PUBLIPRENEUR POLIMEDIA: JURNAL ILMIAH JURUSAN PENERBITAN POLITEKNIK NEGERI MEDIA KREATIF
Vol.13, No. 2, 2025 hal. 46-56

■ **Submitted: 1 Nov 2025** ■ **Revised: 1 Des 2025** ■ **Accepted: 15 Des 2025**

BRUTEFORCE ATTACK ANALYSIS VIA XMLRPC.PHP FILE ON WORDPRESS

Yusuf Nurrachman,ST., M.M.S.I.[1*],R.Sulistiyo Wibowo, S.Sn.,M.Sn[2], Nofiandri Setyasmara, M.T[3].

[1] (Politeknik Negeri Media Kreatif.)
[2] (Politeknik Negeri Media Kreatif.)
[3] (Politeknik Negeri Media Kreatif.)

E-mail: yusuf@polimedia.ac.id[1], sulistiyo@polimedia.ac.id[2] , nofiandri@polimedia.ac.id[3].

ABSTRACT

WordPress provides an XML-RPC feature through the xmlrpc.php file for external communication. However, this filter is often exploited as a brute-force attack vulnerability because it supports system.multicall, which allows multiple login attempts in a single request. This study analyzed brute-force attacks against xmlrpc.php through simulations in a local environment using WPscan and a Python script called lokoscannerX_ver1. Testing was conducted using two scenarios: WordPress without security and WordPress with security using the Disable XML-RPC plugin and .htaccess file configuration. The results showed that WordPress without security was easily attacked and overloaded the virtual server on the test environment. Meanwhile, after implementing the Disable XML-RPC plugin, attacks were blocked and prevented, while the .htaccess configuration only blocked execution but still allowed user information to be detected. This study emphasizes the importance of disabling XML-RPC as a basic WordPress security measure.

Keyword: WordPress, XML-RPC, brute force, cybersecurity

ANALISIS SERANGAN BRUTEFORCE MELALUI FILE XMLRPC.PHP PADA WORDPRESS

ABSTRAK

Wordpress menyediakan fitur XML-RPC melalui file xmlrpc.php untuk komunikasi eksternal, namun filter ini sering dimanfaatkan sebagai celah serangan bruteforce karena mendukug system.multicall yang memungkinkan banyak percobaan login dalam sau permintaan. Penelitian ini menganalisa serangan brute force terhadap xmlrpc.php melalui simulasi pada lingkungan local menggunakan WPscan dan skrip Python yang diberi nama lokoscannerX. Pengujian dilakukan dengan dua skenario yaitu wordpress tanpa keamanan dan wordpress dengan pengamanan menggunakan plugin Disable XML-RPC dan konfigurasi file .htaccess , hasil menunjukkan bahwa wordpress tanpa keamanan dengan mudah diserang dan membebani server virtual pada media uji.Sementara itu setelah dilakukan metode pengamanan dengan plugin Disable XML-RPC maka serangan dapat diblokir dan sekaligus mencegah serangan, sedangkan konfigurasi .htaccess hanya memblokir eksekusi tetapi informasi user masih dapat terdeteksi. Penelitian ini menegaskan pentingnya menonaktifkan XML-RPC sebagai Langkah dasar keamanan wordpress.

Kata kunci: WordPress, XML-RPC, brute force, keamanan siber.

PENDAHULUAN

Dengan semakin berkembangnya kebutuhan akan website sebagai salah satu media informasi dan kebutuhan akan kecepatan dalam pembuatan website tersebut maka banyak orang, perusahaan dan institusi negara banyak yang menggunakan Content Management System / CMS, CMS adalah aplikasi perangkat lunak berbasis web yang digunakan untuk mengelola informasi digital dengan menyediakan fitur pengelolaan konten, pengguna, dan desain, serta memfasilitasi publikasi secara real-time, salah satu cms yang banyak digunakan adalah Wordpress (WordPress.org, n.d.), wordpress sangat memudahkan pengguna dalam melakukan instalasi dan perubahan sesuai dengan kebutuhan dari pengguna itu sendiri. Dengan semakin banyaknya pengguna wordpress juga mengakibatkan banyak juga celah (Hasan et al., 2017) untuk serangan cyber yang mencoba merusak website yang telah dibuat. Serangan semakin meningkat dengan adanya serangan judi online yang juga menyasar ke berbagai website yang menggunakan Wordpress(Wordfence, 2022).

Berbagai cara serangan dapat dilakukan oleh peretas atau hacker salah satunya berupa exploit dengan memanfaatkan kerentanan file pada website yang dibuat dengan wordpress dengan cara Brute Force attack,(Wardaya, 2020) yaitu serangan yang ditujukan untuk mendapatkan informasi berupa username dan password target . Wordpress mempunyai sebuah file yang digunakan sebagai komunikasi dengan aplikasi seluler atau eksternal dengan memanfaatkan protokol XML-RPC yang dijalankan melalui file xmlrpc.php, file ini merupakan salah satu celah kerentanan yang dapat dimanfaatkan untuk melakukan Brute Force attack. (Sucuri, 2023; Cloudflare, 2015; Kravtsov, 2015)

Bahaya dari Brute Force attack ini adalah dapat mengambil alih sistem apabila username dan password dapat di ketahui sehingga penyerang dapat melakukan hal selayaknya sebagai admin system dan ini akan berimbas kepada layanan perusahaan atau institusi tersebut(Wordfence, 2022), selain itu system juga bisa down karena resource sibuk melayani permintaan atau Distributed Denial Of Service. (Sucuri, 2023; Cloudflare, 2015)

Untuk mengetahui bagaimana proses exploitasi dengan metode Brute Force pada xmlrpc.php maka di perlukan sebuah analisa yang dapat memberikan pengetahuan bagaimana proses tersebut berjalan. Serangan Brute Force tidak dilakukan secara langsung dengan mencoba masuk ke dalam situs website target dengan mencoba mengetikan langsung username dan password secara manual tetapi sudah banyak cara yang dilakukan untuk melakukan hal tersebut secara otomatis dengan banyak password atau username secara bersamaan atau system multicall dengan sekali serang. (Cloudflare, 2015; Kravtsov, 2015) Berdasarkan hal tersebut maka dalam penelitian ini penulis ingin menganalisis serangan Brute Force pada xmlrpc.php pada wordpress dengan melakukan simulasi pola serangan dalam lingkungan lokal sekaligus memberikan edukasi dari segi keamanan cyber / cybersecurity terutama bagi masyarakat umum dan khususnya mahasiswa yang sedang

belajar tentang keamanan komputer dan jaringan.

Identifikasi Masalah

1. Celah Kerentanan XML-RPC melalui xmlrpc.php yang dapat dimanfaatkan
2. Masih kurangnya edukasi dalam bentuk simulasi untuk memberikan gambaran proses Brute Force attack melalui celah kerentanan xmlrpc.php.

Batasan Masalah

Pada penelitian ini penulis membatasi masalah yaitu akan melakukan analisis dengan melakukan simulasi serangan terhadap XML-RPC melalui file xmlrpc.php pada wordpress dalam lingkungan lokal.

Rumusan Masalah

Bagaimana menghasilkan analisis serangan melalui xmlrpc.php dengan melakukan simulasi serangan Brute Force /Brute Force attack ?

Pemecahan Masalah

Pada penelitian akan dilakukan beberapa simulasi berupa serangan Brute Force dengan menggunakan beberapa tools dengan target website wordpress yang sudah terinstall, dengan tools tersebut akan dianalisis dari beberapa proses yaitu melakukan scanning dan melakukan exploit dalam bentuk Brute Force dan juga melakukan beberapa penerapan keamanan pada wordpress ketika proses simulasi . Hasil simulasi akan berupa report log dari software yang dikembangkan dalam penelitian.

METODE PENELITIAN

Metode penelitian yang digunakan adalah kualitatif dimana pada penelitian ini akan yang simulasi serangan pada wordpress dengan beberapa tahapan dan melakukan pencatatan serta konfigurasi yang dibutuhkan pada software sebagai media penelitian, beberapa tahapan yang akan dilakukan oleh penulis adalah sebagai berikut :

Tahapan Teknis

Pada tahapan ini akan di persiapkan lingkungan percobaan dalam bentuk perangkat lunak seperti : Virtual Box untuk membuat virtual machine, Sistem operasi kali linux , xampp sebagai lokal web server, wordpress installer dan skrip program attacker python yang akan dibuat serta wpscan untuk melakukan pemindaian target yang berjalan di kali linux.
Melakukan simulasi serangan ke xmlprc.php dengan beberapa skenario serangan tanpa keamanan dan dengan keamanan .

Non Teknis

Untuk mendukung penelitian ini maka dibutuhkan berbagai referensi atau literatur baik buku , jurnal ataupun media online yang berhubungan dengan kerentanan XML-RPC yang diimplementasikan pada file xmlrpc.php di wordpress.

Perangkat Utama Penelitian

Perangkat utama penelitian adalah yang berhubungan dengan software yang di gunakan terutama kebutuhan akan lingkungan percobaan dalam lingkup lokal baik hardware maupun software yang terdiri dari laptop, sistem operasi, server web lokal dan virtual machine serta alat pemindaian yang digunakan untuk melihat kerentanan pada wordpress target.

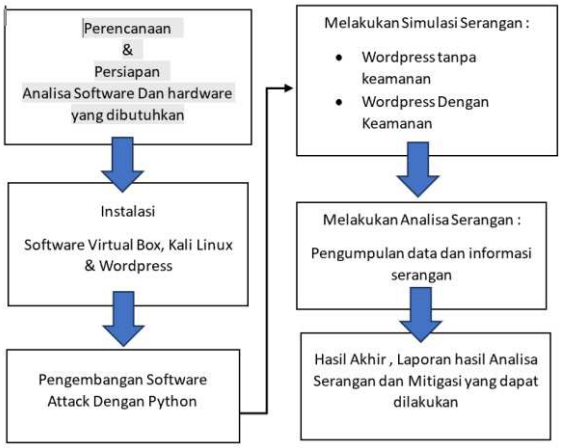
Perangkat Pendukung

Perangkat pendukung adalah perangkat yang digunakan untuk dengan aktifitas yang dilakukan seperti

hardware yaitu laptop dan sistem operasi windows , perangkat lunak yang digunakan untuk melakukan bruteforce dibuat dengan bahasa pemrograman python.

Tahapan Penelitian

Pada tahapan penelitian penulis melakukan beberapa proses yang dilakukan untuk dapat menghasilkan output yang diinginkan, proses yang dilakukan akan melalui beberapa tahapan seperti pada gambar dibawah ini :



Gambar 1. Alur Kerja
Sumber : Pribadi

Perencanaan & Persiapan

Pada tahapan ini penulis melakukan perencanaan yang harus dilakukan untuk menghasilkan output yang diharapkan dan menganalisa software apa saja yang dibutuhkan.

1. Instalasi

Software yang dibutuhkan untuk melakukan penelitian terdiri dari :

Virtual Box

Virtual Box digunakan untuk membuat virtual server yang akan menjalankan sistem operasi kali linux dengan versi 7.0.18.

Kali Linux

Kali Linux versi 2024.4 merupakan Sistem Operasi yang didalamnya disediakan fasilitas untuk melakukan aktifitas hacking salah satunya yang akan digunakan Adalah wpscan.

Xampp

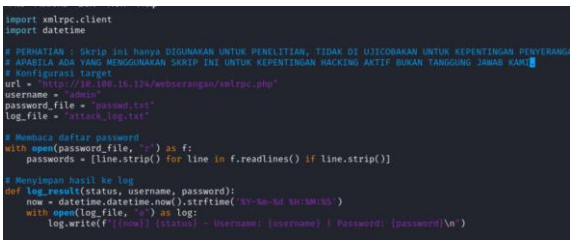
Xampp digunakan sebagai webserver lokal yang yang terpasang pada Sistem Operasi Windows menggunakan versi 3.3.0.

Wordpress

Wordpress yang digunakan pada komputer lokal sebagai target serangan menggunakan versi 6.8.2.

2. Pengembangan Software

Pengembangan software untuk melakukan bruteforce attack dengan menggunakan skrip phyton.



Gambar 2. Skrip Phyton
Sumber : Pribadi

3. Simulasi Serangan

Melakukan simulasi serangan ke website target yang telah di pasang pada komputer lokal , melakukan wordpress pemindaian dengan menggunakan wpscan. (WPScan Team, 2021)

4. Analisis Serangan

Menganalisa hasil serangan baik sebelum website target tanpa keamanan maupun setelah diberikan keamanan.

5. Hasil Akhir

Hasil akhir adalah hasil analisa serangan yang telah dilakukan dan bagaimana apabila dilakukan mitigasi

terhadap serangan yang dilakukan.

HASIL DAN PEMBAHASAN

Pada hasil penelitian akan di jelaskan beberapa tahapan dan beberapa skenario yang dilakukan untuk menghasilkan proses penyerangan serta output laporan serangan dan Solusi yang dapat dilakukan meminimalisir serangan bruteforce.

Tahapan yang dilakukan :

1. Tahapan pertama melakukan serangan bruteforce pada Wordpress tanpa keamanan dengan dua skenario dimana penulis melakukan aktifitas bruteforce setelah melakukan pemindaian dengan menggunakan 2 file yaitu skrip python dan file text sebagai bagian dari serangan yang akan mencocokan dengan password dari database wordpress.

   Skenario yang digunakan adalah serangan gagal dan berhasil, dengan dua skenario diharapkan dapat memberikan pemahaman bahwa XML-RPC yang terbuka sebenarnya sudah terbuka peluang untuk mencocokan password pada file text yang dijalankan oleh file python.
2. Tahapan kedua melakukan serangan pada Wordpress dengan keamanan, dan tahapan ini proses yang dilakukan juga sama pada tahapan pertama.

Untuk melakukan penelitian ini penulis telah membuat beberapa file yang digunakan untuk melakukan serangan yang terdiri dari skrip python dengan nama file lokoscannerX_v1.py. dan file text yang akan dijalankan untuk mencocokan password pada database wordpress

Didalam file python sudah dibuatkan skrip serangan hanya ke user dengan nama admin dan file text dengan nama file passwd.txt yang berisikan daftar data password serta dan akan menghasilkan output file dengan nama attack_log.txt. Tujuan penyerangan ini untuk mengetahui username dan password website target yang nantinya dapat digunakan untuk login website target.

Skenario Serangan Pada Wordpress Tanpa Keamanan.

Pada skenario serangan akan melakukan 2 kegiatan yaitu pemindaian ke website target dengan ip lokal yang ada pada komputer penulis dimana web target tanpa ada pengamanan dari segi plugin dan melakukan serangan bruteforce menjalankan file exploitasi python dengan menggunakan 2 skenario serangan yang gagal dan berhasil.

Pemindaian

Sebelum melakukan penyerangan penulis melakukan aktifitas pemindaian pada web yang sudah dibuat pada localhost untuk melihat celah yang mungkin ada pada web wordpress yang diinstalasikan dan berfokus pada file xmlrpc.php sebagai target serangan. Pada bagian ini penulis akan melakukan perintah, contoh : wpscan --url https://example.com , wpscan ini merupakan salah satu alat yang tersedia pada kali linux, dan dijalankan pada terminal .Beberapa pemindaian yang dilakukan adalah melihat vulnerability dan user yang ada pada wordpress

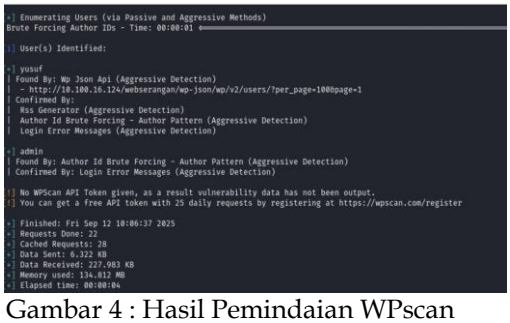
1. Pemindaian awal menggunakan format penulisan atau perintah wpscan --url

http://10.100.16.124/webserangan , ip yang tertera Adalah ip pada jaringan internet yang digunakan oleh penulis.

Gambar 3 : Pemindaian dengan WPscan
Sumber : Pribadi

Hasil pemindaian pada gambar 3, terlihat bahwa file XML-RPC enabled yang dijalankan melalui file xmlrpc.php ini berarti bisa dilakukan exploitasi, Langkah selanjutnya yaitu melakukan pelacakan user yang ada pada wordpress tersebut. (Sucuri, 2023; Cloudflare, 2015)

2. Melakukan pemindaian untuk mengetahui user , dengan menambahkan perintah --enumerate u wpscan --url http://10.100.16.124/webserangan –enumerate u , dengan perintah ini maka akan dilakukan scan kerentanan dari wordpress sekaligus juga memberikan informasi user yang ada pada web tersebut.



Gambar 4 : Hasil Pemindaian WPscan
Sumber : Pribadi

Pada gambar 4 terlihat bahwa ada dua user yaitu user admin dan yusuf, maka dalam penelitian ini akan menargetkan user admin sesuai dengan skrip python yang telah dibuat .

Serangan Bruteforce

Setelah melakukan pemindaian maka penulis akan melakukan serangan bruteforce dengan menggunakan file yang telah dibuat sebelumnya yaitu lokoscannerX_v1.py dan daftar username dan password yang telah dibuat dalam bentuk text dan akan menghasilkan keluaran berupa *log file* . perintah yang akan digunakan untuk menjalankan file Adalah :
python lokoscannerX_v1.py. (Python Software Foundation, n.d.)

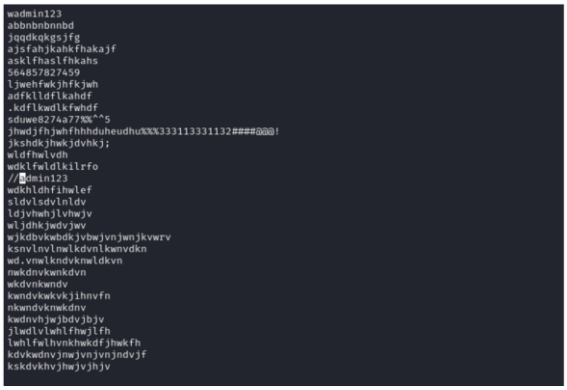
Gambar 5 : Skrip Python
Sumber : Pribadi

Cara kerja dari skrip ini adalah akan mencocokaan username dan password yang ada pada file .txt dan exploitasi password yang ada pada database web target , lalu akan menghasilkan output berupa logfile dalam bentuk text. Tahapan akan dilakukan dua kali percobaan bruteforce yaitu dengan password yang salah dan benar, untuk memberikan Gambaran bagaimana hasil keluaran

yang dihasilkan. ini akan mencocokan kemungkinan password yang ada dalam passwd.txt dengan database website target.

Skenario Serangan Gagal

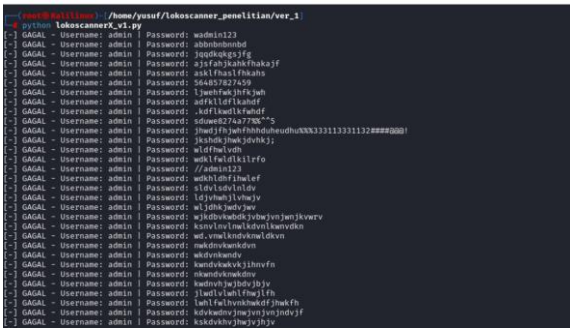
Berikut susunan password yang ada pada file passwd.txt , password yang benar adalah *admin123*, dalam gambar penulis memang sengaja membuat salah password agar terlihat hasil keluaran benar atau salah.



Gambar 6 : isi passwd.txt dengan password salah
Sumber : Pribadi

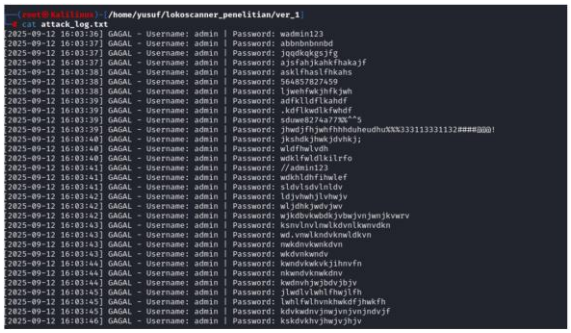
Pada gambar 6 adalah isi dari file passwd.txt dengan banyak kombinasi password salah satunya "//admin123" Dimana password yang sebenarnya pada database adalah "admin123"

Berikut hasil output program setelah menjalankan file python lokoscannerX_v1.py. dengan scenario gagal.



Gambar 7 : Hasil serangan dengan skenario gagal.
Sumber : Pribadi

Hasil dari tahapan ini juga dapat dilihat melalui log file yang dihasilkan oleh file python lokoscannerX_v1.py keluaran file ini diberi nama attack_log.txt yang otomatis dibuat ketika lokoscannerX_v1.py ini dijalankan ketika melakukan serangan.



Gambar 8: output file log
Sumber : Pribadi

Isi dari file log pada gambar 8 terlihat informasi lama waktu serangan dan pencocokan antara username dan password dari wordpressyang dijadikan target.

Skenario Serangan Berhasil

Penulis melakukan edit skrip pada file passwd.txt dengan menggunakan password yang sesuai dengan isi database yaitu "admin123".

Gambar 9 : Hasil serangan dengan skenario berhasil .
Sumber : Pribadi

Dari kedua tahapan ini membuktikan bahwa wordpress yang tidak dipasang keamanan dapat dengan mudah dipindai dan dilakukan serangan bruteforce , hal ini terlihat ketika kedua skenario menghasilkan proses pencocokan database dengan kombinasi password yang terdapat pada file text yang telah dibuat dengan keluaran file log berupa informasi gagal dan berhasil dari setiap serangan yang telah dilakukan.

Tahapan Serangan Pada Wordpress Dengan Keamanan.

Pada tahapan berikut akan di lakukan pemasangan plugin keamanan Disable XML-RPC pada wordpress dan melakukan konfigurasi pada htaccess. Proses yang dilakukan pada tahapan ini juga sama dengan sebelumnya yaitu menggunakan WPScan untuk pemindaian tetap menggunakan file Python yang sama lokoscannerX_ver1.py.

1. Plugin Disable XML-RPC

Pada tahap awal setelah wordpress di pasang plugin Disable XML-RPC akan dilakukan wpscan seperti sebelumnya . dan hasil pemindaian yang di dapat adalah web tidak merespon dengan pesan 403 ini berarti bahwa protocol XML-RPC yang di implementasi pada file xmlrpc.php sudah tidak dapat di akses dan oleh WPScan. (Sucuri, 2023)

Gambar 10 : Hasil pemindaian gagal .
Sumber : Pribadi

Dari hasil pada gambar diatas terlihat WPScan tidak dapat menemukan informasi celah yang dapat dilakukan untuk menyerang endpoint XML-RPC melalui xmlrpc.php dan hal ini mengindikasikan bahwa web target tidak dapat dengan mudah dilakukan bruteforce karena tidak ada respon dari website.

Setelah WPScan gagal maka penulis mencoba melakukan serangan bruteforce dengan file lokoscannerX

Gambar 11 : Hasil serangan error .
Sumber : Pribadi

Pada gambar diatas terlihat bahwa serangan gagal dengan keterangan "Protocol ERROR" . Hal ini membuktikan bahwa file xmlrpc.php sudah tidak dapat diakses.

2. Konfigurasi file htaccess

Pada tahapan ini penulis menonaktifkan plugin yang terpasang sebelumnya dan melakukan konfigurasi pada file .htaccess yaitu dengan menambahkan aturan "deny" untuk menolak semua permintaan yang akan mengakses file xmlrpc.php.

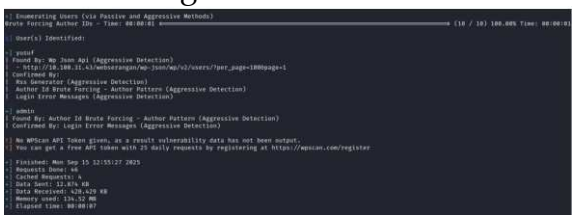
```
# BEGIN WordPress
# The directives (lines) between "BEGIN WordPress" and "END WordPress" are
# dynamically generated, and should only be modified via WordPress filters.
# Any changes to the directives between these markers will be overwritten.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
RewriteBase /webserangan/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /webserangan/index.php [L]
</IfModule>

# menambahkan aturan untuk deny port XML-RPC
<Files xmlrpc.php>
    Order Allow,Deny
    Deny from all
</Files>


# END WordPress
```

Gambar 12 : Penambahan aturan deny port XML-RPC .
Sumber : Pribadi

Setelah melakukan penambahan aturan maka penulis melakukan pemindaian kembali dengan WPScan.



Gambar 13 : hasil WPScan informasi user masih dapat terlihat
Sumber : Pribadi

pada hasil wpscan masih dapat di deteksi user pada wordpress yaitu admin dan yusuf. Walaupun demikian setelah di coba untuk melakukan bruteforce attack dengan file python tidak berhasil dilakukan , dapat terlihat pada gambar berikut :

Gambar 14 : Informasi protocol error
Sumber : Pribadi

Dari hasil percobaan serangan tidak didapatkan informasi seperti sebelumnya ketika tanpa menambahkan keamanan baik berupa plugin maupun pengaturan konfigurasi , hal ini menandakan bahwa file xmlrpc.php tidak dapat di akses, sehingga ketika file dijalankan muncul "Protocol Error ".

Hasil Penelitian

Berikut di tampilkan hasil penelitian pada tabel 1 yaitu lama waktu serangan, status serta skenario yang digunakan dan tabel 2 , untuk menggambarkan efektifitas dari keamanan yang digunakan.

Tabel 1. Waktu Percobaan Serangan

Skenario	Attempts (total)	Attempts/sec (rata-rata)	Status (Berhasil/ Gagal)
Sebelum diberikan keamanan	5.000	25	Gagal
Sebelum keamanan (password terdapat pada file text)	8.200	41	Berhasil
Setelah plugin terpasang	200	2	Gagal

Tabel 2. Efektifitas serangan

Skenario	Status XML-RPC	Identifikasi User	Python	Efektivitas
Tanpa keamanan	Aktif	Bisa	Berhasil	Sangat rentan
Plugin Disable XML-RPC	Tertutup total	Tidak bisa	Gagal	Sangat efektif
.htaccess	Tertutup	Bisa	Gagal	Cukup efektif

Dari tabel 2 terlihat bahwa tanpa keamanan wordpress sangat rentan untuk diserang dan apabila menggunakan plugin seperti disable XML-RPC lebih efektif dibanding konfigurasi .htaccess.

KESIMPULAN

Dari hasil penelitian yang dilakukan dengan menggunakan beberapa tahapan serangan yaitu skenario serangan pada wordpress tanpa keamanan dan wordpress yang sudah tambahkan plugin keamanan serta modifikasi file htaccess , dimana tahapan yang diawali dengan melakukan pemindaian pada web wordpress dan penyerangan bruteforce dengan file yang dibuat, maka dapat diambil Kesimpulan :

1. File xmlrpc.php pada wordpress mempunyai kerentanan yang dapat disalah gunakan terutama pada wordpress yang tidak menggunakan sistem keamanan, sehingga dapat dilakukan manipulasi pada user apabila password sudah dapat dideteksi dan dapat mengambil alih website target.
2. Wordpress dengan tanpa keamanan lebih rawan untuk dilakukan bruteforce yang mengakibatkan sistem menjadi kebanjiran permintaan sehingga gagal diakses atau denial of service, dapat dilihat dari hasil log bahwa ada waktu yang dibutuhkan dalam setiap pencocokan data serangan dengan web target sehingga dapat dibayangkan apabila data serangan dari sangat banyak dalam beberapa kali serangan..
3. Penggunaan Plugin keamanan pada wordpress akan lebih baik dibanding melakukan kustomisasi file htaccess .

DAFTAR PUSTAKA

Buku

Erickson, J. (2008). Hacking: The Art of Exploitation (2nd ed.). No Starch Press.

Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd ed.). Wiley.

Jurnal/Skripsi/Preprint

Hassan, M. M., Arefin, M. S., & Hossain, M. S. (2017). Detection of WordPress Content Injection Vulnerability. arXiv. diakses pada 29 Mei 2025, dari https://arxiv.org/abs/1711.02447

Rabheru, R., Johnson, D., Trippel, C., & Jain, R. (2020). A Hybrid Graph Neural Network Approach for Detecting PHP Vulnerabilities. arXiv. diakses pada 28 Mei 2025, dari https://arxiv.org/abs/2012.08835

Wardaya, M. S. S. (2020). Penetration Testing terhadap Website WordPress Menggunakan Metode Brute Force pada Fitur XML-RPC (Skripsi, UIN Syarif Hidayatullah Jakarta). diakses pada 10 Juni 2025, dari http://repository.uinjkt.ac.id/dspace/handle/123456789/48282

Internet/Web

Cloudflare. (2015, October 16). A look at the new WordPress brute force amplification attack. diakses pada 14 Juni 2025, dari https://blog.cloudflare.com/a-look-at-the-new-wordpress-brute-force-amplification-attack/

Kravtsov, P. (2015). Brute Force Amplification Attacks Against WordPress XMLRPC. Sucuri Blog. diakses pada 20 Mei 2025, dari https://blog.sucuri.net/2015/10/brute-force-amplification-attacks-against-wordpress-xmlrpc.html

OWASP Foundation. (2021). OWASP Top Ten Web Application Security Risks. diakses pada 10 Juni 2025, dari https://owasp.org/www-project-top-ten/

Python Software Foundation. (n.d.). xmlrpc.client — XML-RPC client access. Python 3 documentation. diakses pada 10 Juni 2025, dari https://docs.python.org/3/library/xmlrpc.cli

ent.html

Sucuri. (2023, May 4). What is XML-RPC? Security risks & how to disable. diakses pada 15 Juni 2025, dari https://blog.sucuri.net/2023/05/what-is-xml-rpc-security-risks-how-to-disable.html

Wordfence. (2022). Brute Force Attacks and How to Prevent Them. diakses pada 15 Mei 2025, dari https://www.wordfence.com/learn/brute-force-attacks/

WordPress Developer Resources. (n.d.). XML-RPC API. diakses pada 8 Agustus 2025, dari https://developer.wordpress.org/xml-rpc/

Wordpress.org , About Wordpress, diakses pada 8 Agustus 2025, dari https://wordpress.org/about/

WPScan Team. (2021, June 29). Is WordPress XMLRPC a security problem? WPScan Blog. diakses pada 20 Agustus 2025, dari https://wpscan.com/blog/is-wordpress-xmlrpc-a-security-problem/