

HackerDivulgation.com

DOCS

Lab WordPress

Este laboratorio se crea con el fin de probar herramientas de escaneo y explotación de vulnerabilidades para WordPress.

Contenido

- [Requerimientos](#)
- [Instalación](#)
 - [MySQL](#)
 - [Apache](#)
 - [PHP](#)
- [Descarga WordPress](#)
- [Configuración](#)
 - [MySQL](#)
 - [Permisos](#)
 - [WordPress](#)
- [Verificación](#)
- [Referencias](#)

Requerimientos

1. Software de virtualización. Puede ser: [VirtualBox](#), [VMware Workstation](#), etc.
2. Imagen ISO de una distribución GNU/Linux, se recomienda: [Debian](#) o [Ubuntu Server](#).
3. Instalación del sistema operativo seleccionado en una máquina virtual usando el software previamente mencionado.

Este laboratorio se realizó en Debian 11 y usando VirtualBox.

Instalación

En este apartado se mostrará la instalación de todos los servicios necesarios para el

funcionamiento de WordPress.

Mysql

Actualizar los repositorios de la distribución.

```
sudo apt update
```

Instalar el paquete de MySQL (*MariaDB*).

```
sudo apt install -y mariadb-server
```

Verificar la instalación mostrando la versión.

```
mysql --version
```

```
root@terreros-alex:~# mysql --version
mysql Ver 15.1 Distrib 10.5.12-MariaDB, for debian-linux-gnu (x86_64) using EditLine wrapper
root@terreros-alex:~# _
```

Apache

Instalar el paquete de Apache.

```
sudo apt install apache2
```

Habilitar el servicio en el arranque del sistema.

```
sudo systemctl enable apache2
```

Iniciar el servicio.

```
sudo systemctl start apache2
```

Verificar el estado del servicio.

```
sudo systemctl status apache2
```

```

root@terreros-alex:~# systemctl status apache2
• apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-02-07 08:23:39 PST; 15min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 10961 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 10965 (apache2)
    Tasks: 7 (limit: 1133)
   Memory: 14.3M
      CPU: 107ms
   CGroup: /system.slice/apache2.service
           └─10965 /usr/sbin/apache2 -k start
             └─10966 /usr/sbin/apache2 -k start
               └─10967 /usr/sbin/apache2 -k start
                 └─10968 /usr/sbin/apache2 -k start
                   └─10969 /usr/sbin/apache2 -k start
                     └─10970 /usr/sbin/apache2 -k start
                       └─10971 /usr/sbin/apache2 -k start

Feb 07 08:23:39 terreros-alex systemd[1]: apache2.service: Succeeded.
Feb 07 08:23:39 terreros-alex systemd[1]: Stopped The Apache HTTP Server.
Feb 07 08:23:39 terreros-alex systemd[1]: Starting The Apache HTTP Server...
Feb 07 08:23:39 terreros-alex apachectl[10958]: AH00558: apache2: Could not reliably determine the
Feb 07 08:23:39 terreros-alex apachectl[10964]: AH00558: apache2: Could not reliably determine the
Feb 07 08:23:39 terreros-alex systemd[1]: Started The Apache HTTP Server.
lines 1-24/24 (END)

```

PHP

Instalar el paquete y dependencias de PHP.

```
sudo apt install php libapache2-mod-php php-mysql php-curl php-json php-cgi
```

Reiniciar el servicio Apache.

```
sudo systemctl restart apache2
```

Comprobar la versión de PHP instalada.

```
php --version
```

```

root@terreros-alex:~# php --version
PHP 7.4.25 (cli) (built: Oct 23 2021 21:53:50) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.25, Copyright (c), by Zend Technologies
root@terreros-alex:~#

```

Crear con Nano un archivo `.php` en el directorio `/var/www/html/` que es la raíz por defecto de Apache.

```
nano /var/www/html/info.php
```

```
GNU nano 5.4 /var/www/html/info.php
<?php
    phpinfo();
?>
```

El paso anterior se puede verificar usando el navegador.

`http://IP_SERVER/info.php`



PHP Version 7.4.25



System	Linux terreros-alex 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64
Build Date	Oct 23 2021 21:53:50
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no

Descarga WordPress

Ubicarse en el directorio raíz de Apache.

```
cd /var/www/html
```

Descargar la última versión de [WordPress](https://wordpress.org/latest.tar.gz) usando la herramienta Wget.

```
wget -c http://wordpress.org/latest.tar.gz
```

Descomprimir el archivo.

```
tar -xvf latest.tar.gz
```

Eliminar el archivo comprimido.

```
rm latest.tar.gz
```

Configuración

Configurar de manera correcta los servicios es importante para el funcionamiento, de otra forma no se podrá instalar WordPress.

Se recomienda seguir los pasos como usuario `root`.

MySQL

Ingresar a la línea de comandos de MySQL.

```
mysql -u root -p
```

Crear la base de datos.

```
mysql> CREATE DATABASE wordpress;
```

Crear un nuevo usuario para la conexión de WordPress a la base de datos.

```
mysql> CREATE USER 'wordpress_user'@'localhost' IDENTIFIED BY 'wordpress123';
```

Asignar todos los privilegios sobre la base de datos al usuario anteriormente creado.

```
mysql> GRANT ALL ON wordpress.* TO 'wordpress_user'@'localhost';
```

Recargar las tablas de privilegios guardadas en memoria.

```
mysql> FLUSH PRIVILEGES;
```

Permisos

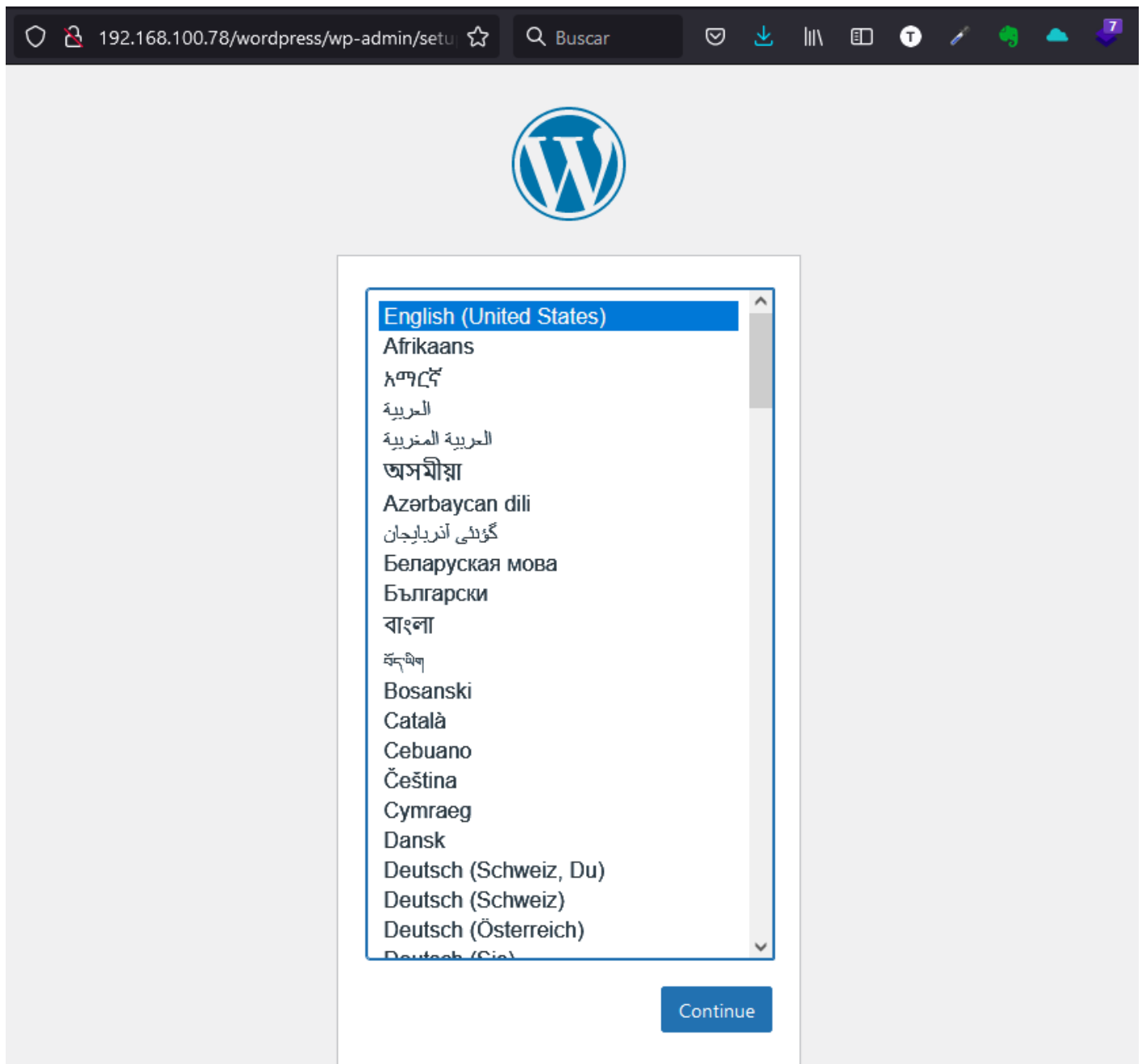
Asignar permisos sobre el directorio `wordpress` al usuario y grupo Apache, de forma recursiva con `-R`.

```
chown -R www-data:www-data /var/www/html/wordpress
```

WordPress

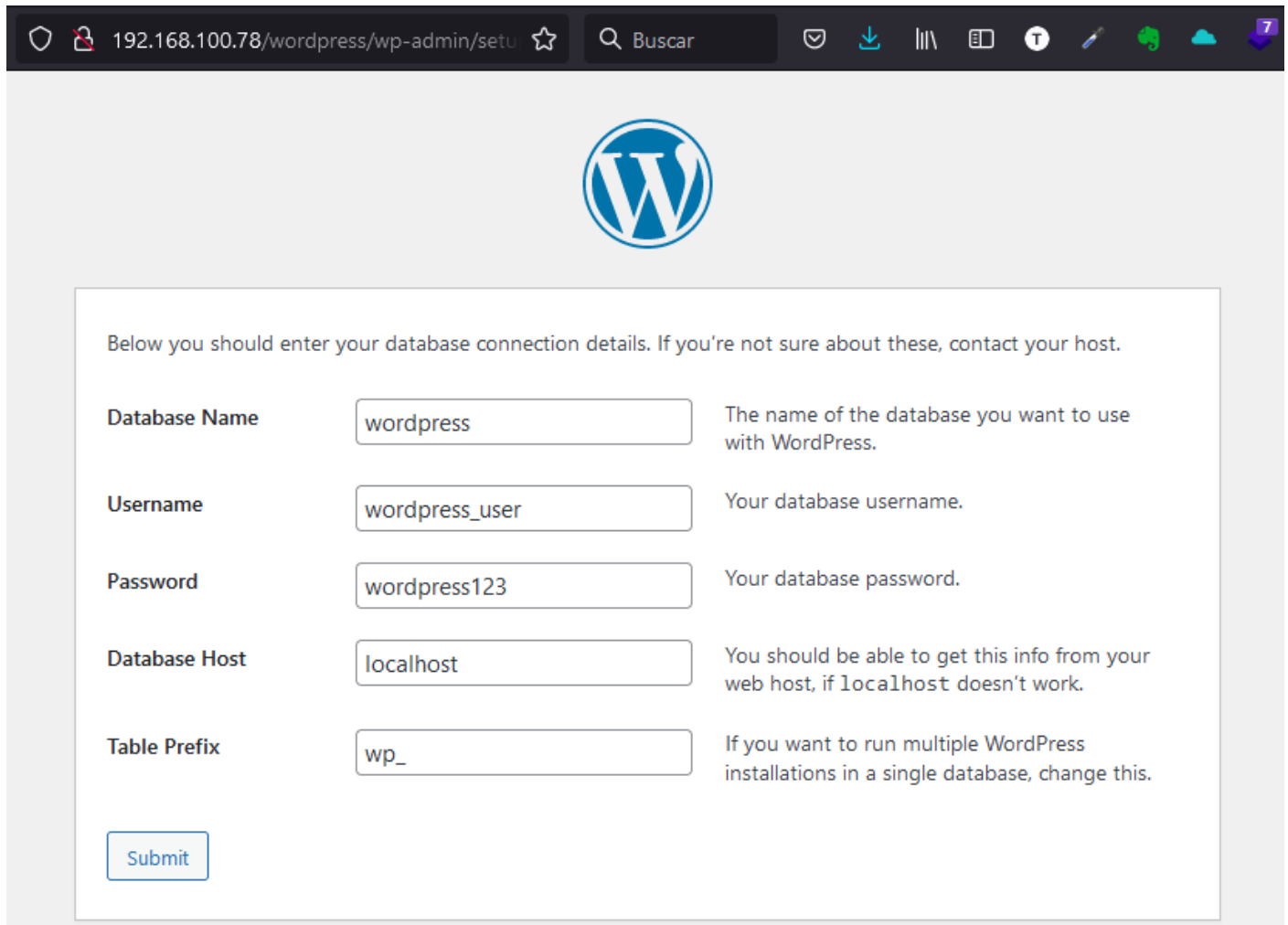
Ingresar desde el navegador usando la IP del servidor.

`http://IP_SERVER/wordpress`



Escribir el nombre, nombre de usuario y contraseña de la base de datos. El prefijo de las tablas

puede dejarse por defecto. Clic en **Submit**.




The screenshot shows a web browser window with the address bar displaying '192.168.100.78/wordpress/wp-admin/setup'. The page features the WordPress logo at the top center. Below the logo, a text instruction reads: 'Below you should enter your database connection details. If you're not sure about these, contact your host.' The form contains five input fields, each with a label on the left and a description on the right:

Field Label	Value	Description
Database Name	wordpress	The name of the database you want to use with WordPress.
Username	wordpress_user	Your database username.
Password	wordpress123	Your database password.
Database Host	localhost	You should be able to get this info from your web host, if localhost doesn't work.
Table Prefix	wp_	If you want to run multiple WordPress installations in a single database, change this.

At the bottom left of the form is a 'Submit' button.

Ingresa el Título del sitio. Crear un usuario y contraseña para el administrador. Se puede colocar un email. Clic en **Install WordPress**.



Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

LAB-HDSEC

Username

admin

Username can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password

admin

Hide

Very weak

Important: You will need this password to log in. Please store it in a secure location.

Confirm Password

☒ Confirm use of weak password

Your Email

admin@lab-hdsec.local

Double-check your email address before continuing.

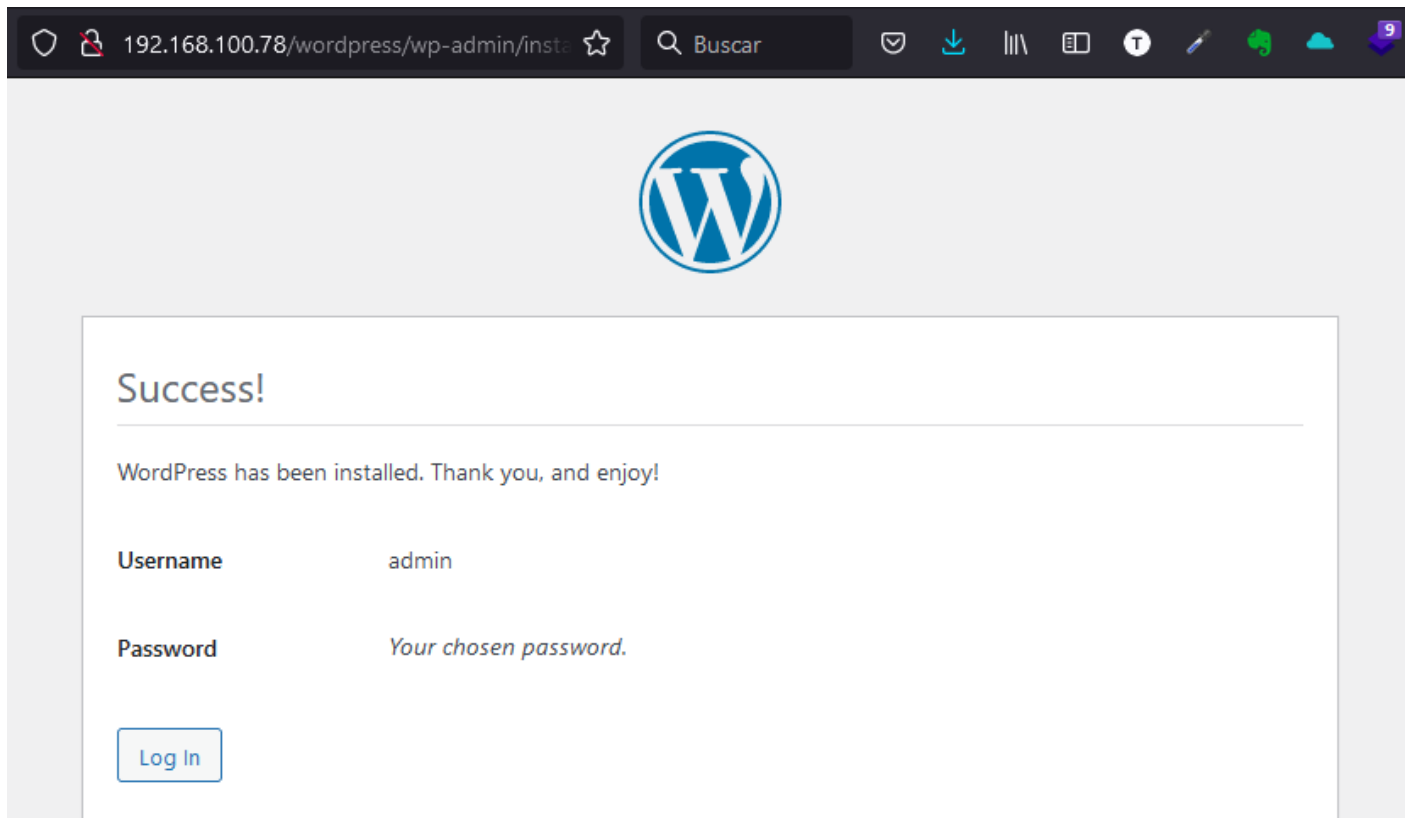
Search engine visibility

☐ Discourage search engines from indexing this site

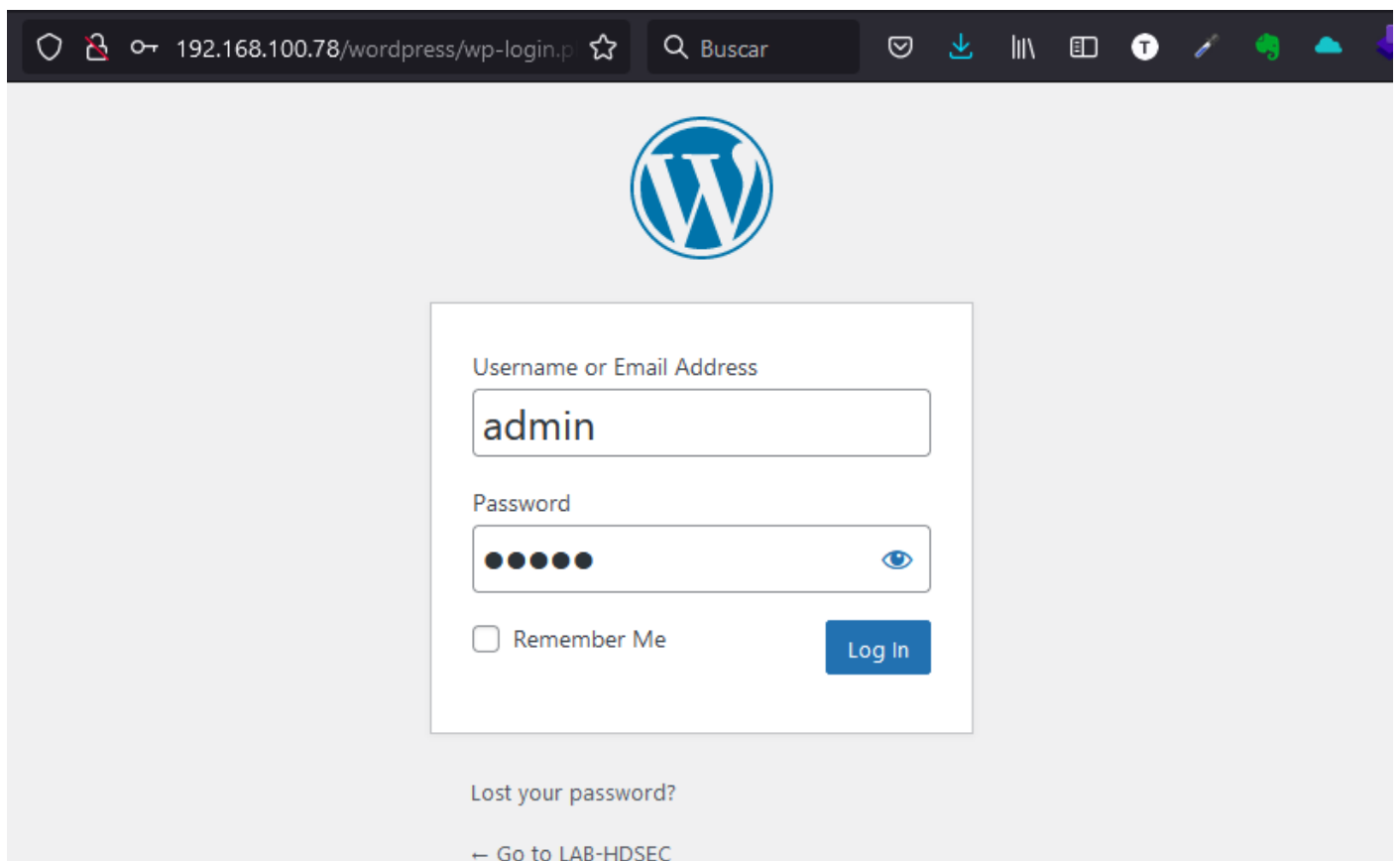
It is up to search engines to honor this request.

Install WordPress

Si todo el proceso se realizó de manera correcta deberá aparecer un mensaje de éxito como el siguiente. Clic en **Login**.

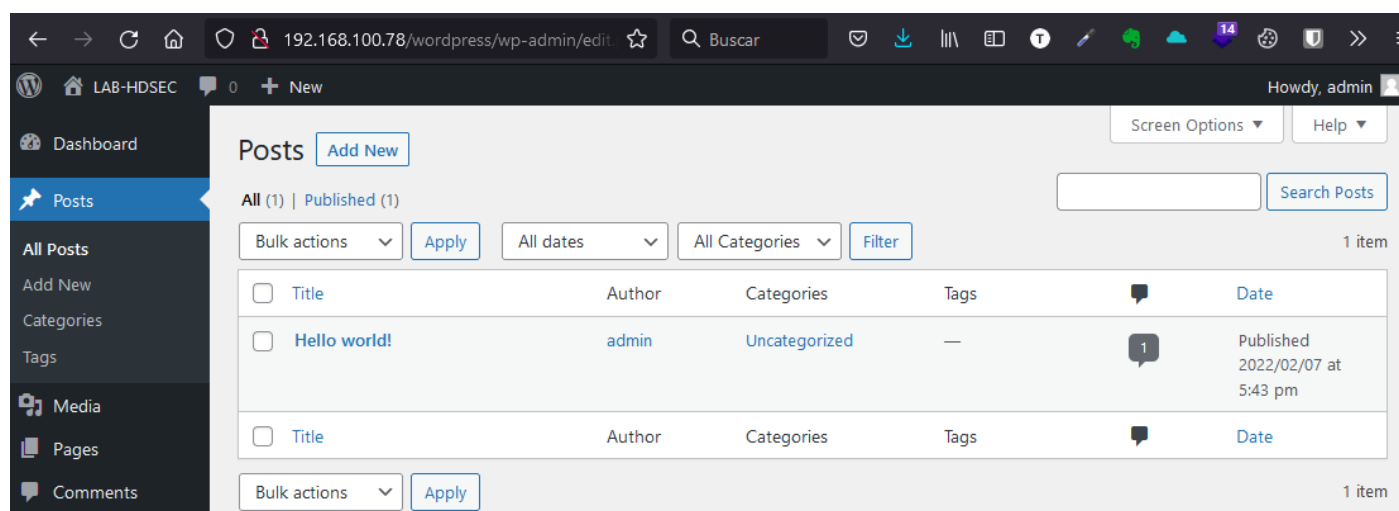


Ingresar las credenciales de administrador.

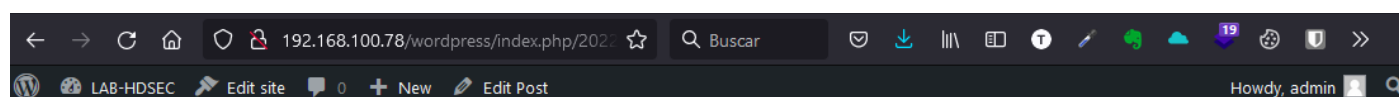


Verificación

Crear una entrada desde el panel de administración para comprobar el funcionamiento del sitio.



Si todo fue correcto deberá mostrarse la entrada creada.



LAB-HDSEC

Sample Page

LAB WORDPRESS

Server: Debian 11

Este es un laboratorio para realizar pruebas de herramientas de escaneo.

February 7, 2022 admin Uncategorized

Referencias

1. VirtualBox software de virtualización. <https://www.virtualbox.org/>
2. VMware software de virtualización. <https://www.vmware.com/products/workstation-pro.html>

3. Sistema operativo Debian. <https://www.debian.org/>
4. Sistema operativo Ubuntu. <https://ubuntu.com/>
5. Sitio del CMS WordPress. <https://wordpress.org/>



Este obra está bajo una [licencia de Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional](https://creativecommons.org/licenses/by-nc-nd/4.0/).