PEMPROV SULTENG
DISKOMINFOSANTIK
DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK

DOKUMEN TERBATAS

PANDUAN PENANGANAN

Username Enumeration

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

2024

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.

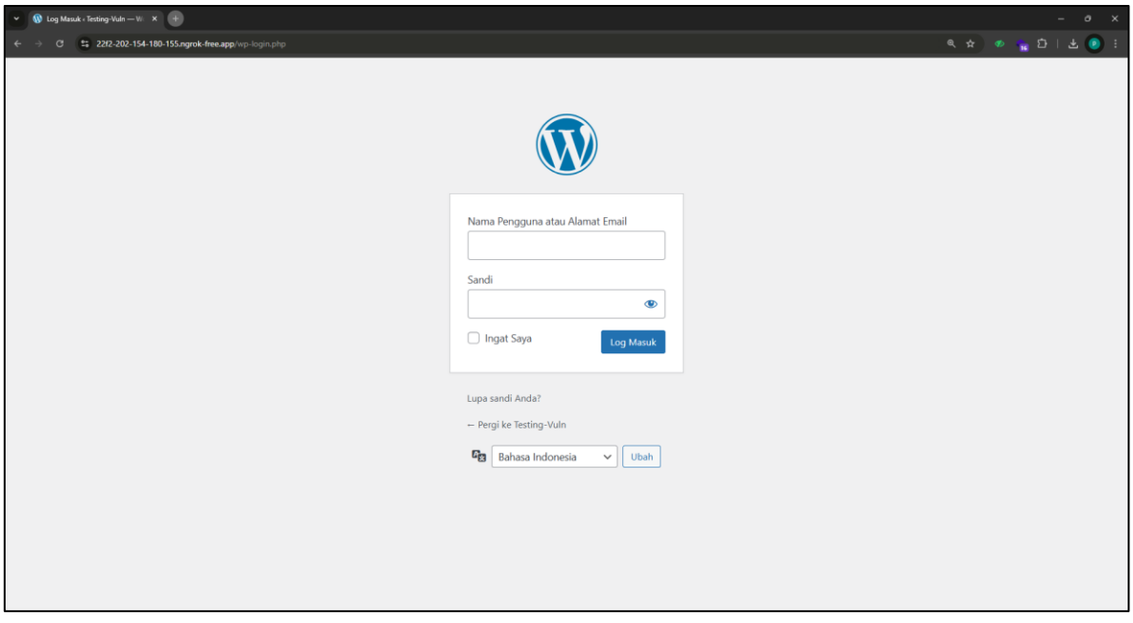
DESKRIPSI

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.

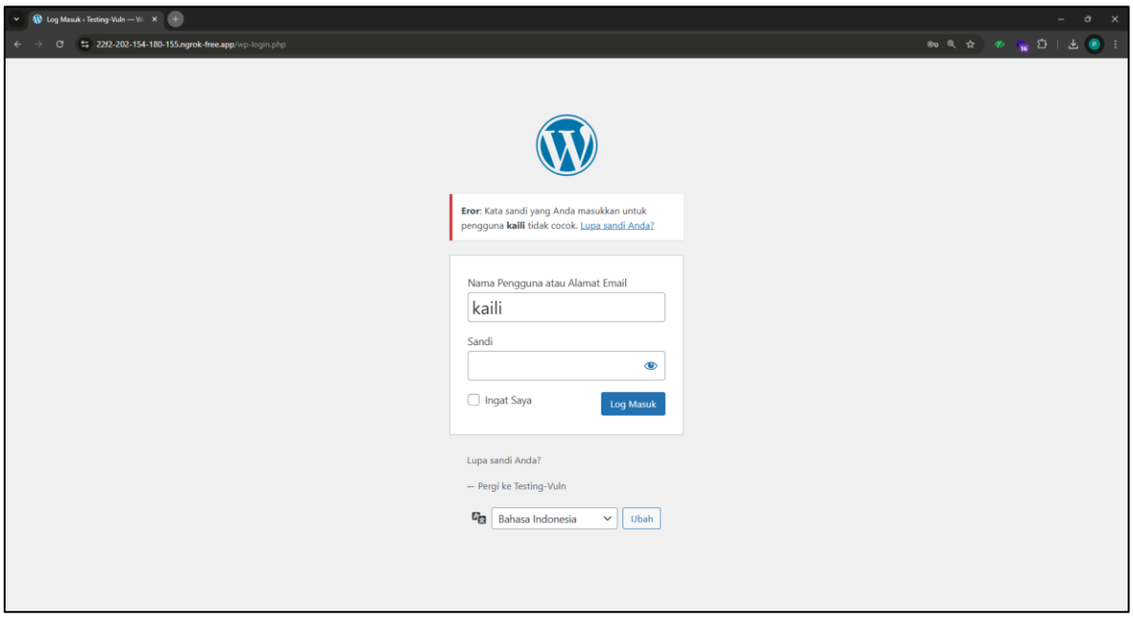
Serangan Username Enumeration dapat menjadi titik awal bagi penyerang untuk melancarkan berbagai jenis serangan lebih lanjut, yang pada akhirnya dapat mengarah pada pelanggaran data yang lebih besar atau akses yang tidak sah.

PROOF OF CONCEPT

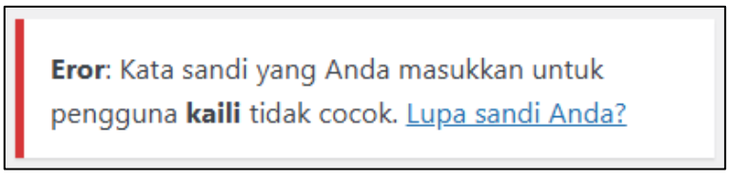
1. Akses URL *login wordpress* atau akses URL utama *web wordpress* dan tambahkan salah satu sub direktori di bawah ini:
   - **/wp-login.php** : https:// url-web-profile-anda.com**/wp-login.php**
   - **/wp-admin.php** : https:// url-web-profile-anda.com**/wp-admin.php**
   - **/wp-login** : https://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



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



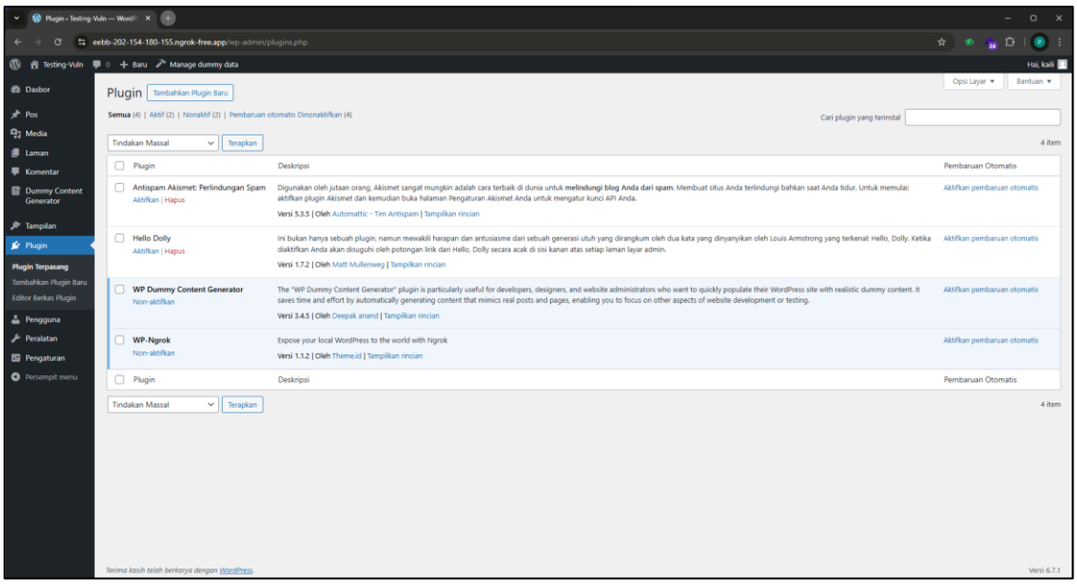
Kemudian akan muncul pesan kesalahan yang menyatakan kata sandi yang di masukkan untuk nama pengguna terkait tidak cocok. Sehingga memberikan informasi bahwa nama pengguna benar.



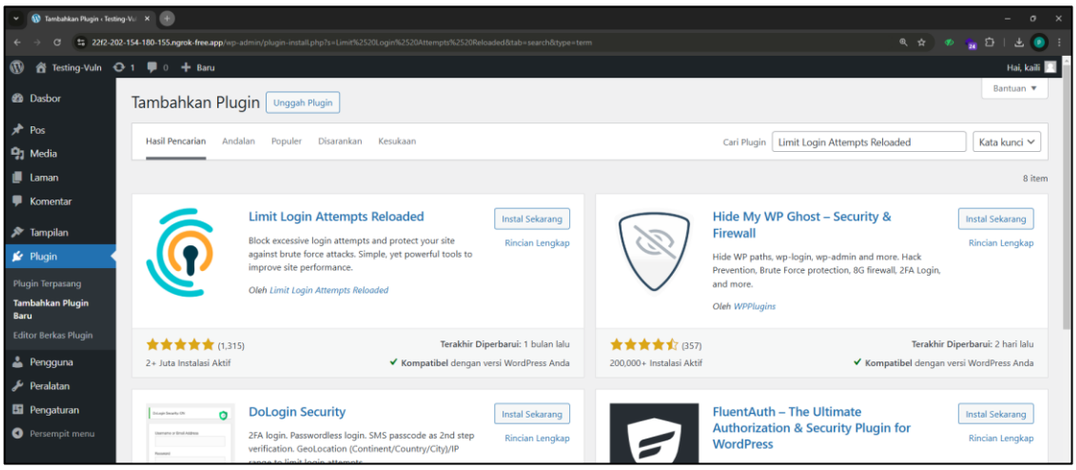
REMEDIASI

A. MENGGUNAKAN *WORDPRESS PLUGIN*

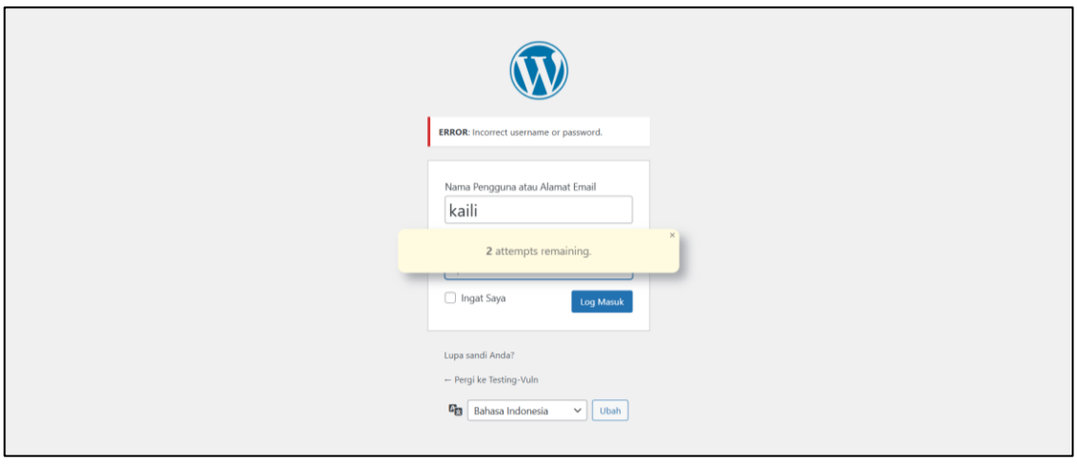
1. *Login* ke *wordpress*, kemudian pergi ke menu *Plugin* dan pilih “Tambah *Plugin* Baru”.



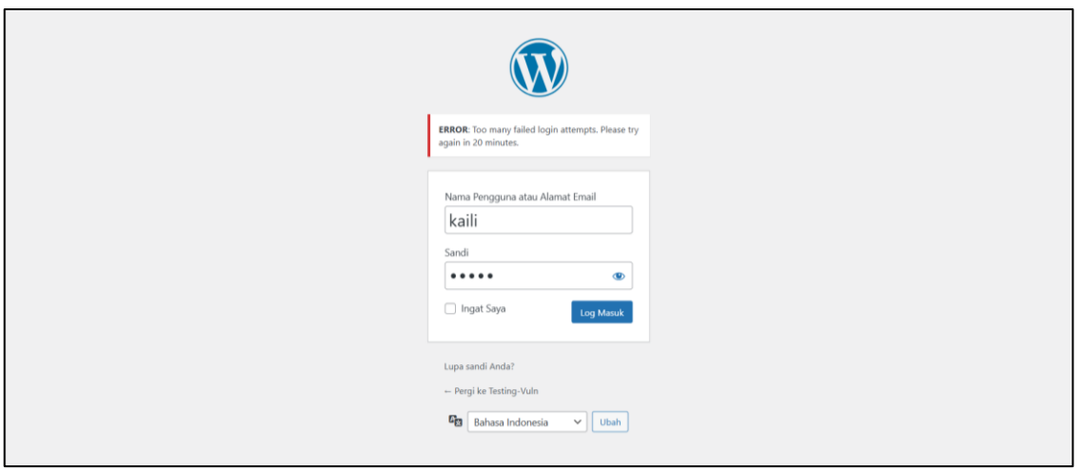
2. Lakukan pencarian “*Limit Login Attempts Reloaded*” , kemudian klik "*Install* Sekarang” dan klik “Aktifkan”.



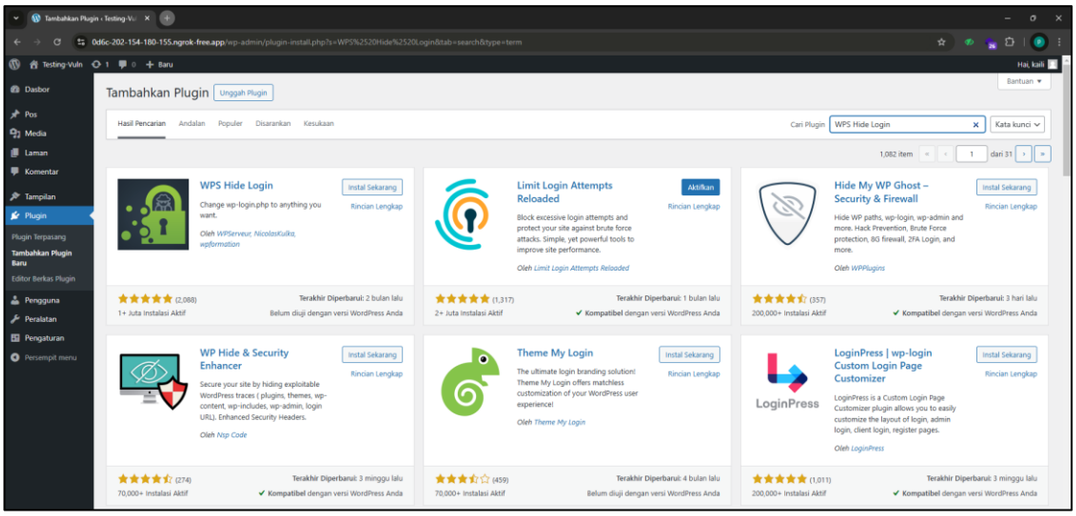
3. Setelah itu, coba akses kembali URL *login* dan masukkan nama pengguna (*username*) yang benar dan kata sandi (*password*) yang salah untuk melihat pesan kesalahan (*error*) yang muncul.



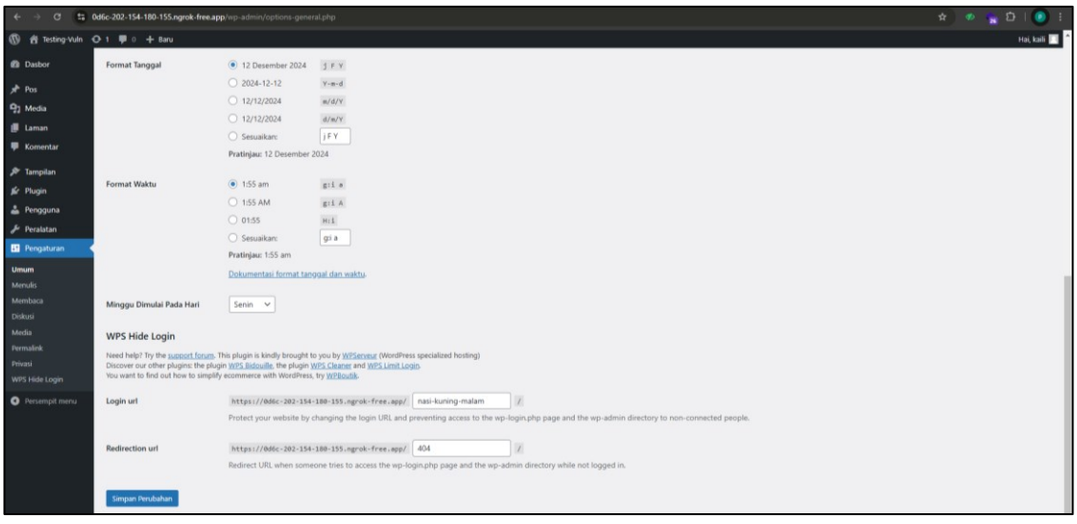
Dari pesan kesalahan yang ditampilkan sudah tidak menampilkan informasi petunjuk apabila nama penggunanya benar. Selain itu apabila penginputan nama pengguna dan kata sandinya salah sebanyak 4 kali, maka akan muncul pesan kesalahan atau *error* bahwa terlalu banyak percobaan *login* yang salah, sehingga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



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

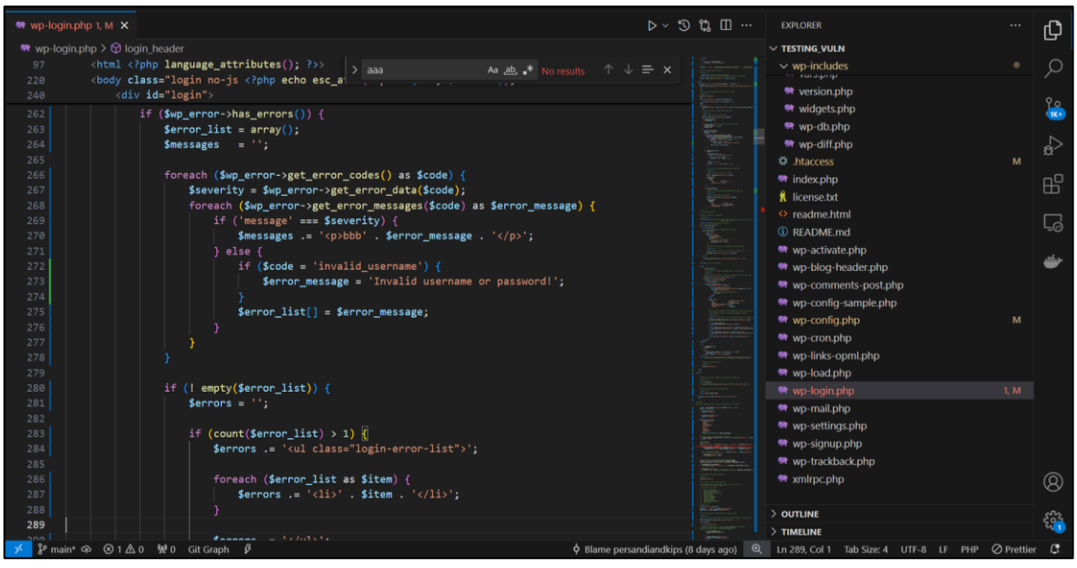


5. Lanjut ke menu Pengaturan → Umum, lalu *scroll* paling bawah dan pada bagian *Login url*, ubah teksnya dari *login* ke teks yang tidak mudah di tebak untuk menjadi *url login* yang baru (**jangan lupa untuk dicatat dan disimpan**) dan gunakan *url login* baru tersebut ketika ingin *login.*



B. KONFIGURASI SECARA MANUAL LEWAT SCRIPT CODE

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



2. Ubah *script* dibawah ini.

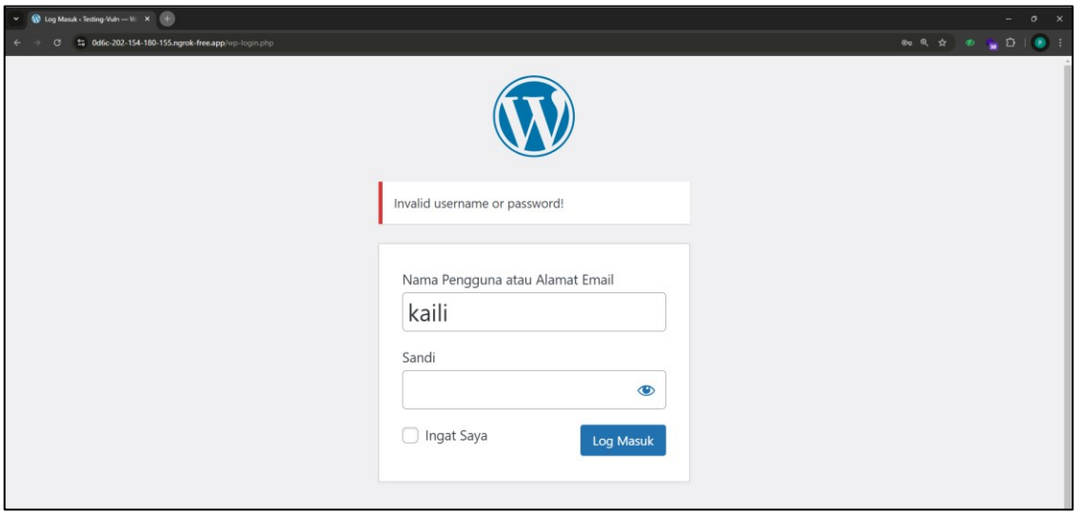
```
foreach ($wp_error->get_error_codes() as $code) {
    $severity = $wp_error->get_error_data($code);
    foreach ($wp_error->get_error_messages($code) as $error_message) {
        if ('message' === $severity) {
            $messages .= '<p>bbb' . $error_message . '</p>';
        } else {
            $error_list[] = $error_message;
        }
    }
}
```

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 .= '<p>bbb' . $error_message . '</p>';
        } else {
            if ($code = 'invalid_username') {
                $error_message = 'Invalid username or password!';
            }
            $error_list[] = $error_message;
        }
    }
}
```

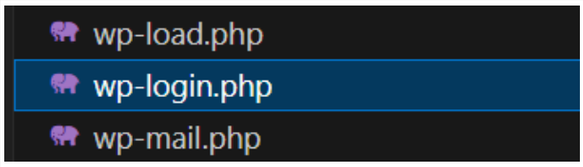
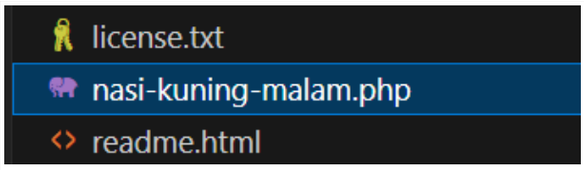
```
foreach ($wp_error->get_error_codes() as $code) {
   $severity = $wp_error->get_error_data($code);
   foreach ($wp_error->get_error_messages($code) as $error_message) {
      if ('message' === $severity) {
         $messages .= '<p>bbb' . $error_message . '</p>';
      } else {
         if ($code = '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*).

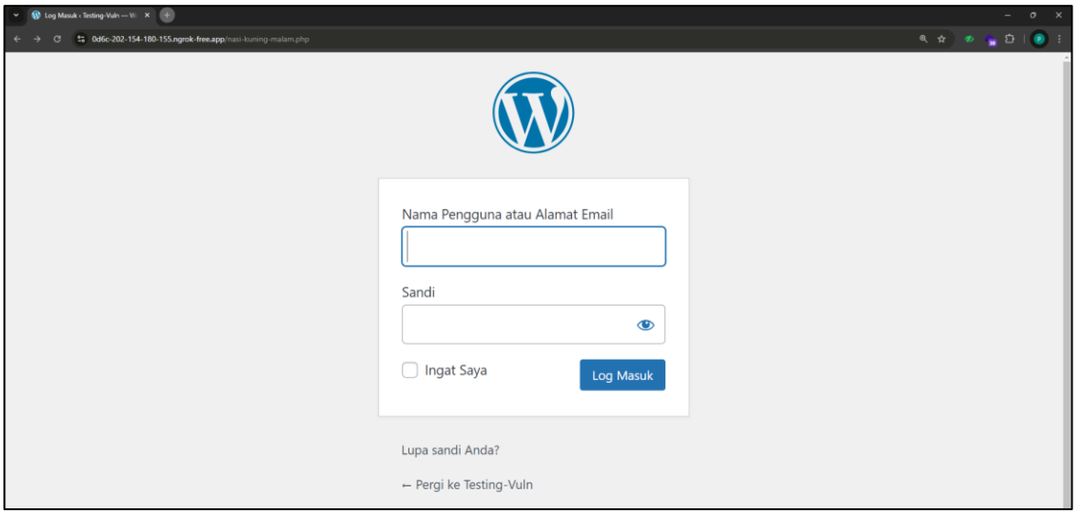


Dari pesan kesalahan yang ditampilkan sudah tidak menampilkan informasi petunjuk apabila nama penggunanya benar.

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	
Setelah diubah	

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



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.