risiko dan konsekuensi dari kejahatan siber (Ramadhani, 2023).

Karena meningkatnya kebutuhan akan tenaga profesional di bidang keamanan digital, pendidikan mengenai pengenalan dan instalasi Kali Linux sangatlah penting. Alat penting untuk manajemen keamanan siber dan pengujian penetrasi adalah Kali Linux. Para profesional dapat memperoleh kemampuan yang diperlukan untuk mempertahankan jaringan dan sistem dari serangan siber dengan kursus ini. Dalam lingkungan digital yang terus berubah, hal ini meningkatkan keamanan secara keseluruhan. (Wahib et al., 2022)

Istilah keamanan siber berasal dari frasa "siber" dan "keamanan". *Cyber* mengacu pada internet atau dunia maya, dan keamanan mengacu pada keamanan. Oleh karena itu, keamanan siber adalah definisi dasar keamanan siber. Tujuan keamanan siber adalah untuk mengidentifikasi, memitigasi, atau menurunkan risiko serangan dan ancaman siber. Hal ini mencakup semua tindakan yang dapat membahayakan keselamatan bagian mana pun dari sistem siber, termasuk infrastruktur, data/informasi, perangkat keras, dan perangkat lunak. (Ramadhani, Muhammad Rifqi & Ahmad, 2022)

Keamanan informasi merupakan bagian dari keamanan siber, menurut Arianto, yang memperkenalkan gagasan Geometripolitika. Hal ini terjadi karena teknik dan strategi pengamanan informasi merupakan komponen penting dari keamanan siber, yang didasarkan pada penelitian keamanan global (Arianto, Adi Rio & Anggraini, 2019).

Keamanan siber melibatkan serangkaian tindakan yang bertujuan untuk melindungi jaringan komputer (perangkat keras dan perangkat lunak) dari intrusi, manipulasi, dan serangan yang berkaitan dengan data yang disimpannya, serta aspek lain dari internet. Tujuan lain dari keamanan siber adalah pertahanan terhadap pemantauan yang tidak sah, seperti yang terlihat dalam operasi intelijen(Aji, 2023).

Keamanan siber merupakan bagian dari cara-cara atau mekanisme yang digunakan untuk melindungi dan meminimalisir gangguan terhadap kerahasiaan data, integritas, serta ketersediaan informasi. Negara-negara yang telah melakukan pembaharuan di bidang pertahanan dan keamanan, telah banyak melakukan gerakan-gerakan pembangunan kapasitas pertahanan keamanan siber masing-masing. Langkah-langkah dasar termasuk merancang dan mengesahkan peraturan atau undang-undang tentang *cybercrime*, meningkatkan sumber daya manusia di bidang teknologi dan informasi, serta meningkatkan kemampuan penegakan hukum. Beberapa negara bahkan membentuk tim khusus tanggap darurat yang biasa disebut *Computer Emergency Response Team* (CERT). Selain itu, ada juga lembaga negara atau organisasi yang secara khusus bekerja dalam

membidangi pertahanan siber atau keamanan siber di negaranya masing-masing. (Makbull Rizki, 2022).

Segala sesuatu bisa dilakukan dengan adanya internet atau yang biasa disebut dengan dunia maya. Dunia maya memberikan beberapa keuntungan, antara lain menjadikan pengetahuan lebih mudah diakses, menumbuhkan kreativitas manusia, serta menawarkan berbagai kemudahan dan keuntungan lainnya. Di sisi lain, Anda harus mengakui bahwa segala sesuatu memiliki aspek positif dan negatif. Meningkatnya perilaku anti-sosial dan kejahatan lain yang menggunakan internet, yang biasa disebut sebagai kejahatan dunia maya (*cybercrime*), merupakan aspek lain yang tidak menguntungkan dari pesatnya perkembangan internet. (Wahib et al., 2022).

WordPress adalah CMS *open-source* yang mendukung lebih dari 40% dari semua situs web di internet. Keamanan WordPress bergantung pada berbagai faktor termasuk pembaruan perangkat lunak, penggunaan *plugin* dan tema yang aman, serta konfigurasi yang tepat. Almeida dan da Silva (2020) menjelaskan bahwa keamanan WordPress sangat dipengaruhi oleh keteraturan pembaruan dan pemeliharaan yang dilakukan oleh pengguna. Dalam studi mereka, ditemukan bahwa sebagian besar kerentanan pada WordPress berasal dari *plugin* dan tema yang tidak diperbarui WordPress memiliki komunitas pengembang yang aktif, kerentanan tetap ada, terutama jika pengguna tidak memperbarui sistem atau menggunakan *plugin* yang rentan. Dalam penelitian mereka menunjukkan bahwa banyak serangan pada WordPress terjadi karena pengguna mengabaikan pentingnya pembaruan dan pengelolaan plugin yang baik. Mereka juga menekankan pentingnya kesadaran pengguna terhadap praktik keamanan dasar seperti penggunaan kata sandi yang kuat dan autentikasi dua faktor (Peralta-argomeda et al., 2016)

CMS merupakan salah satu alat yang dapat digunakan untuk mengelola konten suatu *website*. sebuah program CMS yang berfungsi sebagai layanan web. Sistem manajemen konten (CMS) adalah perangkat lunak. Konten mengacu pada semua jenis informasi digital, termasuk teks, gambar, audio, video, dan file dari komputer lain. Keterampilan bahasa pemrograman berbasis web digunakan untuk membangun CMS, sistem web berbasis aplikasi (Siambaton & Fakhriza, 2016).

Dalam mengelola atau mengubah isi sebuah *website*, CMS sangat diminati oleh para webmaster karena kemudahannya dalam membangun situs. Namun, seiring perkembangan ini, muncul masalah baru. CMS yang bersifat *open source* memungkinkan semua pengembang mengetahui *source code* yang digunakan. Hal ini menimbulkan masalah keamanan, karena *website* yang menggunakan CMS yang sama berpotensi memiliki kerentanan yang sama. Jika kerentanan ini tidak diidentifikasi dan ditanggulangi oleh *webmaster*, maka pihak yang tidak bertanggung jawab dapat memanfaatkannya dan mengancam keamanan situs web tersebut (Kunang et al., 2013).

Lisensi secara umum diartikan sebagai izin yang diberikan dari satu pihak ke pihak lain dalam bentuk perjanjian. Biasanya, perangkat lunak berlisensi memerlukan pembayaran untuk digunakan. Namun, hal ini tidak seperti program CMS, seperti WordPress dan Blogger, yang seringkali bersifat *open source*. Upaya sukarela ini memanfaatkan CMS WordPress (Pratiwi et al., 2020)

WordPress adalah *Content Management System* (CMS) yang dibuat pada tahun 2004 oleh Matt Mullenweg dan Mike Little. Sebagai CMS, WordPress membantu dalam membuat dan mengelola situs web tanpa perlu koding. Pengguna dapat menyesuaikan tampilan, menambahkan fungsionalitas, dan membuat konten untuk situs web dengan mudah, sehingga sangat cocok untuk pemula. WordPress adalah perangkat lunak sumber terbuka, sehingga dapat digunakan tanpa biaya. (Setyo Utomo et al., 2022)

WordPress adalah perangkat lunak sumber terbuka yang banyak digunakan sebagai sistem manajemen konten (CMS). Dengan CMS, membangun situs web menjadi sederhana dan tidak memerlukan pengalaman pemrograman manualWordPress dapat diartikan sebagai suatu platform *website* bersifat *open scouce* dan bisa dikatakan cukup terkenal di kalangan CMS lainnya. WordPress juga dapat digunakan sebagai alat untuk membuat *website* dengan berbagai macam *plugin* didalamnya tanpa perlu memahami bahasa pemrograman (Fadillah & Gaffar, 2023).

WPScan adalah alat yang digunakan untuk mendeteksi kerentanan keamanan pada WordPress. Alat ini sangat berguna untuk mengevaluasi keamanan situs web yang dimiliki. WPScan akan melakukan pemeriksaan pada situs WordPress dengan mengecek pada *database* kerentanan dan eksploitasi. Dengan mengetahui kerentanan lebih awal, kita dapat mengurangi risiko keamanan pada portal WordPress kita. Namun, perlu diingat bahwa alat ini bisa menjadi berbahaya jika disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab seperti *hacker* atau *cracker* (Azis & Yazid, 2021).

WPScan berfungsi untuk memindai kerentanan pada situs web yang menggunakan CMS WordPress. Alat ini dapat memindai daftar *plugin*, jenis tema yang digunakan, serta mengidentifikasi kemungkinan kerentanan pada situs web. Kerentanan ini biasanya ditemukan pada versi *plugin* atau tema yang sudah kadaluwarsa dan belum diperbarui oleh pemilik situs web. Selain itu, WPScan juga dapat memberikan informasi tentang pengguna yang terdaftar dan konfigurasi umum situs. Dengan menggunakan WPScan, administrator situs dapat mengetahui area yang memerlukan perbaikan untuk meningkatkan keamanan dan mencegah potensi serangan (Darra Deandra Modesta, 2021).

Pengujian keamanan *website* menggunakan WPScan adalah langkah yang penting untuk mengetahui celah keamanan yang mungkin ada pada platform WordPress. Dengan melakukan pengujian ini, Ichi Hydroponic Store dapat memastikan bahwa situs web mereka aman dari serangan peretas atau eksploitasi kelemahan. WPScan membantu dalam

mengidentifikasi potensi kerentanan dan memberikan wawasan yang diperlukan untuk meningkatkan keamanan situs.(Cahyo et al., 2022)

WPScan adalah alat yang digunakan untuk mencari celah-celah keamanan pada WordPress. Alat ini sangat bermanfaat untuk mengetahui kekuatan dan kerentanan dari situs web yang dimiliki. Namun, WPScan bisa sangat berbahaya jika digunakan oleh pihak yang tidak bertanggung jawab seperti *hacker* atau *cracker* (Azis & Yazid, 2021).

WPScan adalah sebuah alat khusus yang dirancang untuk mendeteksi kerentanan keamanan pada situs web yang menggunakan platform WordPress. Keberadaan WPScan menjadi kunci penting dalam upaya menjaga keamanan situs web berbasis WordPress. Dengan menggunakan WPScan, administrator situs dapat secara proaktif mengidentifikasi dan mengatasi potensi kerentanan keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.(Prihanto et al., 2023)

Metode

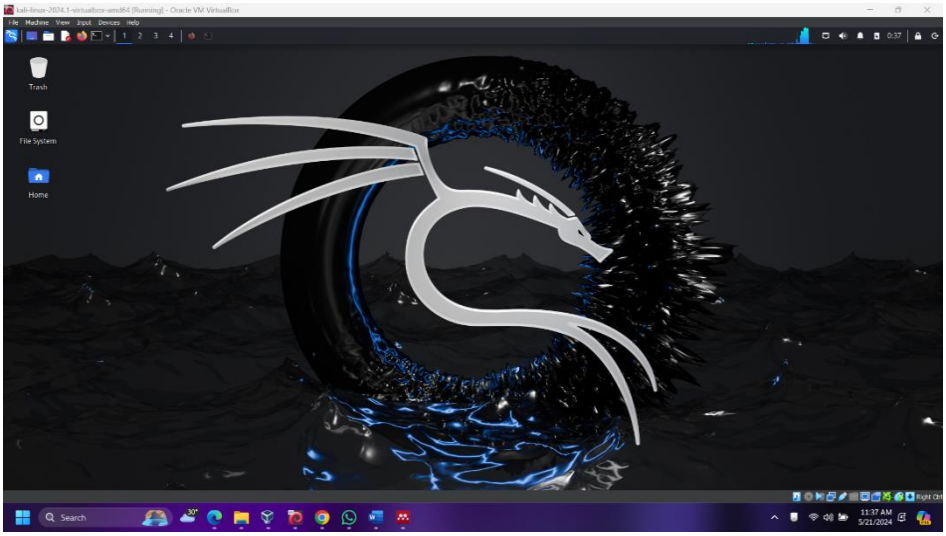
Studi literatur ini akan dilakukan dalam waktu satu minggu, dari pertemuan ke-12 di bulan April hingga pertemuan ke-14 di bulan Mei, di Sekolah Vokasi IPB University. Penelitian ini terdiri dari empat tahap: pengumpulan data, analisis, implementasi, dan evaluasi solusi dalam keamanan siber. Pengumpulan data melibatkan pencarian dan analisis dokumen, artikel, dan sumber daya lain yang relevan terkait dengan efektivitas WPScan dalam mengidentifikasi kerentanan di situs WordPress, mekanisme penyerangan yang digunakan peretas dengan memanfaatkan WPScan, serta strategi mitigasi yang dapat diterapkan untuk mengurangi risiko serangan tersebut.

Analisis data melibatkan analisis mendalam terhadap informasi yang terkumpul untuk mengidentifikasi temuan kunci dan pola yang muncul. Meskipun tahap implementasi tidak diperlukan dalam studi literatur, evaluasi akan dilakukan terhadap temuan dan analisis yang telah dilakukan untuk menyusun rekomendasi dan strategi mitigasi yang dapat diterapkan untuk mengurangi risiko serangan menggunakan WPScan. Studi literatur ini menggabungkan pendekatan kualitatif dan kuantitatif. Pendekatan kualitatif digunakan untuk memahami mekanisme penyerangan dan strategi mitigasi, sementara pendekatan kuantitatif digunakan untuk menganalisis efektivitas WPScan dalam mengidentifikasi kerentanan.

Hasil dan Pembahasan

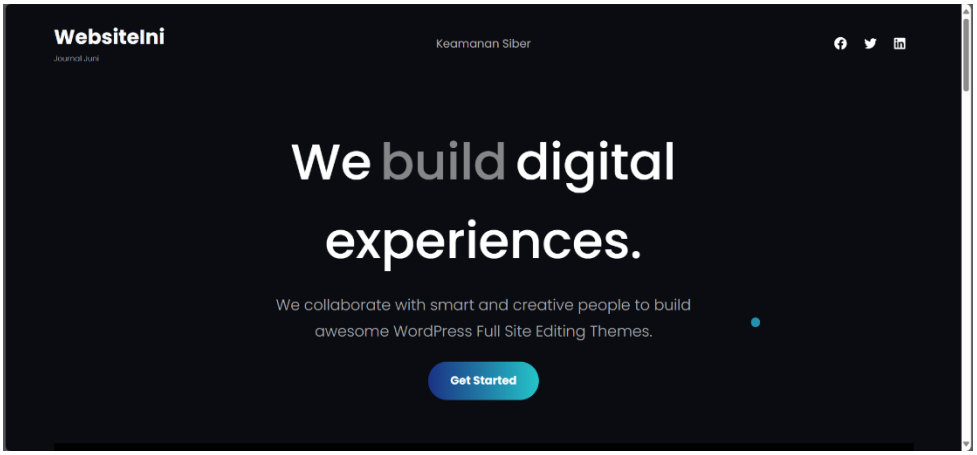
Langkah-Langkah Penggunaan WPScan

Pertama-tama install terlebih dahulu kali linux. Kali Linux yang kami gunakan adalah versi 2024.1 untuk sebuah penyerangannya.

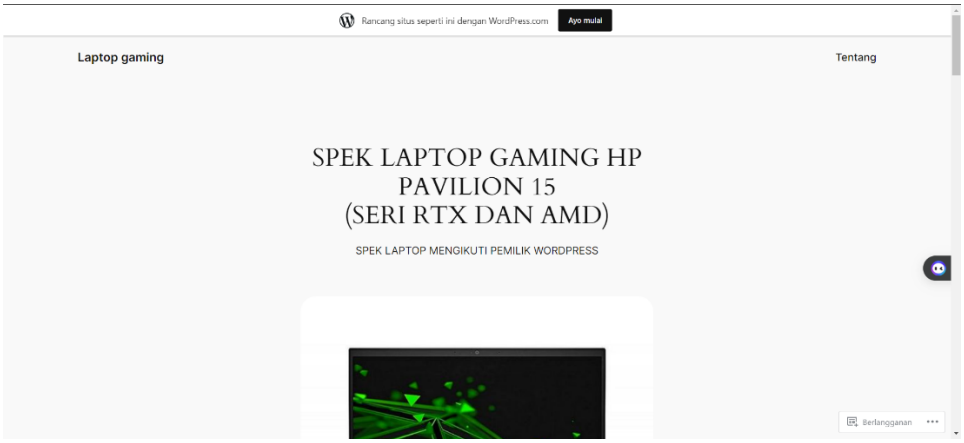


Gambar 1. Tampilan Kali Linux

Selanjutnya siapkan target yang ingin di serang, di sini kami menggunakan dua *website* wordpress yang dimana satunya menggunakan ubuntu dan tidak di proteksi apapun, yang kedua menggunakan proteksi hosting wordpress.com.



Gambar 2. Tampilan Website 01

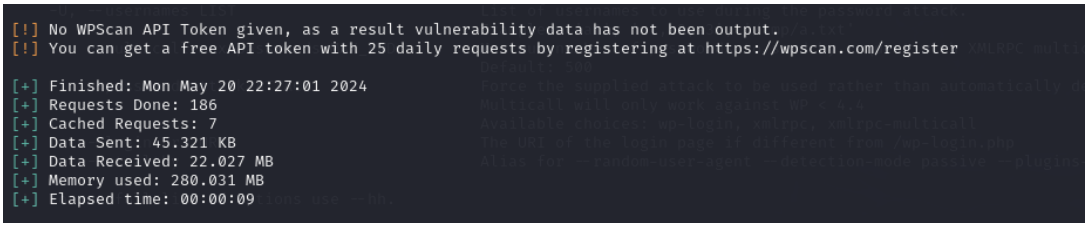


Gambar 3. Tampilan website 02

Bukalah terminal linux dan jalankan *command* "wpscan -h". Disini akan menampilkan banyak variant dari wpscan. Kita akan fokus kebagian enumerate atau mengecek kerentanan dalam *website* wordpress.

Gambar 4. *WPScan*

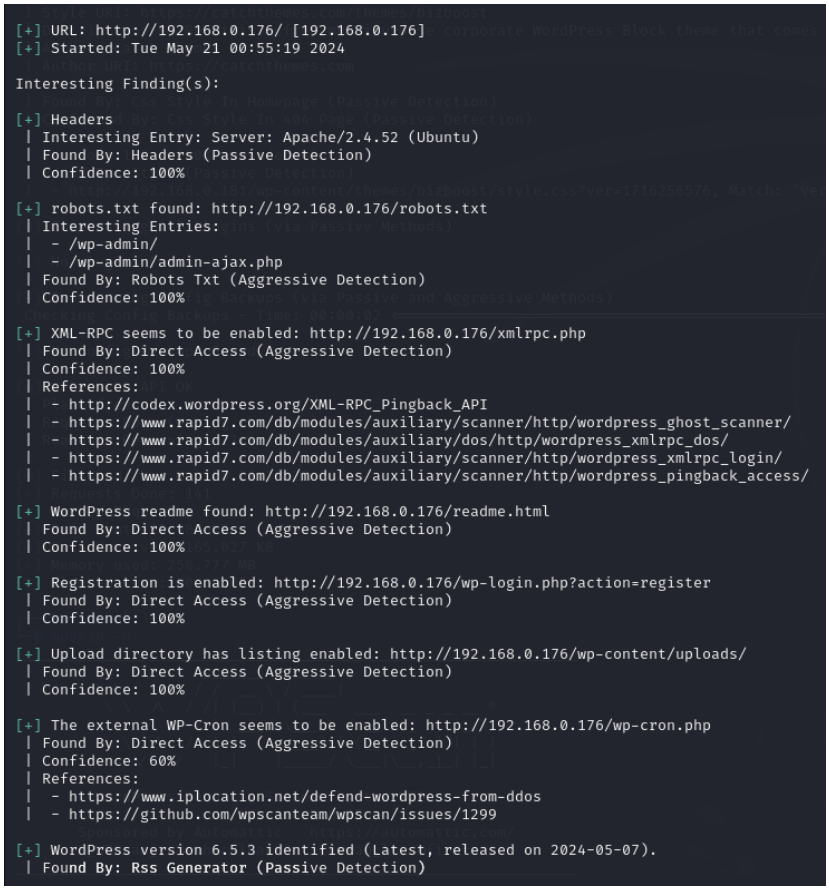
Selanjutnya kita bisa mencoba mengidentifikasi bagian apa yang rentan dengan *command* "wpscan –url (halaman *website*)". Di sini akan menampilkan bagaimana website itu terbuat dan bagian apa saja, namun untuk output dari kerentanannya tidak ditampilkan karena membutuhkan registrasi dari wpscan. Registerlah ke dalam wpscan ke halaman https://wpscan.com/register/. Ketika sudah maka anda akan diberi token yang bisa digunakan untuk memberikan output pada wpscan tersebut.



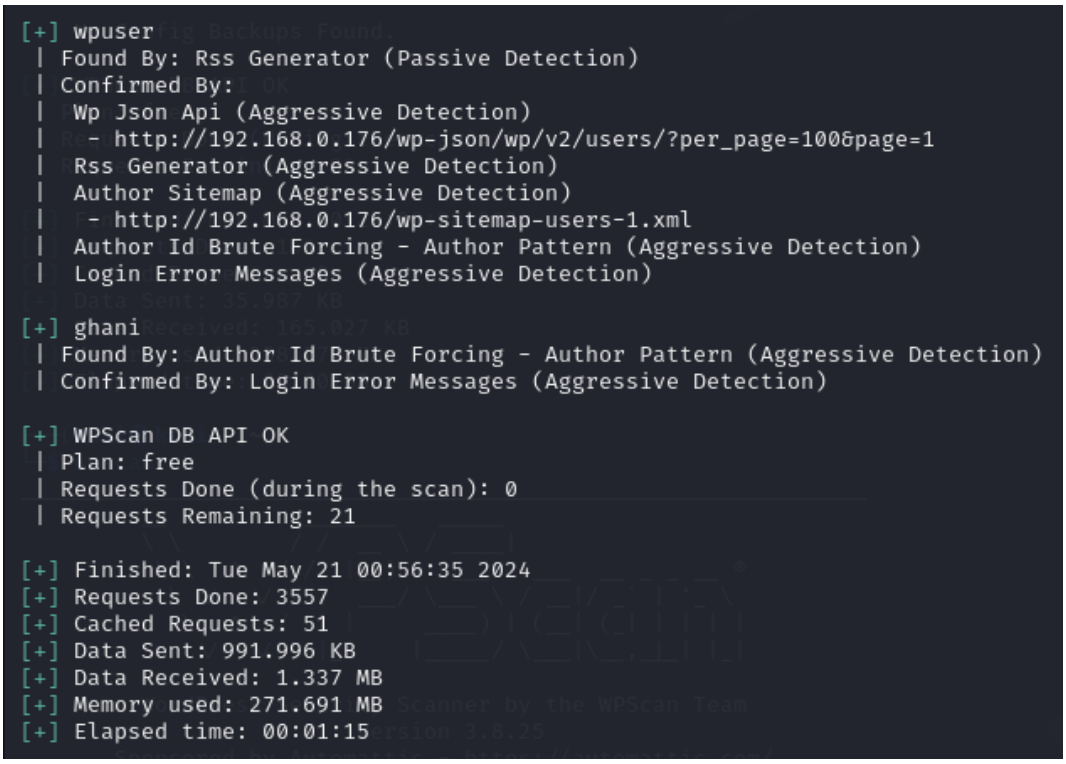
Gambar 5. Tampilan sebelum WPScan Register

Gambar 6. Tampilan sesudah Wpscan Register

Dari sini kita bisa mengecek enumerate apa saja yang rentan dari awal hingga akhir, jika *website* tersebut sudah terproteksi maka akan menampilkan seperti ini ketika di enumerate.



Gambar 7. Hasil Wpscan



Gambar 8. Wpscan Hasil 02

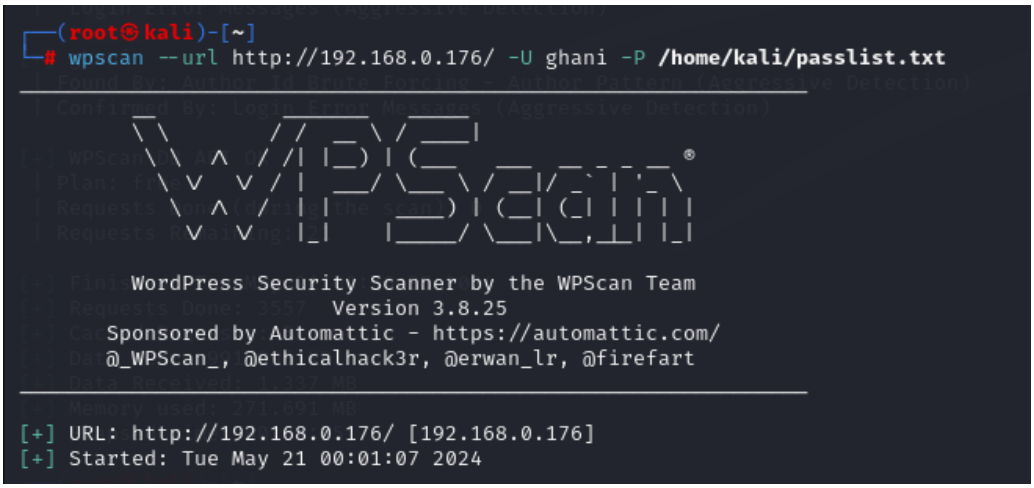
Di sini dapat terlihat tampilan dari apa saja informasi dalam wordpress yang dibuat hingga user yang terdapat di dalamnya.

Gambar 9. Wpscan Tampilan Ketika Hosting by Wordpress

Ini untuk tampilan ketika *website* tersebut sudah di publik dengan wordpress.com akan dilindungi dan WPScan sendiri tidak *support* untuk melakukan enumeratenya.

Memasuki Akun Wordpress

Dari data akun salah satu *website* wordpress tadi kita bisa membuat sebuah percobaan untuk memasuki halaman *website* itu dengan menggunakan wpscan dan passlist. Pertama-tama siapkan dulu passlistnya, bisa didapatkan dalam github atau membuat sendiri dengan crunch. Gunakan *Command* "wpscan –url (halaman website) -U (nama user) –P (/direktori dari passlist).



Gambar 10. Tampilan Wpscan untuk *check password*

Gambar 11. Tampilan Wpscan *password*

Teknik Mitigasi

1. Menggunakan Domain

Memastikan penggunaan domain yang terpercaya dan terjamin keamanannya dapat membantu mengurangi risiko serangan. Melalui pemilihan domain yang tepat, risiko serangan dapat diminimalkan karena serangan biasanya lebih ditargetkan pada situs-situs dengan domain yang lemah atau rentan. Sebagai contoh, memilih domain yang didaftarkan melalui penyedia layanan domain terkemuka dan terpercaya seperti GoDaddy atau Namecheap dapat memberikan jaminan keamanan tambahan. Dengan menggunakan domain yang terpercaya, Anda dapat menghindari risiko serangan yang mungkin terkait dengan domain yang diambil alih atau tautan yang meragukan.

2. Menggunakan HTTPS agar *website secure*

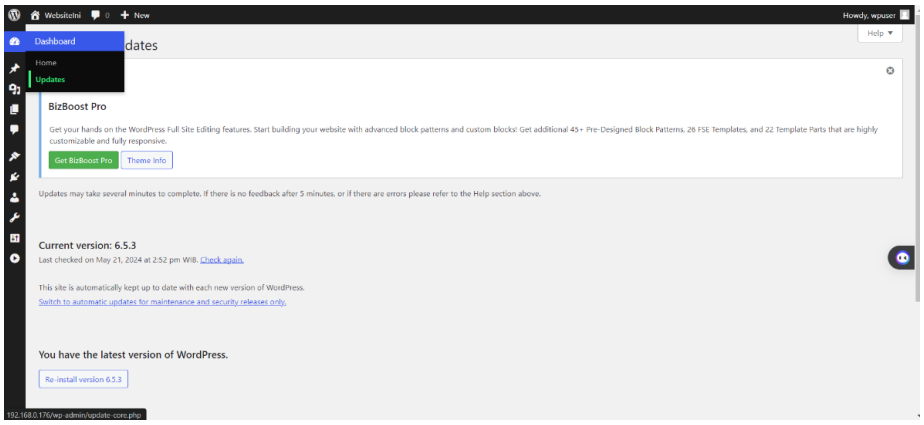
Mengimplementasikan protokol HTTPS pada situs WordPress adalah langkah kunci dalam meningkatkan keamanan. Dengan menggunakan HTTPS, semua komunikasi antara pengguna dan server dilindungi dengan enkripsi, sehingga mengurangi risiko peretasan dan pencurian data. Sebagai contoh, Anda dapat menginstal dan mengonfigurasi sertifikat SSL/TLS dari penyedia layanan sertifikat seperti Let's Encrypt. Dengan menggunakan HTTPS, situs Anda akan dienkripsi, sehingga memastikan bahwa informasi sensitif seperti kata sandi atau data pengguna tidak dapat dengan mudah diretas oleh pihak yang tidak berwenang.

3. Gunakan Google *password* atau *update password* secara berkala

Memperkuat keamanan dengan menerapkan kebijakan penggunaan kata sandi yang kuat dan aman adalah langkah yang penting. Menggunakan layanan otentikasi ganda seperti Google password dapat memberikan lapisan keamanan tambahan. Selain itu, memastikan untuk secara teratur memperbarui kata sandi juga penting untuk mengurangi risiko akses yang tidak sah ke situs WordPress. Sebagai contoh, menerapkan kebijakan penggunaan kata sandi yang kuat seperti kombinasi huruf besar-kecil, angka, dan karakter khusus serta menggunakan manajer kata sandi seperti LastPass atau Dashlane dapat membantu meningkatkan keamanan. Selain itu, mengatur periode reguler untuk meminta pengguna untuk memperbarui kata sandi mereka, misalnya setiap 90 hari, juga merupakan praktik yang baik dalam menjaga keamanan situs.

4. Update Software

Selalu memastikan bahwa seluruh perangkat lunak yang digunakan, termasuk WordPress core, tema, dan *plugin*, selalu diperbarui ke versi terbaru. Pembaruan perangkat lunak sering kali mengandung perbaikan keamanan untuk memperbaiki celah yang dapat dieksploitasi oleh peretas. Dengan menjaga semua *software* terkini, Anda dapat mengurangi risiko serangan yang dimungkinkan melalui kerentanan perangkat lunak yang sudah diketahui.



Gambar 12. Mitigasi Software Wordpress

Konfigurasi Izin File dan Direktori

Aturlah izin konfigurasi dengan *command* berikut

```
root@tekcloud:~# cd /var/www/html/wordpress/
```

Gambar 13. Masuklah ke dalam direktori Wordpress

```
root@tekcloud:/var/www/html/wordpress# find . -type d -exec chmod 755 {} \;
root@tekcloud:/var/www/html/wordpress# find . -type f -exec chmod 644 {} \;
root@tekcloud:/var/www/html/wordpress#
```

Gambar 14. Berikanlah izin pada direktori ini

Dengan melakukan command ini akan memberikan command untuk direktori dapat dibaca, tulis dan ekseskusi sedangkan untuk file hanya dapat dibaca dan ditulis

Simpulan

Penelitian ini mengkonfirmasi bahwa WPScan adalah alat yang efektif untuk mengidentifikasi kerentanan pada situs WordPress. WPScan mampu menemukan berbagai jenis kerentanan, mulai dari *plugin* yang usang hingga tema yang rentan. Namun, alat ini juga memiliki potensi disalahgunakan oleh peretas untuk mengeksploitasi kelemahan pada situs WordPress yang tidak dilindungi dengan baik. Oleh karena itu, pemahaman yang mendalam tentang penggunaan WPScan dan implementasi strategi mitigasi yang tepat sangat penting untuk menjaga keamanan situs WordPress. Dengan pemindaian yang rutin dan tindakan preventif, administrator situs dapat mengurangi risiko serangan dan melindungi data pengguna secara efektif.

Daftar Pustaka

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Arianto, Adi Rio & Anggraini, G. (2019). *Melalui Indonesia Security Incident Response Team on*. *09 Nomo 1*, 13–30.

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. surya, & Rezi. (2023). Korelasi Kejahatan Siber Dengan PercepatanDigitalisasi Di Indonesia. *Jurnal Ilmu Hukum Universitas Pasundan*, *1*, 1–12.

Azis, R., & Yazid, S. (2021). Pengujian Kerentanan Website Wordpress Dengan Menggunakan Penetration Testing Untuk Menghasilkan Website Yang Aman. *Jurnal Restikom : Riset Teknik Informatika Dan Komputer*, *3*(3), 93–105. https://restikom.nusaputra.ac.id/article/view/87

Cahyo, O. A. T., Setiawan, D., & Mei Lenawati. (2022). Implementasi Digital Marketing Berbasis Wordpress pada Ichi Hydroponic Store Madiun. *JURNAL PILAR TEKNOLOGI Jurnal Ilmiah Ilmu Ilmu Teknik*, *7*(2), 18–25. https://doi.org/10.33319/piltek.v7i2.121

Darra Deandra Modesta, B. (2021). *ANALISIS PENGUJIAN KEAMANAN JARINGAN FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM UNIVERSITAS LAMPUNG MENGGUNAKAN METODE BRUTE FORCE*.

Fadillah, P. N. N., & Gaffar, M. R. (2023). Perancangan Dan Pembuatan Company Profile Berbasis Website Menggunakan Cms Wordpress Pada Kafe Kajja Korean Street Food Di Garut. *Applied Business and Administration Journal*, *2*(1), 91–99. https://doi.org/10.62201/abaj.v2i1.43

Kunang, Y. N., Muklis, F., & Sauda, S. (2013). PENGUJIAN CELAH KEAMANAN PADA CMS (Content Management System). *Prosiding Seminar Nasional Ilmu Komputer (SNAIK 2013)*, *November*, 398–406. https://doi.org/10.13140/RG.2.1.3163.6080

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Peralta-argomeda, J., Huamantinco-araujo, A., Luz Yolanda Toro Suarez, Pimentel, H. F., Quispe Phocco, R. F., Roldán-Pérez, G., Estudiantes, V. De, Gustavson, S. S., Cosme, L. A., Trama, F. A., Ayala R., A., Ambrosio, E. S., Vasquez, M., Luz Yolanda Toro Suarez, Cepeda, J. P., Pola, M., Zuleta, C., González, C., Luz Yolanda Toro Suarez, … Villanueva, I. (2016). No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title. *Ucv*, *I*(02), 0–116. http://dspace.unitru.edu.pe/bitstream/handle/UNITRU/10947/Miñano Guevara%2C Karen Anali.pdf?sequence=1&isAllowed=y%0Ahttps://repository.upb.edu.co/bitstream/handle/20.500.11912/3346/DIVERSIDAD DE MACROINVERTEBRADOS ACUÁTICOS Y SU.pdf?sequence=1&isAllowed=

Pratiwi, D., Santoso, G. B., Mardianto, I., Sediyono, A., & Rochman, A. (2020). Pengelolaan Pengelolaan Konten Web Menggunakan Wordpress, Canva dan Photoshop untuk Guru-Guru Wilayah Jakarta. *Abdihaz: Jurnal Ilmiah Pengabdian Pada Masyarakat*, *2*(1), 11. https://doi.org/10.32663/abdihaz.v2i1.1093

Prihanto, D., Sholeh, A., Setiawan, C. B., & Al Badawi, M. A. A. (2023). Analisis Kerentanan Menggunakan Vulnerability Assessment pada Situs Web Perguruan Tinggi. *Teknomatika: Jurnal Informatika Dan Komputer*, *16*(2), 66–72. https://doi.org/10.30989/teknomatika.v16i2.1248

Ramadhani, Muhammad Rifqi & Ahmad, R. P. (2022). Analisis Kesadaran Cybersecurity Pada

Pengguna Media Sosial Di Kalangan Mahasiswa Kota Bandung. *Jurnal Darma Agung*, *30*(1), 1164. https://doi.org/10.46930/ojsuda.v30i1.3167

Ramadhani, F. (2023). Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *1*(1), 89–97. https://jurnal.kolibi.org/index.php/kultura/article/view/98/95

Sanksi, P., Terhadap, P., Siber, K., Kajian, S., Perkembangan, T., Fakhriah, H. S., Mutmainnah, I., Palembang, U. M., & Pepabri Makassar, U. (2024). *Journal of Internasional Multidisciplinary Research*. *2*(1), 470–477. https://journal.banjaresepacific.com/index.php/jimr

Setiyawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State Sovereignty of the Republic of Indonesia. *Journal USM Law*, *3*(2), 275–295.

Setyo Utomo, H., Supriyanto, A., Rahmanto, O., & Wan, Y. (2022). Pemanfaatan Wordpress Sebagai Media Informasi. *Jurnal Pengabdian Kepada Masyarakat MEDITEG*, *7*(November), 65–74.

Siambaton, M. Z., & Fakhriza, M. (2016). Aplikasi Content Management System (Cms) Pada Joomla Untuk Membuat Web Service. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *1*(1), 11–13. https://doi.org/10.30743/infotekjar.v1i1.32

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & ... (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal …*, *6*(1), 2319–2327. http://journal.upy.ac.id/index.php/pkn/article/view/2989

Wahib, P., Tunggal Narotama, A., Muhamad Rijki, N., Sahrudin, Permana, F., Sagara, D., Ibrahim Azkhal, D., Anwar, M., & Rifqi Juniawan, M. (2022). Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Ajp-Abdi Jurnal Publikasi*, *1*(2), 64–68. https://jurnal.portalpublikasi.id/index.php/AJP/index