

PANDUAN PENANGANAN *Username Enumeration*

Jl. R.A. Kartini, Kel. Lolu Selatan Kec. Palu Timur, Kota Palu Sulawesi Tengah, 94235

© SultengProv-CSIRT

2024

DOKUMEN

TERBATAS

Tabel Versi Dokumen

No	Versi	Tanggal	Deskripsi Perubahan
1	1.0	2024-12-10	Versi awal dokumen

Tabel Anggota Tim

No	Nama	Peran
1	Tatin Supriatin, S.Kom.	Proofreader
2	Ir. Moh. Arham Rahim, S.Kom.	Content Writer
3	Nael Amany, S.Kom.	Graphic Designer
4	Muhammad Adi Agum, S.Kom.	Layout Editor

CATATAN

Sebelum melanjutkan ke tahap ini, sangat disarankan untuk melakukan backup guna menghindari hal-hal yang tidak diinginkan.

DESKRIPSI

Username Enumeration adalah suatu teknik yang digunakan oleh penyerang untuk memverifikasi apakah suatu username valid atau tidak dalam sistem tertentu, seperti pada aplikasi web atau situs. Penyerang memanfaatkan perbedaan respons yang diberikan oleh sistem ketika username yang dimasukkan valid atau tidak untuk mengidentifikasi username yang ada di dalam sistem. Username enumeration dapat digunakan oleh penyerang untuk melakukan serangan brute force dengan menebak username valid dan kemudian mencoba menebak password-nya. Selain brute force, penyerang juga dapat mencoba serangan phishing untuk mendapatkan informasi login dari pengguna yang teridentifikasi.

Serangan Username Enumeration dapat menjadi titik awal bagi penyerang untuk melancarkan berbagai jenis serangan lebih lanjut, yang pada akhirnya dapat mengarah pada pelanggaran data yang lebih besar atau akses yang tidak sah.

PROOF OF CONCEPT

- 1. Akses URL *login wordpress* atau akses URL utama *web wordpress* dan tambahkan salah satu sub direktori di bawah ini:
 - o /wp-login.php : https:// url-web-profile-anda.com/wp-login.php
 - o /wp-admin.php : https:// url-web-profile-anda.com/wp-admin.php
 - o /wp-login : https:// url-web-profile-anda.com/wp-login
 - o /wp-admin : https:// url-web-profile-anda.com/wp-admin

♥ B Log Manuk + Testing-Vuln → W: × +	- • ×
← → C 🗱 22/2-202-154-180-155.ngrok-free.app/wp-login.php	९ 🖈 💩 🙀 छे। 🕹 💽 :
	Nama Pengguna atau Alamat Email
	Lupa sandi Anda? Pergi ke Testing-Vuln Ca Bahasa Indonesia V Ubah

2. Masukkan nama pengguna (username) yang benar dan kata sandi (password) yang salah untuk melihat pesan kesalahan (error) yang muncul.

♥ W Log Masuk + Testing-Vuln — W × +		
← → O 😫 22f2-202-154-180-155.ngrok-free.app/wp-login.php		👓 ९ 🖈 🛷 🐂 🖸 । 🛓 💽 :
	Eror: Kata sandi yang Anda masukkan untuk pengguna kalil tidak cocok. <u>Lupa sandi Anda?</u>	
	Nama Pengguna atau Alamat Email	
	Sandi ©	
	Ingat Saya Log Masuk	
	Lupa sandi Anda?	
	- Pergi ke lesting-vuin	

Kemudian akan muncul pesan kesalahan yang menyatakan kata sandi yang di masukkan untuk nama pengguna terkait tidak cocok. Sehingga memberikan informasi bahwa nama pengguna benar.

Eror: Kata sandi yang Anda masukkan untuk pengguna **kaili** tidak cocok. <u>Lupa sandi Anda?</u>

REMEDIASI

A. MENGGUNAKAN WORDPRESS PLUGIN

1. *Login* ke *wordpress*, kemudian pergi ke menu *Plugin* dan pilih "Tambah *Plugin* Baru".

Y 🛞 Plugin « Testing-V	Word® × +			
← → σ ≅ •	ebb-202-154-180-155.ngrok-free.app/wp-admin/p		🖈 🛷 🖕 🎦 i 🥑) :
🛞 👌 Testing-Vuln 🖣	🖡 0 🕂 Baru 🥕 Manage dummy data		Hai, ka	alli 🔳
2 Dasbor	Plugin Tambahkan Plugin Baru		Opsi Layar 🔻 🛛 Bantuan 🔹	•
📌 Pos	Semua (4) Aktif (2) Nonaktif (2) Pembaruan c	tomatis Dinonaktifkan (4) Cari plugin yang terinstal		
9] Media	Tindakan Massal		4	item
📕 Laman	Physic	Dashvinsi	Pambaruan Otomatis	
 Komentar Dummy Content Generator 	Antispam Akismet: Perlindungan Spam Aktifkan Hapus	Digmalan oleh jutan orang. Aktimet sanga mungkin adalah cara terbak di dunia untuk melindangi blog Anda dari gam. Membuat aku Anda terindungi bahan saat Anda tidur. Untuk memulai: adalifan puloja Aktimet dari kemudai huka halman Pengataran Aktimet Anda untuk mengatar kunci API Anda.	Aktifkan pembaruan otomatis	
Tampilan Plugin Plugin Terpasang	Hello Dolly Aktifkan Hapus	Ini bukan hanga sebuah plugin, namun mewalili hangan dan antunisame dari sebuah generasi utuh yang dirangkum oleh dua kata yang dinyanyikan oleh Louis Armstrong yang terkenat. Helio, Dolly, Ketika diaktifikan Anda akan disuguh oleh potongan link dari Helio, Dolly secara acak di sisi kanan atas setap taman lagar admin. Wersi 122 Oleh Matt Mullemang Tampilkan rincian	Aktifkan pembaruan otomatis	
Tambahkan Plugin Baru Editor Berkas Plugin	WP Dummy Content Generator	The VHD commy Content Generative" slight is particularly used for developers, designers, and whole administrators who want to quickly product their WordPress site with realistic during content. It saves time and effortly automatically generating content that minics real posts and pages, enabling you to focus on other aspects of website development or testing- WHJ LAS (OM to require a read) TampBar minics.	Aktifkan pembaruan otomatis	
✗ Peralatan ☑ Pengaturan	WP-Ngrok Non-aktifkan	Epose your local WordPress to the world with Ngrok Wersi 1.1.2 (Oldh Themeid) Tampilian rincian	Aktifkan pembaruan otomatis	
Persempit menu	Plugin	Deskripsi	Pembaruan Otomatis	
	Tindalan Masal v Tergilan		41	item
	Terima kasih telah berkarya dengan <u>WordPress</u> .		Versi d	6.7.1

2. Lakukan pencarian "*Limit Login Attempts Reloaded*", kemudian klik "*Install* Sekarang" dan klik "Aktifkan".



3. Setelah itu, coba akses kembali URL *login* dan masukkan nama pengguna (*username*) yang benar dan kata sandi (*password*) yang salah untuk melihat pesan kesalahan (*error*) yang muncul.

ERROR: Inc	ncorrect username or password.
Nama Pe kaili	Pengguna atau Alamat Email
	2 attempts remaining.
ingat	at Saya Log Mesuk
Lupa sand	rdi Anda?
- Pergi kr	ke Testing-Vuln
G Ba	Jahasa Indonesia 👻 Ubah

Dari pesan kesalahan yang ditampilkan sudah tidak menampilkan informasi petunjuk apabila nama penggunanya benar. Selain itu apabila penginputan nama pengguna dan kata sandinya salah sebanyak 4 kali, maka akan muncul pesan kesalahan atau *error* bahwa terlalu banyak percobaan *login* yang salah, sehingga harus menunggu 20 menit lagi untuk bisa mencoba *login*, seperti yang terlihat pada gambar berikut.

ERROR: Too many failed login attempts. Please try again in 20 minutes.
Nama Pengguna atau Alamat Email kaili Sandi ••••• Ingat Saya Log Manuk
Lupa sandi Anda? Pergi ke Testing-Vuln PD Bahasa Indonesia V Ubah

4. Install dan aktifkan plugin "WPS Hide Login".



5. Lanjut ke menu Pengaturan → Umum, lalu scroll paling bawah dan pada bagian Login url, ubah teksnya dari login ke teks yang tidak mudah di tebak untuk menjadi url login yang baru (jangan lupa untuk dicatat dan disimpan) dan gunakan url login baru tersebut ketika ingin login.

 ↔ σ ∰ 	d6c-202-154-180-155.ngrok-free.app	/wp-admin/options-genera	Lphp :	🖈 🙍 🙀 🖸 i 🙆 🗄
🚯 👩 Testing-Vuln	🗅 1 👎 0 🕂 Baru			Hai, kaili 🔲 📍
Dasbor	Format Tanggal	12 Desember 2024	314	
📌 Pos		0 2024-12-12	V-m-d	
9] Media		0 12/12/2024	m/d/Y	
📕 Laman		0 12/12/2024	<i>d/m/</i> Y	
Komentar		 Sesuaikan:) F Y	
		Pratinjau: 12 Desember 20	24	
🔎 Tampilan	Format Waktu	1:55 am	and a	
Jir Plugin	romat matu	0 1/55 AM		
🚢 Pengguna		0 0155 AM	u.l	
🎤 Peralatan		O Seruaikan:	ma .	
Pengaturan		Pratinjau: 1:55 am	β. «	
Umum		Dokumentasi format tang	ail dan waktu	
Membaca Diskusi	Minggu Dimulai Pada Hari	Senin 🛩		
	WPS Hide Login			
	Need help? Try the <u>support forum</u> . TI Discover our other plugins: the plugi You want to find out how to simplify	ns plugin is kindly brought to n <u>WPS Bidouille</u> , the plugin <u>W</u> ecommerce with WordPress, 1	you by (Schart et al.)	
Persempit menu	Login url	https://0d6c-202-154-1	88-155.ngrok-free.app/ nasi-kuning-malam /	
		Protect your website by cl	anging the login URL and preventing access to the wp-login.php page and the wp-admin directory to non-connected people.	
	Redirection url	https://0d6c-202-154-: Redirect URL when some	88-135.ngrok-free.agr/. 804 Z	
	Simpan Perubahan			

B. KONFIGURASI SECARA MANUAL LEWAT SCRIPT CODE

1. Buka file "wp-login.php".



2. Ubah *script* dibawah ini.



menjadi seperti berikut:



```
foreach ($wp_error->get_error_codes() as $code) {
   $severity = $wp_error->get_error_data($code);
   foreach ($wp_error->get_error_messages($code) as $error_message) {
      if ('message' === $severity) {
         $messages .= 'bbb' . $error_message . '';
    } else {
        if ($code = 'invalid_username') {
            $error_message = 'Invalid username or password!';
        }
        $error_list[] = $error_message;
    }
}
```

3. Akses kembali halaman *login* dan inputkan nama pengguna (*username*) yang benar dan kata sandi (*password*) yang salah untuk memunculkan pesan kesalahan (*error*).

♥ Q9 Log Masuk c Testing-Wah → W: × +		- o i x
← → C 12 0d6c-202-154-180-155.ngrok-free.app/wp-login.php		ବ୍ୟ 🖈 👷 🗗 i 😰 :
	Invalid username or password!	
	Nama Pengguna atau Alamat Email kaili	
	Sandi	
	Ingat Saya Log Masuk	

Dari pesan kesalahan yang ditampilkan sudah tidak menampilkan informasi petunjuk apabila nama penggunanya benar.

4. Selanjutnya untuk mengubah *url* akses *login*-nya dari /wp-login.php menjadi sesuai yang diinginkan, contohnya /nasi-kuning-malam.php, dengan mengubah nama *file*-nya seperti berikut:

Sebelum diubah	💏 wp-load.php	
	💏 wp-login.php	
	🗬 wp-mail.php	
Setelah diubah	🧎 license.txt	
	🗬 nasi-kuning-malam.php	
	readme.html	

 Akses url login yang sebelumnya memakai /wp-login.php menjadi /nasi-kuningmalam.php, apabila berhasil maka akan tetap memunculkan halaman *login*, seperti yang terlihat pada gambar berikut.

♥ Stog Masuk ← Testing-Yuln — W: × +		
← → C 2 0d6c-202-154-180-155.ngrok-free.app/nasi-kuning-malam.php		९ 🖈 🛷 🖕 छे। 📀 ह
A C S Olic 202-154-180-155.agrak free.agg/nasi-koning-malam.php	Nama Pengguna atau Alamat Email	(\$\mathcal{A}\$) \$\mathcal{A}\$ \$\mathcal{A}\$ \$\mathcal{B}\$ \$\mathcal{A}\$ \$\mathcal{B}\$ \$\mathcal{A}\$ \$\mat
	Lupa sandi Anda? Pergi ke Testing-Vuln	

REKOMENDASI

- 1. Mengganti URL *login default* (wp-login.php) ke URL yang lebih aman dan tidak gampang di tebak oleh orang yang tidak berkepentingan dan juga menyulitkan penyerang dalam mengidentifikasi halaman login.
- 2. Mengganti pesan kesalahan menjadi lebih umum yang tidak mengungkapkan apakah *username* atau *password* yang dimasukkan benar.
- 3. Membatasi jumlah percobaan *login* yang gagal agar mencegah serangan *brute force* dan enumerasi *username* dengan memblokir akses setelah beberapa upaya *login* yang gagal.
- 4. Menggunakan *firewall* dapat membantu memblokir permintaan *login* dari alamat IP yang mencurigakan atau melakukan *filtering* terhadap upaya *login* yang berpotensi berbahaya.