

IAW_U2_T1:Installing Wordpress

WORDPRESS

BY:Eduardo Gómez Paredes

Índice.

Ejercicio 1	pag 3
Ejercicio 2	pag 4
Ejercicio 3	pag 5
Ejercicio 4	pag 7
Ejercicio 5	pag 10
Ejercicio 6	pag 12
Ejercicio 7	pag 13

Versiones.

SO – Ubuntu 16,04

Apache 2,4,18

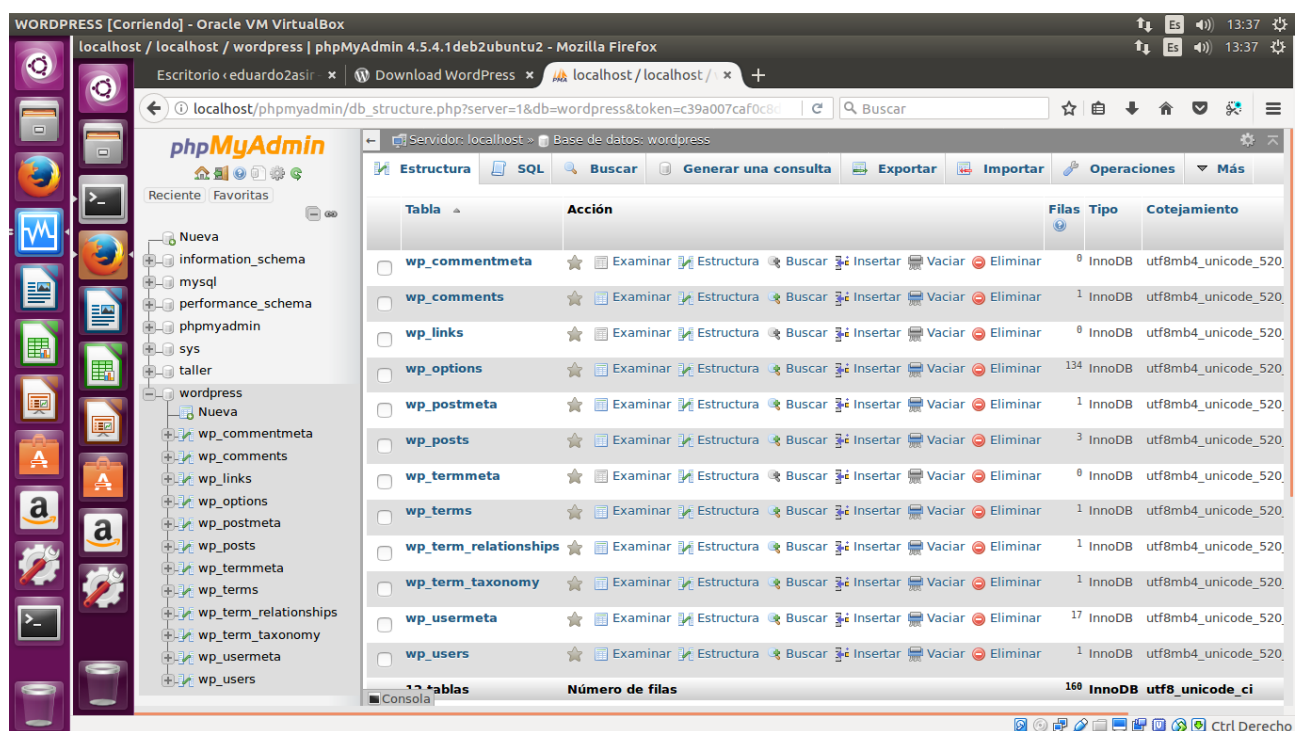
Mysql 14,14

Php 7.0.22

WordPress 4,8,2

Ejercicio 1

Once Wordpress is installed explains the meaning of each of the created tables (Exercise 1)



wp_commentmeta → Aquí se almacenan los comentarios.

wp_comments → Almacena los comentarios de wordpress.

wp_links → Almacena la información de los enlaces añadidos.

wp_options → Almacena los ajustes que se configuran en wordpress.

wp_postmeta → Almacena la información de las entradas (data).

wp_posts → Almacena las entradas, páginas y elementos de menú

wp_termmeta → Almacena la información de las categorías, enlaces o etiquetas (data)

wp_terms → Almacena las categorías de las entradas y los enlaces y las etiquetas de las entradas

wp_term_relationships → Almacena las asociaciones entre entradas y enlaces con categorías y /o etiquetas

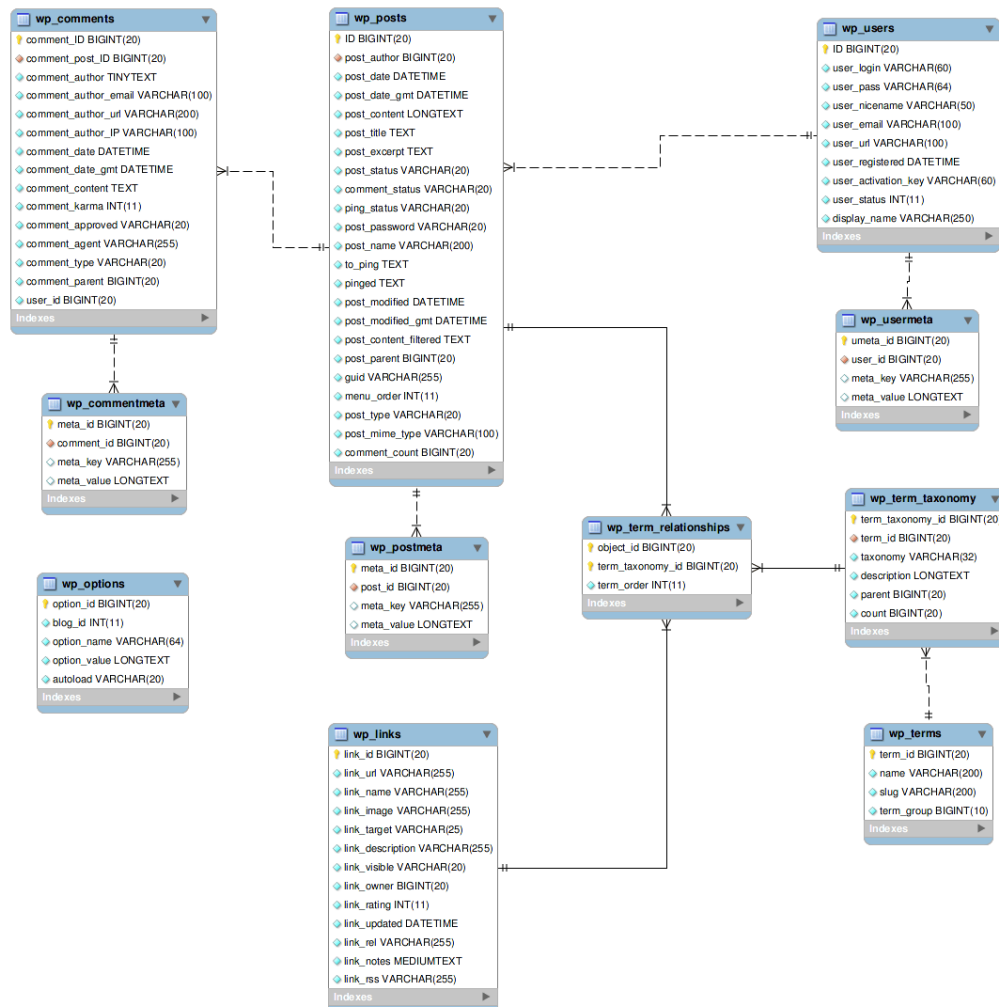
wp_term_taxonomy → Describe la taxonomía (categoría, enlace o etiqueta) de cada línea de la tabla wp_terms

wp_usermeta → Almacena la información de cada usuario (data)

wp_users → Almacena la lista de usuarios

Ejercicio 2

Create the database Diagram (Exercise 2)



Ejercicio 3

Find the main configuration file, open it and explain every option in it
(Exercise 3)

```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'wordpressedu');  
  
/** MySQL database password */  
define('DB_PASSWORD', '2asirtriana');  
  
/** MySQL hostname */  
define('DB_HOST', 'localhost');  
  
/** Database Charset to use in creating database tables. */  
define('DB_CHARSET', 'utf8mb4');  
  
/** The Database Collate type. Don't change this if in doubt. */  
define('DB_COLLATE', '');
```

DB_NAME: Nombre de la base de datos

DB_USER: Usuario del servidor base de datos

DB_PASSWORD: Contraseña del servidor base de datos

DB_HOST: Servidor de la base de datos

DB_CHARSET: Codificación de los datos de la base de datos

DB_COLLATE: Cotejamiento de la base de datos

```
*/
define('AUTH_KEY',          'xx|wtp+cF2M)e}JZ!syZ#J@TcFf#_DR4d3K-^$]4>^n8mVy>8_V$
define('SECURE_AUTH_KEY',  'S<okl0}/+Q8l(m/4v<N127k(0./!EBaxY2Kks(7J+@Th[m]l_Za$
define('LOGGED_IN_KEY',    'q]ln.aN[M]u!^S:Z:&J(HQJ /z1s@t$C%g{&;9|t2HC`Ys#p)+6$
define('NONCE_KEY',        '5Cx1^[+PCMRQ[v,Z,#}yvu_<AN_j76MuT5?= 269bt6L~6l}1BC$
define('AUTH_SALT',        '^Gh/*}4!No2[g|;4u])+%Fn<o`!6,D;^M;GDxo^VC,#18({95b}$
define('SECURE_AUTH_SALT', 'mhG#8^dZp?8SuGVq3l)BNr^h1/Y#HL(jsQiTE.o+s}OU!8Sgq*k$
define('LOGGED_IN_SALT',   'JW=G1$`VMAGwv zN$OW&WU=zXtR%8oL2#P,X5Cz~*-m^TAa~[II$
define('NONCE_SALT',       '{OMNz*GEM;u&%Bes6LdyI7y11)1q&2nq8M|J*y>!0wzp^L`[b s$
```

Las llaves de seguridad son unas constantes utilizadas para mejorar la encriptación de datos sensibles.

Las llaves de autenticación se usan como controles de seguridad, mientras que las llaves salts son usadas en las contraseñas.

```
/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the Codex.
 *
 * @link https://codex.wordpress.org/Debugging_in_WordPress
 */
define('WP_DEBUG', false);

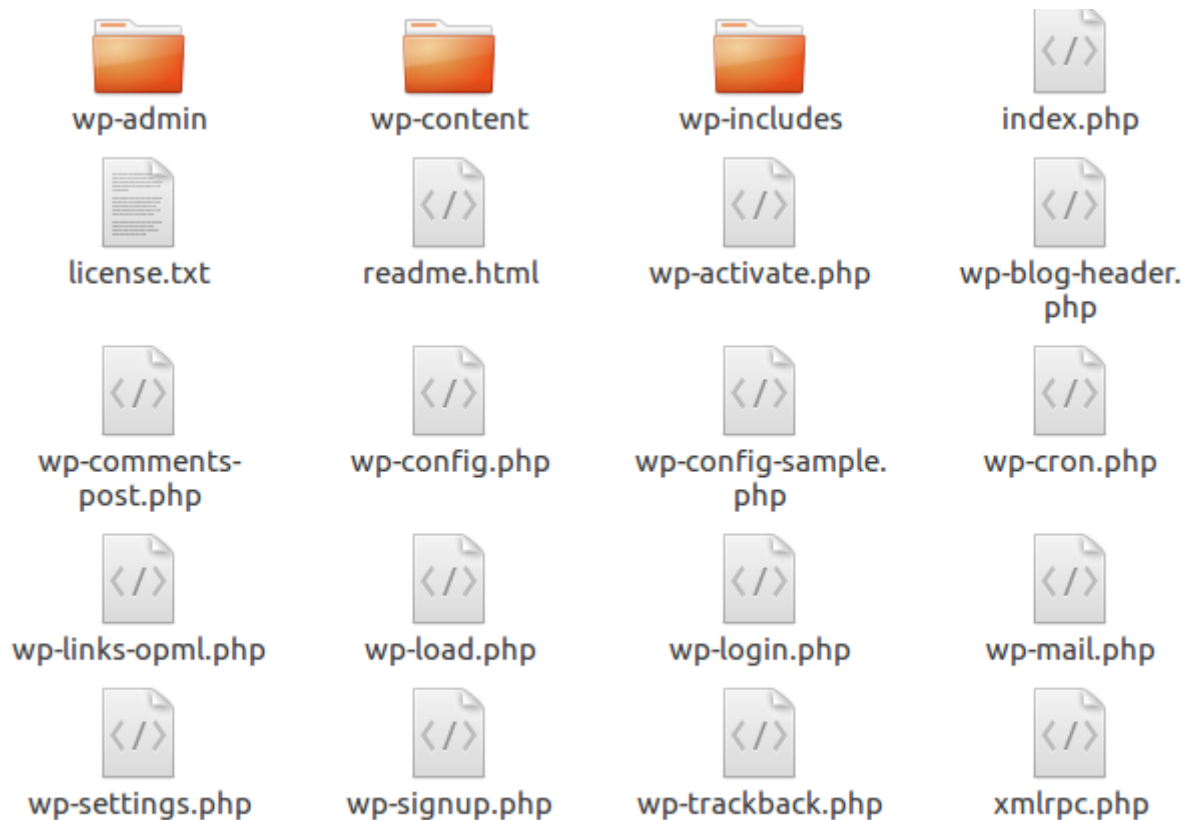
/* That's all, stop editing! Happy blogging. */
```

\$table_prefix = 'wp_'; → Prefijo para las tablas de instalación, si se cambia nos protegemos de ataques automatizados.

define('WP_DEBUG', false); → Wordpress no muestra por defecto los errores de PHP. Para que los muestre : **define('WP_DEBUG', true);**

Ejercicio 4

Explain the file structure and the meaning of the mains folders (up to level 2) (Exercise 4)



En la imagen se ve el directorio raíz, pero vamos a centrarnos en los más importantes para el usuario:

Carpeta WP-CONTENT: Es la carpeta donde se guarda todo el contenido en formato de archivos (no base de datos) que tiene una instalación de WordPress. Si se quiere hacer una copia de seguridad del contenido, se debe copiar esta carpeta, aparte de la BDD

Archivo INDEX.PHP: Archivo principal al que se accede y desde donde se cargan el resto de partes de WordPress.

Archivo WP-CONFIG-SAMPLE.PHP: Este archivo es la plantilla de lo que finalmente será el archivo WP-CONFIG.PHP tras la instalación del CMS.

Archivo WP-CONFIG.PHP : Archivo principal de configuración de WordPress, donde se guardan los datos de conexión con la base de datos de WordPress y algunos parámetros como la seguridad o el prefijo de las tablas

Eduardo Gómez Paredes

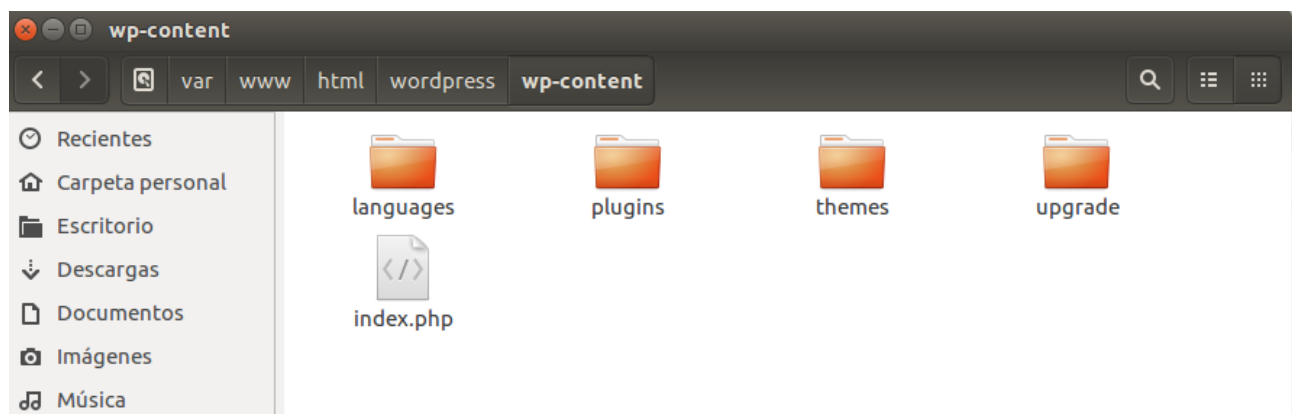
Archivo XMLRPC.PHP: Ofrece la comunicación mediante el protocolo XMLRPC.PHP. Importante su seguridad y protección por los ataques que sufre wordpress por este archivo

Carpeta WP-ADMIN: Carpeta donde se guardan los archivos del back-end de WordPress.

Carpeta WP-INCLUDES: Es una carpeta de archivos que necesita WordPress para funcionar, su API y las librerías principales.

Archivo WP-LOGIN.PHP: Es un archivo bastante importante, ya que es el que se encarga de gestionar el login de los usuarios, tanto usuarios normales como administradores.

Carpetas y archivos dentro de wp-content.



Carpeta languages: Aquí se guardan los archivos de traducción tanto de temas y plugins como del propio WordPress.

Carpeta plugins: Aquí se guardan los plugins de la instalación, tanto los plugins activos como los que no están activos.

Carpeta themes: Aquí se guardan los temas, tanto el tema principal activo como los temas instalados

Archivo index: Índice de la estructura de wordpress

Carpetas wp-admin:



CSS → CSS del sitio

Images → Imágenes del wordpress

Includes → Archivos .php que realizan funciones determinadas. Se llaman desde otros .php

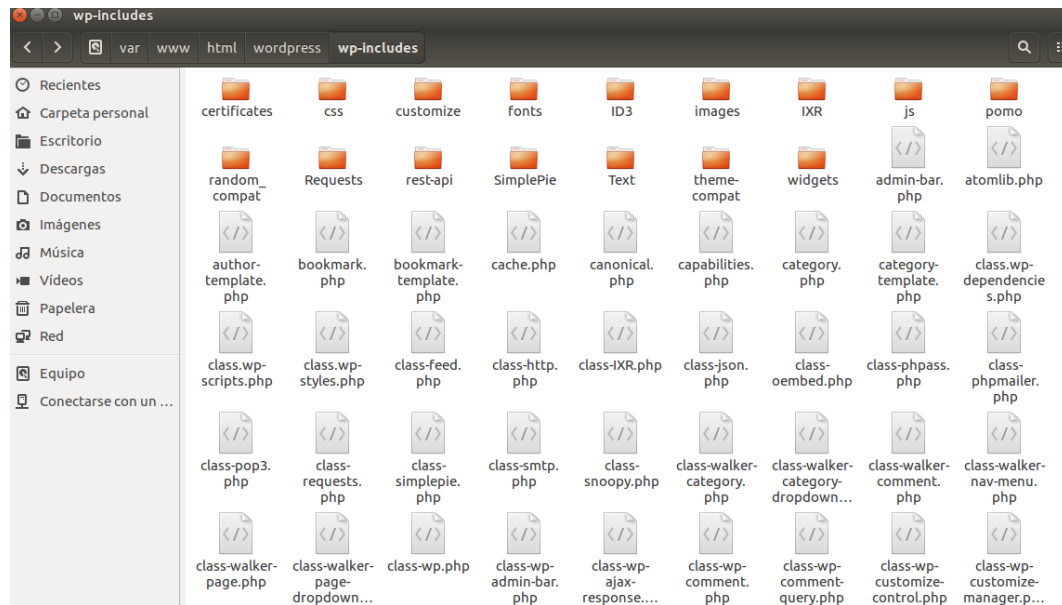
js → Incluye el javascript

Maint → Un script de mantenimiento

Network → Información acerca de la página

User → Información del usuario

Carpeta wp-includes:



Certificates → Certificados del sitio

Widgets → widgets de la página

rest-api → Apis para que funcione la web

fonts → Fuentes

Customize → Personalización

theme-compat → Librerías varias

random_compat → Librerías varias

pomo → Librerías varias

css → CSS del sitio

request → Librerías varias

js → Javascript

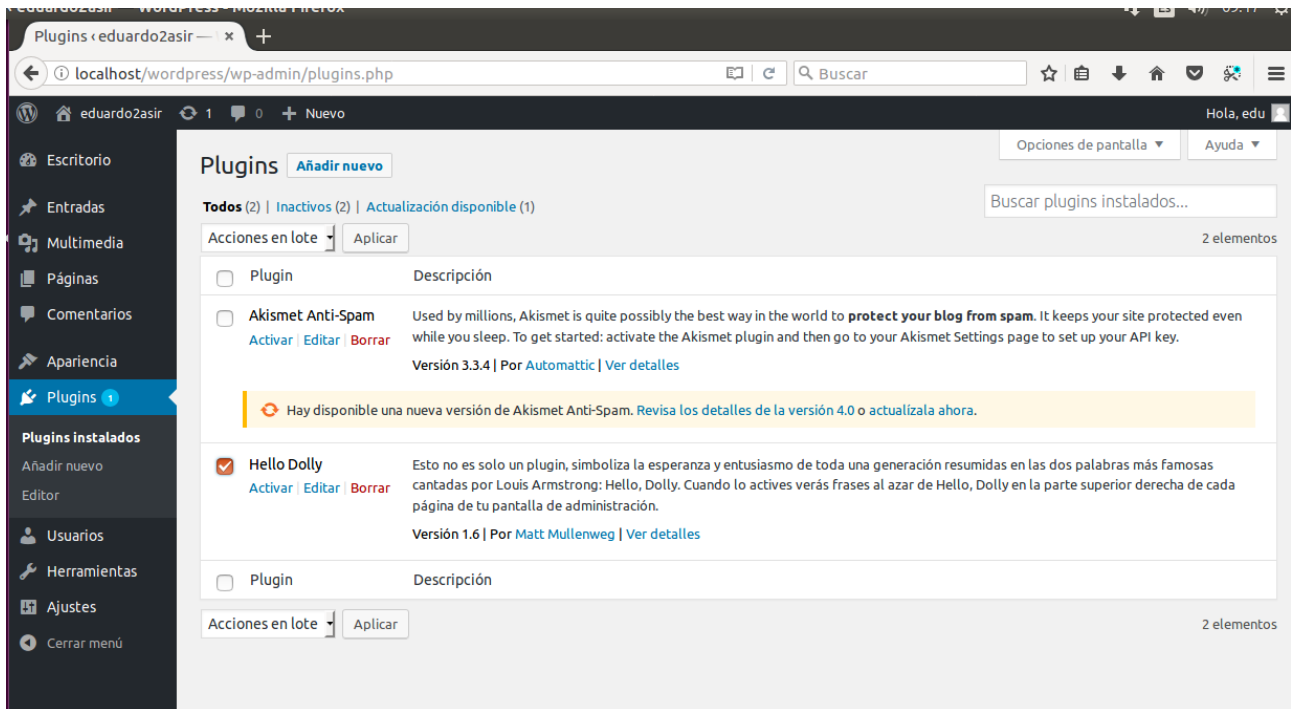
ID3 → Librerías varias

Simplepie → Librerías varias

Text → Librerías varias

Ejercicio 5

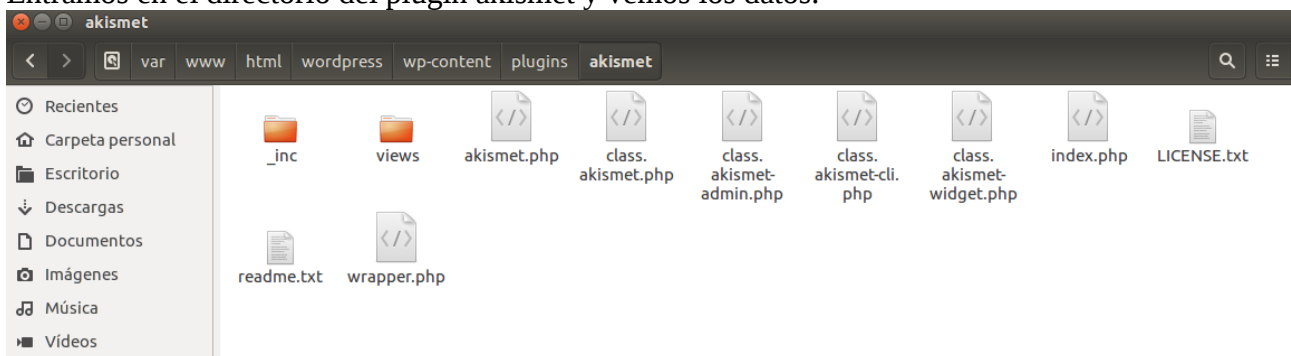
Describe the installation process of a new plugin (with Snapshots) and explain where are the recently created files (Exercise 5)



Hemos elegido instalar Akismet.

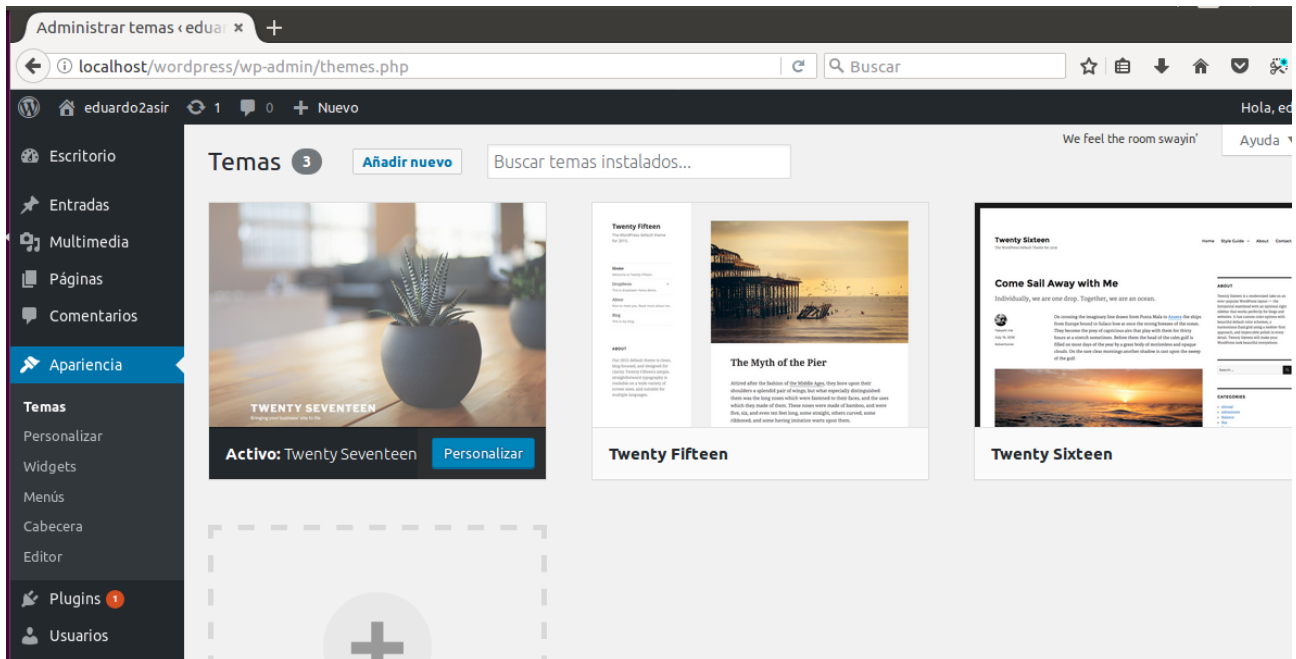
Los archivos de cualquier plugin se encuentra en /var/www/html/wordpress/wp-content/plugins

Entramos en el directorio del plugin akismet y vemos los datos.



Ejercicio 6

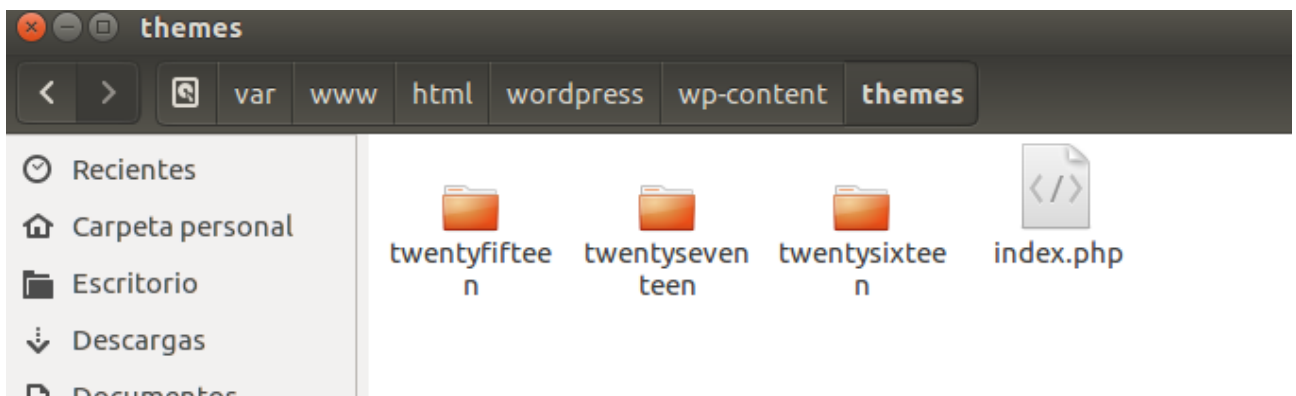
Describe the installation process of a new theme (with Snapshots) and explain where are the recently created files (Exercise 6)



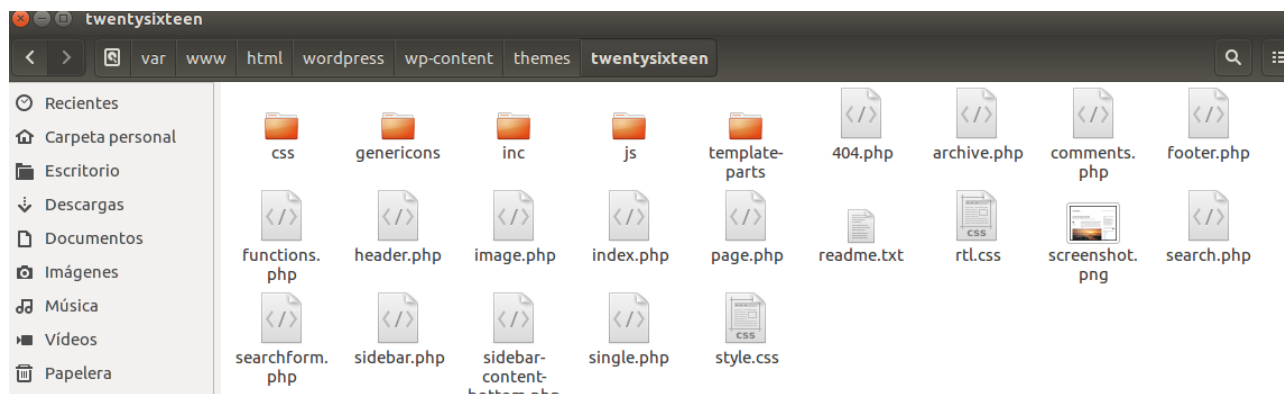
Desde Apariencia → Temas podemos ver los distintos temas entre los que podemos escoger o añadir.

Nosotros elegiremos Twenty Sixteen. Le daremos al boton Activar.

Los archivos sobre los temas se encuentran en: /var/www/html/wordpress/wp-content/themes



Entraremos en el Twenty Sixteen y veremos los archivos.



Ejercicio 7

Look for 10 things to secure Wordpress after installation (according to your versions) (Exercise 7)

Contraseñas robustas → Contraseña y usuarios complejos, tanto como para la base de datos como para el wordpress.

Herramientas de seguridad → Herramientas como Wordreference Security son un extra muy bueno de seguridad.

Colocar una CDN por delante → Una CDN, del inglés Content Delivery Network, o red de entrega de contenidos, es una red de servidores, estratégicamente situados en distintas partes del mundo. Así se previenen ataques de fuerza bruta y se enmascara la dirección real de nuestra máquina.

Eliminar el archivo readme.html de la carpeta raíz → Hay que eliminar este archivo que trae la versión de wordpress ya que aportas información que puede volverse en tu contra.

Eliminar plugins y temas que no utilices → Un tema o plugin nuevo es una puerta nueva que se abre, por lo que hay más que supervisar. Solo instalar plugins o temas de confianza.

Eliminar cuenta “admin” → Es el usuario por defecto y el que tiene todos los poderes, lo que lo hace muy apetecible para ataques de fuerza bruta: Sabiendo el username prueban todas las contraseñas posibles pueden entrar.

Utilizar un nick en lugar de user → Las cuentas nuevas, utilizan por defecto el valor username. Este es el valor que WordPress muestra como autor al escribir un post. Al igual que pasa con la cuenta admin, a partir de un username conocido obtener contraseñas a base de fuerza bruta no es complicado.

Cambiar la URL de acceso a wp-admin → Se debe cambiar al ser la misma en todas las instalaciones de wordpress, por lo que mediante Protect Wp-Admin o modificando el archivo .htaccess.

Cambiar lo siguiente: RewriteRule ^panel-admin\$ http://tusitio.com/wp-admin.php [NC,L]

Eduardo Gómez Paredes

Proteger wp-config.php → Contiene detalles de configuración de la base de tu sitio, y claves de seguridad de WordPress e información de conexión de base de datos. Esta información, por supuesto, es sensible y cualquier persona que acceda a ella puede acabar afectando a tu sitio. La mejor forma de proteger este archivo es agregando el siguiente fragmento de código en el archivo .htaccess:

```
<files wp-config.php>  
order allow,deny  
deny from all  
</files>
```

Utilizar SSL → Utilizar y forzar SSL como protocolo de acceso a nuestros sitio, no solo para la administración, también para el acceso de los lectores.