Enumeración de Usuarios en WordPress

¿Qué es la enumeración de usuarios?

La enumeración de usuarios, es una forma de obtener datos de usuarios de su sitio web a través de scripts maliciosos. Aunque el pirata informático solo puede obtener los detalles del nombre de usuario con esto, sigue siendo un riesgo grave. Conocer el nombre de usuario es la mitad del trabajo realizado por un pirata informático al ejecutar un ataque de fuerza bruta.

Método 1: Archivos de autor

Quizás el método más fácil para encontrar nombres de usuario de WordPress es revisar los archivos del autor. Para enumerar nombres de usuario a través del método de archivos del autor. Para enumerar nombres de usuario a través del método de archhivos de autor, simplemente agregue un número entero (es decir: 1,2,3,etc.) como valor al parámetro "autor". Por ejemplo:

- https://tusitio.com/?author=1
- https://tusitio.com/?author=2
- https://tusitio.com/?author=3

Estos valores luego obtendrían resultados como los siguientes:

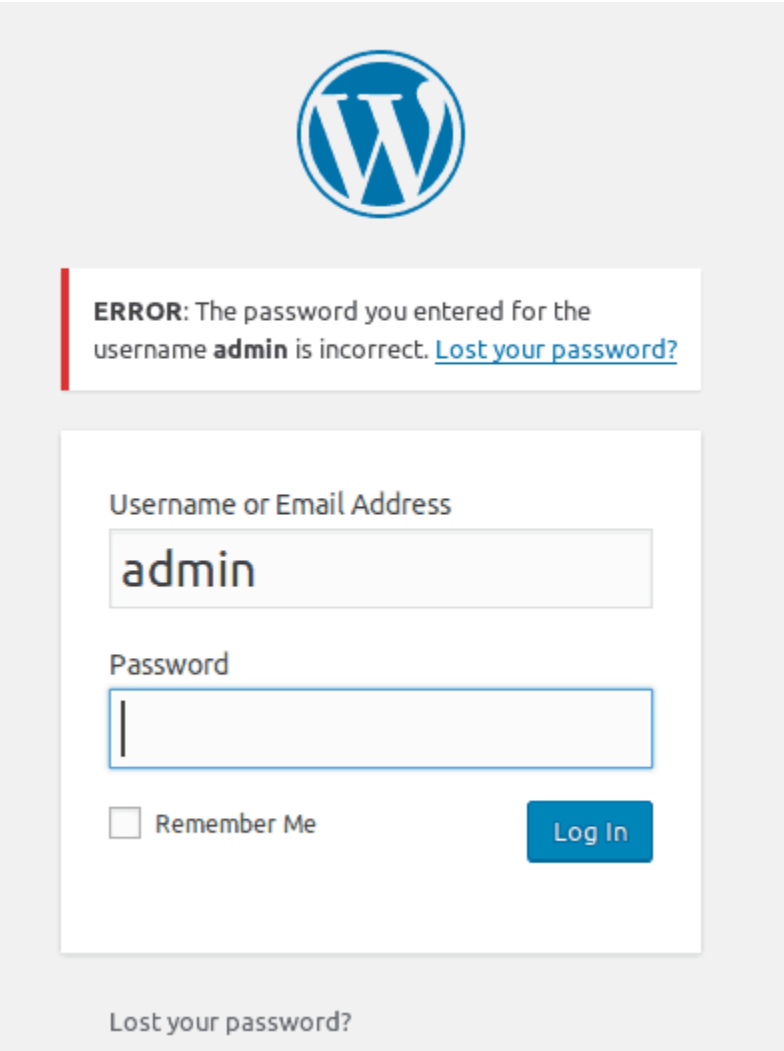
- https://tusitio.com/author/admin/
- https://tusitio.com/author/user2/
- https://tusitio.com/author/user3/

Por lo tanto, al confundir el autor del parámetro en la URL de inicio de WordPress, se pueden enumerar varios nombres de autor.

Método 2: Mensajes de error

A veces, el atacante intenta iniciar sesión en su sitio de WordPress con un nombre de usuario aleatorio. Si el nombre de usuario existe, el mensaje de error revelará que el nombre de usuario es

correcto pero la contraseña es incorrecta. De manera similar, si el nombre de usuario adivinado es incorrecto, el mensaje de error especificaría que el nombre de usuario no existe. Ahora, al utilizar el enfoque de fuerza bruta, el atacante puede enumerar nombres de usuario en función de los mensajes de error.



El mensaje de error revela el nombre de usuario como "admin" se encuentra registrado como usuario del sistema.

Solución a la enumeración de usuarios

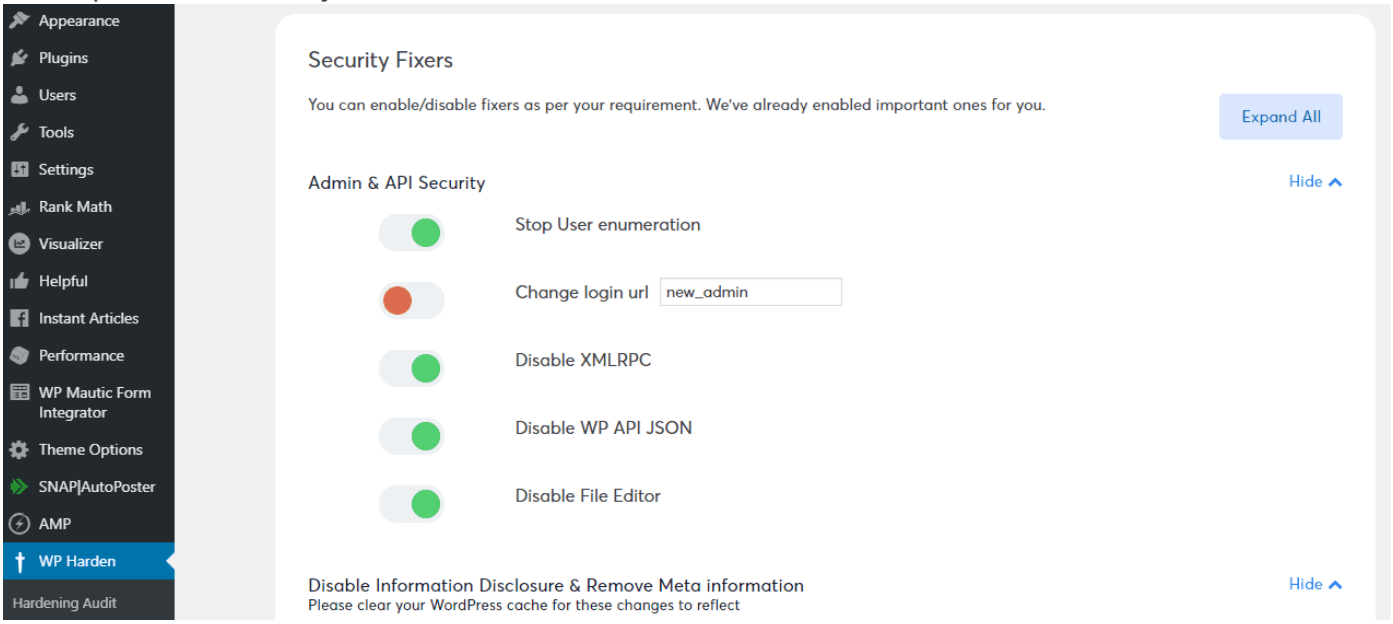
Aplique una de las siguientes opciones para evitar la enumeración de usuarios en WordPress (preferente la opción 1):

1. Instalación de WP-Hardening

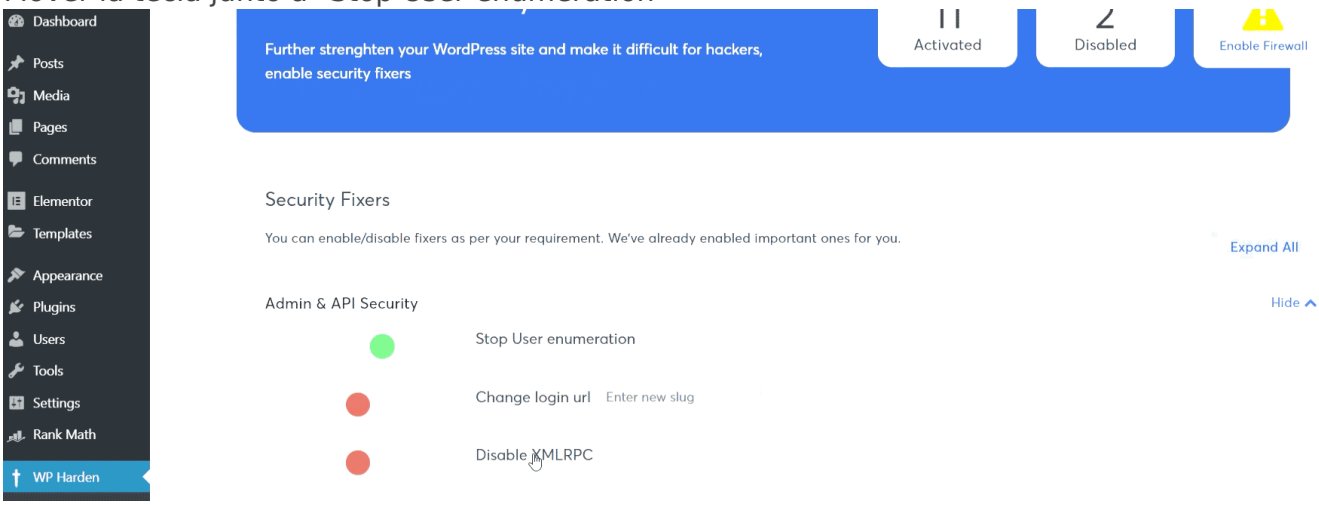
1. Instalar y activar el complemento.
    1. Ir a ‘Plugins > Add New’ en el panel de administración.
    2. Buscar ‘WP-Hardening’

3. Instalar WP-Hardening una vez que aparezca.
4. Activarlo desde su página Plugins.
5. El botón WP-Hardening aparecerá en la parte inferior izquierda de su panel de administración.

2. Ir a la pestaña 'Security Fixers'



3. Mover la tecla junto a "Stop User enumeration"



2. Editando archivos de WordPress

Agregando un fragmento de código al archivo functions.php o al archivo .htaccess en el nivel raíz. El archivo .htaccess debe editarse solo si desea bloquear la solicitud a nivel del servidor.

Método 1: Modificar el archivo functions.php.

- Paso 1: Inicie sesión en el panel de administración de su servidor donde pueda acceder a los archivos.

- Paso 2: Navegar hasta el directorio de instalación de WordPress:
  Ir a wp-content>themes
  Buscar el archivo functions.php
- Paso 3: Abrir el archivo functions.php y copiar el siguiente código:

```
if (!is_admin()) {
// default URL format
if (preg_match('/author=([0-9]*)/i', $_SERVER['QUERY_STRING'])) die(); add_filter('redirect_canonical',
'shapeSpace_check_enum', 10, 2);
}
function shapeSpace_check_enum($redirect, $request) {
// permalink URL format
if (preg_match('/\?author=([0-9]*)(\/*)/i', $request)) die(); else return $redirect;
}
```

Método 2: Modificar el archivo .htaccess.

- Paso 1: Iniciar sesión en el servidor como administardor.
- Paso 2: En el administrador de archivos, busque el archivo .htaccess en la raíz de su servidor.
- Paso 3: Abrir el archivo .htaccess y copie el siguiente código:

```
<IfModule mod_rewrite.c>
RewriteCond %{QUERY_STRING} ^author=([0-9]*)
RewriteRule .* https://tusitioweb.com/? [L,R=302]
</IfModule>
```

3. Eliminar los mensajes de error en páginas de inicio de sesión

Para eliminar los mensajes de error detallados en la ventana de wp-login, debe ingresar el siguiente código en el archivo **functions.php** (Nota.- En caso de funcionar esta solución puede aplicar el código en el archivo **wp-login.php**):

```
<?php
//* NO incluyas la etiqueta de apertura


// Cambia el mensaje de error de inicio de sesión en WordPress


function failed_login() {
    return 'Las credenciales de acceso son incorrectas.';
```

```
}
add_filter('login_errors', 'failed_login');
```

Revision #6
Created 14 abril 2023 09:01:48 by Vladimir Urquiola
Updated 10 abril 2024 11:05:56 by Vladimir Urquiola