GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-461)

SEGURIDAD EN DRUPAL

JUNIO 2016

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2016.06.23 20:20:14 +02'00'

NIPO: 002-16-017-3

Fecha de Edición: junio 2016

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

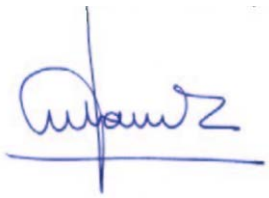
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Junio 2016



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

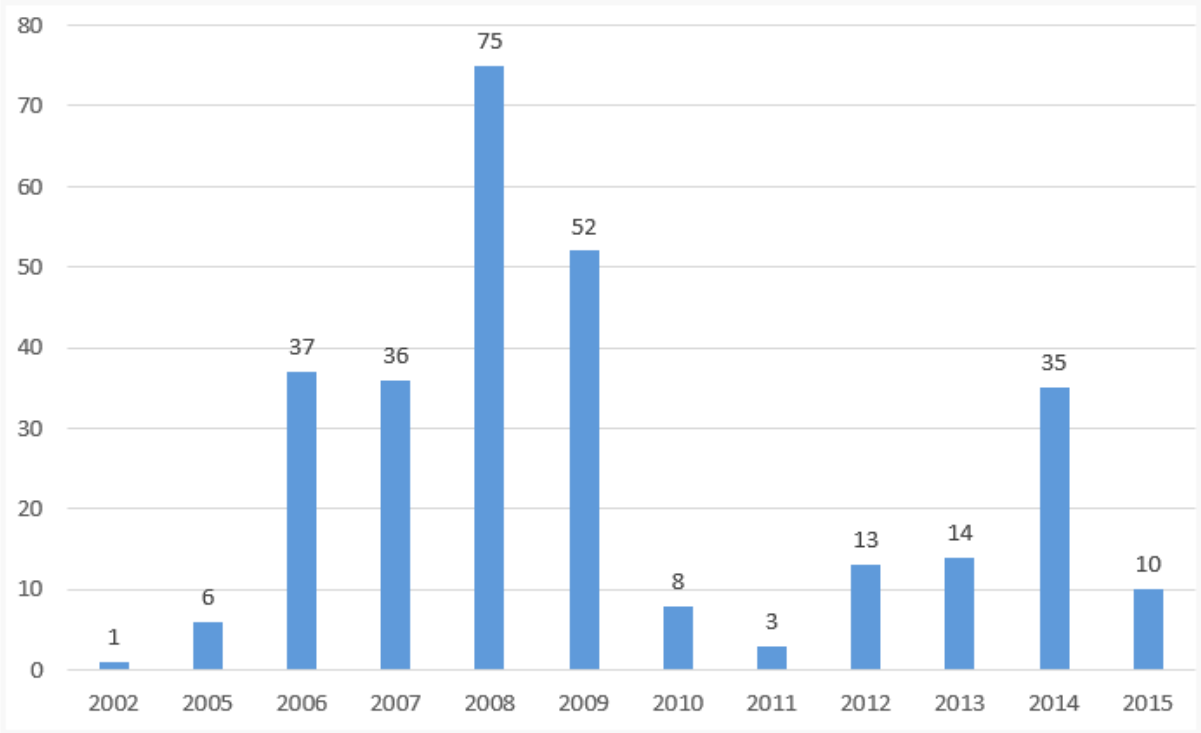
1. Drupal[1] es un CMS (por sus siglas en inglés, *Content Management System*) libre, modular multipropósito y muy configurable que permite publicar artículos, imágenes, archivos y otras cosas u otros archivos y servicios añadidos como foros, encuestas, votaciones, blogs y administración de usuarios y permisos. Drupal es un sistema dinámico: en lugar de almacenar sus contenidos en archivos estáticos en el sistema de ficheros del servidor de forma fija, el contenido textual de las páginas y otras configuraciones son almacenados en una base de datos y se editan utilizando un entorno Web.
2. El diseño de Drupal es especialmente idóneo para construir y gestionar comunidades en Internet, también destaca por su flexibilidad y adaptabilidad, así como la gran cantidad de módulos adicionales disponibles, hace que sea adecuado para realizar muchos tipos diferentes de sitio web.
3. Existen tres tipos de módulos de Drupal, llamadas las "3 C":
    - **Core** (núcleo): son los módulos provistos por Drupal al instalarse, algunos de ellos fueron contribuciones de la comunidad de Drupal que se incorporaron.
    - **Contributed** (contribuciones): son los módulos que son compartidos para la comunidad de Drupal, están bajo GNU de Licencia Pública (GPL).
    - **Custom** (personalizados): son los módulos creados por el desarrollador del sitio.4
4. Entre los más importantes que no están incluidos en la distribución oficial, se pueden destacar:
    - Views
    - Content Construction Kit (CCK)
    - Token
    - Pathauto
    - FileField
    - Administration menu
    - ImageField
    - ImageAPI
    - ImageCache
    - WYSIWYG

1.1. HISTÓRICO DE VULNERABILIDADES[2]

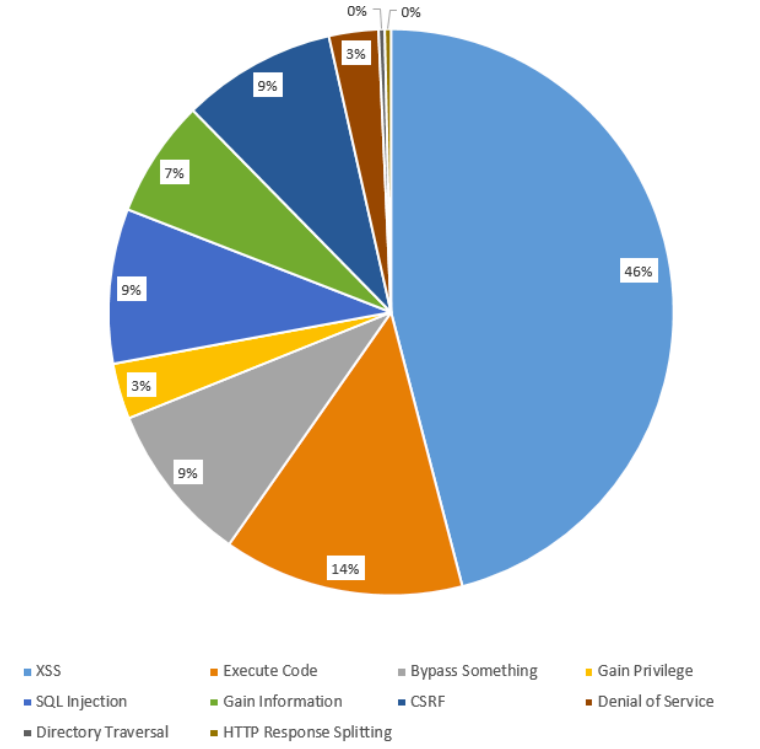
5. De acuerdo a la página CVE Details, se han reportado 290 vulnerabilidades en el periodo de tiempo comprendido entre 2002 y 2015:

[1] **DRUPAL:** https://es.wikipedia.org/wiki/Drupal

[2] **COMPLETE GUIDE ON DRUPAL SECURITY:** https://www.keycdn.com/blog/drupal-security



6. Cabe destacar que el 46% de las vulnerabilidades públicas conocidas corresponden a XSS (Cross-Site Scripting):



7. Por este motivo, utilizaremos las mejores prácticas que se muestran a lo largo de esta guía para mantener el CMS lo más seguro posible y mitigar posibles ataques de fuentes externas.

1.2. VERSIONES MÁS IMPORTANTES

8. Drupal fue originalmente escrito por Dries Buytaert y es el software usado para impulsar por ejemplo a los sitios web Debian Planet, Spread Firefox, Kernel Trap y White House.

9. A continuación mostramos las versiones más relevantes que han sido publicadas:

Versión	Fecha de lanzamiento
1.0	15 de enero de 2001
2.0	15 de marzo de 2001
3.0	15 de septiembre de 2001
4.0	16 de junio de 2002
4.5	16 de octubre de 2004
4.6	16 de abril de 2005
4.7	16 de mayo de 2006
5.0	15 de junio de 2007
6.0	13 de febrero de 2008
7.0	5 de junio de 2011
7.32	15 de octubre de 2014
7.33	7 de noviembre de 2014

7.34	19 de noviembre de 2014
7.38	17 de junio de 2015
7.39	19 de agosto de 2015
7.40	14 de octubre de 2015
7.41	21 de octubre de 2015

1.3. CONCEPTOS GENERALES DE DRUPAL

10. Módulo: el módulo (module) es un software que extiende las funcionalidades y/o características de Drupal. Viene con módulos precargados según la versión, a los cuales se les puede añadir los que se necesite según la funcionalidad que tenga el sitio.
11. Usuario, Permiso, Rol: cada visitante del sitio que tenga ingreso al mismo o no (como visitante anónimo) es considerado un Usuario para Drupal. Se pueden definir los tipos de usuario desde el núcleo de Drupal en la parte de Perfil (profile) y los campos asociados a cada usuario. Los Usuarios anónimos tendrán el ID cero (0), mientras que los que se encuentran registrados el ID uno (1). A estos usuarios se les asignará los Permisos por medio de Roles, pudiendo crear diferentes tipos de roles además de los preestablecidos por defecto, para luego agregarle o quitarle permisos según la necesidad del sitio.
12. Nodo: el nodo (node) es un término genérico para cada pieza de contenido del sitio. Algunos ejemplos de nodos pueden ser: páginas en libros, temas de discusión en foros, entradas en blogs, nuevos artículos, etc. Cada nodo será un tipo de contenido que tendrá un ID, un título, una fecha de creación, un autor, un cuerpo o body y otras propiedades, también según qué otros módulos se encuentre usando agregará más propiedades a cada nodo.
13. Comentario: el comentario (comment) es otro tipo de contenido dentro de Drupal, ya que cada comentario es una pequeña pieza de contenido que un usuario envía a un nodo específico, por ejemplo, cada pieza de comentario dentro de una discusión en el foro.
14. Taxonomía: la taxonomía (taxonomy) es el sistema mediante el cual Drupal clasifica el contenido y es uno de los módulos del núcleo de Drupal. Se pueden definir los vocabularios propios como grupos de términos de taxonomía. Cada tipo de vocabulario puede ser agregado como uno o más tipos de contenido y por ello, los nodos en el sitio pueden ser clasificados según agrupaciones en categorías, etiquetas o como cualquier cosa que se elija.

15. Base de datos: la información de Drupal depende de la base de datos. Cada información se encuentra en una tabla dentro de dicha base de datos. Por ejemplo, la información básica de los nodos se encuentra en la tabla de Node.
16. Path: cuando se visita un sitio con Drupal, una parte de la dirección de URL es conocida como path. Es la información enviada por el navegador a la base de datos. Si se está viendo la página http://drupal.org/node/16785 el path será "node/16785". Por defecto, luego de la instalación del sitio se proseguirá con "?q=". Pero con el sistema de URL limpias que se puede activar desde la administración se puede quitar ese atributo.
17. Plantilla: la plantilla (theme) controlará cómo se visualizará el sitio, el diseño y los colores. Consiste en uno o más archivos en PHP que definen la salida HTML, con uno o más archivos en CSS definiendo las fuentes, colores y otros estilos.
18. Región, Bloque, Menú: Drupal se encuentra dividido en Regiones (regions) que pueden incluir la cabecera, el pie, las barras laterales, la sección principal de contenido. Los Bloques (blocks) es la información que se visualiza en las diferentes regiones, pudiendo tomar la forma de menús (como el menú de navegación) o visualizaciones de módulos (como los contenidos más vistos del foro) o información estática o dinámica que fue creada por un usuario (como eventos). Existen tres menús estándar en Drupal: enlaces primarios, enlaces secundarios y menú de navegación. Los primarios y secundarios son construidos a criterio de los administradores y mostrados automáticamente. También se pueden crear menús personalizados mediante la creación de bloques.

2. INSTALACIÓN Y ACTUALIZACIÓN

2.1. ANTES DE COMENZAR: REQUERIMIENTOS

19. Antes de comenzar, existen una serie de requerimientos mínimos a cumplir para poder finalizar la instalación de forma exitosa:

    1. Drupal 8:

       MySQL 5.5.3/MariaDB 5.5.20/Percona Server 5.5.8 or superior, con PDO y motor de almacenamiento primario compatible con InnoDB

       PHP 5.5.9 o superior

    2. Drupal 7:

       MySQL 5.0.15/MariaDB 5.1.44/Percona Server 5.1.70 o superior, con PDO

       PHP 5.2.5 o superior, aunque se recomienda 5.4

    3. Drupal 6:

       MySQL 4.1.1 o superior

       PHP 5.x o superior, aunque se recomienda 5.2.5

20. Además, será necesario instalar un servidor Web que gestione las peticiones realizadas por parte del cliente. Durante el desarrollo de esta guía utilizaremos como ejemplo Apache (que deberá ser asegurada siguiendo la guía CCN-STIC 671 “Configuración segura de servidores web Apache”), aunque puede utilizarse cualquier otro que soporte PHP y MySQL, como podría ser Nginx.

COMPROBAR LA VERSIÓN DE PHP INSTALADA EN EL SISTEMA

En el caso de que tener acceso por línea de consola al sistema, ejecutaremos el siguiente comando:

```
root@guiaDrupal:~# php -v
PHP 5.5.9-1ubuntu4.16 (cli) (built: Apr 20 2016 14:31:27)
Copyright (c) 1997-2014 The PHP Group
Zend Engine v2.5.0, Copyright (c) 1998-2014 Zend Technologies
    with Zend OPcache v7.0.3, Copyright (c) 1999-2014, by Zend Technologies
    with Suhosin v0.9.37.1, Copyright (c) 2007-2014, by SektionEins GmbH
```

En caso contrario, crearemos un fichero, al que llamaremos como ejemplo info_php.php, y lo subiremos a nuestra estructura web. El código que debe contener este fichero será:

```
root@guiaDrupal:/var/www/html# cat info_php.php
<?php phpinfo(); ?>
root@guiaDrupal:/var/www/html#
```

Una vez creado, tan sólo deberemos acceder desde nuestro navegador a http://nuestroservidor/ruta/info_php.php, donde deberemos ver algo como la siguiente captura:

PHP Version 5.5.9-1ubuntu4.16

System	Linux guiaDrupal 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:16:20 UTC 2015 x86_64
Build Date	Apr 20 2016 14:31:04
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-suhosin.ini

En la parte superior nos mostrará la versión de PHP que está instalada y corriendo en el sistema, en nuestro caso 5.5.9-1. En caso de no estar ejecutando PHP 5, será necesario contactar con los administradores para solicitar su instalación.

Una vez realizada esta prueba, el fichero que hemos creado deberá ser eliminado, ya que puede proporcionar información adicional y necesaria para que un atacante realice una intrusión sobre nuestro sistema.

21. Además de estos requerimientos mínimos, utilizaremos una serie de herramientas de apoyo para realizar la configuración del servicio:

    - Acceso al servidor web (vía consola, SSH o FTP)
    - Un editor de texto
    - Un cliente FTP/SFTP
    - Un navegador Web (en nuestro caso utilizaremos la última versión de Firefox 46.01)

2.2. INSTALACIÓN DE REQUERIMIENTOS

2.2.1. INSTALACIÓN DE MYSQL

22. Antes de comenzar, será necesario descargar la última versión de MySQL disponible desde la web oficial: http://dev.mysql.com/downloads/mysql/. En nuestro caso, descargaremos la última reléase disponible en el momento de la publicación de esta guía: mysql-5.7.12.tar.gz.

23. La secuencia de comandos necesaria para la instalación será la siguiente, y será realizado desde la cuenta de 'root' o mediante el uso de una cuenta con permisos de administración del sistema:

 # Descargamos MySQL
$ wget https://dev.mysql.com/get/Downloads/MySQL-5.6/mysql-5.7.12.tar.gz
 # Descomprimimos el paquete
$ tar xzvf mysql-5.7.12.tar.gz
$ cd mysql-5.7.12/
 # Comprobación de dependencias
~/mysql-5.7.12$ BUILD/autorun.sh
 # Compilamos MySQL, generando los ejecutables
~/mysql-5.7.12$ CFLAGS="-O3" CXX=gcc CXXFLAGS="-O3 -felide-constructors -fno-exceptions -fno-rtti"
./configure --prefix=/usr/local/mysql --enable-assembler --with-mysqld-ldflags=-all-static

```
[root@guiaDrupal:~/mysql-5.7.12# CFLAGS="-O3" CXX=gcc CXXFLAGS="-O3 -felide-constructors -fno-exceptions -fno-rtt
i" ./configure --prefix=/usr/local/mysql --enable-assembler --with-mysqld-ldflags=-all-static
configure.pl : switching CXX compiler from gcc to g++
configure.pl : stripping off -fno-exceptions CXXFLAGS=-O3 -felide-constructors  -fno-rtti
configure.pl : ignoring with-mysqld-ldflags=-all-static
configure.pl : calling cmake /root/mysql-5.7.12  -DCMAKE_INSTALL_PREFIX=/usr/local/mysql -DENABLE_ASSEMBLER=1
-- Running cmake version 2.8.12.2
-- Found Git: /usr/bin/git (found version "1.9.1")
-- Configuring with MAX_INDEXES = 64U
-- Looking for SHM_HUGETLB
-- Looking for SHM_HUGETLB - found
-- Looking for sys/types.h
-- Looking for sys/types.h - found
-- Looking for stdint.h
-- Looking for stdint.h - found
-- Looking for stddef.h
-- Looking for stddef.h - found
-- Check size of void *
-- Check size of void * - done
-- SIZEOF_VOIDP 8
-- MySQL 5.7.12
```

 # Instalamos los paquetes generados
~/mysql-5.7.12$ make install
 # Añadimos el grupo y usuario 'mysql'
~/mysql-5.7.12$ groupadd mysql
~/mysql-5.7.12$ useradd -g mysql mysql
~/mysql-5.7.12$ cd /usr/local/mysql
/usr/local/mysql$ chown -R mysql .
/usr/local/mysql$ chgrp -R mysql .
/usr/local/mysql$ scripts/mysql_install_db --user=mysql
/usr/local/mysql$ chown -R root .
/usr/local/mysql$ chgrp -R mysql .
/usr/local/mysql$ chown -R mysql data/
/usr/local/mysql$ chmod -R go-rwx data/
 # Generamos un fichero de configuración desde la plantilla
/usr/local/mysql$ cp support-files/my-default.cnf /etc/my.cnf
 # Cambiamos la contraseña de acceso del usuario 'root'

/usr/local/mysql$ bin/mysqladmin -u root password 'new-password'

24. Una vez que la instalación ha finalizado, arrancaremos el servicio utilizando el siguiente comando:

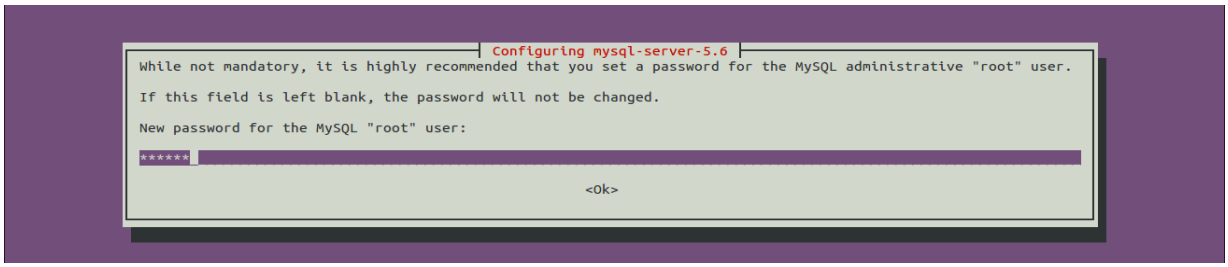
    $ bin/mysqld_safe --user=mysql &

25. Desde este momento dispondremos de MySQL en nuestro sistema, dentro de la ruta '/usr/local/mysql'.

26. Como alternativa, en sistemas Debian/Ubuntu, podremos utilizar el gestor de paquetes propio para realizar la instalación, sin compilar las fuentes. Para ello, ejecutaremos los siguientes comandos:

    $ sudo apt-get install mysql-server php5-mysql libapache2-mod-auth-mysql

27. Introduciremos la contraseña de 'root' para poder acceder posteriormente a MySQL:



28. Al finalizar el proceso, tendremos instalada la última version de MySQL así como los módulos necesarios para que poder utilizarlo bajo PHP.

2.2.2. INSTALACIÓN DE PHP

29. Antes de comenzar, será necesario descargar la última versión de PHP disponible desde la web oficial: http://php.net/downloads.php. En nuestro caso, descargaremos la última release disponible en el momento de la publicación de esta guía: php-5.6.21.tar.gz.

30. La secuencia de comandos necesaria para la instalación será la siguiente, y será realizado desde la cuenta de 'root' o con permisos de administración del sistema:

```
root@guiaDrupal:/tmp# wget http://es1.php.net/get/php-5.6.21.tar.gz/from/this/mirror
--2016-05-12 16:15:10--  http://es1.php.net/get/php-5.6.21.tar.gz/from/this/mirror
Resolviendo es1.php.net (es1.php.net)... 80.64.47.13
Conectando con es1.php.net (es1.php.net)[80.64.47.13]:80... conectado.
Petición HTTP enviada, esperando respuesta... 302 Found
Ubicación: http://es1.php.net/distributions/php-5.6.21.tar.gz [siguiente]
--2016-05-12 16:15:10--  http://es1.php.net/distributions/php-5.6.21.tar.gz
Reutilizando la conexión con es1.php.net:80.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 18415513 (18M) [application/x-gzip]
Grabando a: "mirror"

100%[=============================================================================================================
=============================================================================>] 18.415.513  1,
11MB/s   en 20s

2016-05-12 16:15:29 (921 KB/s) - "mirror" guardado [18415513/18415513]

root@guiaDrupal:/tmp# mv mirror php-5.6.21.tar.gz
root@guiaDrupal:/tmp# tar zxf php-5.6.21.tar.gz
root@guiaDrupal:/tmp# cd php-5.6.21/
root@guiaDrupal:/tmp/php-5.6.21#
```

 # Configuramos la instalacion
$ tar zxvf php-5.6.21.tar.gz
$ cd php-5.6.21/

 # Especificamos la ruta de instalacion a /usr/local/mysql
$ ./configure --with-mysql=/usr/local/mysql

```
[root@guiaDrupal:/tmp/php-5.6.21# ./configure --with-mysql=/usr/local/mysql ]
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for a sed that does not truncate output... /bin/sed
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu
checking for cc... cc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether cc accepts -g... yes
checking for cc option to accept ISO C89... none needed
checking how to run the C preprocessor... cc -E
checking for icc... no
checking for suncc... no
checking whether cc understands -c and -o together... yes
checking how to run the C preprocessor... cc -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
```

$ make
$ make install
 # Generamos un fichero de configuración desde la plantilla
$ cp php.ini-dist /usr/local/lib/php.ini

NOTA

Existen gran cantidad de opciones de configuración para PHP cuando se compila en entornos Unix-like. La mayoría hacen referencia a ubicaciones concretas o configuraciones que no han sido incluidas en el ejemplo.

Para una lista completa de estas opciones, accederemos a http://php.net/manual/en/configure.about.php y seleccionaremos las más adecuadas a nuestro entorno.

31. Finalmente, nos aseguraremos que desde el archivo de configuración se carga la extensión de MySQL, buscando el siguiente texto (o añadiéndolo a la configuración en caso contrario):

    extension=mysql.so

32. De la misma forma que con MySQL, en sistemas Debian/Ubuntu podremos utilizar el gestor de paquetes propio para la descarga e instalación de PHP, utilizando los siguientes comandos:

    $ apt-get install php5 php5-mysql libapache2-mod-php5

33. Un vez finalizada la instalación, tendremos correctamente configurado PHP para trabajar con Apache, así como MySQL. Podemos comprobar que la instalación se ha realizado correctamente, generando un fichero de información de PHP, llamado "phpinfo.php", en la ruta por defecto de Apache (/var/www/html) con el siguiente contenido:

    <?php
    phpinfo();
    ?>

34. Utilizando el navegador accederemos la dirección IP de nuestro servidor, de la forma http://IP/phpinfo.php. Si obtenemos la pantalla de información de debugging de PHP, nuestro servidor estará listo para continuar el proceso de instalación.

2.2.3. ACTIVACIÓN DE MOD_REWRITE

35. Para activar el módulo "mod_rewrite" en Apache, será necesario ejecutar lo siguiente:

    $ sudo a2enmod rewrite

36. Después, revisaremos la configuración por defecto de nuestro Apache (en nuestro caso "etc/apache2/sites-enabled/000-default") y especificaremos el valor "All" para la directiva "AllOverride":

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

<Directory /var/www/html/drupal-8.0.4>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                allow from all
</Directory>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

37. Una vez realizado esto, reiniciaremos el servicio:

    $ apache2ctl restart

2.3. INSTALACIÓN DE DRUPAL

2.3.1. INSTALACIÓN DESDE EL ARCHIVO OFICIAL

38. Si disponemos acceso a la línea de consola de nuestro servidor, podremos descargar la última versión de Drupal utilizando wget (o Lynx o cualquier navegador de texto), que en el momento de la escritura de esta guía es la 8.0.4.

39. Ahora deberemos descomprimir el paquete en la ruta definida por nuestro servidor web, utilizando el siguiente comando:

```
root@guiaDrupal:/var/www/html# wget https://ftp.drupal.org/files/projects/drupal-8.0.4.tar.gz
--2016-05-12 16:22:55--  https://ftp.drupal.org/files/projects/drupal-8.0.4.tar.gz
Resolviendo ftp.drupal.org (ftp.drupal.org)... 23.235.43.68
Conectando con ftp.drupal.org (ftp.drupal.org)[23.235.43.68]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 11746172 (11M) [application/octet-stream]
Grabando a: “drupal-8.0.4.tar.gz”

100%[=====================================================================>] 11.746.172  15,3MB/s   en 0,7s

2016-05-12 16:22:55 (15,3 MB/s) - “drupal-8.0.4.tar.gz” guardado [11746172/11746172]

root@guiaDrupal:/var/www/html# tar xzf drupal-8.0.4.tar.gz
root@guiaDrupal:/var/www/html# mv drupal-8.0.4 drupal
root@guiaDrupal:/var/www/html# rm drupal-8.0.4.tar.gz
root@guiaDrupal:/var/www/html# ls
drupal
root@guiaDrupal:/var/www/html#
```

40. Drupal se descomprimirá en un directorio nuevo, llamado "drupal-8.0.4", dentro del mismo directorio raíz donde hemos descargado el fichero, que renombraremos a "drupal"

DIRECTORIO .GIT EN SERVIDORES PÚBLICOS
No debe mantenerse expuesta la versión de Drupal en instalaciones de producción, ya que facilitan información a posibles atacantes acerca de la versión que está siendo utilizada, facilitando así la búsqueda de vulnerabilidades conocidas que pueden llegar al compromiso el nuestro servidor.

2.3.2. INSTALACIÓN UTILIZANDO GIT

41. Otra alternativa para la instalación de Drupal consiste en utilizar la herramienta para desarrolladores GIT, un software de control de versiones que tiene como objetivo el control de los cambios que se puedan producir durante el desarrollo de un determinado software, permitiendo conocer con detalle el estado actual, personas que intervinieron, cambios en determinados archivos del código fuente, restaurar versiones antiguas etc.
42. Lo primero que haremos será configurar el repositorio por primera vez, y descargar la última versión disponible:

```
root@guiaDrupal:/var/www/html# git clone --branch 8.0.x https://git.drupal.org/project/drupal.git
Clonar en «drupal»...
remote: Counting objects: 537921, done.
remote: Compressing objects: 100% (104939/104939), done.
remote: Total 537921 (delta 387352), reused 535359 (delta 385121)
Receiving objects: 100% (537921/537921), 116.46 MiB | 4.88 MiB/s, done.
Resolving deltas: 100% (387352/387352), done.
Checking connectivity... hecho.
root@guiaDrupal:/var/www/html# ls
drupal
root@guiaDrupal:/var/www/html#
```

43. Con la ejecución de este comando se creará un nuevo directorio llamado "drupal", donde se encontrarán los ficheros de la última versión.

DIRECTORIO .GIT EN SERVIDORES PÚBLICOS
El comando anteriormente ejecutado descargará una copia de todos los ficheros, incluido un directorio oculto con el nombre de ".git".

Este directorio puede contiene información sensible::

```
root@guiaDrupal:/var/www/html# cd drupal/
root@guiaDrupal:/var/www/html/drupal# ls -al .git
total 1600
drwxr-xr-x 8 root root    4096 may 12 16:27 .
drwxr-xr-x 9 root root    4096 may 12 16:27 ..
drwxr-xr-x 2 root root    4096 may 12 16:26 branches
-rw-r--r-- 1 root root     264 may 12 16:27 config
-rw-r--r-- 1 root root      73 may 12 16:26 description
-rw-r--r-- 1 root root      22 may 12 16:27 HEAD
drwxr-xr-x 2 root root    4096 may 12 16:26 hooks
-rw-r--r-- 1 root root 1570128 may 12 16:27 index
drwxr-xr-x 2 root root    4096 may 12 16:26 info
drwxr-xr-x 3 root root    4096 may 12 16:27 logs
drwxr-xr-x 4 root root    4096 may 12 16:26 objects
-rw-r--r-- 1 root root   18558 may 12 16:27 packed-refs
drwxr-xr-x 5 root root    4096 may 12 16:27 refs
root@guiaDrupal:/var/www/html/drupal#
```

Deberemos borrar esta información si se trata de un servicio expuesto al público, o añadir la siguiente regla al fichero .htaccess:

```
root@guiaDrupal:/var/www/html/drupal# head -n 3 .htaccess
RewriteEngine On
RewriteRule ^(.*/)?\.git/ - [F,L]
ErrorDocument 403 "Access Forbidden"
root@guiaDrupal:/var/www/html/drupal#
```

Para comprobar si esta medida adicional está funcionando, accederemos a http://nuestroservidor/ruta/.git/. Si obtenemos un error 403, el directorio habrá quedado protegido.

2.3.3. CONFIGURACIÓN DE LA BASE DE DATOS

44. Para el correcto funcionamiento de Drupal, será necesario crear una base de datos nueva, con un usuario que tenga permisos para acceder a ella:

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 47
Server version: 5.5.44-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE guiadrupal CHARACTER SET utf8 COLLATE utf8_general_ci;
Query OK, 1 row affected (0.00 sec)

mysql> CREATE USER 'usuariodrupal'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, CREATE TEMPORARY TABLES ON guiadrupal.*
TO 'usuariodrupal'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> EXIT
Bye
```

45. El ejemplo anterior muestra el acceso como la cuenta de administrador por defecto de MySQL. Este nombre de usuario depende de los valores iniciales con los que la base de datos fuera configurada e instalada al inicio, por lo que en ciertos sistemas puede ser un valor diferente.

46. El resto de valores deberán ser elegidos por parte del usuario, como el nombre de la base de datos o el usuario que se va a utilizar para acceder, así como el campo hostname, que será generalmente "localhost".

47. Respecto a las contraseñas de acceso, se recomienda seguir una serie de pautas para la creación y establecimiento de contraseñas seguras:

    - Se deben utilizar al menos 12 caracteres para crear la clave
    - Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.
    - Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas.
    - Utilizar signos de puntuación, así como diferentes símbolos
    - En lo posible, utilizar una *passphrase* (una frase de contraseña o secuencia de palabras), debido a su sencillez para recordar y ser más segura, debido a su longitud

48. Podremos utilizar el siguiente comando de línea de consola para generar una contraseña segura de 12 caracteres:

```
$ tr -dc [:graph:] < /dev/urandom | head -c 12 | xargs -0
X#}C")?q1&Xy
$
```

49. Además, en caso de necesidad, podremos modificar el valor de la longitud de la contraseña, incrementando el valor entero después del comando 'head':

```
$ tr -dc [:graph:] < /dev/urandom | head -c 20 | xargs -0
Y_W[PQ5Wghi,^J(%}1Re
$
```

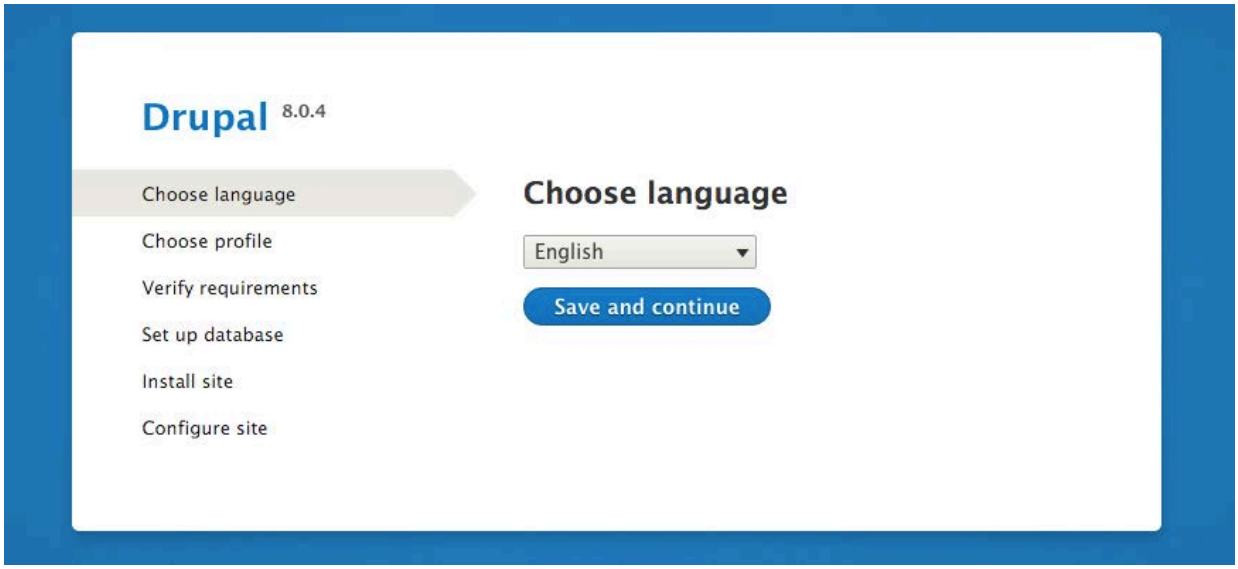
2.3.4. FINALIZANDO LA INSTALACIÓN

50. Ahora que tenemos los ficheros necesarios para realizar la instalación, es necesario configurar Drupal para indicarle ciertos valores, como la información de la base de datos.

51. Para ello, primero copiamos el fichero de configuración por defecto de la distribución a la ruta adecuada:

```
$ cp ./sites/default/default.settings.php ./sites/default/settings.php
$ chmod 644 sites/default/settings.php
```

52. Después accedemos a la URL http://direccion_servidor/drupal/, y nos encontraremos una pantalla como la siguiente:

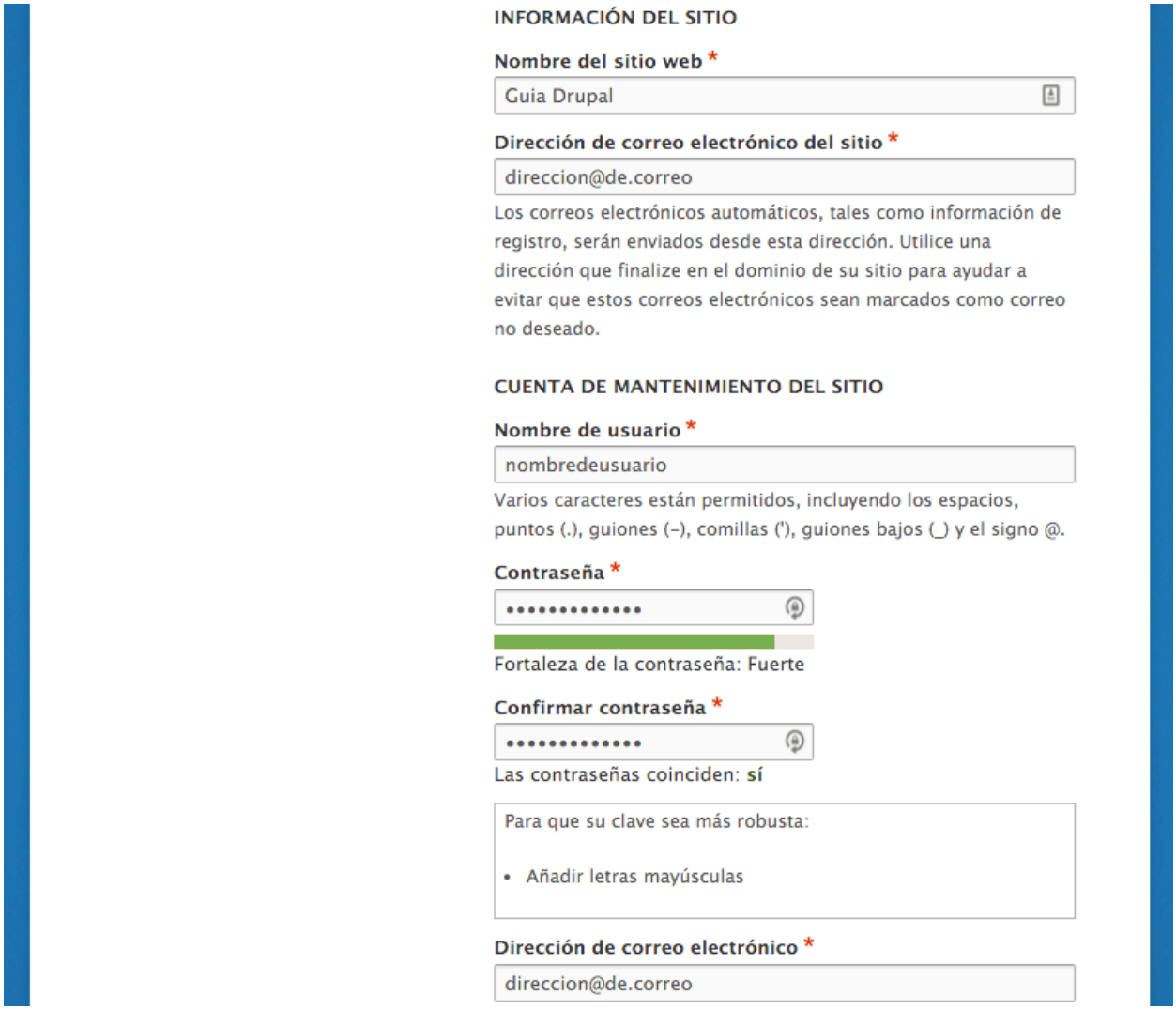


53. Seleccionaremos el modelo de instalación adecuado para nuestras necesidades y comprobaremos que el sistema cumple con los requisitos de la instalación de Drupal elegida. En caso de que no se cumplan, debido a la falta de alguna dependencia o creación de algún directorio, procederemos a su subsanación y comenzaremos la instalación de Drupal de nuevo desde el principio.

54. Cuando lleguemos a la pantalla de configuración de la base de datos, introduciremos los valores que hayamos elegido en el momento de la configuración de MySQL:

55. Una vez introducidos estos datos de configuración interna, llegaremos a la pantalla de la configuración propia de Drupal, donde deberemos introducir una serie de valores adicionales:

- **Nombre del sitio web**: el título que se mostrará en la generación de páginas dinámicas
- **Dirección de correo electrónico del sitio:** Los correos electrónicos automáticos, tales como información de registro, serán enviados desde esta dirección. Utiliza una dirección que finalice en el dominio de su sitio para ayudar a evitar que estos correos electrónicos sean marcados como correo no deseado.
- **Nombre de Usuario**: el nombre de usuario del administrador del sitio
- **Contraseña**: la contraseña correspondiente al administrador (se recomienda seguir las pautas indicadas anteriormente)
- **Dirección de correo electrónico**: la dirección de correo asociada al administrador
- Además de los anteriores campos, deberemos introducir información adicional, como 'País Predefinido', 'Zona horaria preferida', así como marcar campos para comprobar y recibir actualizaciones de forma automática de Drupal por correo electrónico. De esta forma se nos notificará cuando estén disponibles actualizaciones y rutinas importantes de seguridad para los componentes instalados.



56. Una vez finalicemos de introducir los valores que hemos seleccionado, pulsamos en “Guardar y continuar” y la instalación habrá finalizado.

3. SEGURIDAD EN LA BASE DE DATOS

57. MySQL es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones, entre las que podemos destacar, además de las realizadas por usuarios o administradores, a empresas como Yahoo!, Alcatel-Lucent, Google, Nokia, Youtube y muchas otras.

58. Como la mayor parte de los servicios, MySQL vendrá pre configurado en nuestro sistema si hemos optado por su instalación como paquete, por lo que deberemos ajustar ciertos parámetros para adaptarnos a las mejores prácticas.

3.1. DESHABILITAR O RESTRINGIR EL ACCESO REMOTO

59. La primera consideración a tener en cuenta es determinar si el servicio de MySQL será accesible desde la red o solamente desde nuestro servidor (el caso más común). En caso de necesitar acceso remoto al servicio, debemos asegurarnos que existe un filtrado de qué direcciones estarán autorizadas, utilizando TCP Wrappers, Iptables o cualquier firewall software/hardware que esté disponible.

60. En caso contrario, evitaremos que MySQL abra un socket de red (sin impedir que las conexiones locales sigan funcionando) que permita esta conexiones, añadiendo el siguiente código a la parte "[mysqld]" del fichero "/etc/my.cnf" o "/etc/msqyl/my.ini":

61. Skip-networking

62. Otra opción disponible será forzar a MySQL a escuchar sólo las conexiones realizadas desde "localhost", añadiendo la siguiente línea en el mismo apartado del fichero anterior:

Bind-address=127.0.0.1

```
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 127.0.0.1
```

3.2. DESHABILITAR EL USO DE 'LOCAL INFILE'

63. La siguiente tarea a realizar será deshabilitar el uso del comando "LOAD DATA LOCAL INFILE", que evitará que un posible atacante sea capaz de leer ficheros locales utilizando diferentes tipos de ataques comunes, como un SQL Injection.

64. Además, en ciertas ocasiones, el comando "LOCAL INFILE" será utilizado para acceder a ficheros del sistema operativo, como "/etc/passwd", intentando ejecutar una sentencia como la siguiente:

mysql> LOAD DATA LOCAL INFILE '/etc/passwd' INTO TABLE table1

65. O incluso de forma más sencilla:

mysql> SELECT load_file("/etc/passwd")

66. Para deshabilitar el uso de este comando, añadiremos el siguiente código a la sección '[mysqld]' de nuestro fichero de configuración:

set-variable=local-infile=0

3.3. MODIFICAR EL NOMBRE DE USUARIO DEL ADMINISTRADOR

67. El nombre de usuario por defecto de la instalación de MySQL es "root", por lo que los atacantes intentarán acceder de diferentes formas a esta cuenta para lograr control completo de nuestro sistema.

68. Para endurecer esta tarea, modificaremos el nombre de la cuenta a otra más complicada de adivinar de forma remota, añadiendo una contraseña compleja. Para renombrar la cuenta de administrador del sistema, introduciremos el siguiente comando en la consola de MySQL:

mysql> RENAME USER root TO nuevo_user;

69. El comando "RENAME USER" se introdujo por primera vez en la versión 5.0.2, por lo que si nos encontramos con una versión anterior, será necesario realizar el proceso de forma diferente con los siguientes comandos:

mysql> use mysql;
mysql> update user set user="nuevo_usuario" where user="root";
mysql> flush privileges;

3.4. ELIMINAR LA BASE DE DATOS DE PRUEBAS

70. MySQL, por norma general, almacena una base de datos, llamada 'test', que puede ser accedida por usuarios anónimos, por lo que podría recibir gran número de ataques. Para eliminar esta base de datos, utilizaremos el comando DROP de la siguiente forma desde la línea de comandos:

mysql> drop database test;

71. También podemos realizar esta tarea desde la Shell utilizando 'mysqladmin':

$ mysqladmin -u username -p drop test

3.5. ELIMINAR LA CUENTA ANÓNIMA Y OTRAS CUENTAS OBSOLETAS

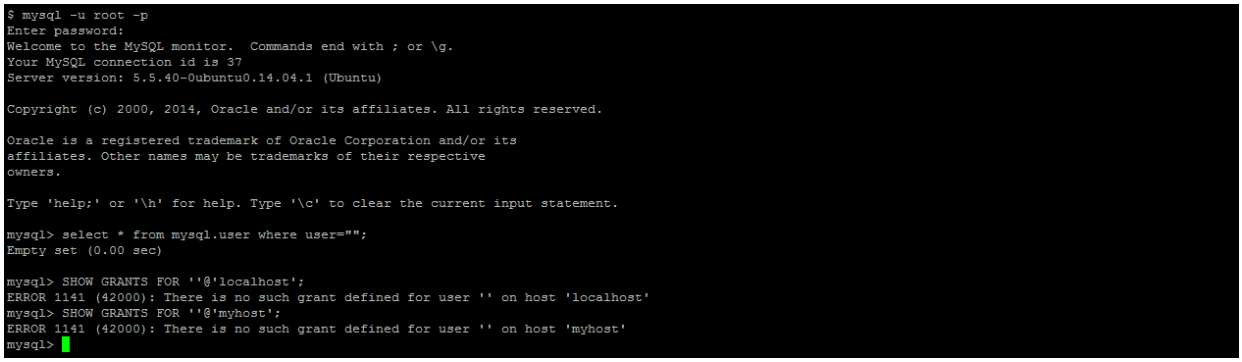
72. Por defecto, MySQL activará ciertas cuentas anónimas, que no necesitan contraseña, por lo que cualquier atacante podría conseguir acceso al sistema de forma sencilla. Para comprobar si están activadas en nuestro servidor, realizaremos la siguiente consulta:

*mysql> select * from mysql.user where user="";*

73. Otra forma de realizar la consulta, sería de la siguiente forma:

mysql> SHOW GRANTS FOR ''@'localhost';
mysql> SHOW GRANTS FOR ''@'myhost';

74. En sistemas seguros, no deberíamos obtener resultado alguno:



75. Se deberán eliminar estas cuentas, ejecutaremos el siguiente comando:

mysql> DROP USER "";

76. El comando DROP USER fue introducido en la versión 5.0. Si nos encontramos con una versión anterior de MySQL, podremos eliminar estas cuentas con las siguientes consultas:

mysql> use mysql;
mysql> DELETE FROM user WHERE user="";
mysql> flush privileges;

3.6. REDUCIR LOS PRIVILEGIOS DEL SISTEMA

77. Se deberán reducir los privilegios con los que se ejecuta MySQL para evitar la exposición de nuestro sistema a gran cantidad de ataques.

78. En el caso de que estemos trabajando con versiones superiores a la 5.0, los permisos estarán ajustados y no será necesario realizar ninguna variación.

79. En otro caso, existen algunas premisas que deberemos cumplir para asegurar el servicio. Primero, comprobaremos que el directorio del servicio está asignado al grupo y usuario 'mysql':

$ ls -l /var/lib/mysql

```
total 36880
-rw-r--r-- 1 root  root         0 dic 30 14:40 debian-5.5.flag
drwx------ 2 mysql mysql     4096 ene 10 22:37 guiawordpress
-rw-rw---- 1 mysql mysql 27262976 ene 11 01:11 ibdata1
-rw-rw---- 1 mysql mysql  5242880 feb  9 18:13 ib_logfile0
-rw-rw---- 1 mysql mysql  5242880 feb  9 18:13 ib_logfile1
drwx------ 2 mysql root     4096 dic 30 14:41 mysql
-rw-rw---- 1 root  root         6 dic 30 14:41 mysql_upgrade_info
drwx------ 2 mysql mysql     4096 dic 30 14:41 performance_schema
```

80. Comprobaremos, además, que el usuario "mysql" y "root" tienen acceso al directorio "/var/lib/mysql".

81. Finalmente, los binarios que se encuentran en el directorio "/usr/bin/", deberán tener como propietario al usuario 'root' o el correspondiente a la ejecución de "mysql". Ningún otro usuario debe tener permisos de escritura a estos ficheros:

*$ ls -l /usr/bin/my**

82. La siguiente captura muestra un ejemplo de un sistema con los permisos correctos:

```
$ ls -l /usr/bin/my*
-rwxr-xr-x 1 root root 3301584 oct 11 03:13 /usr/bin/myisamchk
-rwxr-xr-x 1 root root 3190416 oct 11 03:13 /usr/bin/myisam_ftdump
-rwxr-xr-x 1 root root 3177104 oct 11 03:13 /usr/bin/myisamlog
-rwxr-xr-x 1 root root 3211440 oct 11 03:13 /usr/bin/myisampack
-rwxr-xr-x 1 root root 2903024 oct 11 03:13 /usr/bin/my_print_defaults
-rwxr-xr-x 1 root root 3469920 oct 11 03:13 /usr/bin/mysql
-rwxr-xr-x 1 root root  111539 oct 11 00:02 /usr/bin/mysqlaccess
-rwxr-xr-x 1 root root 3338016 oct 11 03:13 /usr/bin/mysqladmin
lrwxrwxrwx 1 root root      10 oct 11 03:12 /usr/bin/mysqlanalyze -> mysqlcheck
-rwxr-xr-x 1 root root 3456608 oct 11 03:13 /usr/bin/mysqlbinlog
-rwxr-xr-x 1 root root   11075 oct 11 00:02 /usr/bin/mysqlbug
-rwxr-xr-x 1 root root 3338976 oct 11 03:13 /usr/bin/mysqlcheck
-rwxr-xr-x 1 root root 3745984 oct 11 03:13 /usr/bin/mysql_client_test
-rwxr-xr-x 1 root root    4245 oct 11 00:02 /usr/bin/mysql_convert_table_format
-rwxr-xr-x 1 root root   23756 oct 11 00:02 /usr/bin/mysqld_multi
-rwxr-xr-x 1 root root   24885 oct 11 00:02 /usr/bin/mysqld_safe
-rwxr-xr-x 1 root root 3404960 oct 11 03:13 /usr/bin/mysqldump
-rwxr-xr-x 1 root root    7402 oct 11 00:02 /usr/bin/mysqldumpslow
-rwxr-xr-x 1 root root    3315 oct 11 00:02 /usr/bin/mysql_find_rows
-rwxr-xr-x 1 root root    1261 oct 11 00:02 /usr/bin/mysql_fix_extensions
-rwxr-xr-x 1 root root   34852 oct 11 00:02 /usr/bin/mysqlhotcopy
-rwxr-xr-x 1 root root 3334336 oct 11 03:13 /usr/bin/mysqlimport
-rwxr-xr-x 1 root root   14785 oct 11 00:02 /usr/bin/mysql_install_db
lrwxrwxrwx 1 root root      10 oct 11 03:12 /usr/bin/mysqloptimize -> mysqlcheck
-rwxr-xr-x 1 root root 2911352 oct 11 03:13 /usr/bin/mysql_plugin
lrwxrwxrwx 1 root root      10 oct 11 03:12 /usr/bin/mysqlrepair -> mysqlcheck
-rwxr-xr-x 1 root root   39016 oct 11 03:11 /usr/bin/mysqlreport
-rwxr-xr-x 1 root root    8198 oct 11 00:02 /usr/bin/mysql_secure_installation
-rwxr-xr-x 1 root root   17473 oct 11 00:02 /usr/bin/mysql_setpermission
-rwxr-xr-x 1 root root 3332992 oct 11 03:13 /usr/bin/mysqlshow
-rwxr-xr-x 1 root root 3352064 oct 11 03:13 /usr/bin/mysqlslap
-rwxr-xr-x 1 root root 3589872 oct 11 03:13 /usr/bin/mysqltest
-rwxr-xr-x 1 root root 2872944 oct 11 03:13 /usr/bin/mysql_tzinfo_to_sql
-rwxr-xr-x 1 root root 2979096 oct 11 03:13 /usr/bin/mysql_upgrade
-rwxr-xr-x 1 root root 2898224 oct 11 03:13 /usr/bin/mysql_waitpid
-rwxr-xr-x 1 root root    3888 oct 11 00:02 /usr/bin/mysql_zap
```

3.7. ACTIVAR LOS LOGS DEL SISTEMA

83. Se deberá activar la generación de logs añadiendo las siguientes líneas a la sección "[mysqld]" de nuestro fichero de configuración:

log =/var/log/mylogfile

```
[mysqld]
#
# * Basic Settings
#
user            = mysql
pid-file        = /var/run/mysqld/mysqld.pid
socket          = /var/run/mysqld/mysqld.sock
port            = 3306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
lc-messages-dir = /usr/share/mysql
skip-external-locking
#
# Log
#
log=/var/log/fichero_de_logs_mysql
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 127.0.0.1
```

84. Además, comprobaremos que sólo el usuario "root" o "mysql" tiene acceso a estos ficheros (al menos permisos de escritura).

3.8. ELIMINAR HISTORIAL

85. Durante el proceso de instalación y generación de bases de datos, tablas etc. es probable que se utilice información sensible que debe de ser eliminada de tal forma que cualquier atacante que consiga acceso a nuestro sistema no tenga acceso a ella. Esta información puede ser almacenada dentro del historial, por lo que debe ser eliminada, así como todas las peticiones que almacena.

86. Esta tarea puede realizarse incluyendo el siguiente comando en nuestro fichero de inicio de sesión de la Shell (en el caso de utilizar Bash sería .bashrc):

    cat /dev/null > ~/.mysql_history

3.9. LIMITAR LOS PERMISOS DE USUARIO

87. Para la operativa normal de Drupal, como generar nuevos posts, comentarios, crear usuarios o instalar módulos, el usuario utilizado para acceder a nuestra base de datos sólo debe tener permisos de lectura y escritura; es decir, debe poder ejecutar sentencias SELECT, INSERT, UPDATE y DELETE, por lo que podremos eliminar el resto de privilegios.

88. Para ello, introduciremos la siguiente consulta en nuestra consola MySQL:

    mysql> REVOKE ALL PRIVILEGES ON guiadrupal. FROM 'usuariodrupal'@'localhost';*

89. Después, asignaremos nuevos privilegios a nuestro usuario:

    mysql> GRANT SELECT, INSERT, UPDATE, DELETE ON guiadrupal. TO 'usuariodrupal'@'localhost';*

NOTA:
Algunos *plugins*, temas o actualizaciones de Drupal pueden requerir realizar cambios estructurales en la base de datos, como añadir nuevas tablas etc. En ese caso, antes de realizar la instalación será necesario otorgar privilegios completos a nuestro usuario de Drupal en MySQL. En este caso el procedimiento será el contrario:

mysql> REVOKE ALL PRIVILEGES ON guiadrupal. FROM 'usuariodrupal'@'localhost';*

mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, CREATE TEMPORARY TABLES ON guiadrupal. TO 'usuariodrupal'@'localhost' IDENTIFIED BY 'password';*

Se recomienda generar un *backup* del sistema antes de realizar estos cambios mayores.

4. CONFIGURACIÓN SEGURA DE PHP

4.1. INSTALACIÓN DE SUHOSIN

90. A pesar de que existen gran cantidad de recursos para mejorar la seguridad de PHP, muchos administradores no los implantan en sus sistemas. En este caso vamos a utilizar una herramienta de securización para PHP, llamada Suhosin, que generará una configuración más robusta y prevendrá gran cantidad de ataques, ya que está diseñada para proteger tanto a servidores como usuarios de vulnerabilidades, tanto conocidas como desconocidas, en las aplicaciones y Core de PHP.

    - Algunas de las características principales que proporciona Suhosin son:
    - Protección contra buffer overflows (Canary y SafeUnlink Protection)
    - Protección del core y extensiones de PHP contra vulnerabilidades format string
    - Protección contra el secuestro de sesiones, usando cifrado de forma transparente para la aplicación
    - Soporte para sha256(), sha256_file() y CRYPT_BLOWFISH en crypt()
    - Cifrado de cookies
    - Baneo automático en la carga de ficheros binarios o ejecutables ELF
    - Configuración de respuestas frente a violaciones de política de seguridad: bloqueo, redirección a nivel de cliente, envío de código HTTP o ejecución de script PHP
    - etc.

91. Para la instalación en sistemas Ubuntu y Debian, ejecutaremos los siguientes comandos:

```
$ wget https://sektioneins.de/files/repository.asc
$ sudo apt-key add repository.asc
$ echo 'deb http://repo.suhosin.org/ ubuntu-trusty main' >> /etc/apt/sources.list
$ apt-get update
$ apt-get install php5-suhosin-extension
$ php5enmod suhosin
$ apache2ctl restart
```

92. En el caso de que deseemos una instalación manual, deberemos descargar la última versión estable (en el momento de la escritura de esta guía es la 0.9.38), y ejecutar los siguientes comandos:

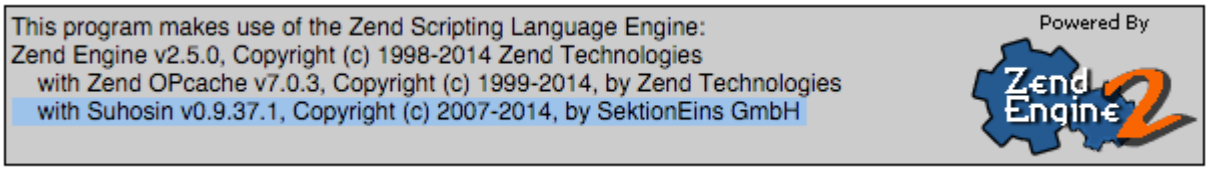
```
$ cd /tmp
$ wget https://download.suhosin.org/suhosin-0.9.38.tar.gz
$ tar xzvf suhosin-0.9.38.tar.gz
$ cd suhosin-0.9.38
$ phpize
$ make
$ make test
$ make install
```

93. Esto debería instalar la extensión 'suhosin.so' en el directorio correcto. Ahora sólo tendremos que añadir la siguiente directiva al fichero php.ini:

extension=suhosin.so

94. Se puede obtener más información detallada para realizar la instalación desde la página oficial del proyecto: https://suhosin.org/stories/install.html#installing-on-debian-and-ubuntus

95. Finalmente, crearemos un fichero de prueba con la función "phpinfo()", tal como hicimos en el inicio de esta guía, para comprobar que la instalación ha sido satisfactoria, pudiendo visualizar:



96. Debemos recordar nuevamente que este fichero de prueba debe ser borrado inmediatamente después de haber realizado las comprobaciones necesarias.

4.2. CONFIGURACIÓN DE VARIABLES[3]

97. Existen gran cantidad de variables que pueden ser asignadas vía Apache, así como en el fichero de configuración de PHP. Lo más recomendable es mantener la configuración de seguridad de PHP centralizada en el fichero "php.ini".

98. Por ejemplo, implementar el flag "httpOnly" cuando se genera una cookie puede reducir el riesgo de un ataque XSS (Cross-Site Scripting), ya que las cookies de sesión mediante código Javascript. Además, implementaremos el flag "httpSecure", que impedirá que un posible atacante acceda o intercepte los datos de la sesión, ya que estos sólo viajarán únicamente por canales HTTPS seguros. Por último, seleccionaremos el algoritmo hash utilizado para generar el identificador ID de la sesión, utilizando en este caso el llamado "whirlpool".

99. Para realizar estas tareas, agregaremos el siguiente código a nuestro fichero "php.ini":

session.cookie_httponly = 1
session.use_only_cookies = 1
session.cookie_secure = 1
session.hash_function = whirlpool

100. A continuación, vamos a limitar y controlar ciertos recursos del sistema, como la memoria máxima, el tamaño máximo de fichero que podrá cargar un usuario o el tiempo de ejecución. En nuestro mismo fichero incluiremos las siguientes líneas:

memory_limit = 128M
max_input_time = 60
max_execution_time = 30
upload_max_filesize = 2M

101. Como medida adicional, también vamos a ocultar la versión de PHP que está siendo utilizada en el sistema, para reducir información que pudiera utilizar un atacante, añadiendo la siguiente línea:

[3] **SETTING INI VARIABLES:** https://openconcept.ca/sites/openconcept/files/drupal_security_best_practices_v1.3_-_2015-12-8_0.pdf

expose_php = off

102. También deshabilitaremos funciones de PHP que permiten a los scripts referenciar a otras URLs:

allow_url_include = off
allow_url_fopen = off

103. También deshabilitaremos funciones de PHP que se consideran peligrosas. Será necesario comprobar si nuestra instalación y módulos asociados a Drupal no utilizan alguna de esta funciones (esto podemos realizarlo utilizando el comando "grep" desde la línea de comando):

disable_functions = php_uname, getmyuid, getmypid, passthru, leak, listen, diskfreespace, tmpfile, link, ignore_user_abord, shell_exec, dl, set_time_limit, exec, system, highlight_file, source, show_source, fpaththru, virtual, posix_ctermid, posix_getcwd, posix_getegid, posix_geteuid, posix_getgid, posix_getgrgid, posix_getgrnam, posix_getgroups, posix_getlogin, posix_getpgid, posix_getpgrp, posix_getpid, posix, _getppid, posix_getpwnam, posix_getpwuid, posix_getrlimit, posix_getsid, posix_getuid, posix_isatty, posix_kill, posix_mkfifo, posix_setegid, posix_seteuid, posix_setgid, posix_setpgid, posix_setsid, posix_setuid, posix_times, posix_ttyname, posix_uname, proc_open, proc_close, proc_get_status, proc_nice, proc_terminate, popen

104. Finalmente, nos aseguraremos que la ruta donde se guardan las sesiones se encuentra fuera del directorio web y no pueden ser leídas por otros usuarios del sistema. También indicaremos a PHP que el directorio donde se realizarán las cargas del fichero se encontrará fuera del directorio web, con el siguiente código:

session.save_path = "/tmp"
upload_tmp_dir = "/tmp"

4.3. CONFIGURACIÓN DE APACHE VIRTUAL HOST

105. A pesar de que a partir de Drupal 7 se deshabilita la ejecución de PHP en los directorios donde se pueden subir este tipo de ficheros, será necesario comprobar el fichero ".htaccess" de este directorio, y añadir la siguiente directiva a la configuración del "Virtual Host" de Apache, por si alguna comprobación ha sido pasada por alto:

```
<Directory /var/www/drupal/sites/default/files/>
    # Important for security, prevents someone from
    # uploading a malicious .htaccess
    AllowOverride None
    SetHandler none
    SetHandler default-handler
    Options -ExecCGI
    php_flag engine off
    RemoveHandler .cgi .php .php3 .php4 .php5 .phtml .pl .py .pyc .pyo
    <Files *>
        AllowOverride None
        SetHandler none
        SetHandler default-handler
        Options -ExecCGI
        php_flag engine off
        RemoveHandler .cgi .php .php3 .php4 .php5 .phtml .pl .py .pyc .pyo
    </Files>
</Directory>
```

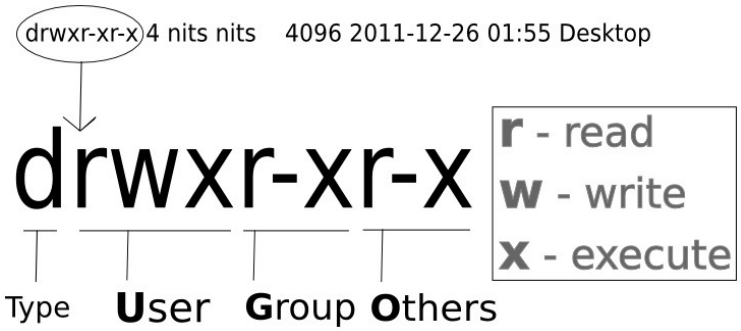
5. CONFIGURACIÓN DE PERMISOS

106. Los distintos ficheros y directorios poseen permisos que especifican quien y que puede leer, escribir, modificar y accederlos. Esto es importante, puesto que Drupal puede necesitar acceso de escritura a ficheros en su directorio para activar ciertas funcionalidades.

107. El modo de permisos se realiza sumando los valores para el usuario, el grupo y para el resto. Este diagrama se muestra como:

- **R**ead (4): permitido leer ficheros/leer directorio
- **W**rite (2): permitido escribir/modificar ficheros/directorios
- e**X**ecute (1): permitido ejecutar el archivo o acceder al directorio

108. Estos permisos pueden ser representados en notación octal, que no es más que un valor en base 8. Siendo así, si el primer elemento de izquierda a derecha está activo (lectura) su valor es 4. Si el segundo elemento está activo (escritura) su valor es dos y si el tercer elemento está activo (ejecución), su valor es 1. Por ejemplo, si quisiéramos representar en notación octal permisos de lectura y ejecución, el valor sería 5. Para permisos de lectura y escritura el valor es 6 y para permisos de lectura, escritura y ejecución el valor es 7.4



109. Además, existen una serie de categorías de permisos:

- **U**suario o propietario (user, abreviada como u)
- **G**rupo (group, abreviada como g)
- **O**tros (others, abreviada como o)

110. Cada categoría de permisos se representa con tres caracteres. El primer conjunto de caracteres representa la categoría de usuario, el segundo conjunto representa la categoría de grupo y el tercer conjunto representa a la categoría otros. Cada uno de los tres caracteres representa los permisos de lectura, escritura y ejecución respectivamente.

111. Visto de esta forma, algunos ejemplos con su simbología completa serian:

[4] **FUENTE:** http://hipertextual.com/archivo/2014/05/permisos-linux/

Modo	Cadena perms.	Explicación
0477	-r--rwxrwx	el propietario solo puede leer (4), los otros y el grupo tienen acceso total rwx (7)
0677	-rw-rwxrwx	el propietario tiene sólamente lectura y escritura rw (6), los otros y el grupo tienen acceso total rwx (7)
0444	-r--r--r--	todos pueden sólamente leer (4)
0666	-rw-rw-rw-	todos pueden sólamente leer y escribir rw (6)
0400	-r--------	el propietario tiene solo lectura(4), los otros y el grupo no tienen permiso(0)
0600	-rw-------	el propietario tiene sólamente lectura y escritura rw, los otros y el grupo no tienen permiso(0)
0470	-r--rwx---	el propietario tiene sólamente lectura, el grupo tiene acceso total rwx, los otros no tienen permiso
0407	-r-----rwx	el propietario tiene sólamente lectura, los otros tienen acceso total rwx, el grupo no tiene permiso
0670	-rw-rwx---	el propietario tiene sólamente lectura y escritura rw, el grupo tiene acceso total rwx, los otros no tienen permiso
0607	-rw----rwx	el propietario tiene sólamente lectura y escritura rw, el grupo no tienen permiso y los otros tienen acceso total rwx

112. Los permisos de Drupal serán diferentes de un host a otros host, así que esta guía solamente detalla principios genéricos. No puede cubrir todos los casos.

113. Típicamente, todos los ficheros deberían pertenecer a la cuenta de usuario de tu servidor web, y deberían ser escribibles por esa cuenta. En hosting compartido, los ficheros nunca deben pertenecer al proceso mismo del servicio web (generalmente será www, o apache, o nobody).

114. Cualquier fichero que necesite acceso de escritura desde Drupal debería pertenecer al grupo de la cuenta de usuario utilizada por Drupal (la cual puede que sea diferente de la cuenta del servidor). Por ejemplo, puede que se disponga de una cuenta específica de FTP que se utilice para cargar/descargar ficheros en el servidor, pero que ésta se encuentre utilizando un usuario separado, en un grupo de usuario aparte, como apache, www-data o nobody. Si Drupal se ejecuta como la cuenta de FTP, esta cuenta necesita tener permisos de escritura, ser el propietario de los ficheros, o pertenecer a un grupo que tenga permiso de escritura. En este último caso, implicaría que los permisos están establecidos más permisivamente que por defecto:

- 775 en vez de 755 para directorios
- 664 en vez de 644 para ficheros

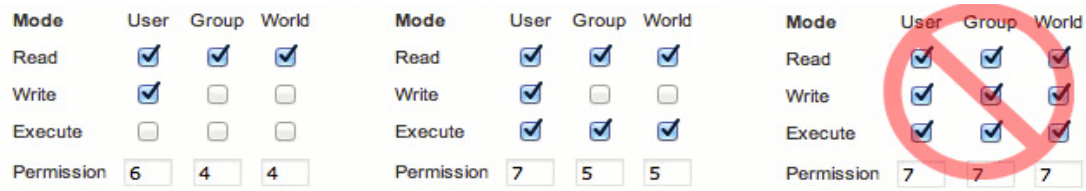
115. Los permisos de fichero y directorio de Drupal deberían ser los mismos para la mayoría de usuarios, dependiendo del tipo de instalación que hayas realizado y la configuración de umask del entorno de sistema en el momento de la instalación.

116. Son muchas las ocasiones en que pueden surgir graves problemas de seguridad por unos permisos inadecuados de estos ficheros y directorios, por lo que especificaremos unas reglas básicas:

1. Los ficheros del núcleo de Drupal deberían poseer permisos de escritura solamente por la cuenta de usuario utilizada
2. Para garantizar la seguridad de los archivos, utilizaremos el siguiente comando:

   $ find /var/www/html/directorio_drupal -type d -exec chmod u=rwx,g=rx,o= '{}' \;
3. Para garantizar la seguridad de los directorios, es necesario mantenerlos en 755.

   $ find /var/www/html/directorio_drupal -type f -exec chmod u=rw,g=r,o= '{}' \;



4. Si por algún motivo debe modificarse un fichero o dar permisos de escritura a un directorio, deben ser 666 y comprobar si funciona. En caso de error, procederemos a asignarle los permisos 777 y una vez finalizado, le asignaremos el valor estándar de nuevo: 644 para ficheros y 755 para directorios.
5. Al final la instalación, Drupal mantendrá los permisos necesarios en directorios y ficheros. A pesar de ello, deberemos comprobar que:
   a. El directorio 'sites/default' tiene permisos [dr-xr-xr-x]:

      $ chmod 555 sites/default

   b. El fichero settings.php tiene permisos [-r--r--r--]:

      $ chmod 444 sites/default/settings.php

5.1. SCRIPT PARA PERMISOS DE FICHEROS Y DIRECTORIOS ADECUADOS

117. A continuación se muestra un script para solucionar los permisos de ficheros y directorios de una instalación de Drupal. Para ello copiaremos el código que se muestra a continuación en un fichero nuevo, llamado 'fix-permissions.sh', que podremos lanzar como a continuación:

$ sudo bash fix-permissions.sh --drupal_path=/ruta/directorio/drupal --drupal_user=usuario_al_que_asignar

118. Por defecto el grupo al que serán asignados tanto ficheros como directorios será "www-data", pero podemos modificarlo utilizando el argumento "--http_group=grupo_que_deseemos".

119. El código del script5 es el siguiente:

```
#!/bin/bash

# Help menu
print_help() {
cat <<-HELP
This script is used to fix permissions of a Drupal installation
you need to provide the following arguments:

  1) Path to your Drupal installation.
  2) Username of the user that you want to give files/directories ownership.
  3) HTTPD group name (defaults to www-data for Apache).

Usage: (sudo) bash ${0##*/} --drupal_path=PATH --drupal_user=USER --httpd_group=GROUP
Example: (sudo) bash ${0##*/} --drupal_path=/usr/local/apache2/htdocs --drupal_user=john --
httpd_group=www-data
HELP
exit 0
}
```

[5] **SECURING FILE PERMISSIONS AND OWNERSHIP**: https://www.drupal.org/node/244924

```
if [ $(id -u) != 0 ]; then
  printf "**************************************\n"
  printf "* Error: You must run this with sudo or root*\n"
  printf "**************************************\n"
  print_help
  exit 1
fi

drupal_path=${1%/}
drupal_user=${2}
httpd_group="${3:-www-data}"

# Parse Command Line Arguments
while [ "$#" -gt 0 ]; do
  case "$1" in
    --drupal_path=*)
       drupal_path="${1#*=}"
       ;;
    --drupal_user=*)
       drupal_user="${1#*=}"
       ;;
    --httpd_group=*)
       httpd_group="${1#*=}"
       ;;
    --help) print_help;;
    *)
      printf "*************************************************************\n"
      printf "* Error: Invalid argument, run --help for valid arguments. *\n"
      printf "*************************************************************\n"
      exit 1
  esac
  shift
done

if [ -z "${drupal_path}" ] || [ ! -d "${drupal_path}/sites" ] || [ ! -f
"${drupal_path}/core/modules/system/system.module" ] && [ ! -f
"${drupal_path}/modules/system/system.module" ]; then
  printf "***********************************************\n"
  printf "* Error: Please provide a valid Drupal path. *\n"
  printf "***********************************************\n"
  print_help
  exit 1
fi

if [ -z "${drupal_user}" ] || [[ $(id -un "${drupal_user}" 2> /dev/null) != "${drupal_user}" ]]; then
  printf "**************************************\n"
  printf "* Error: Please provide a valid user. *\n"
  printf "**************************************\n"
  print_help
  exit 1
fi

cd $drupal_path
printf "Changing ownership of all contents of "${drupal_path}":\n user => "${drupal_user}" \t group =>
"${httpd_group}"\n"
chown -R ${drupal_user}:${httpd_group} .

printf "Changing permissions of all directories inside "${drupal_path}" to "rwxr-x---"...\n"
find . -type d -exec chmod u=rwx,g=rx,o= '{}' \;
```

```
printf "Changing permissions of all files inside "${drupal_path}" to "rw-r-----"...\n"
find . -type f -exec chmod u=rw,g=r,o= '{}' \;

printf "Changing permissions of "files" directories in "${drupal_path}/sites" to "rwxrwx---"...\n"
cd sites
find . -type d -name files -exec chmod ug=rwx,o= '{}' \;

printf "Changing permissions of all files inside all "files" directories in "${drupal_path}/sites" to "rw-rw----
"...\n"
printf "Changing permissions of all directories inside all "files" directories in "${drupal_path}/sites" to
"rwxrwx---"...\n"
for x in ./*/files; do
  find ${x} -type d -exec chmod ug=rwx,o= '{}' \;
  find ${x} -type f -exec chmod ug=rw,o= '{}' \;
done
echo "Done setting proper permissions on files and directories"
```

6. CREACIÓN DE UN FICHERO ‘ROBOTS.TXT’

120. Todos los buscadores, como Google, Bing, etc., para analizar los millones de webs existentes, utilizan programas que van continuamente escaneando todo tipo de información y añadiéndola a sus bases de datos (indexación). A estos programas se les denomina de diferentes formas, como robots, arañas, crawlers, etc. En el caso de Google, su robot principal se llama Googlebot. El fichero "robots.txt" te permite bloquear o permitir el acceso de los robots a las partes de tu web que a ti te interesen. Cuando el robot llegue a tu sitio web, comprobará si existe el fichero robots.txt, y si es ese el caso, seguirá las instrucciones que ahí se le indiquen para analizar la información.

121. Hay que tener en cuenta que aunque este es el funcionamiento general de la mayoría de motores de búsqueda (buscadores), esto no quiere decir que todos sigan estas reglas. Gente que se dedica a fines poco éticos como SPAM, etc., utiliza sus propios motores para captar información y darle un mal uso, saltándose todas estas reglas. Si tienes información privada en tu web, protégela con contraseñas o con cualquier otro sistema que evite que cualquiera pueda verla.

122. Por defecto, el fichero robots.txt de las instalaciones de Drupal contiene:

```
User-agent: *
# JS/CSS
Allow: /core/*.css$
Allow: /core/*.js$
# Directories
Disallow: /core/
Disallow: /profiles/
# Files
Disallow: /README.txt
Disallow: /web.config
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
```

Disallow: /user/logout/# Paths (no clean URLs)
Disallow: /index.php/admin/
Disallow: /index.php/comment/reply/
Disallow: /index.php/filter/tips/
Disallow: /index.php/node/add/
Disallow: /index.php/search/
Disallow: /index.php/user/password/
Disallow: /index.php/user/register/
Disallow: /index.php/user/login/
Disallow: /index.php/user/logout/

123. Cualquier directorio que deseemos excluir de este indexado de buscadores, deberá introducir con la opción Disallow, indicando la ruta completa al directorio deseado.

NOTA:
Existe una serie de datos adicionales que necesitaremos saber:
1. Se recomienda no incluir en un fichero robots.txt más de 200 líneas de Disallow.
2. Una vez que incluyamos el Disallow de una carpeta, si nos equivocamos y queremos volver a indexarla, pueden pasar hasta 3 meses desde que se agregue hasta que los buscadores vuelvan a mostrarla.
3. Se utilizan los Disallow cuando se quiera bloquear carpetas completas. Si es sólo una página suelta, las etiquetas meta son más eficaces.
4. Para ver qué ha indexado Google de nuestra web y compararlo con lo que le hemos dicho que no indexe en meta o robots.txt, introduciremos en la búsqueda “site:www.direccionweb.com“.

7. RESTRICCIONES DE ACCESO

124. Un módulo bastante interesante para nuestro uso será "mod_authz_host", ya que es capaz de restringir el acceso a páginas como /user o /admin/*, y apenas necesita configuración.

125. Mostraremos una serie de capacidades, mostrando ejemplos de funcionamiento que deben ser adaptados a cada situación específica e instalación. Para evitar que cualquier usuario pueda editar un nodo, salvo las direcciones IP 192.0.2.1 y 192.0.2.25, incorporamos el siguiente código en el fichero de configuración de Apache:

```
<Localtion - "/node/.*/edit">
  Order Deny, Allow
  Deny from all
  Allow from 192.168.1.1 192.168.1.2
</Location>
```

126. Este tipo de restricción de acceso también puede realizarse utilizando "mod_rewrite", escribiendo el siguiente código dentro del fichero ".htaccess" o el fichero de configuración de Apache. En este caso sólo proporcionamos el acceso a "admin/" a las direcciones IP anteriormente indicadas:

```
<IfModule mod_rewrite.c>
  RewriteEngine on
  # Allow only internal access to admin
  RewriteCond %{REMOTE_ADDR}
  !^(192\.168\.1\.1|192\.168\.1\.2)$
  RewriteRule ^admin/.* - [F]
</IfModule>
```

127. Drupal tiene una serie de procesos que pueden ser inicializados desde una URL. Estos deben ser bloqueados utilizando Apache, para que no puedan ejecutarse desde un navegador. Los procesos que evitaremos serán "update", "install", "cron" etc. Incluiremos la siguiente línea dentro del fichero ".htaccess" o el fichero de configuración de Apache

```
<FilesMatch "(authorize|cron|install|upgrade).php">
```

```
Order deny,allow
deny from all
Allow from 127.0.0.1
</FilesMatch>
```

8. ASEGURANDO EL ENTORNO Y EL USUARIO #1

128. La cuenta creada durante la instalación de Drupal (llamada user #1) es una cuenta con permisos especiales, ya que posee todos los permisos por defecto, y el acceso a ella por parte de un atacante implicaría un alto riesgo de seguridad, por lo que debe ser tratada como la cuenta "root" de los sistemas Linux.

129. Por este motivo, es necesario establecer una serie de medidas adicionales para protegerla de posibles atacantes, entre las que incluimos las siguientes:

- Deshabilitar el usuario #1: Drupal no necesita la cuenta del usuario #1 para la administración, esto sólo era necesario en versiones anteriores para tareas vitales como la actualización del software. Si por cualquier razón excepcional necesitáramos utilizar este usuario, podríamos activarlo de nuevo:
  - Deshabilitar usuario #1 desde MySQL:

    mysql> UPDATE users SET status=0 WHERE uid=1;
  - Habilitar usuario #1 desde MySQL:

    mysql> UPDATE users SET status=1 WHERE uid=1;
- Limitar y restringir el acceso a direcciones IP autorizadas, como hemos visto en las secciones anteriores, o utilizando un módulo como veremos más adelante.
- Habilitar el acceso por HTTPS, de tal forma que el acceso de tanto usuarios como administrador no pueda verse capturado o expuesto por un posible atacante en la red
- Crear una nueva cuenta para el uso diario, cuyo nombre no sea fácilmente adivinable por un atacante, como "admin", "administrador" etc.
- En lo posible, utilizar una *passphrase* (una frase de contraseña o secuencia de palabras), debido a su sencillez para recordar y ser más segura, debido a su longitud.
- No compartir las credenciales de acceso del sistema. Si es necesario que un desarrollador acceda al panel de control, se creará una cuenta temporal con permisos de administrador, y cuando el trabajo finalice, esta se eliminará definitivamente
- Utilizar una contraseña fuerte para todos y cada uno de los usuarios del sistema:
  - Al menos 12 caracteres
  - No debe ser predecible ni encontrarse en algún diccionario
  - No debe coincidir con datos personales del usuario, tales como el nombre de un conocido, pareja, mascota, o la ciudad donde nació
  - Debe incluir mayúsculas, minúsculas y caracteres especiales como $,!,? etc.

- Debe ser modificada con cierta frecuencia (por ejemplo, cada dos o tres meses)
- Para evitar olvidar la contraseña se puede utilizar los diferentes gestores disponibles, como 1Password o LastPass. Nunca debe apuntarse las credenciales en papel, en la cartera o con una nota sobre el monitor.
- Podremos utilizar el siguiente comando de línea de consola para generar una contraseña segura de 12 caracteres:

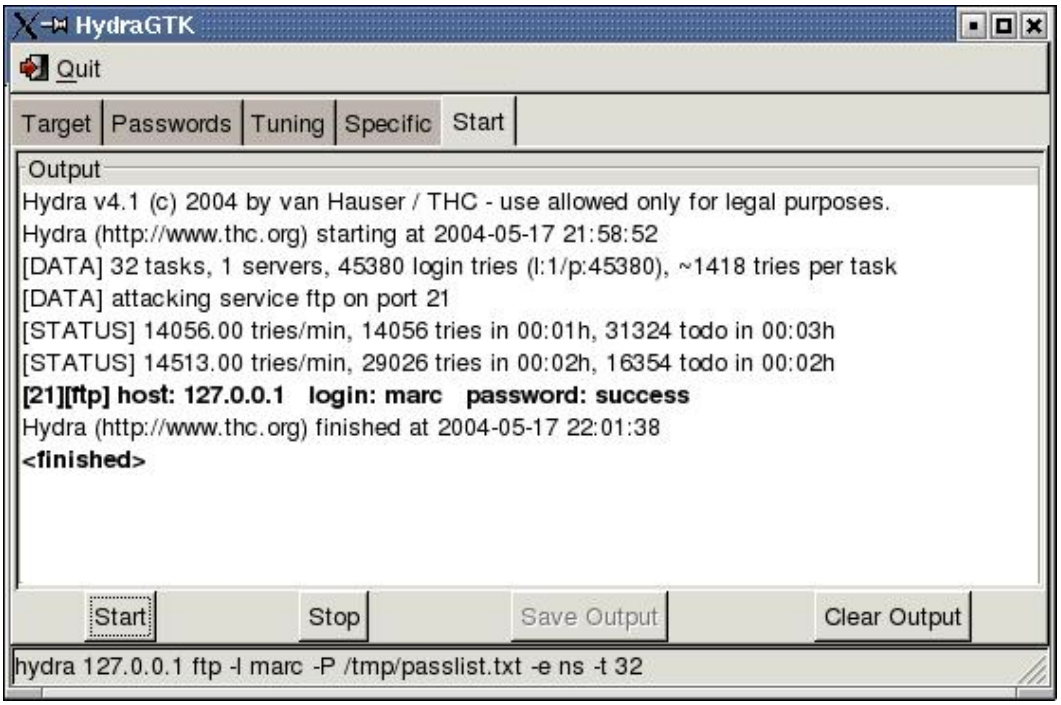
```
$ tr -dc [:graph:] < /dev/urandom | head -c 12 | xargs -0
X#}C")?q1&Xy
$
```

130. Además, en caso de necesidad, podremos modificar el valor de la longitud de la contraseña, incrementando el valor entero después del comando 'head':

```
$ tr -dc [:graph:] < /dev/urandom | head -c 20 | xargs -0
Y_W[PQ5Wghi,^J(%}1Re
$
```

8.1. PROTECCIÓN CONTRA ATAQUES DE FUERZA BRUTA

131. Un ataque por fuerza bruta es un método que realiza comprobaciones, en el nombre de usuario y/o contraseñas, de todas las combinaciones de los caracteres indicados, hasta averiguar Un ataque por fuerza bruta es el método para averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Este tipo de ataques garantizan un alto éxito, debido a que sólo es cuestión de tiempo hallar la combinación adecuada para acceder al servicio atacado, y pueden realizarse tanto de forma manual como automatizada.



THC-HYDRA: http://sectools.org/tool/hydra/

132. Desde la versión 7 de Drupal, existe un filtro contra ataques de fuerza bruta que realiza las siguientes tareas:

- Bloquea un usuario que haya fallado su acceso más de 5 veces en 6 horas
- Bloquea una dirección IP que haya fallado más de 50 intentos durante 1 hora. Para ello, accederemos por línea de consola a nuestro servidor y accederemos a MySQL:

133. Esta información acerca de los logins fallidos se almacena en una tablada llamada "flood", que se encuentra dentro de la base de datos de Drupal:

```
mysql> desc flood;
+------------+--------------+------+-----+---------+----------------+
| Field      | Type         | Null | Key | Default | Extra          |
+------------+--------------+------+-----+---------+----------------+
| fid        | int(11)      | NO   | PRI | NULL    | auto_increment |
| event      | varchar(64)  | NO   | MUL |         |                |
| identifier | varchar(128) | NO   |     |         |                |
| timestamp  | int(11)      | NO   |     | 0       |                |
| expiration | int(11)      | NO   | MUL | 0       |                |
+------------+--------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

134. En caso de que deseemos reiniciarla, utilizaremos el siguiente comando:

mysql> DELETE FROM 'flood';

135. Si por el contrario no deseamos borrar todas las entradas de la tabla, pero deseamos desbloquear a un usuario que ha sido bloqueado accidentalmente, utilizaremos el siguiente comando en MySQL, donde hemos utilizado el identificador de usuario de ejemplo "1234":

mysql> DELETE FROM 'flood' WHERE event='failed_login_attempt_user' AND identifier LIKE '1234-%';

9. CONFIGURACIÓN SEGURA DE INPUT FORMATS

136. Los formatos de entrada de Drupal proporcionan una gran variedad de beneficios, ya que pueden ser utilizados para mejorar la funcionalidad, pero uno de los propósitos principales es asegurar que los datos introducidos son seguros para los visitantes. Por ejemplo, si se permite la inserción de comentarios anónimos cono formato de entrada "HTML Completo", un visitante podría introducir desde una imagen inadecuada hasta código Javascript malicioso para cambiar o apoderarse de la sesión del usuario.

137. La configuración por defecto en Drupal 8 se encuentra en Configuración->Formato y editores de texto, y como vemos a continuación, está gestionada según el rol de uso:

NOMBRE	EDITOR DE TEXTO	ROLES	OPERACIONES
HTML Básico	CKEditor	Usuario autenticado,Administrador	Configurar
HTML Restringido	—	Usuario anónimo,Administrador	Configurar
HTML completo	CKEditor	Administrador	Configurar
Texto sin formato	—	*Este formato se muestra cuando no hay otros formatos disponibles*	Configurar

138. Esta configuración por defecto de formatos de entrada y permisos es segura, pero existen una serie de modificaciones que el administrador podría realizar, convirtiéndolas en un riesgo de seguridad, como:

- Añadir etiquetas avanzadas a los filtros de entrada, en especial con los siguientes: SCRIPT, IMG, IFRAME, EMBED, OBJECT, INPUT, LINK, STYLE, META, FRAMESET, DIV, SPAN, BASE, TABLE, TR, TD.
- Reorganizar el orden de los filtros, especialmente para los usuarios no confiables, tales como usuarios anónimos o con roles muy bajos. El filtro de "HTML completo" deberá ser el último de ellos.
- El cambio de permisos en los filtros sólo debería permitir el uso de etiquetas avanzadas y "HTML Completo" a los usuarios registrados y de confianza.

139. A pesar de que es tentador activar más etiquetas o activar la opción de "HTML completo" para enriquecer la experiencia de usuarios anónimos, especialmente cuando se utilizan editores WYSIWYG, esto convertirá nuestro sitio en un objetivo. Es solamente cuestión de tiempo y suerte que nuestro sitio sea comprometido o utilizado para atacar a un tercero.

10. ADMINISTRACIÓN Y NAVEGACIÓN SOBRE SSL

140. Como hemos visto anteriormente, reforzar nuestro Drupal es una tarea vital, ya que existen muchos factores externos que pueden amenazar su seguridad, a pesar de las diferentes medidas que vayamos incorporando.

141. Por este motivo, vamos a activar el protocolo HTTPS.

NOTA:
Para poder completar este paso, SSL deberá estar correctamente configurado en nuestro servidor. En caso contrario, seguiremos los pasos mostrados a continuación:

```
# Activamos SSL sobre Apache2
$ a2enmod ssl
# Reiniciamos el servicio
$ service apache2 restart
# Creamos un nuevo directorio donde almacenar la clave y certificado del servidor
$ mkdir /etc/apache2/ssl
# Generamos un nuevo certificado con 365 días de validez, así como la clave asociada
```

$ openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

Ahora, utilizaremos el editor de texto que prefiramos para modificar el fichero de configuración de Apache SSL "/etc/apache2/sites-available/default-ssl.conf" y para adaptarlo a nuestras necesidades, incluyendo el nuevo certificado que hemos generado. Modificaremos los campos apropiados, como "ServerName", de la misma forma que las conexiones HTTP, incluyendo las siguientes líneas, si no se encontraran activas:

SSLEngine on
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key

Finalmente, activaremos el nuevo sitio y recargaremos el servicio:

$ sudo a2ensite default-ssl
$ service apache2 reload

142. Si deseamos forzar al cliente a utilizar HTTPS para la visualización del contenido de nuestro Drupal, incluiremos la siguiente directiva dentro del fichero ".htaccess" del directorio raíz de la aplicación:

ReWriteEngine On
ReWriteCond %{SERVER_PORT} 80
ReWriteCond ^(.)$ https://direccion_drupal/$1 [R,L]*

143. En el ejemplo anterior sustituiremos "direccion_drupal" por la ruta completa, utilizando dirección IP o dominio, de la instalación de la aplicación

11. ADMINISTRAR DRUPAL POR LÍNEA DE COMANDOS

144. Drush es una aplicación que correo bajo línea de comandos y permite interactuar con una instalación de Drupal de forma sencilla. Viene equipado con una serie de comandos para realizar modificaciones sobre los módulos, perfiles, o temas, y realizar actualizaciones de forma sencilla e incluso lanzar querys SQL sobre la base de datos.

145. Para la correcta instalación de Drush, es necesario también instalar Composer, un gestor de dependencias de proyectos, capaz de declarar, descargar y mantener actualizados los paquetes de software de los que dependa tanto un sencillo programa PHP como un amplio framework de desarrollo.

146. Para su correcta instalación, primero tendremos que añadir la siguiente línea al fichero de configuración de Suhosin, localizado en "/etc/php5/mods-available/suhosin.ini":

suhosin.executor.include.whitelist = phar

147. Después, procederemos a la instalación de Composer y Drush de la siguiente forma:

 # Instalacion de composer
$ cd /tmp
$ php -r "readfile('https://getcomposer.org/installer');" > composer-setup.php
$ php -r "if (hash('SHA384', file_get_contents('composer-setup.php')) === 'fd26ce67e3b237fffd5e5544b45b0d92c41a4afe3e3f778e942e43ce6be197b9cdc7c251dcde6e2a52297ea269370680') { echo 'Installer verified'; } else { echo 'Installer corrupt'; unlink('composer-setup.php'); }"
$ php composer-setup.php
$ php -r "unlink('composer-setup.php');"
$ php composer-setup.php --install-dir=/bin --filename=composer
 # Instalacion de Drush
$ wget http://files.drush.org/drush.phar
$ php drush.phar core-status

$ chmod +x drush.phar
$ sudo mv drush.phar /usr/local/bin/drush
$ drush init

148. Comprobaremos que Drush ha sido correctamente instalado ejecutando el siguiente comando, para obtener información sobre la versión de la aplicación, así como los ficheros de configuración de los que depende:

$ drush status

```
root@guiaDrupal:~# drush status
 PHP configuration      :  /etc/php5/cli/php.ini
 PHP OS                 :  Linux
 Drush script           :  /usr/local/bin/drush
 Drush version          :  8.0.3
 Drush temp directory   :  /tmp
 Drush configuration    :
 Drush alias files      :
```

149. Para conocer los detalles de nuestra instalación de Drupal, entraremos en el directorio donde lo hayamos instalado y ejecutaremos el mismo comando:

```
root@guiaDrupal:/var/www/html/drupal# drush status
 Drupal version                :  8.0.7-dev
 Site URI                      :  http://default
 Database driver               :  mysql
 Database hostname             :  localhost
 Database port                 :  3306
 Database username             :  usuariodrupal
 Database name                 :  guiadrupal
 Drupal bootstrap              :  Successful
 Drupal user                   :
 Default theme                 :  bartik
 Administration theme          :  seven
 PHP configuration             :  /etc/php5/cli/php.ini
 PHP OS                        :  Linux
 Drush script                  :  /usr/local/bin/drush
 Drush version                 :  8.0.3
 Drush temp directory          :  /tmp
 Drush configuration           :
 Drush alias files             :
 Install profile               :  standard
 Drupal root                   :  /var/www/html/drupal
 Drupal Settings File          :  sites/default/settings.php
 Site path                     :  sites/default
 File directory path           :  sites/default/files
 Temporary file directory path :  /tmp
 Sync config path              :  sites/default/files/config_mixUDred6PkY_H1upP_pKTnT-XWKYRqK3zdYwXY9_nf2rD5iIaTgJ1TO5sd78r_fhdrF74FjMA/sync
```

150. Algunos de los comandos más interesantes que podremos realizar con esta aplicación son los siguientes:

- Descargar e instalar un módulo:

  $ drush dl {modulo}

- Activar un módulo

  $ drush en {modulo}

- Deshabilitar un módulo

  $ drush dis {modulo}

- Comprobar actualizaciones disponibles, descargar módulos actualizados y ejecutar update.php:

  $ drush up

- Limpiar todas las caches:

  $ drush cc all

- Ejecutar cron:

  $ drush cron

- Creación de nuevos usuarios

$ drush user-create nombre_usuario --mail="direccion@de.email.com" --password="password"

```
root@guiaDrupal:/var/www/html/drupal# drush user-create nombre_usuario --mail="direccion@de.email.com" --password="password"
 User ID       :  4
 User name     :  nombre_usuario
 User mail     :  direccion@de.email.com
 User roles    :  authenticated
 User status   :  1
```

- Borrar un usuario existente en el sistema:

$ drush user-cancel nombre_usuario

```
root@guiaDrupal:/var/www/html/drupal# drush user-cancel nombre_usuario
Cancel user account?:  (y/n): y
Cancelled user(s): nombre_usuario
Se ejecutó la actualización.
Se ha eliminado nombre_usuario.
```

- Cambiar la contraseña de un usuario:

$ drush user-password nombre_usuario --password="nuevo_password"

```
root@guiaDrupal:/var/www/html/drupal# drush user-password nombre_usuario --password="nuevo_password"
Changed password for nombre_usuario
```

151. Como se puede ver, el uso de Drush hace la vida más fácil para los desarrolladores de Drupal. Estos son sólo algunos de los comandos más comunes y básicos que se pueden utilizar a diario, sin necesidad de utilizar el interfaz web con la cuenta de administración, haciendo nuestro sistema más seguro frente a posibles ataques externos.

12. GUÍA PARA LA INSTALACIÓN DE MÓDULOS

152. Los módulos permiten extender las funcionalidades de Drupal para añadir características que vengan integradas dentro de la distribución original. Los módulos se clasifican en 2 grandes tipos:

- **Core modules**: generados por los desarrolladores de Drupal, proporcionan las funcionalidades básicas.
- **Contributed modules**: desarrollados por la comunidad.

153. Existen varias formas para realizar la instalación de módulos dentro del entorno de Drupal 8, tanto desde el interfaz de administración Web como desde la línea de comandos.

12.1. UTILIZANDO DRUSH

154. Para realizar la descarga local del módulo seleccionado, utilizaremos el comando:

$ drush dl {modulo}

155. Posteriormente, necesitaremos activarlo:

$ drush en {modulo} -y

156. Si en algún momento deseamos deshabilitar un módulo, también podremos hacerlo vía línea de comandos:

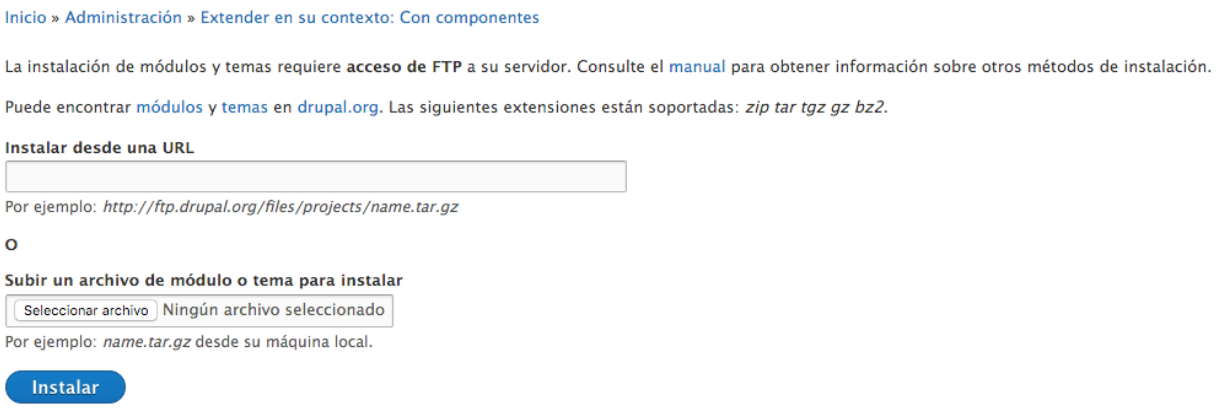
$ drush dis {modulo} -y

12.2. UTILIZANDO EL PORTAL WEB DE ADMINISTRACIÓN

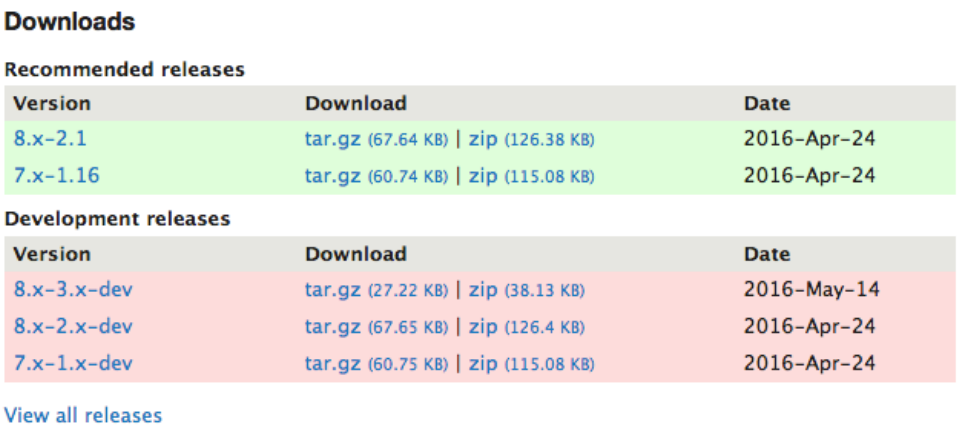
157. A través del interfaz web de administración podremos también realizar este tipo de descargas de módulos, pero para ello es necesario realizar la instalación del módulo principal "Update Manager".

158. Para ello, primero pulsaremos sobre "Administrar" y después sobre la pestaña "Extender". A continuación aparecerán una serie de módulos en diferentes secciones, activaremos la casilla de "Update Manager" en la sección de Núcleo y pulsaremos Instalar:

159. Una vez el módulo se encuentre instalado y activo, aparecerá un nuevo botón dentro de la pestaña "Extender", llamado "Instalar nuevo módulo:



160. A continuación tendremos que indicar la ruta del fichero de instalación del módulo, o podremos realizar la carga de éste desde nuestro PC. Cada módulo en la página de Drupal tiene una serie de enlaces en la parte posterior, donde vienen los ficheros correspondientes a cada versión y que podremos copiar e introducir en la URL del módulo a instalar:



Ejemplo del módulo **SITE AUDIT:** https://www.drupal.org/project/site_audit

12.3. CARGA MANUAL DEL MÓDULO

161. Si no podemos utilizar ninguno de los anteriores sistemas, siempre podremos realizar la carga de forma manual. Para ello deberemos tener acceso por línea de comandos en el servidor donde tengamos Drupal corriendo.

162. Deberemos descargar el fichero acorde con nuestra versión y descomprimirlo dentro del directorio "/modules" que se encuentra en la raíz de la instalación, con el siguiente comando:

$ tar -zxvf modulo.tar.gz

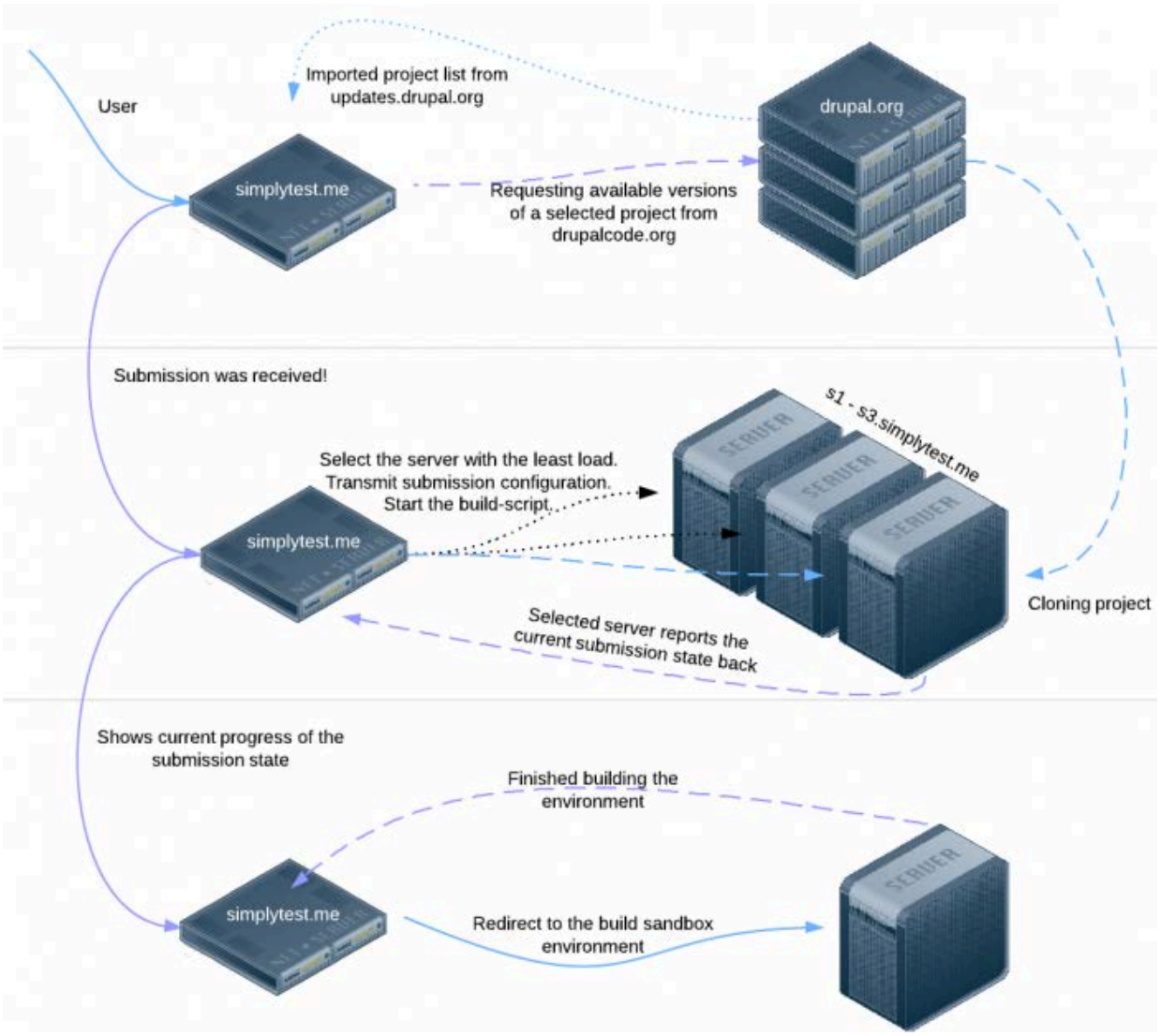
163. Después, inevitablemente deberemos activarlo desde el panel de administración Web, dentro de la pestaña "Extender"

13. SISTEMA DE PRUEBA DE MÓDULOS Y TEMAS

164. Existe una plataforma online, llamada simplytest.me, que permite crear sandbox de 24horas de duración y probar con diferentes módulos, temas, versiones del core de Drupal o cualquier otro parcha antes de instalarlo en producción.

165. Este servicio básicamente corre un servidor web, y tiene diferentes workers para cubrir la demanda de las sandbox solicitadas por el cliente. La lista de proyectos e importada y actualizada desde la API oficial en updates.drupal.org y la lista de versiones de core se extrae desde drupalcode.org.

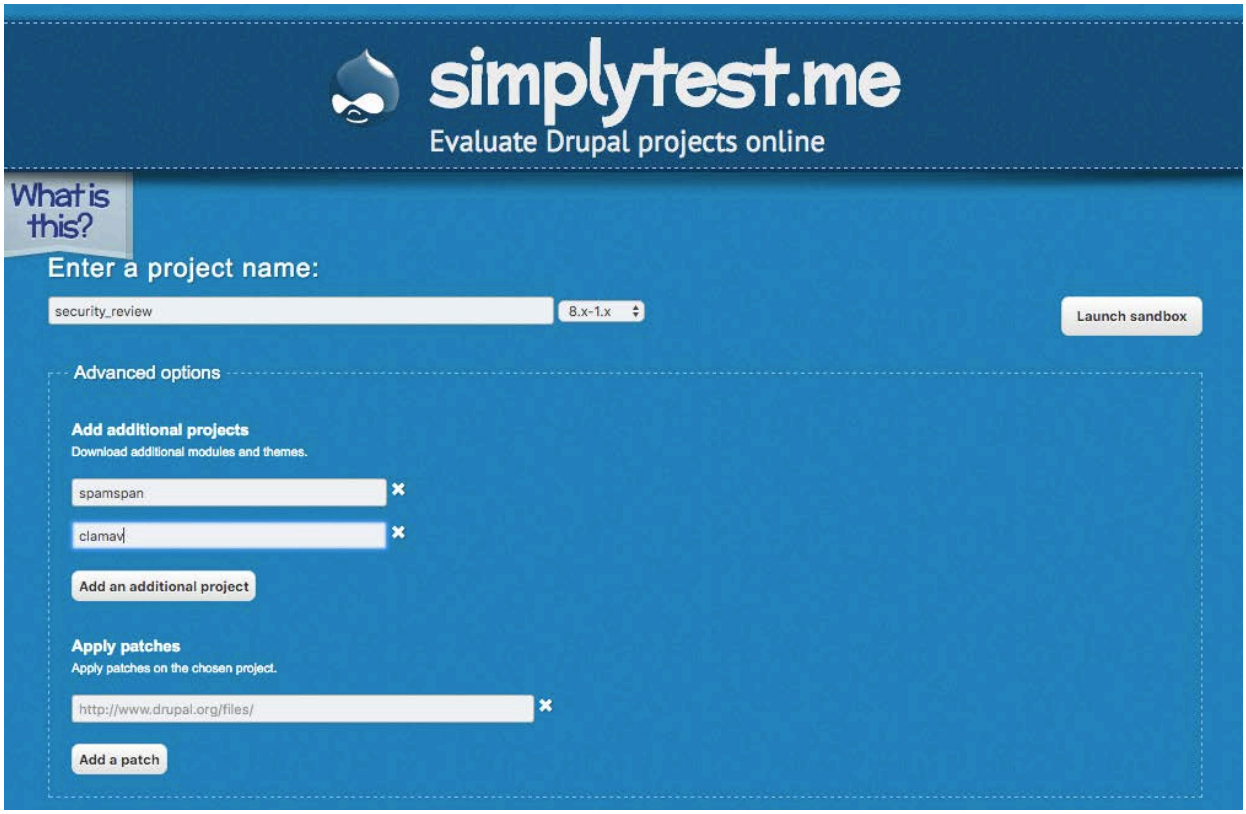
166. Cuando se recibe una solicitud, el worker con menos carga será seleccionado y se le asignará los módulos y versiones solicitadas, que serán transferidas por SSH, para después lanzar un script de shell que finalizará la instalación y la dejará lista para funcionar al usuario.



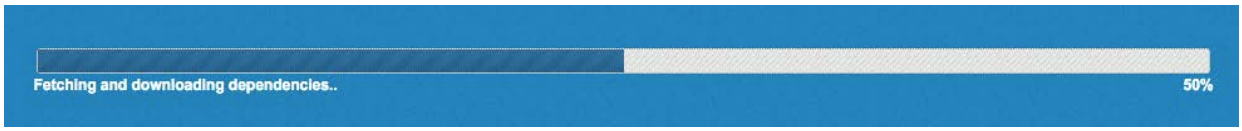
SIMPLYTEST.ME: https://www.drupal.org/project/simplytest

167. Para comenzar a trabajar con ella, sólo deberemos acceder a la URL "https://www.simplytest.me" desde un navegador. Rellenaremos los siguientes campos:

- *Project name*: nombre, que será autocompletado, del módulo, tema o versión del core que deseamos probar. Una vez seleccionado, nos mostrará las diferentes versiones disponibles.
- *Add additional projects*: permite añadir paquetes adicionales de temas o módulos a nuestra instalación
- *Apply patches*: incluir un parche que deseemos ejecutar en nuestra plataforma.



168. Una vez finalizada la selección, pulsamos sobre "Launch sandbox". Nos mostrará una barra de progreso según se vaya finalizando la solicitud realizada:



169. Finalmente nos llevará a la pantalla de instalación de la versión solicitada, ya completada con los parámetros de base de datos y configuración, que continuaremos como si fuera una instalación normal:

170. Una vez acabado el proceso, dispondremos de nuestra sandbox con Drupal y los módulos, temas y parches solicitados instalados, a la que podremos acceder en las siguientes 24horas desde la URL que nos hayan asignado y que podemos ver en la barra del navegador:

NOTA
Esta *sandbox* es pública, y cualquier persona que conozca la URL podrá acceder de forma sencilla a los datos y al panel de administración, por lo que no se recomienda introducir información de carácter confidencial en este tipo de pruebas.

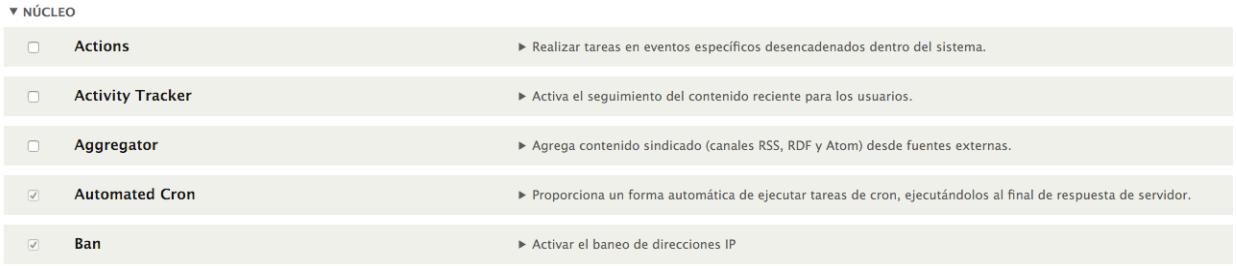
14. MÓDULOS A INSTALAR

14.1. BAN[6]

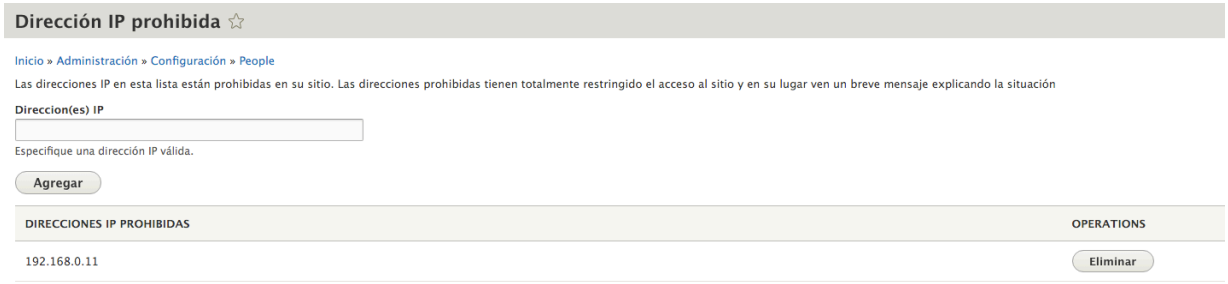
171. En ocasiones podemos comprobar que desde una dirección IP concreta se está accediendo de un modo inusual, bien por el número de accesos o bien por la cantidad de tráfico consumida. Estas direcciones IPs pueden corresponder a robots de búsqueda, a particulares, a otros servidores, posibles atacantes etc.

172. El módulo de BAN permite a los administradores bloquear el acceso al sitio de Drupal a direcciones IP concretas a través del interfaz Web. Esta funcionalidad está incluida dentro del núcleo de la versión 8, por lo que no es necesario realizar ninguna descargar e instalación posterior.

173. Por defecto no se encuentra activado, por lo que deberemos acceder a "Administrar"->"Extender"' localizarlo, y proceder a su activación:



174. Una vez activado, iremos a "Configuración" y pulsaremos sobre "Dirección IP prohibida"'. Tan solo deberemos introducir de una en una la lista de direcciones IP que queremos restringir, e ir pulsando el botón "Agregar":



[6] **BAN AN IP ADDRESS:** https://www.drupal.org/documentation/modules/ban

175. Para desbloquear una dirección IP, simplemente pulsaremos el botón "Eliminar" que cada una dispone a su lado derecho.

NOTA
El origen de ese acceso de dirección IP puede ser muy diverso, y hemos de tener cuidado si queremos restringir ese acceso a una dirección, puesto que podría ser contraproducente.

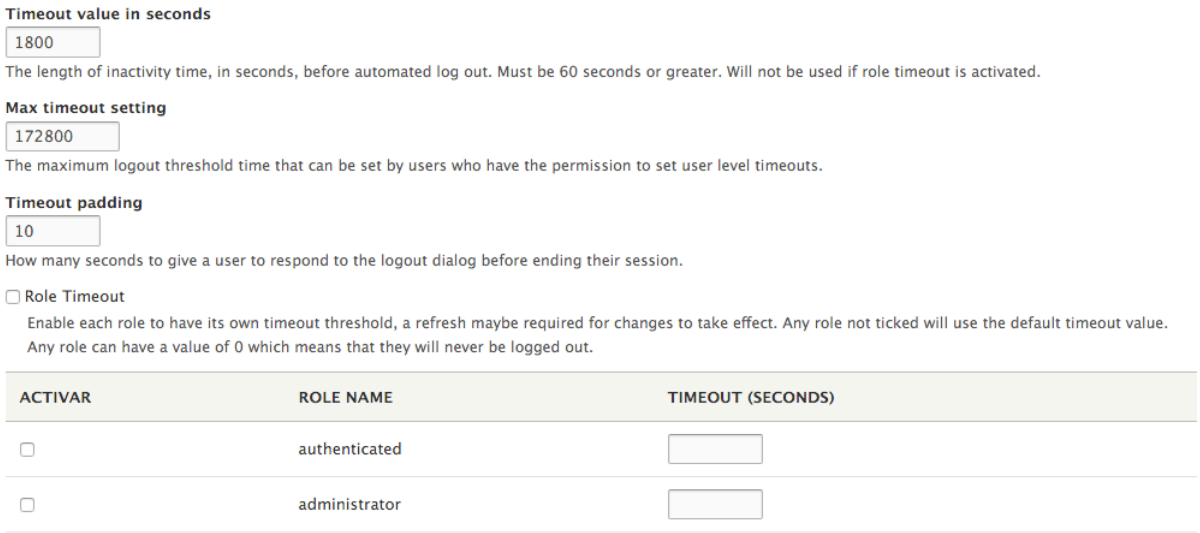
Esto puede suceder cuando por ejemplo bloqueemos la dirección IP de un buscador. Lo que sucedería es que nuestra web dejaría de ser accesible a todos aquellos que trataran de llegar a nosotros a través de los resultados de búsqueda de esa web de referencia

14.2. AUTOMATED LOGOUT[7]

176. Con este módulo proporcionamos capacidades al administrador para seleccionar que roles, basado en políticas, tienen un tiempo de espera para cerrar su sesión. Además de esto, nos permitirá:

- Desactivar este tiempo de espera según el rol del usuario
- Permitir a los usuarios configurar su propio tiempo de espera
- Incluye algunos mecanismos JavaScript para mantener a los usuarios logueados, incluso si éste tiene múltiples pestañas del navegador abiertas o se encuentra trabajando en un formulario durante un largo periodo de tiempo

177. Una vez instalado, accederemos a su configuración desde "Personas"->"Autologout settings", donde tendremos gran cantidad de parámetros que podremos configurar:

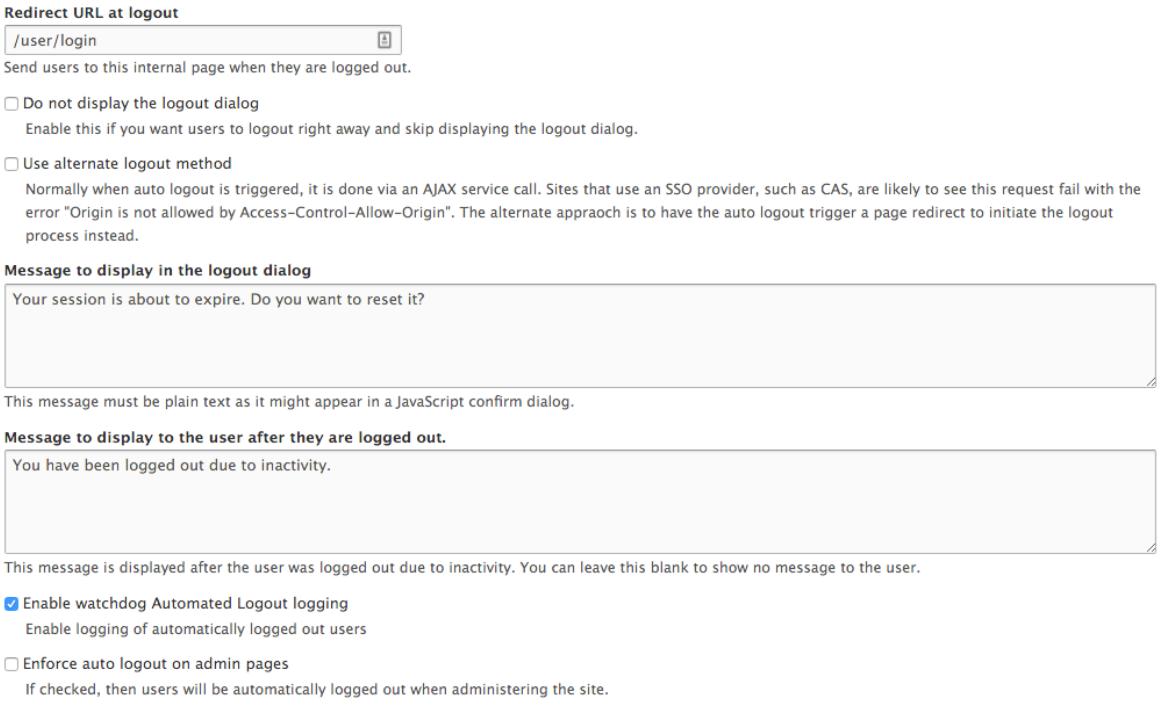


- *Timeout value in seconds*: tiempo en segundos de esperar para cerrar la sesión de un usuario si no se encuentra actividad. Debe ser superior a 60 segundos, y si el rol tiene un valor asignado, no se aplicará por defecto.
- *Max timeout setting*: tiempo máximo en segundos que el usuario puede asignarse antes de cerrar la sesión
- *Timeout padding*: tiempo en segundos que dispone el usuario para responder sobre el cuadro de diálogo que será mostrado antes de cerrar su sesión

[7] **AUTOMATED LOGOUT:** https://www.drupal.org/project/autologout

- *Role timeout*: nos permite configurar el tiempo de espera antes de cerrar la sesión para cada uno de los roles presentes en el sistema. Un valor de 0 significa que la sesión no será cerrada de forma automática.

178. Existen otros valores a configurar:

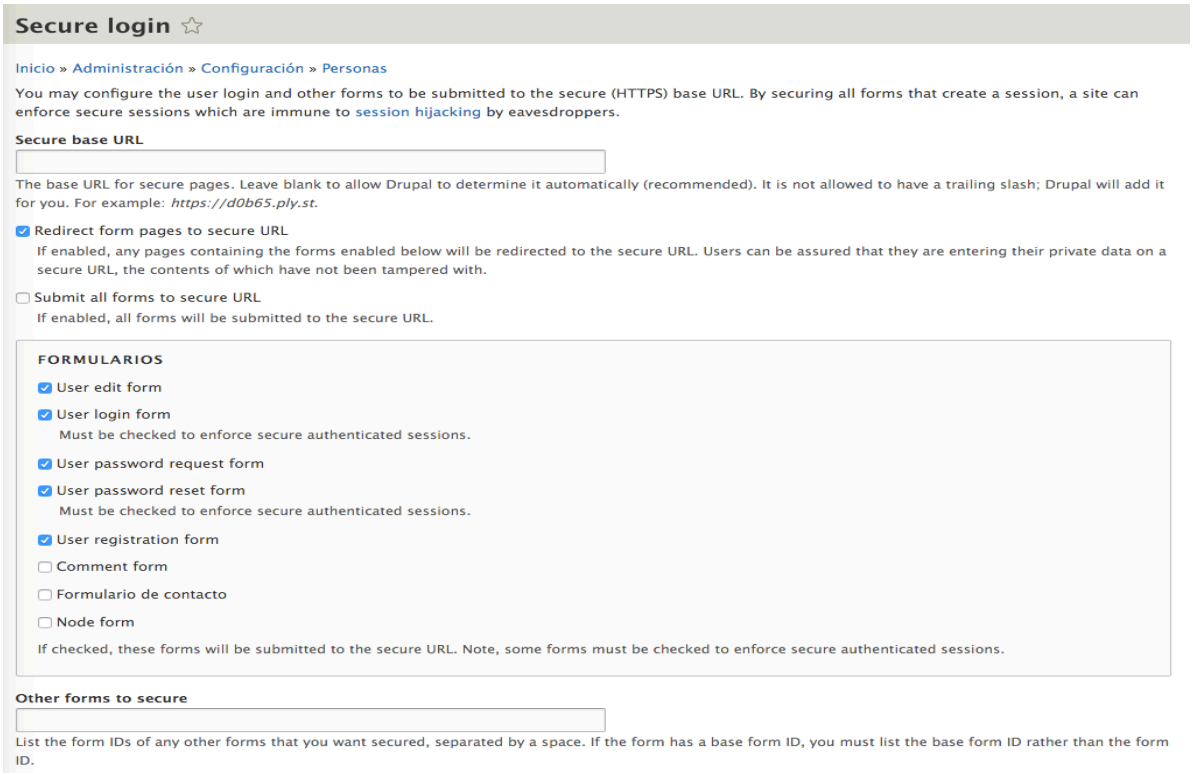


- *Redirect URL at logout*: permite especificar la URL donde el usuario será redirigido cuando se cierre su sesión. Por defecto será la página de login del sistema
- *Do not display the logout dialog*: si activamos esta opción, no se mostrará notificación al usuario de que su sesión será cerrada en el tiempo que hayamos establecido anteriormente.
- *Message to display in the logout dialog*: texto que será mostrado en el cuadro de diálogo que será presentado al usuario cuando su sesión vaya a finalizar
- *Message to display to the user after they are logged out*: mensaje que será mostrado al usuario una vez que su cuenta haya sido cerrada por inactividad
- *Enable watchdog Autmated Logout logging*: nos permite activar la opción de registro de los cierres de sesión que se produzcan en el sistema
- *Enforce auto logout on admin pages*: al marcar esta opción activaremos el tiempo de espera de cierre de sesión para la zona de administración de Drupal

14.3. SECURE LOGIN[8]

179. Para sitios que estén disponibles tanto por HTTP como por HTTPS, el módulo "Secure Login" asegura que el inicio de sesión de los usuarios, así como cualquier otro formulario que configuremos, sea enviado de forma segura por HTTPS, evitando así que las contraseñas y datos de usuario sean transmitidas en claro y puedan ser interceptadas por un posible atacante.

180. La configuración del módulo es sencilla, y una vez instalado sólo debemos acceder al menú "Configuración"->"Secure Login", donde modificaremos los parámetros en base a nuestras necesidades:



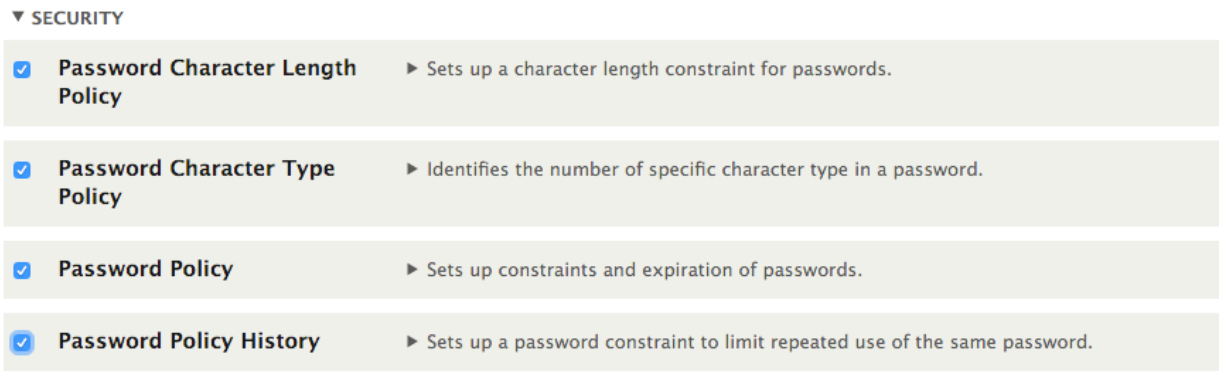
- *Secure base URL*: será la URL base de nuestro dominio, por ejemplo https://nuestro.dominio.com. La mejor opción es dejar el campo en blanco para que Drupal asigne el valor de forma automática
- *Redirect form pages to secure URL*: activando esta opción forzamos a todas las páginas que contengan un formulario a que sean reenviadas utilizando la conexión segura por HTTPS.
- *Submit all forms to secure URL*: si la activamos, todos los formularios disponibles en el sistema serán reenviados utilizando la conexión segura. En caso contrario, a continuación tendremos una lista de los formularios disponibles e iremos activando esta opción de forma individual en cada uno de ellos
- *Other forms to secure*: nos permite introducir los ID de los formularios que queremos asegurar, en caso de que no aparezcan en la lista anteriormente mostrada

[8] **SECURE LOGIN:** https://www.drupal.org/project/securelogin

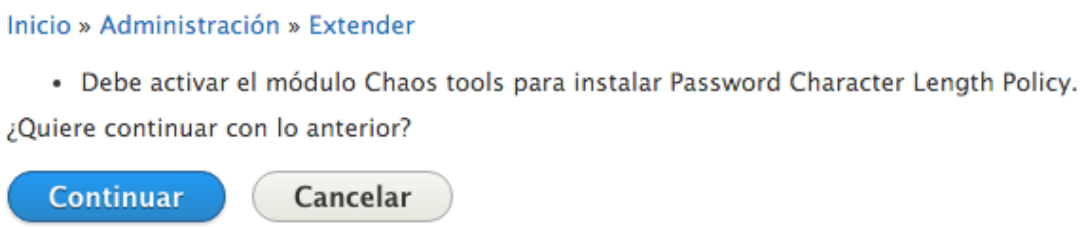
14.4. PASSWORD POLICY[9]

181. El módulo que instalaremos a continuación nos permitirá definir un conjunto de restricciones que se deben cumplir antes de que se acepte un cambio de contraseña en el sistema. Cada restricción tiene un parámetro que contiene el número mínimo de condiciones válidas que deben cumplirse.

182. Una vez instalado el paquete original, accederemos al menú "Extender" y seleccionaremos todos los módulos para instalar de los que depende:



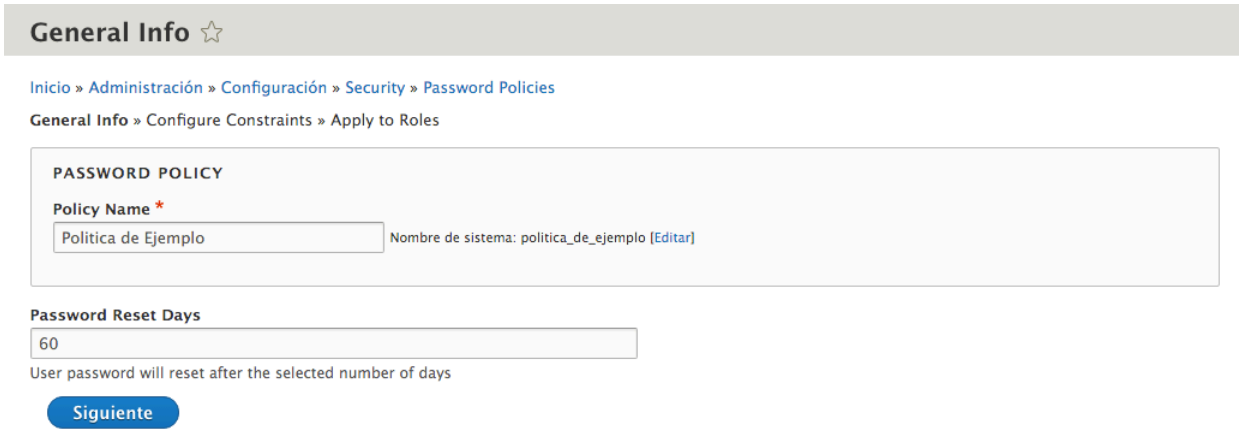
183. Cuando el sistema nos pregunte si deseamos instalar el módulo "Chaos tools", pulsaremos sobre Continuar, ya que es una dependencia necesaria para el correcto funcionamiento.



184. Una vez finalizado el proceso de instalación, podremos crear nuestra nueva política desde "Configuracion"->"Password Policy". Una vez dentro, pulsaremos sobre "Add Policy":

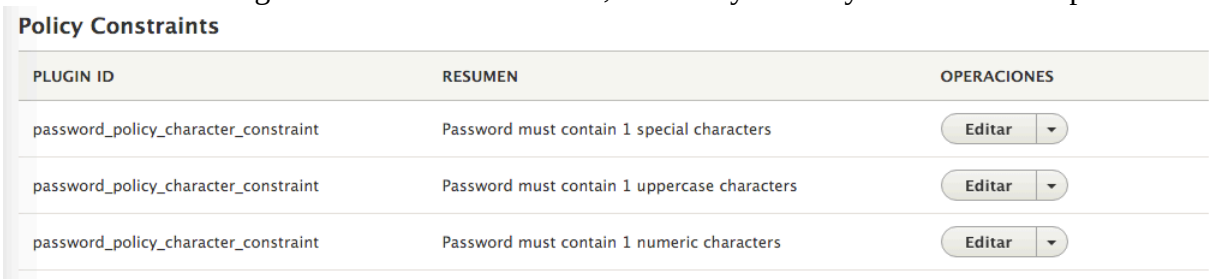
185. El primer valor que tendremos que asignar será un nombre para esta nueva política. En nuestro caso será "Política de Ejemplo" y forzaremos al usuario a cambiar la contraseña cada 60 días, introduciendo el valor en el campo inferior:

[9] **PASSWORD POLICY:** https://www.drupal.org/project/password_policy



186. En la pantalla a continuación podremos implementar las restricciones que deseemos para las contraseñas. En el desplegable de "Add Contraint" encontraremos tres opciones diferentes:

- *Password character type*: nos permite seleccionar el número de valores de cada clase que deben ser introducidos para satisfacer la política. Podremos elegir entre: mayúsculas, minúsculas, números y caracteres especiales. En nuestro ejemplo, forzaremos a que las contraseñas contengan al menos un número, una mayúscula y un carácter especial:

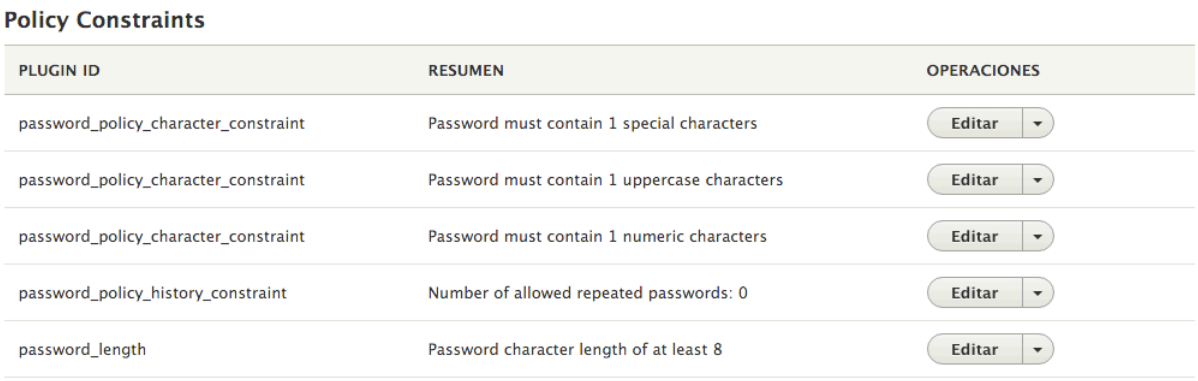


Policy Constraints

PLUGIN ID	RESUMEN	OPERACIONES
password_policy_character_constraint	Password must contain 1 special characters	Editar
password_policy_character_constraint	Password must contain 1 uppercase characters	Editar
password_policy_character_constraint	Password must contain 1 numeric characters	Editar

- *Password history*: nos permitirá establecer el valor máximo de veces que un usuario puede repetir su contraseña. El valor 0 implica que un usuario no podrá repetir nunca una contraseña anterior.
- *Password character length*: finalmente, podremos seleccionar el tamaño mínimo o máximo para las contraseñas del sistema.

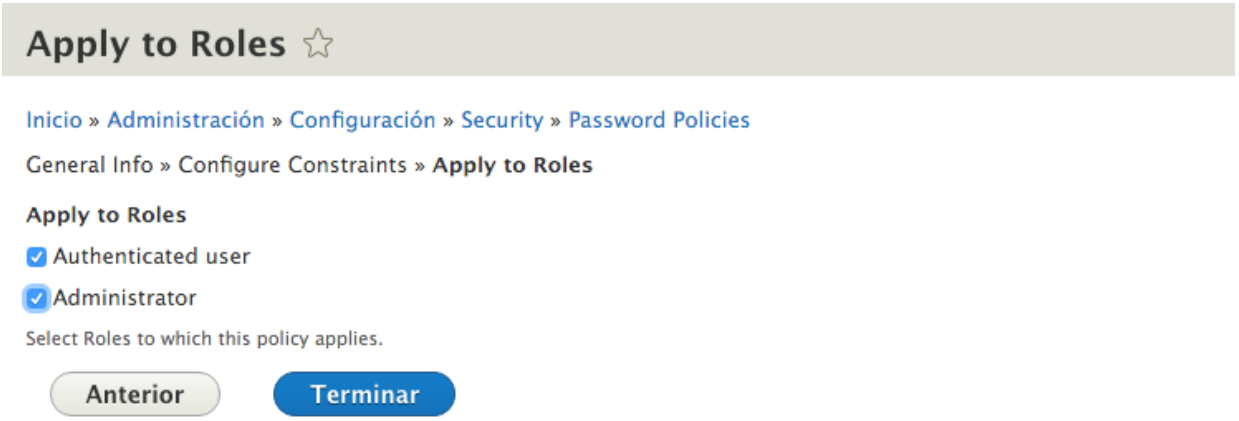
187. Como veremos en la imagen a continuación, nuestra política de prueba ha añadido además que los usuarios no pueden repetir contraseña y que el tamaño mínimo de esta debe ser de al menos 8 caracteres



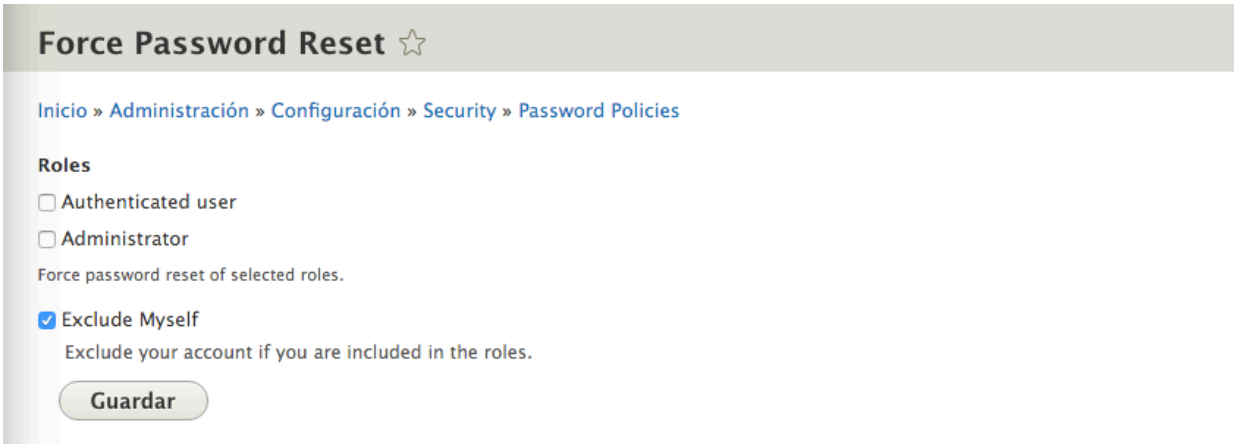
Policy Constraints

PLUGIN ID	RESUMEN	OPERACIONES
password_policy_character_constraint	Password must contain 1 special characters	Editar
password_policy_character_constraint	Password must contain 1 uppercase characters	Editar
password_policy_character_constraint	Password must contain 1 numeric characters	Editar
password_policy_history_constraint	Number of allowed repeated passwords: 0	Editar
password_length	Password character length of at least 8	Editar

188. Cuando tengamos nuestra política lista, pulsaremos sobre continuar y a continuación podremos seleccionar los roles a los que aplica. Podemos generar diferentes políticas según el rol, introduciendo restricciones diferentes en función de las necesidades de seguridad de cada uno de ellos:



189. Finalmente, otra característica interesante del módulo "Password Policy" es la de forzar al usuario a cambiar la contraseña en su primer acceso al sistema. Para activar esta opción, accederemos de nuevo sobre "Configuración"->"Password policies" y pulsaremos el botón de "Force Password Reset". Dentro de la nueva pantalla nos mostrará los roles a los que es posible asignar esta nueva función, que es recomendable para todos ellos:



NOTA
Las políticas de contraseñas solo aplicarán a los cambios que sean realizados a través del interfaz web de Drupal. Cualquier cambio realizado de otra forma, como con Drush, web services etc. no estará ligado a las restricciones impuestas por el módulo.

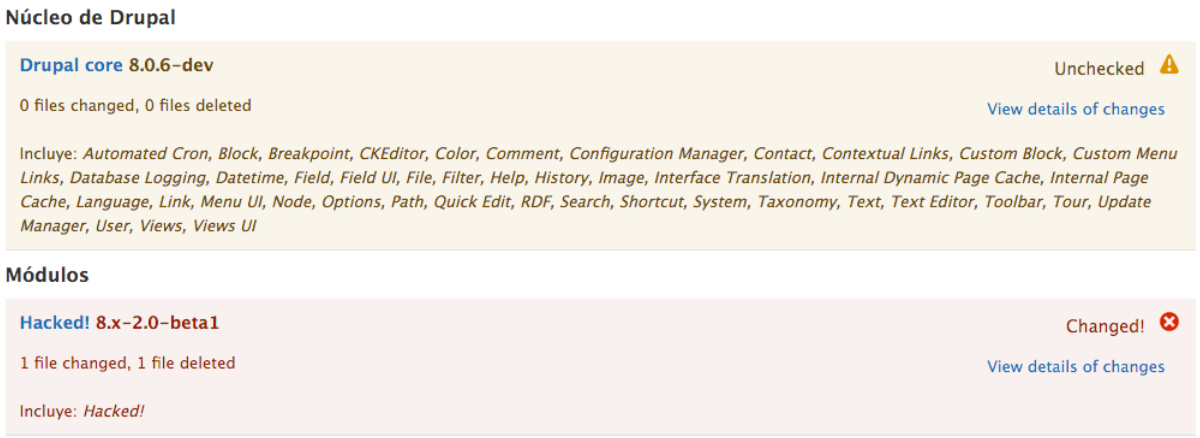
14.5. HACKED[10]

190. El funcionamiento de este módulo es sencillo, ya que explora nuestra instalación de Drupal, con los temas y módulos activos, los descargará de nuevo y comprobará si existe algún tipo de modificación dentro de los ficheros originales.

[10] **HACKED:** https://www.drupal.org/project/hacked

191. Existen módulos similares como "md5check", "File integrity change" o "Sentry", pero dado que ninguno de ellos tiene versión disponible para Drupal 8 en el momento de escritura de esta guía, utilizaremos "Hacked".

192. Una vez realizada la instalación sobre nuestro Drupal, podremos acceder a la configuración desde "Administración"->"Informes"->"Hacked". Nos mostrará una pantalla con los informes para cada uno de los módulos, temas y el core del sistema, con la información correspondiente de posibles cambios:



193. Pulsando sobre los informes, accederemos a una nueva pantalla que nos mostrará con exactitud que ficheros han sido modificados, agregados o eliminados:

NOTA
Será necesario comprobar frecuentemente este módulo, ya que puede indicarnos que ficheros del sistema han sufrido una modificación no autorizada, que podría ser indicativo de una posible intrusión en el servidor, con la consecuente modificación en el sistema para robar credenciales, atacar los equipos de visitantes o usuarios registrados, o incluso mantener una puerta trasera para acceder de forma remota en cualquier momento.

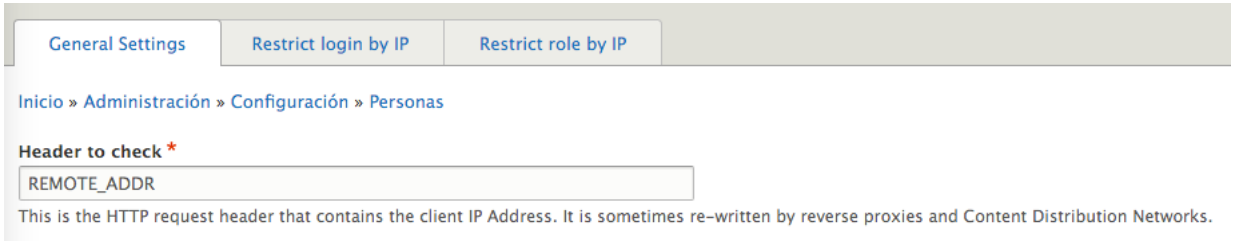
14.6. RESTRICT LOGIN OR ROLE ACCESS BY IP ADDRESS[11]

194. Este módulo nos proporciona una nueva funcionalidad que nos va a permitir restringir el acceso de los usuarios a una dirección IP o a un rango específico. Actualmente hay dos características implementadas, restricción por IP y restricción por rol.

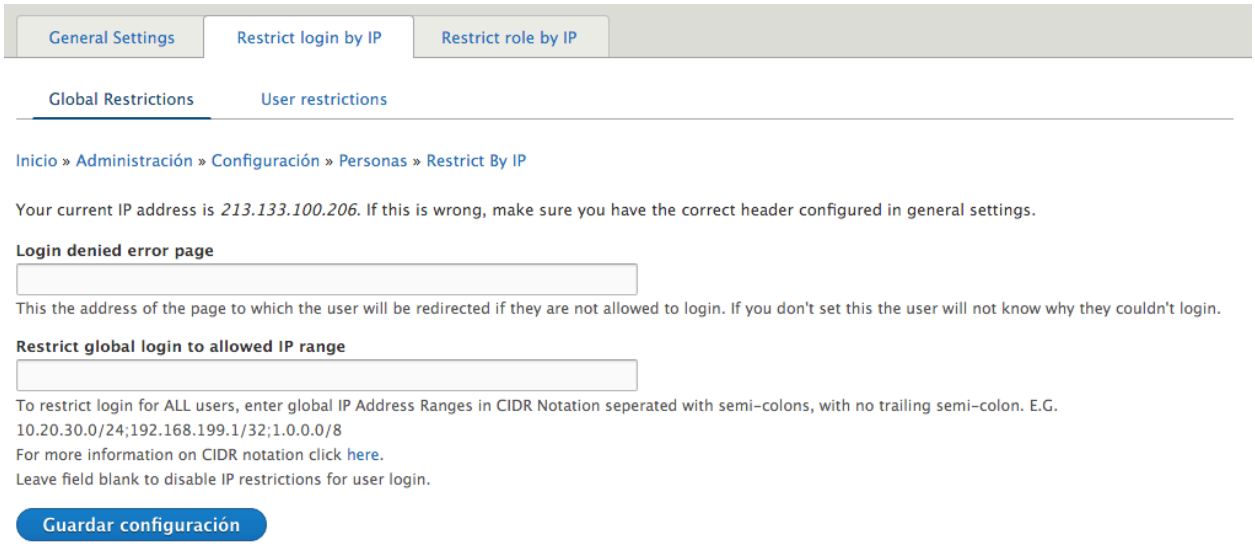
195. Una vez instalado en el sistema, podremos acceder a su configuración desde "Configuración"->"Restrict by IP".

[11] **RESTRICT LOGIN OR ROLE ACCESS BY IP ADDRESS:** https://www.drupal.org/project/restrict_by_ip

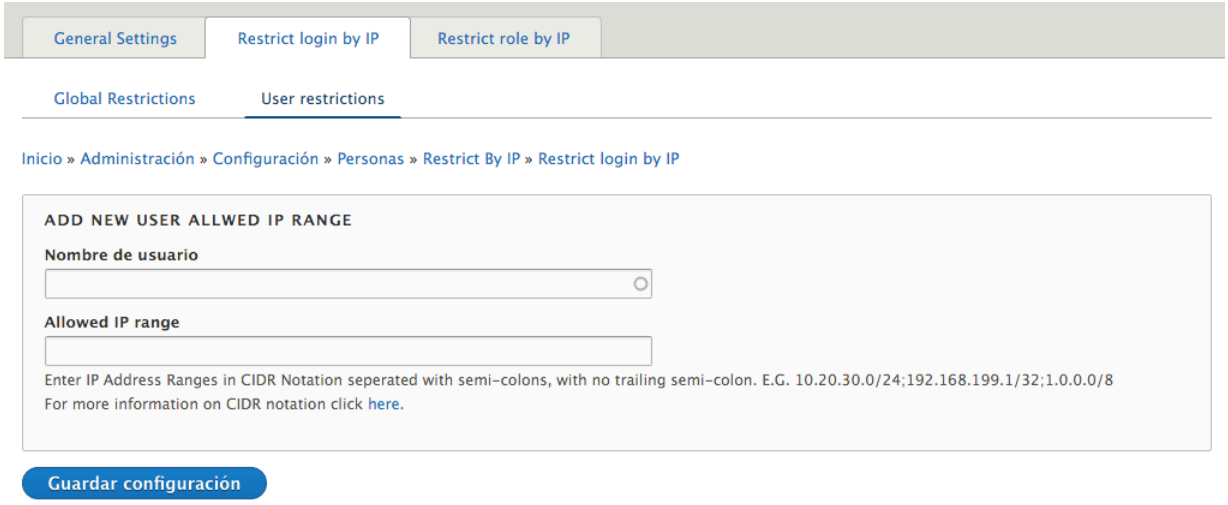
196. La pestaña de "General Settings" nos permitirá especificar la cabecera HTTP que contiene la dirección IP que desea ser analizada. Por defecto, mantendremos el valor "REMOTE_ADDR", pero es posible modificarla si el servidor se encuentra detrás de un proxy inverso o un CDN (Content Distribution Network):



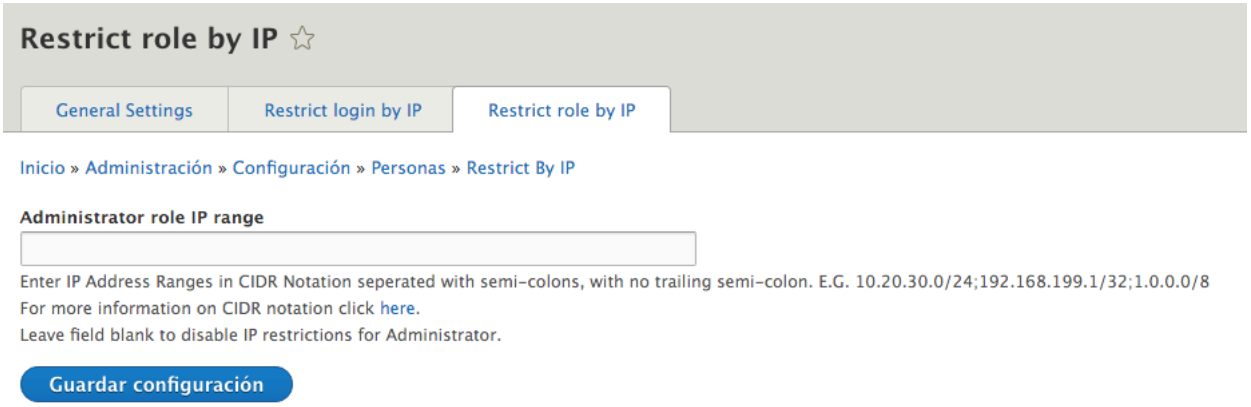
197. La siguiente pestaña es "Restrict login by IP". Cuando activemos esta opción, el usuario sólo será capaz de loguearse en el sistema desde la dirección o direcciones que hayamos especificado:



198. También es posible especificar un rango de direcciones IP desde las que solamente se puede loguear un usuario, incluido el user #1. Cuando se produzca un intento de acceso de una dirección no autorizada, el usuario será automáticamente redirigido a la página que hayamos especificado:



199. La última pestaña de configuración será "Restrict role by IP", y nos permitirá especificar una lista blanca de direcciones IP basado en roles. Esta restricción no afecta a la capacidad del usuario para loguearse en el sistema. Esta restricción de roles afecta a todos los roles del sistema menos al "usuario anónimo" y al "usuario autenticado":



14.7. FILTRO SPAMSPAN[12]

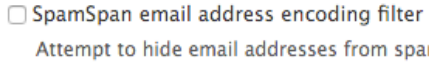
200. El módulo "Spamspan" permite ofuscar las direcciones de correo electrónico publicadas en las diferentes páginas de Drupal para evitar que los bots de spam puedan reconocerlas y almacenarlas para envíos no deseados.

201. Se trata de un pequeño código, de 2KB, escrito en JavaScript, que mostrará las direcciones de forma más segura, incluso si el navegador no soporta esta tecnología. Además, es compatible con la mayoría de los navegadores (más del 99% de los navegadores del mercado), entre los que destacan:

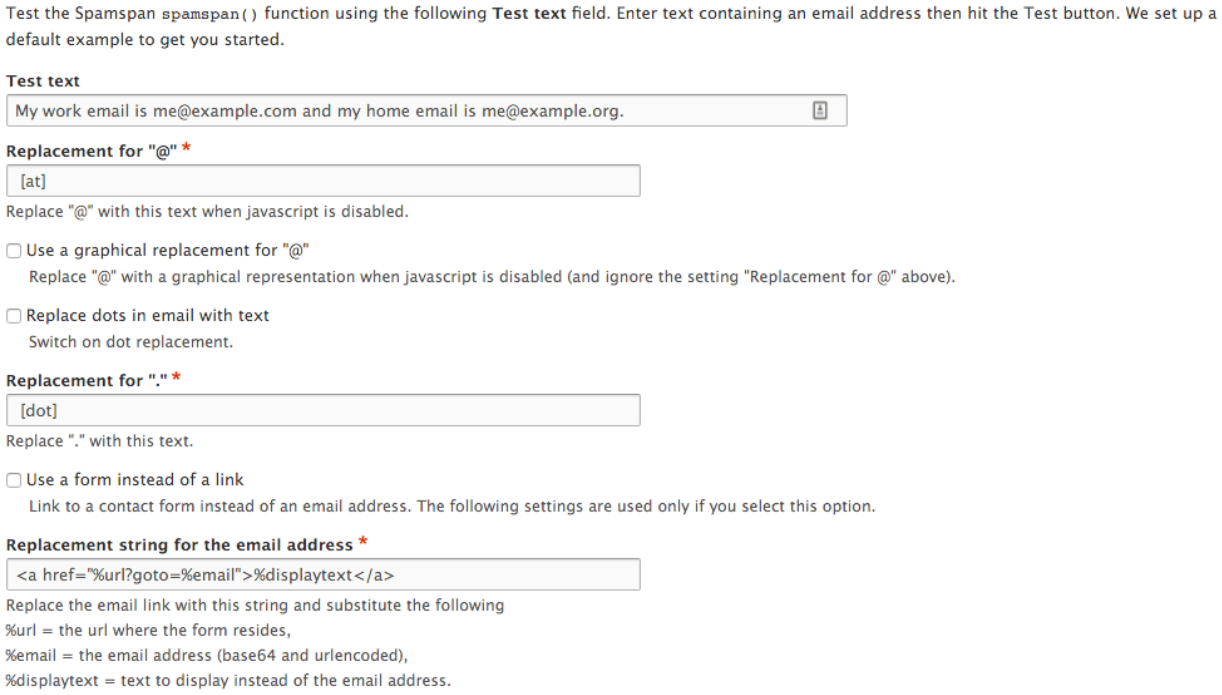
- AOL
- Blazer
- Camino
- Firefox
- Internet Explorer
- Konqueror
- Mozilla
- Netscape
- Opera
- Safari
- Chrome

[12] **SPAMSPAM:** https://www.drupal.org/project/spamspan

202. Tras la instalación del módulo desde el repositorio oficial de Drupal, nos dirigiremos a "Administración"->"Configuración"->"Autoría del contenido"->"Formato y editores de texto". Dentro de la configuración de formatos de texto, debemos acceder a cada formato donde deseamos habilitar el filtro, y seleccionar "Configurar". Una vez dentro, marcaremos la casilla correspondiente:



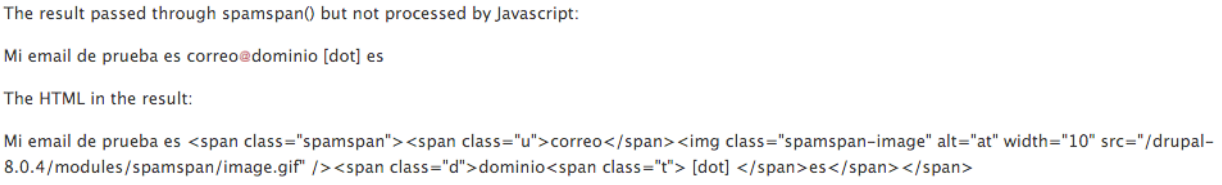
203. Para la configuración global del módulo, accederemos de nuevo al menú anterior y pulsaremos sobre la pestaña "Spamspan test page":



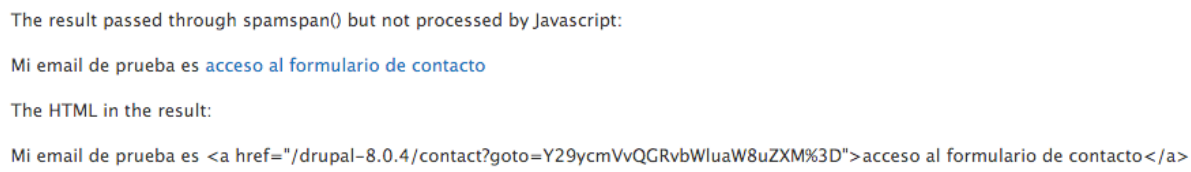
204. Las opciones más relevante que podremos modificar es la forma en la que Spamspan modifica las direcciones de correo:

- *Replacemente for "@":* es el texto por el que se sustituirá el carácter @ cuando estemos en presencia de un navegador sin soporte para Javascript. Por defecto se sustituye por [at]
- *Use a graphical replacement for "@":* nos permite sustituir el carácter @ por una imagen con la representación gráfica, que no muestra texto
- *Replace dots in email with text*: permite sustituir los . encontrados en una dirección de correo por el texto deseado, que por defecto será [dot] y se encuentra en el campo de texto a continuación.

205. Podemos ver una muestra del resultado pulsando sobre el botón inferior "Prueba":



206. La última opción de modificación es "Use a form instead of a link", que transformará la dirección de correo electrónico en un formulario que al pulsar nos permitirá completar para enviar el correo, tal y como se muestra a continuación:



207. Que nos redirigirá a un formulario similar al siguiente:

14.8. ANTIVIRUS CLAMAV[13]

208. Este módulo nos va a permitir escanear los ficheros que los usuarios suban a nuestro sitio para comprobar que no se encuentren infectados con un virus, bloqueando y poniendo en cuarentena los ficheros sospechosos.

209. Este módulo sólo instala los mecanismos necesarios para interactuar con Drupal, por lo que primero necesitaremos instalar ClamAV en nuestro sistema. Para sistemas corriendo sobre Debian o Ubuntu, utilizaremos el comando "apt-get":

[13] **CLAMAV:** https://www.drupal.org/project/clamav

```
$ apt-get install clamav
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesarios.
  php-console-table
Use 'apt-get autoremove' to remove it.
Se instalarán los siguientes paquetes extras:
  clamav-base clamav-freshclam libclamav6
Paquetes sugeridos:
  clamav-docs libclamunrar6
Se instalarán los siguientes paquetes NUEVOS:
  clamav clamav-base clamav-freshclam libclamav6
0 actualizados, 4 se instalarán, 0 para eliminar y 121 no actualizados.
Necesito descargar 3.522 kB de archivos.
Se utilizarán 13,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
Des:1 http://es.archive.ubuntu.com/ubuntu/ trusty-updates/main libclamav6 amd64 0.98.7+dfsg-0ubuntu0.14.04.1 [3.218 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu/ trusty-updates/main clamav-base all 0.98.7+dfsg-0ubuntu0.14.04.1 [110 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu/ trusty-updates/main clamav-freshclam amd64 0.98.7+dfsg-0ubuntu0.14.04.1 [107 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu/ trusty-updates/main clamav amd64 0.98.7+dfsg-0ubuntu0.14.04.1 [87,3 kB]
Descargados 3.522 kB en 0seg. (6.548 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete libclamav6 previamente no seleccionado.
(Leyendo la base de datos ... 67012 ficheros o directorios instalados actualmente.)
Preparing to unpack .../libclamav6_0.98.7+dfsg-0ubuntu0.14.04.1_amd64.deb ...
Unpacking libclamav6 (0.98.7+dfsg-0ubuntu0.14.04.1) ...
Seleccionando el paquete clamav-base previamente no seleccionado.
Preparing to unpack .../clamav-base_0.98.7+dfsg-0ubuntu0.14.04.1_all.deb ...
Unpacking clamav-base (0.98.7+dfsg-0ubuntu0.14.04.1) ...
Seleccionando el paquete clamav-freshclam previamente no seleccionado.
Preparing to unpack .../clamav-freshclam_0.98.7+dfsg-0ubuntu0.14.04.1_amd64.deb ...
Unpacking clamav-freshclam (0.98.7+dfsg-0ubuntu0.14.04.1) ...
Seleccionando el paquete clamav previamente no seleccionado.
Preparing to unpack .../clamav_0.98.7+dfsg-0ubuntu0.14.04.1_amd64.deb ...
Unpacking clamav (0.98.7+dfsg-0ubuntu0.14.04.1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Configurando libclamav6 (0.98.7+dfsg-0ubuntu0.14.04.1) ...
Configurando clamav-base (0.98.7+dfsg-0ubuntu0.14.04.1) ...
Configurando clamav-freshclam (0.98.7+dfsg-0ubuntu0.14.04.1) ...
 * Starting ClamAV virus database updater freshclam
Processing triggers for ureadahead (0.100.0-16) ...
Configurando clamav (0.98.7+dfsg-0ubuntu0.14.04.1) ...
Processing triggers for libc-bin (2.19-0ubuntu6.6) ...
```

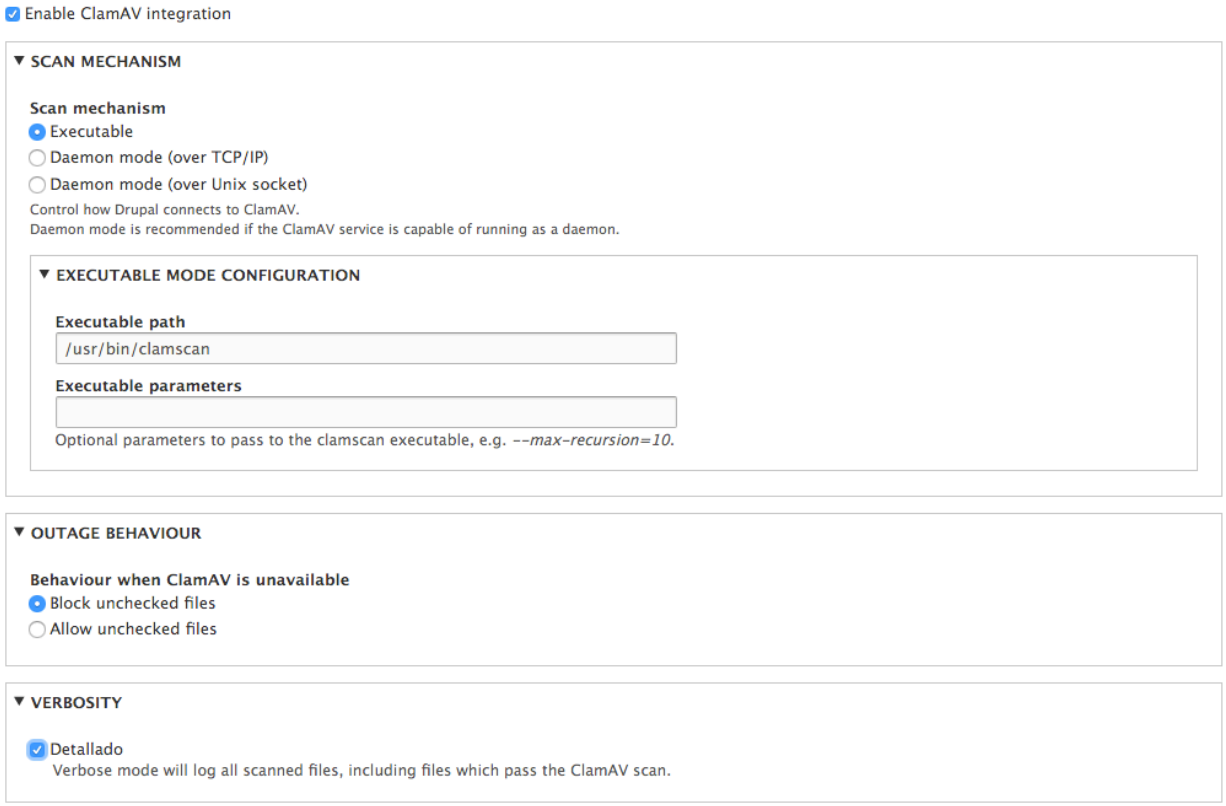
210. Para sistemas corriendo sobre Redhat / CentOS, primero activaremos el repositorio EPEL (Extra Packages for Enterprise Linux) y a continuación ejecutaremos:

$ yum install clamav
$ yum install clamd

211. Ahora actualizaremos las firmas existentes con el comando:

$ freshclam -v

212. Una finalizada la instalación y actualización del antivirus, procedemos a instalar el módulo en Drupal y accedemos a su configuración en "Configuración" -> "ClamAV configuration":



- *Enable ClamAV integration*: activa o desactiva la funcionalidad de escaneo de ficheros
- *Scan mechanism*: permite seleccionar la forma de ejecución y comunicación con el motor de antivirus. Nos presenta tres alternativas:
    - *Executable*: lanza directamente la ejecución sobre línea de comandos, para ello sólo tenemos que especificar la ruta donde "clamscan" ha sido instalado. En caso de desconocerla, ejecutaremos los siguientes comandos:

      $ updatedb; locate clamscan

    - *Daemon mode (over TCP/IP)*: la conexión se realizará sobre un socket vía TCP/IP. Esta opción es interesando cuando el motor de antivirus se encuentre en un servidor remoto, o sea completamente necesaria la conexión por TCP/IP al equipo local. Para ello necesitaremos añadir las siguientes líneas al fichero /etc/clamav/clamd.conf:

      TCPSocket 3310
      TCPAddr 127.0.0.1

213. En este caso, será necesario prestar especial atención para evitar que las comunicaciones impliquen un riesgo de seguridad para alguno de los sistemas involucrados.

    - *Daemon mode (over Unix socket)*: permite la comunicación a través de un socket Unix, y tan sólo tendremos que indicar la ruta donde ClamAV está trabajando. En caso de haber modificado la configuración original, podremos obtener la ruta ejecutando el siguiente comando:

      $ cat /etc/clamav/clamd.conf | grep LocalSocket

- *Outage behaviour*: permite indicar al administrador si se deben bloquear los ficheros infectados, o permitir su carga igualmente

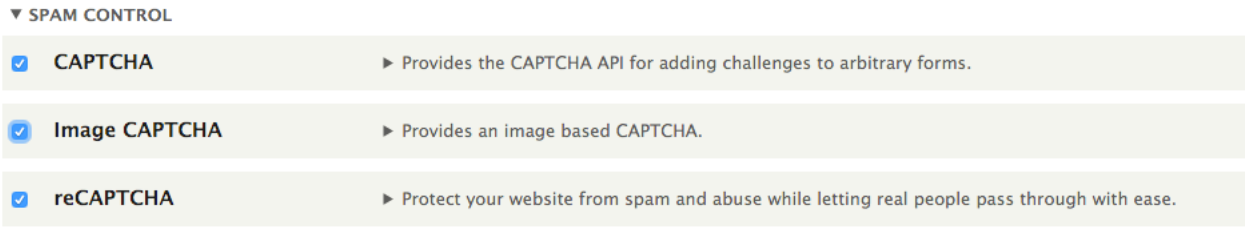
- *Verbosity*: nos permitirá incluir en el log del sistema toda la información de los ficheros analizados, así el resultado del análisis

14.9. CAPTCHA[14]

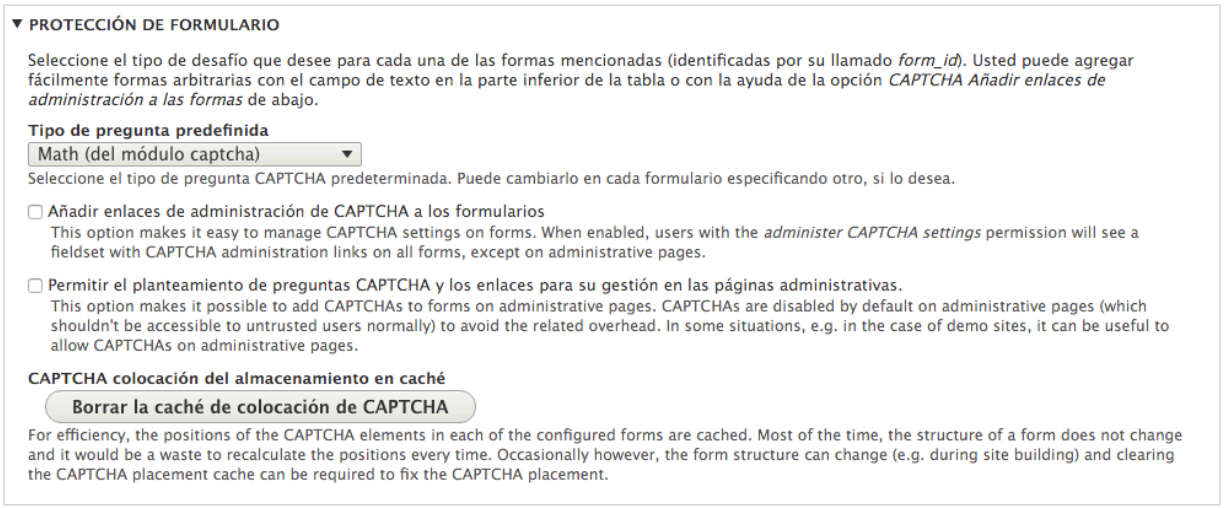
214. Un CAPTCHA es una prueba desafío-respuesta, que a menudo se encuentra insertado dentro de los formularios web para determinar si un usuario es humano. El propósito de estos captcha es bloquear el envío de spam, a través de estos formularios, por bots automatizados, que colocan el contenido no deseado en todas las partes del sitio que pueden.

215. El módulo CAPTCHA proporciona esta función para prácticamente cualquier usuario que disponga de formularios web en un sitio Drupal. Además, instalaremos el módulo reCHAPTCHA, que utiliza el sistema mejorado de Google.

216. Una vez descargados los ficheros correspondientes en el sistema, procederemos a instalar los siguientes módulos:



217. Para acceder a su administración, pulsaremos sobre "Configuración"->"CAPTCHA module settings":

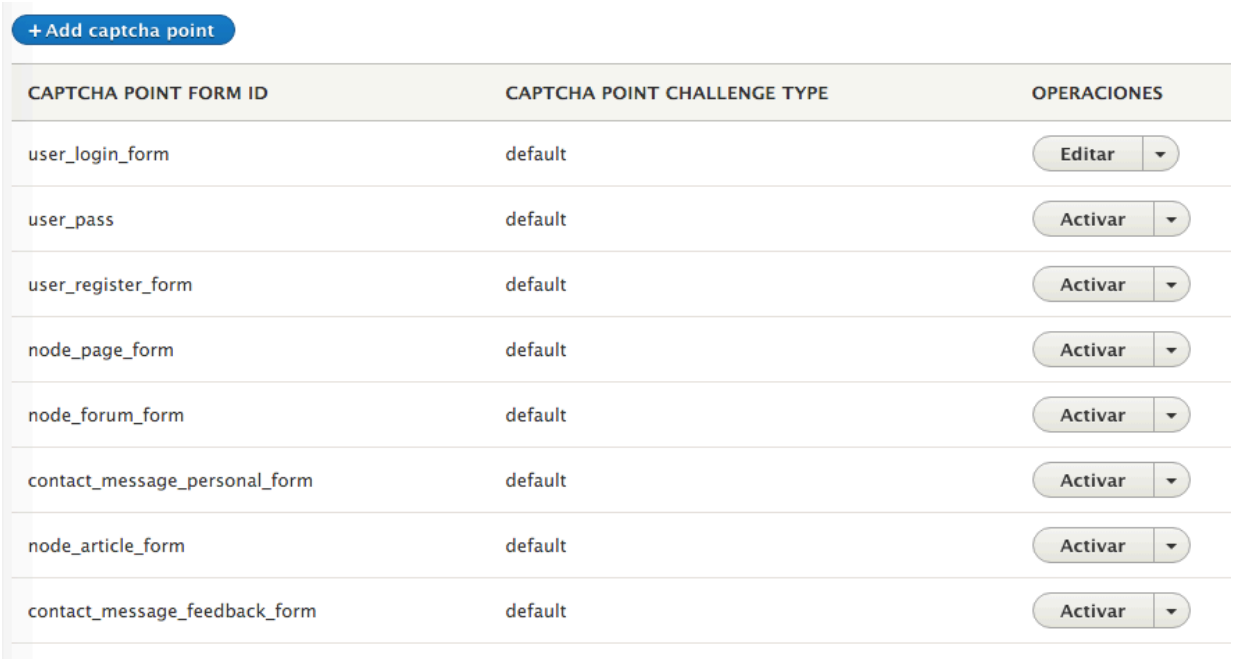


218. Lo primero que deberemos seleccionar es el tipo de pregunta predefinida que deseamos incluir en nuestro sitio. Existen tres opciones disponibles: Math (del módulo captcha), Image (del módulo image_captcha) y reCAPTCHA (del módulo recaptcha), cuyos ejemplos veremos en la imagen a continuación, en la pestaña "CAPTCHA Settings":

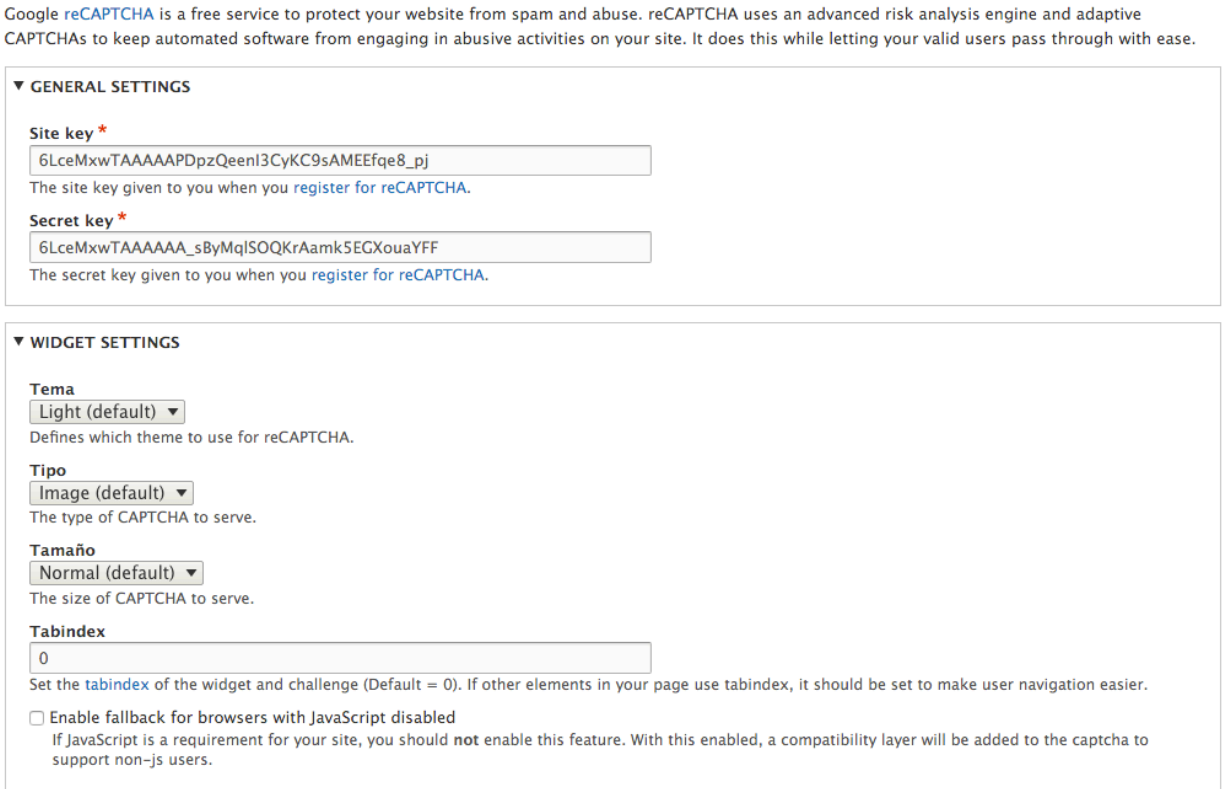
[14] **CAPTCHA:** https://www.drupal.org/project/captcha

- *Añadir enlaces de administración de CAPTCHA a los formularios*: esta opción permite al administrador manejar de forma más eficiente la inserción de captchas en los formularios, dado que cuando éste visite uno, se mostrará un campo que permitirá su configuración (salvo en las páginas de administración)
- *Permitir el planteamiento de preguntas CAPTCHA y los enlaces para su gestión en las páginas administrativas*: permite incluir el sistema de captcha en las páginas de administración de Drupal. Esta opción será desactivada, debido a que esta zona debería estar protegida y no ser accesible a usuarios sin privilegios, aunque puede ser de utilidad en el caso de sitios de prueba
- *Borrar la caché de colocación de CAPTCHA*: permite borrar la caché del módulo, debido a posibles modificaciones en los formularios durante la construcción del sitio
- *Añadir una descripción a la pregunta CAPTCHA*: permite añadir una descripción de texto para explicar la finalidad del sistema al usuario
- *Validación predefinida de CAPTCHA*: permite especificar si el sistema de validación diferenciará entre mayúsculas y minúsculas
- *Activar estadísticas y Registrar respuestas erróneas*: permite realizar un seguimiento del sistema de CAPTCHA, tanto en validaciones correctas como en intentos erróneos, que serán incluidos de forma automática en el log del sistema.

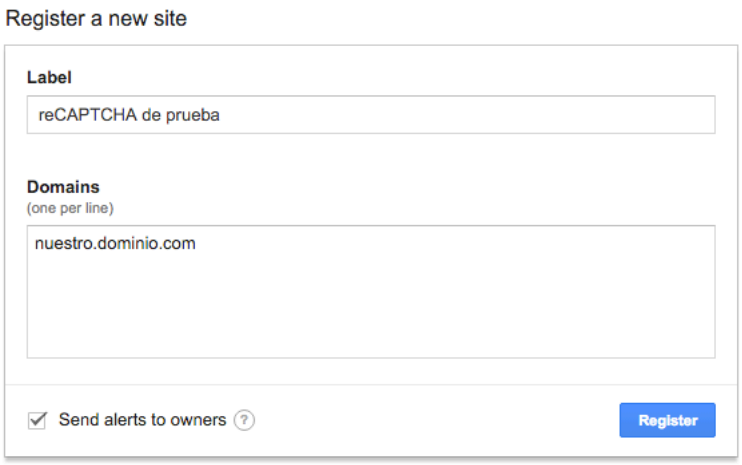
219. Dentro de la pestaña "CAPTCHA Points" encontraremos los diferentes formularios donde podemos introducir nuestro sistema de validación. Se mostrará una lista de formularios disponibles en el sistema, donde podremos activarlos de forma individual, añadir nuevos, o editar cada uno de ellos para especificar otro sistema de CAPTCHA diferente al que está configurado por defecto:



220. Finalmente, encontraremos la pestaña "reCAPTCHA", donde deberemos configurar nuestras claves del sistema de Google, además de poder modificar el tema utilizado por defecto, si deseamos un sistema por imagen o por audio, además del tamaño del widget que será incluido:



221. Los campos "Site key" y "Secret key" deben ser obligatoriamente completados para el correcto funcionamiento. Para obtenerlos, visitaremos la URL "http://www.google.com/recaptcha/admin", e introduciremos en la pantalla mostrada la descripción de nuestro sitio así como los dominios donde el sistema funcionará:



222. Una vez hayamos pulsado sobre "Register", accederemos a la página de configuración del sitio donde obtendremos los valores que necesitamos insertar en la configuración del módulo en Drupal:

14.10. SECURITY REVIEW[15]

223. El módulo "Security Review" nos permite realizar un chequeo automatizado de posibles problemas de seguridad y errores que hayamos cometido durante la configuración de nuestro sitio Drupal, y que puede convertirlo en inseguro.

224. Entre los chequeos que realiza cabe destacar:

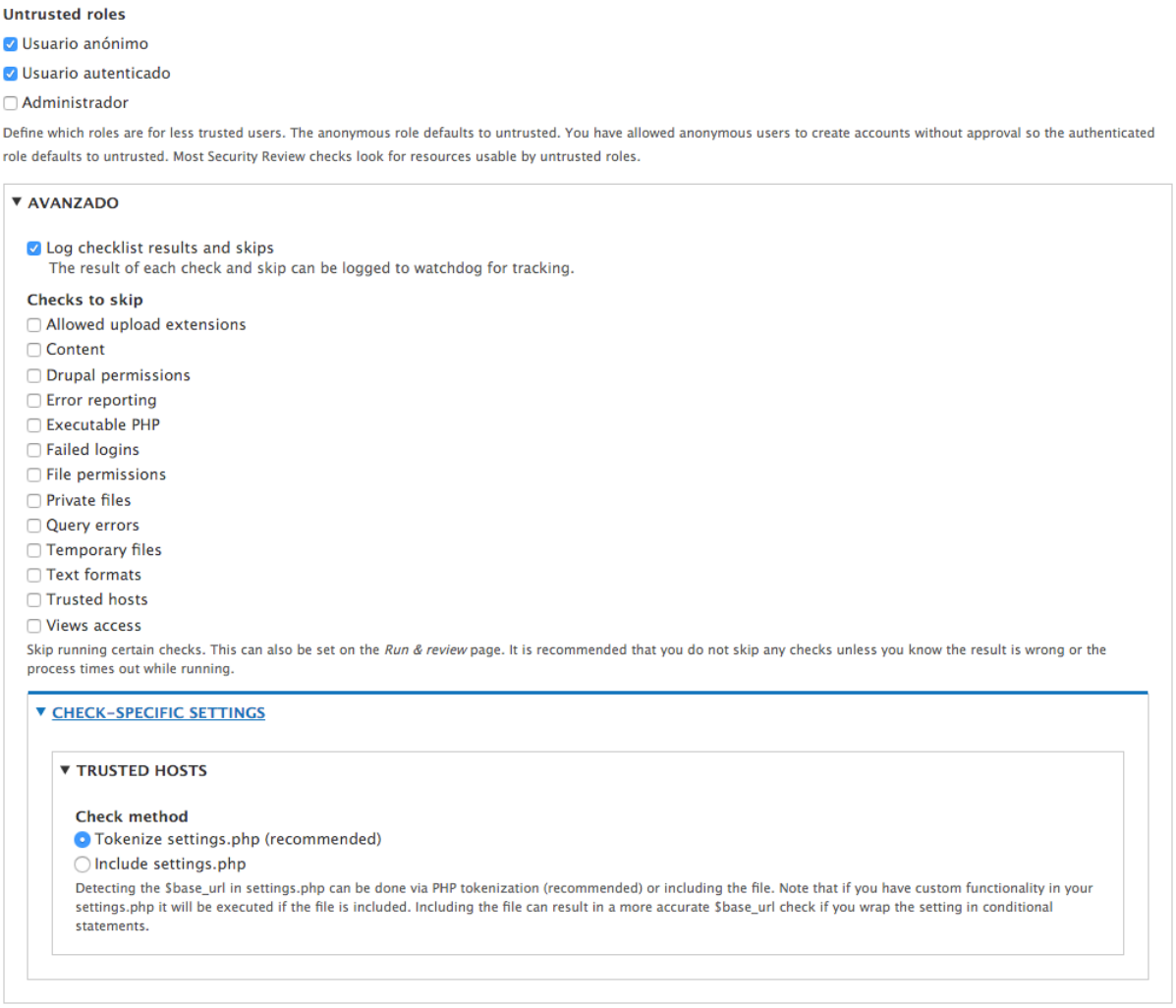
- Permisos correctos de los ficheros del sistema y protección contra ejecución de código arbitrario
- Comprobación de etiquetas peligrosas y protección contra ataques XSS
- Eliminación de código PHP y Javascript en contenido
- Protección contra fuga de información
- Protección contra la carga de ficheros maliciosos
- Protección contra intentos de ataque SQLi
- Comprobación de permisos de administración correctos
- Gestión de contraseñas inseguras
- Protección contra ejecución de código PHP

[15] **SECURITY REVIEW:** https://www.drupal.org/project/security_review

- Protección contra ataques de phishing con Trusted Hosts

NOTA
Es necesario destacar que este módulo no realizará cambios de forma automatizada en nuestra instalación, por lo que deberá ser utilizado como un *checklist* que deberemos utilizar para más tarde securizar los puntos débiles detectados de forma manual, y acorde a las necesidades de nuestro sistema.

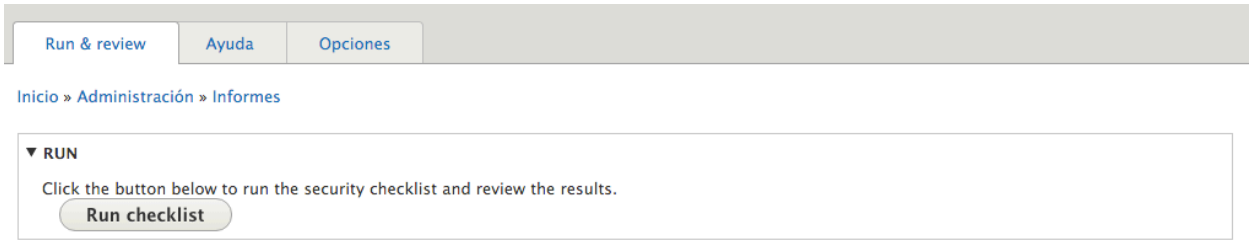
225. Una vez realizada la instalación y activación del módulo, podremos encontrarlo en la sección "Configuración" de nuestro sitio. Al acceder nos encontraremos la siguiente pantalla:



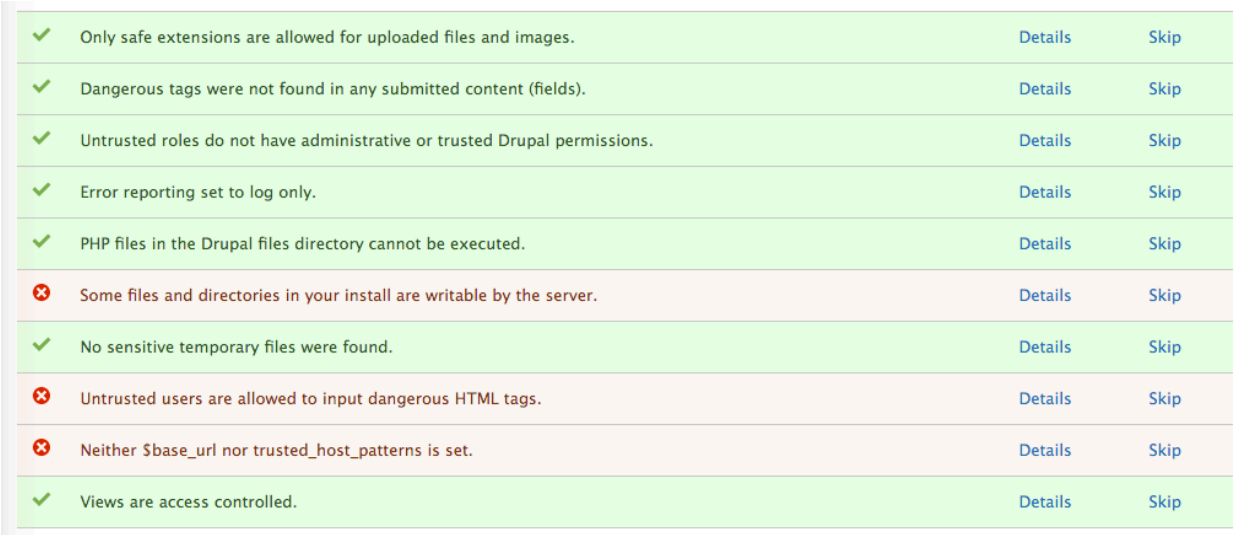
226. La configuración por defecto mostrará que tanto "Usuario anónimo" como "Usuario autenticado" no son roles de confianza, y que sólo se considerará de confianza el administrador del sitio.

227. Mantendremos, en la sección "Avanzado", todos los chequeos posibles que van a realizarse, salvo que por necesidades concretas o posibles demoras de tiempo deseemos eliminar alguno y posteriormente pulsaremos el botón "Guardar configuración".

228. Para ejecutar el chequeo, pulsaremos sobre "Run & Review" en la barra superior y en el botón "Run checklist":

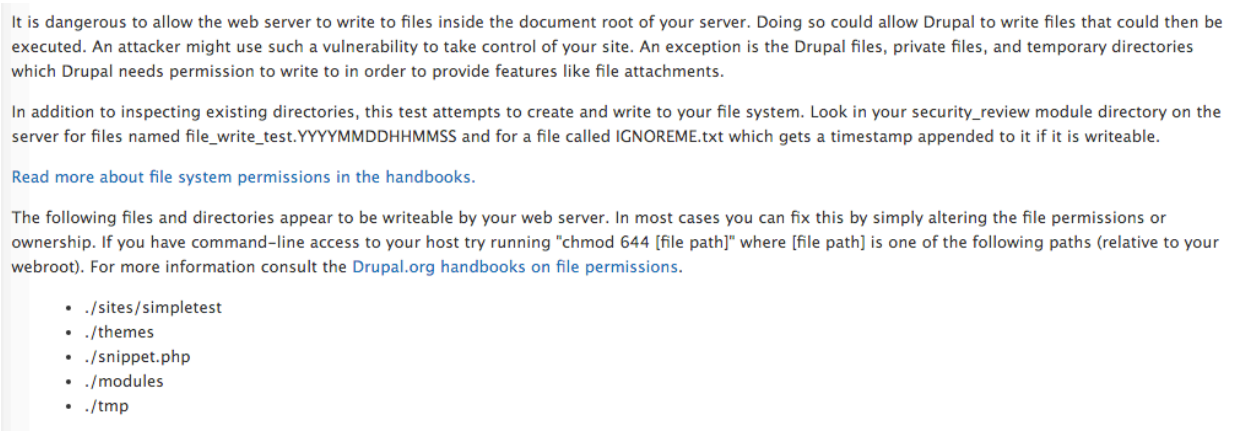


229. A continuación, una vez finalizado, podremos ver los resultados del escaneo, así como acceder a los detalles de los chequeos fallidos, como por ejemplo:



230. En este ejemplo de configuración insegura, vemos que existen tres problemas que requieren la atención directa del administrador. Como ejemplo, nos centraremos en "Some files and directories in your install are writable by the server".

231. El módulo detecta que existen una serie de ficheros inseguros en nuestra instalación, y al pulsar sobre "Details" nos mostrará aquellos que han sido detectado, así como la explicación:



232. Como vemos, existen una serie de ficheros y directorios que no disponen de los permisos correctos, por lo que deberemos configurarlos de forma correcta.

NOTA
Cada chequeo realizado por este módulo ha sido tratado a lo largo de la configuración segura de esta guía, por lo que será necesario acudir a cada punto correspondiente y realizar las tareas indicadas.

Este chequeo deberá ser lanzado después de haber implementado las medidas de seguridad indicadas para comprobar que está solucionado y no disponer de ningún error de configuración en ninguno de los puntos auditados por el módulo.

15. CREACIÓN Y RECUPERACIÓN DE BACKUPS

233. Es necesario realizar un correcto respaldo de los sitios en producción, ya que, a pesar de que los discos donde se almacena la información suelen ser bastantes seguros, están expuestos a fallos lógicos, ataques de terceros, errores humanos, cortes de luz etc. que ponen en peligro la información almacenada. Recuperar la información sin un adecuado respaldo es posible, pero puede llegar a ser un proceso lento y excesivamente costoso, por lo que muchos usuarios desisten de recuperarla.

234. Esta guía no es objeto de discusión sobre los diferentes métodos de almacenamiento de backup, que van desde un soporte físico como una memoria USB o DVD, hasta el servicio externo de una empresa.

235. Se recomienda tener las siguientes consideraciones generales en cuenta a la hora de realizar una copia de seguridad:

236. Identificar los datos críticos: No toda la información almacenada en un servidor es relevante. Es importante, durante la fase de planificación, que se tenga claro que información es la más importante, para no gastar tiempo, esfuerzo y espacio en copiar datos que no son relevantes.

237. Determinar la frecuencia adecuada: hay que determinar la periodicidad de los backup, en función de cada cuánto tiempo cambia nuestra información. Por ejemplo, si nuestros archivos cambian una vez en semana no tiene sentido hacer copias de seguridad diarias, ya que estaremos almacenando los mismos datos una y otra vez.

238. Sistemas de copia continua: lo ideal es que el backup esté permanentemente actualizado, es decir, que en caso de pérdida de la información podamos recuperar todo, incluso lo que haya sucedido sólo unos segundos antes del incidente.

239. Rápida recuperación: Prácticamente tan importante es la correcta gestión de una réplica de nuestra información como el uso de un mecanismo que nos permita su restauración en el menor espacio de tiempo posible.

240. Verificar los backups: Es aconsejable que cada cierto tiempo se compruebe que los datos que se almacenan en el backup son los correctos, y que se puede acceder a ellos sin ningún tipo de problema.

241. Recuperación granular: Puede que sea necesario recuperar tan sólo un archivo concreto, no toda su estructura, por lo que deberemos contar con esta posibilidad en la fase de planificación.

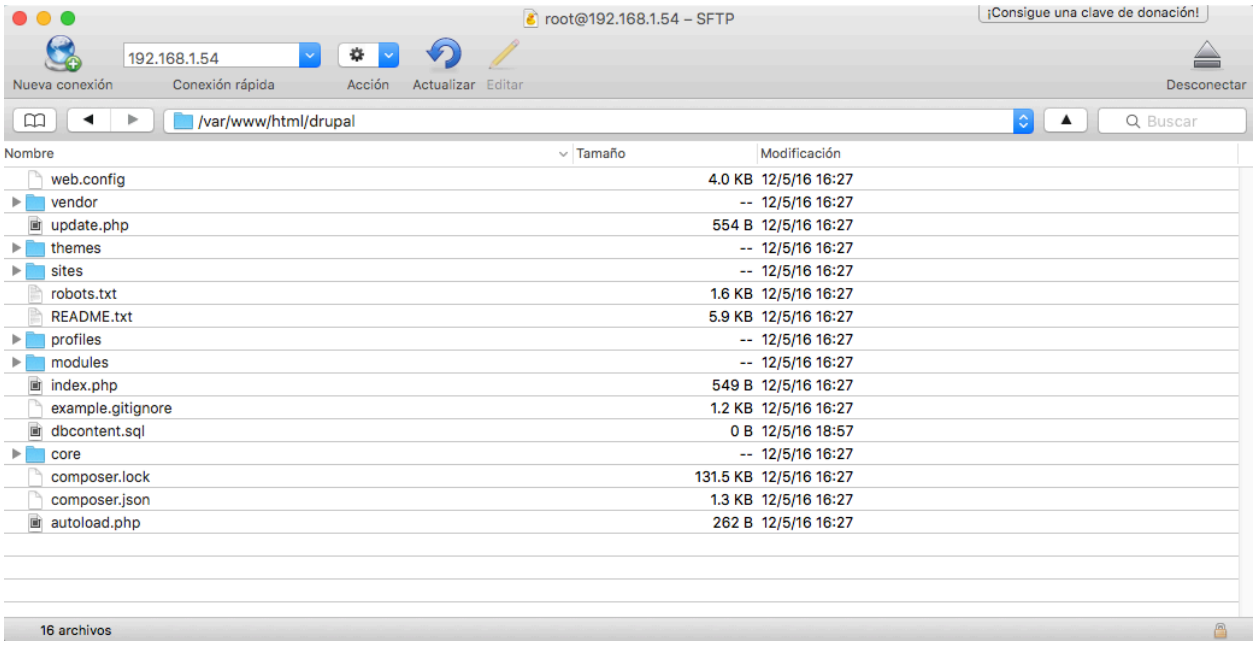
242. Externalizar una copia cifrada: Cuando estemos tratando con información de gran importancia o confidencialidad, se deberá considerar la posibilidad de realizar un segundo backup en un depósito seguro, fuera de las instalaciones donde se encuentra el servicio. De esta manera, las posibilidades de pérdida de información se verán reducidas al mínimo.

243. Destrucción de los backups: a la hora de destruir estas copias de seguridad es fundamental asegurarnos de que el proceso cumple con las leyes de protección de datos, así como asegurar que ningún tipo de información pueda caer en manos de un tercero o un posible atacante.

15.1. BACKUP VÍA FTP Y PHPMYADMIN

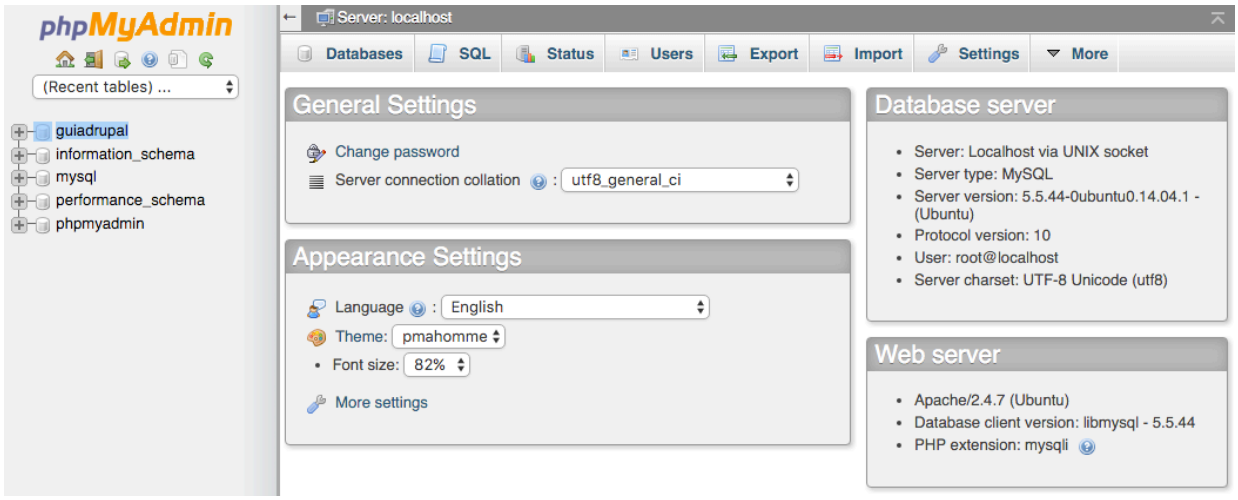
244. Las fases necesarias para realizar esta tarea serán las siguientes:

245. Copia de seguridad de los ficheros de Drupal: este proceso se realizará utilizando cualquier forma de copia de archivos, sea a un soporte físico externo, o a otra máquina utilizando FTP, SCP etc.

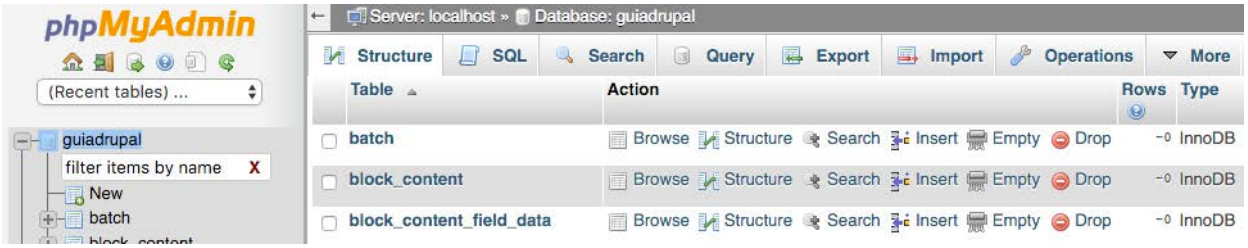


CYBERDUCK es uno de los clientes que permite FTP/SFTP/WebDav etc.

246. Copia de seguridad de la base de datos con phpMyAdmin: accederemos a nuestra instancia personal de phpMyAdmin, y seleccionaremos de la lista que se encuentra a la izquierda la base de datos que deseamos exportar, en nuestro caso 'guiadrupal'

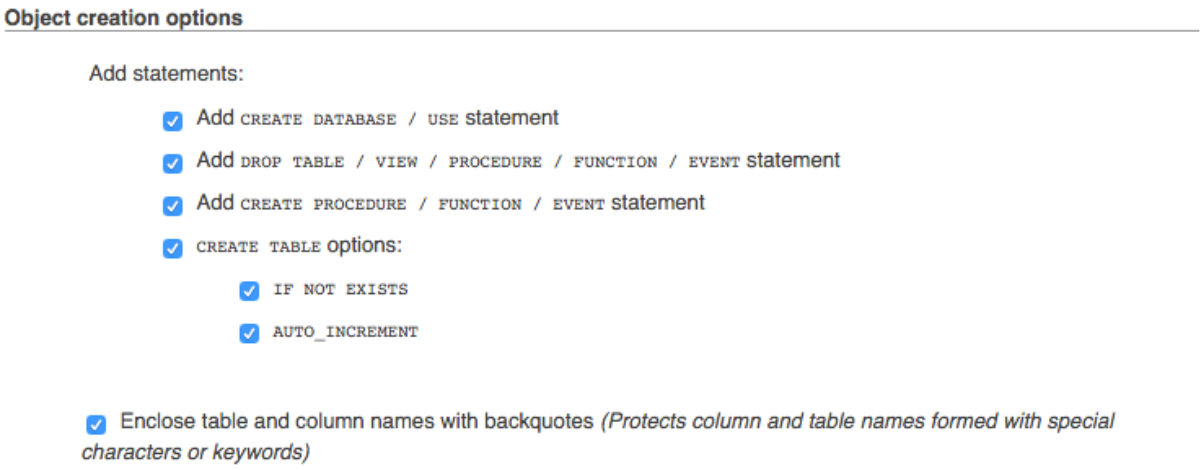


247. A continuación pulsamos sobre la pestaña "Export":



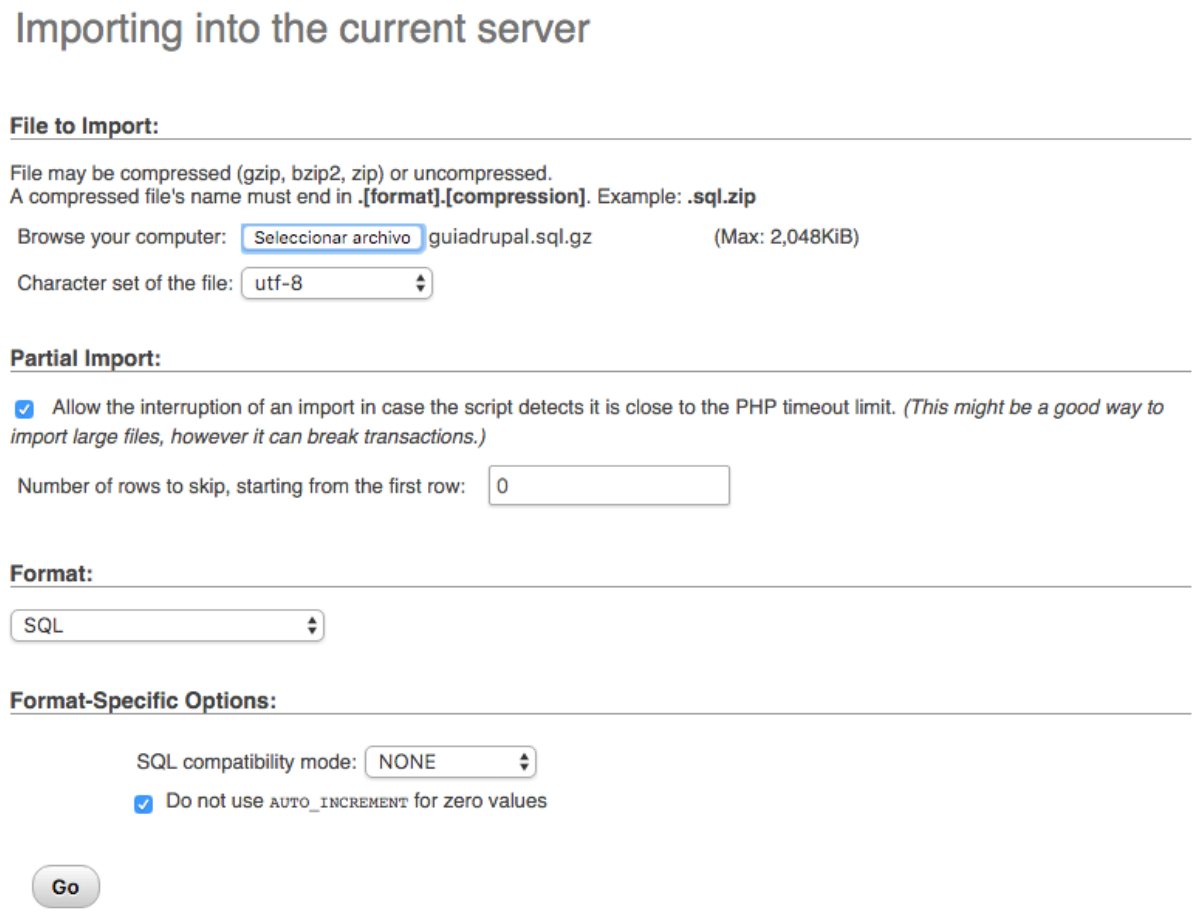
248. Una vez en la nueva pantalla, seleccionaremos el método "Custom" y pulsaremos sobre las siguientes opciones:

- *Tables*: seleccionamos todas
- *Output/Compression*: gzipped
- *Format*: SQL
- *Objetct creation options*: seleccionamos todas

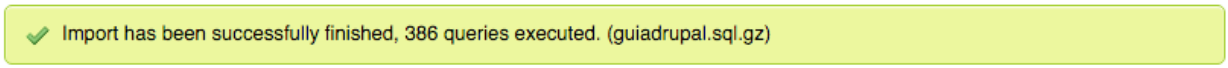


249. Pulsamos sobre el botón "Go", y a través del navegador, nos descargará el fichero generado.

250. Para restaurar el backup, sólo tendremos que copiar los ficheros del directorio de Drupal de nuevo en la ruta especificada, utilizando el mismo sistema (FTP, SCP etc.), y accederemos a phpMyAdmin y pulsaremos sobre la pestaña "Import":



251. Seleccionamos el fichero que contiene la copia de la base de datos, y pulsamos sobre el botón "Go". Una vez realizado, el sistema nos mostrará si la restauración de la base de datos ha sido o no satisfactoria:



15.2. BACKUP VÍA LÍNEA DE COMANDOS

252. Copia de los ficheros del sistema: de la misma forma que en el método anterior, podemos copiar los ficheros a un equipo persona u otro servidor utilizando protocolos como FTP, SCP etc. Otra opción es copiarlos a una ruta diferente o generar un archivo comprimido que pondremos a salvo:

$ cp -rp /ruta/de/drupal /ruta/del/backup
o
$ tar cvf drupalbackup.tgz /ruta/de/drupal

253. Copia de seguridad de la base de datos: aquí podremos utilizar dos mecanismos diferentes, utilizando los comandos:

- *mysqldump*: nos permitirá, mediante herramientas de mysql, generar una copia de la base de datos con el siguiente comando:

  $ mysqldump -u NOMBRE_USUARIO -p'PASSWORD' nombre_bbdd > /ruta/del/backup/backup_ddbb.sql

254. La restauración del backup se realizará a través del comando:

$ mysql -u NOMBRE_USUARIO -p'PASSWORD' nombre_bbdd < /ruta/del/backup/backup_ddbb.sql

- *Drush*: permite generar una copia de la base de datos, para lo que utilizaremos el comando desde el directorio donde esté instalado Drupal:

$ drush sql-dmp > /ruta/del/backup/backup_ddbb.sql
o podemos realizar un backup completo con
$ drush archive-backup

```
root@guiaDrupal:/var/www/html/drupal# drush archive-backup
Database dump saved to /tmp/drush_tmp_1463577331_573c6af321724/guiadrupal.sql                    [success]
Archive saved to /root/drush-backups/archive-dump/20160518131529/guiadrupal.20160518_131530.tar.gz [ok]
/root/drush-backups/archive-dump/20160518131529/guiadrupal.20160518_131530.tar.gz
root@guiaDrupal:/var/www/html/drupal#
```

255. La restauración del backup de la base de datos se realizará a través del comando:

$ drush sql-cli < /ruta/del/backup/backup_ddbb.sql

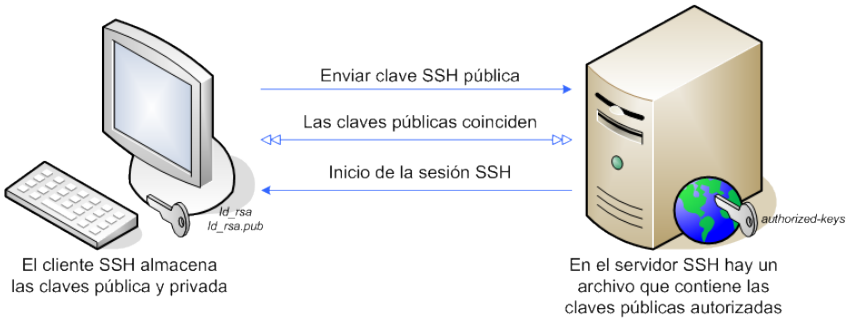
256. En la restauración completa de base de datos y ficheros se utilizará el siguiente parámetro:

$ drush archive-restore /ruta/del/backup/backupcompleto.tar.gz

```
root@guiaDrupal:~/drush-backups# drush archive-restore  archive-dump/20160518131529/guiadrupal.20160518_131530.tar.gz
Archive restored to /root/drush-backups/drupal                                                  [ok]
/root/drush-backups/drupal
root@guiaDrupal:~/drush-backups#
```

15.3. SCRIPT DE AUTOMATIZACIÓN DE COPIA DE SEGURIDAD

257. Para realizar este tipo de copia de seguridad, utilizaremos una conexión segura SSH a nuestro servidor remoto, sin utilizar contraseña y en su lugar utilizando una clave pública generada por el servidor.



258. Para ello, primero tendremos que realizar una serie de pasos sencillos:

1. Asegurarnos que el servidor remoto de respaldo tiene SSH instalado, y la cuenta de usuario que vamos a utilizar dispone del directorio ".ssh" en su interior
2. Crearemos el par de clave privada y pública en nuestro servidor con el comando "ssh-keygen":

```
root@guiaDrupal:~# ssh-keygen -b 4096 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
b9:88:32:8e:24:44:0c:73:d2:1f:a0:9c:24:b0:78:59 root@guiaDrupal
The key's randomart image is:
+--[ RSA 4096]----+
|Boo.E            |
|B*oo.            |
|+=o. .           |
|..  .    .       |
| .      S        |
|.    . . .       |
|..o . . .        |
|oo o             |
|. .              |
+-----------------+
root@guiaDrupal:~#
```

3. Copiamos la clave pública a nuestro equipo de respaldo con el comando "ssh-copy-id", que introducirá nuestra clave en el fichero "authorized_keys" remoto:

```
root@guiaDrupal:~# ssh-copy-id -i ./.ssh/id_rsa.pub drupalbackup@          0.69
The authenticity of host '139.162.200.69 (139.162.200.69)' can't be established.
ECDSA key fingerprint is e3:8b:bc:22:d4:ec:2d:0b:8c:7f:8c:6f:fd:41:b2:74.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
drupalbackup@139.162.200.69's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'drupalbackup@139.162.200.69'"
and check to make sure that only the key(s) you wanted were added.
```

4. Comprobamos que podemos realizar la conexión sin contraseña:

```
root@guiaDrupal:~# ssh drupalbackup@          0.69
Linux (none) 4.4.0-x86_64-linode63 #2 SMP Tue Jan 19 12:43:53 EST 2016 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
drupalbackup@(none):~$
```

I. REALIZANDO LA COPIA DE SEGURIDAD

259. Una vez que tengamos esta configuración realizada, procederemos a instalar el script para la realización de copias de seguridad en nuestro servidor. Necesitaremos modificar una serie de variables iniciales para adaptarlo a nuestra configuración, como:

- **BLOG_DIR**: directorio donde Drupal se encuentra instalado
- **BACKUP_DIR**: directorio local donde se almacenará el backup
- **REMOTE_USER**: usuario remoto que se usará en la conexión SSH
- **REMOTE_HOST**: dirección de la máquina a la que nos conectaremos por SSH
- **REMOTE_BACKUP_DIR**: directorio remoto donde almacenaremos el backup

260. El script que crearemos en nuestra máquina contendrá el siguiente código:

```
#!/bin/bash
#
# Script para la realizacion de copias de seguridad en Drupal por SSH
```

```
#
# Ruta de la instalacion de Drupal
BLOG_DIR=/var/www/html/drupal/
# Directorio donde almacenar las copias en local
BACKUP_DIR=/var/backups/drupal
# Datos de conexion remota por SSH/SCP
REMOTE_USER=drupalbackup
REMOTE_HOST=XXX.XXX.XX.XX
# Directorio remoto donde almacenar las copias de seguridad
REMOTE_BACKUP_DIR=/backups/drupal

# Variables de configuracion de acceso a la base de datos de Drupal
DB_NAME=guiadrupal
DB_USER=usuariodrupal
DB_PASS=password
DB_HOST=127.0.0.1

echo "Realizando volcado de la base de datos... "
DUMP_NAME=${DB_NAME}-$(date +%Y%m%d).sql.bz2
mysqldump --user=${DB_USER} --password=${DB_PASS} --host=${DB_HOST} --databases ${DB_NAME} | bzip2 -c
> ${BACKUP_DIR}/${DUMP_NAME}
if [ "$?" -ne "0" ]; then
        echo "error!"
        exit 1
fi

echo "Realizando copia de seguridad de los ficheros de Drupal... "
TAR_NAME=${BLOG_DIR##*/}-$(date +%Y%m%d).tar.bz2
tar -cjf ${BACKUP_DIR}/${BLOG_DIR##*/}-$(date +%Y%m%d).tar.bz2 --exclude cache ${BLOG_DIR}
if [ "$?" -ne "0" ]; then
        echo "error!"
        exit 2
fi


echo "Enviando copia de seguridad de BBDD/ficheros a host remoto... "
scp "${BACKUP_DIR}/${DUMP_NAME}" "$REMOTE_USER@$REMOTE_HOST:$REMOTE_BACKUP_DIR"
scp "${BACKUP_DIR}/${TAR_NAME}" "$REMOTE_USER@$REMOTE_HOST:$REMOTE_BACKUP_DIR"

if [ "$?" -ne "0" ]; then
        echo "Se ha producido un error!"
        exit 3
fi
echo "Copia de seguridad finalizada!"
```

261. Una vez creado en nuestro sistema, su ejecución es muy sencilla. Tan sólo deberemos otorgarle permisos de ejecución y lanzarlo desde la línea de consola:

```
root@guiaDrupal:~# ./backup.sh
Realizando volcado de la base de datos...
Realizando copia de seguridad de los ficheros de Wordpress...
tar: Eliminando la `/' inicial de los nombres
Enviando copia de seguridad de BBDD/ficheros a host remoto...
guiadrupal-20160518.sql.bz2                                   100%  578KB 577.8KB/s   00:00
drupal-20160518.tar.bz2                                       100%  134MB   2.9MB/s   00:47
Copia de seguridad finalizada!
root@guiaDrupal:~#
```

262. Ahora que tenemos la certeza de que el script está funcionando correctamente, podremos programarlo para realizar copias de seguridad diarias de forma automática y sin necesidad de la interacción del administrador del sistema. Para ello sólo tendremos que añadir una nueva entrada en el "crontab" del sistema, especificando la hora a la que debe realizarse la copia de seguridad. En nuestro ejemplo configuraremos la tarea para que se realice de forma automática todos los días a las 2.30 AM:

```
$ crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
30 2 * * * /path_del_script/backup.sh > /dev/null 2>&1
$
```

II. RESTAURANDO LA COPIA DE SEGURIDAD

263. El proceso para restaurar la copia de seguridad será el siguiente:

1. Descargar los ficheros correspondientes a la copia de seguridad de la base de datos y de los ficheros de Drupal a nuestro servidor
2. Importamos el backup en formato *.sql* a MySQL y comprobamos que se restaura correctamente

```
root@guiaDrupal:/var/backups/drupal# ls
drupal-20160518.tar.bz2  guiadrupal-20160518.sql.bz2
root@guiaDrupal:/var/backups/drupal# bunzip2 guiadrupal-20160518.sql.bz2; mysql -u usuariodrupal -p < guiadrupal-20160518.sql
Enter password:
root@guiaDrupal:/var/backups/drupal# mysql -u usuariodrupal -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 92
Server version: 5.5.49-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| guiadrupal         |
+--------------------+
2 rows in set (0.00 sec)

mysql>
```

3. Descomprimimos el archivo correspondiente a la copia de seguridad de los ficheros. Es importante saber que se expandirá la ruta completa donde el anterior Drupal fue instalado, por lo que será importante mantenerla. En caso que los directorios correspondientes ya existan, procederemos a mover el directorio de la instalación a la ruta completa

```
root@guiaDrupal:/var/backups/drupal# mv drupal-20160518.tar.bz2 /var/www/html/drupal/
root@guiaDrupal:/var/backups/drupal# cd /var/www/html/drupal/
root@guiaDrupal:/var/www/html/drupal# tar -xjf drupal-20160518.tar.bz2
root@guiaDrupal:/var/www/html/drupal# ls
autoload.php   composer.lock  dbcontent.sql           example.gitignore  modules   README.txt  sites   update.php  vendor
composer.json  core           drupal-20160518.tar.bz2  index.php          profiles  robots.txt  themes  var         web.config
```

4. Comprobamos que los ficheros tienen los permisos correspondientes. La información detallada de este proceso se encuentra en la sección “Configuración de permisos”

264. Una vez finalizado este paso, nuestra copia de seguridad habrá sido restaurada correctamente y podremos acceder de nuevo a nuestro Drupal de la forma habitual.

16. RECUPERACIÓN ANTE UN COMPROMISO DE SEGURIDAD

265. A pesar de las medidas anteriormente descritas, es posible que en algún momento suframos un compromiso en nuestro sistema, porque un atacante descubra una vulnerabilidad, o más habitualmente porque algún bot/gusano acabe tomando el control de forma automatizada de nuestro sitio.

266. En este apartado veremos algunos de los pasos que serán necesarios para mitigar el impacto de este compromiso y restaurar el servicio:

1. **Realizar una copia de seguridad con fines forenses**: a pesar de que nuestro sitio haya sido infectado, es importante realizar una copia de seguridad de los datos. Esta copia debe ser completa, incluyendo toda la información de la base de datos y ficheros en el sistema. Si fuera posible, realizaremos un snapshot de los servidores que hayan sido comprometidos.
2. **Uso del módulo Hacked!:** utilizaremos el módulo Hacked!, anteriormente instalado en esta guía, para comprobar las posibles modificaciones que se hayan realizado en el código por parte de los atacantes. Otra forma de comprobar los posibles cambios en el código del sitio es utilizar las herramientas Git o SVN, en función del tipo de instalación que hayamos realizado.

267. El atacante ha podido modificar algún fichero para mantener el posterior acceso, como en el acceso a usuarios:

```
switch ($form_id) {
   case 'user_login':
   case 'user_login_block':

    // only allow for Drupal login fields if this is the /backdoor page
    if (strcmp(current_path(),"backdoor")!=0) {
     $form['name']['#access'] = FALSE;
     $form['pass']['#access'] = FALSE;
          $form['#submit'][] = 'yourmodule_external_submit';
          unset($form['#validate']);
          $form['#validate'][] = 'yourmodule_external_validate';
    }
    break;
```

268. También es posible haber aprovechado alguna vulnerabilidad conocida, como una Inyección SQL, para insertar código o un backdoor en el Core de Drupal, como:

```
mysql> INSERT INTO `menu_router` (`path`, `load_functions`, `to_arg_functions`, `description`, `access_callback`, `access_arguments`) VALUES ('mziogj', '', '', 'mziogj', 'file_put_contents','[TROJAN]');
```

3. **Restaurar el servicio**: a la hora de restaurar el servicio, lo más recomendable es realizar una instalación limpia del sistema, así como la distribución desde el sitio oficial. Si conocemos con exactitud la fecha del compromiso, procederemos a restaurar, si existe, una copia de seguridad de la base de datos y los ficheros necesarios. Solamente en casos concretos, seremos capaces de asegurar que ficheros han sido comprometidos, restaurarlos, asegurar el sitio y mantener los datos almacenados.

4. **Modificar la contraseña de acceso a la base de datos**: debido a que en el momento inicial no conoceremos el alcance del ataque, será necesario generar un nuevo usuario y contraseña para gestionar la base de datos de MySQL. En el caso de que hayaoms restaurado una copia de seguridad anterior, entraremos en la consola de administración de la base de datos y procederemos al cambio de contraseña:

   mysql> SET PASSWORD FOR 'usuario'@'' = PASSWORD('nueva_contraseña');*

269. Deberemos modificar esta contraseña también en el fichero de configuración de Drupal "/ruta/web/drupal/sites/default/settings.php":

```
$databases['default']['default'] = array (
  'database' => 'guiadrupal',
  'username' => 'usuariodrupal',
  'password' => 'password',
  'prefix' => '',
  'host' => 'localhost',
  'port' => '3306',
  'namespace' => 'Drupal\\Core\\Database\\Driver\\mysql',
  'driver' => 'mysql',
);
```

5. **Revisión de los usuarios**: deberemos comprobar los roles, así como los usuarios que se encuentran activos en la plataforma. Es posible que durante el proceso del ataque, se haya creado un usuario nuevo con permisos avanzados para mantener el acceso a la máquina comprometida. Por ejemplo, la siguiente sentencia, de un ataque real, ha insertado un nuevo usuario con el valor de *UID* más alto disponible en nuestra instalación:

   mysql> set @a=(SELECT MAX(uid) FROM users)+1;INSERT INTO users set uid=@a,status=1,name='phantom' , pass = 'HASH';INSERT INTO users_roles set uid=@a,rid=3;

6. **Revisión de sesiones activas:** Deberemos comprobar las sesiones que se encuentren activas, debido a que es posible que el atacante continúe realizando tareas hasta que pulse el botón de *logout*, o haya suplantado la sesión de otro usuario.

```
mysql> desc sessions;
+-----------+------------------+------+-----+---------+-------+
| Field     | Type             | Null | Key | Default | Extra |
+-----------+------------------+------+-----+---------+-------+
| uid       | int(10) unsigned | NO   | MUL | NULL    |       |
| sid       | varchar(128)     | NO   | PRI | NULL    |       |
| hostname  | varchar(128)     | NO   |     |         |       |
| timestamp | int(11)          | NO   | MUL | 0       |       |
| session   | longblob         | YES  |     | NULL    |       |
+-----------+------------------+------+-----+---------+-------+
5 rows in set (0.00 sec)

mysql> select * from sessions;
+-----+---------------------------------------------+-------------+------------+---------------------------------------------
| uid | sid                                         | hostname    | timestamp  | session
    |
+-----+---------------------------------------------+-------------+------------+---------------------------------------------
|   1 | UhzYo7BqRCJa87lGjyxGsk5-ldeA3X_WwF_A-GYwsXo | 192.168.1.39 | 1463080477 | 2hZ0ZBpxyxlQSvHjR3cHtPA7LHPbAopAwi3GBT_psWBXZ-Stq56c-aklFtJ-I8f3
b4wSFZeFOOO-A4foH_0dzkuIx_7XzOaSVH8ZL_Mr3QMlk8t8C_XXZVMloyzyvibYLFNDKe8bhRV7gS4nJRSFF8JfCV9Djrcark2Jgrzg-bz_QQxke_5CjEo8BbZ8mfyzjosY-93UMtAuDuEE8E
xhcA.. |
+-----+---------------------------------------------+-------------+------------+---------------------------------------------
1 row in set (0.00 sec)
```

7. **Reiniciar las contraseñas de todos los usuarios**: En el caso de utilizar una instalación nueva, las contraseñas de los usuarios deben ser diferentes a las anteriores, debido a que han podido ser obtenidas durante el ataque. En el caso de estar utilizando una copia de seguridad de respaldo, procederemos a utilizar la siguiente *query* desde la consola de administración de MySQL para modificarlas:

   mysql> UPDATE users SET pass = concat('ZZZ', sha(concat(pass, md5(rand()))));

270. Cuando un usuario acceda al sitio Drupal, deberá pulsar el botón de "Solicitar una nueva contraseña" para finalizar el proceso de cambio.

8. **Revisión y reinstalación de módulos**: ahora procederemos a localizar los módulos que estaban anteriormente instalados y los reinstalaremos del repositorio oficial de Drupal de nuevo.
9. **Google Webmaster Tools**: las herramientas de Webmaster de Google nos permitirán comprobar si nuestro sitio ha sido marcado como infectado, además de obtener información valiosa de los ficheros sospechosos. Si hemos sido incluidos en la lista de sitios infectados, una vez finalizada la limpieza, deberemos solicitar la revisión de nuestro sitio.
10. **Asegurar el sitio de nuevo**: una vez finalizado el proceso anterior, procederemos de nuevo a aplicar las medidas de seguridad explicadas a lo largo de esta guía.

ANEXO 1. CHECKLIST DE REVISIÓN DE SEGURIDAD

TAREAS A REALIZAR	REALIZADA	NO REALIZADA	NO APLICA
MySQL			
Restricción de acceso remoto	☐	☐	☐
Modificación del usuario administrador	☐	☐	☐
Eliminado de cuenta de invitados y obsoletas	☐	☐	☐
Reducción de privilegios del sistema	☐	☐	☐
Activación de logs	☐	☐	☐
Eliminado de historial	☐	☐	☐
Limitación de los permisos del usuario de Drupal	☐	☐	☐
PHP			
Instalación de Suhosin	☐	☐	☐
Configuración segura de variables	☐	☐	☐
GENERAL			
Eliminación de ficheros innecesarios de instalación	☐	☐	☐
Configuración segura de permisos	☐	☐	☐
Revisión del fichero 'robots.txt'	☐	☐	☐
Habilitación de restricciones de acceso	☐	☐	☐
Asegurando el entorno y el usuario #1	☐	☐	☐
Configuración segura de Input Formats	☐	☐	☐
Activación de la navegación sobre SSL	☐	☐	☐
MÓDULOS			
Ban	☐	☐	☐
Automated Logout	☐	☐	☐
Secure Login	☐	☐	☐
Password Policy	☐	☐	☐
Hacked	☐	☐	☐

Restrict login or role access by IP address	☐	☐	☐
Filtro Antispam	☐	☐	☐
Integración de antivirus ClamAV	☐	☐	☐
Captcha	☐	☐	☐
Security Review	☐	☐	☐
BACKUPS			
Generación manual de copias de seguridad	☐	☐	☐
Adecuación y uso del script de automatización	☐	☐	☐