Establecer contraseña de superusuario de MySQL (que no son los del sistema)

$ sudo mysql\_secure\_installation

Responder todo con Yes, excepto: ¿Remove test database…………..?

Ya tenemos nuestra contraseña de root y a continuación entramos

$ mysql -u root -p

Mysql> CREATE USER ‘alicia’@’localhost’ IDENTIFIED BY ‘conejo89$’

Todos nos hemos creado el mismo usuario y password

Algunos comandos vistos para moverse por mysql:

Mysql> use mysql

Mysql> show colum from ……

Mysql> select host,user from users

A continuación creamos la base de datos zoo

Mysql> CREATE DATABASE zoo

Mysql> show databases

Ahora damos privilegios a Alicia

Mysql> GRANT ALL privileges ON zoo.\* to ‘alicia’@’localhost’

El siguiente paso es instalar phpmyadmin y asignar contraseña para ello:

$ sudo apt install phpmyadmin

“Importante marcar con el espacio la casilla de apache”

Ahora instalamos los modulos que teníamos qpendiente de instalar

$ sudo apt install php7.3-mysqli

$ sudo apt install php7.3-mbstring

Ya podemos conectarnos desde el navegador para crear las tablas en la base de dato zoo:

<http://ip_servidor/phpmyadmin>

y nos logueamos con la cuenta de Alicia creada previamente

y creamos la tabla animales con las columnas:

alias char(8)

peso int

sexo char(1)

use zoo; //cambiar base de datos

insert into animales values ('joe', 21, 'V'),('winter',24, 'V'); //tobi, 20, v. robi,100,v. lisa,10, f;

ctrl + r; //Busqueda incremental hacia detras;

SCP para subir archivos;

//desde pc local

scp \*.php arturo@vps612581.ovh.net:/home/arturo

VERSION PHP Y APACHE

php -v

more /etc/apache2/sites-enabled/vps.conf //el de por defecto

nano vps.conf

>> DocumentRoot /var/www/vps

DirectoryIndex index.php index.html

CAMBIAR PERMISOS:

sudo chown -R arturo /var/www/vps

sudo nano index.php

<?php phpinfo() ?>

cp \*.php /var/www/vps

Nos conectamos al vps //nombre=status

apachectl -k graceful //sustituye al restart

Contextos: server config, virtual host, directory, .htacces

Modulos: mods-avaliable (modulos disponibles), mods-enabled (enlaces)

apache2ctl -M sort | more //Modulos disponibles

Saber si un modulo esta cargado

apache2ctl -M | grep nombre

a2enmod o a2dismond

sudo a2dismond nombre

Contenido ficheros de conf de los modulos:

cat nombre.load

conf-avaliable //configuracion phpyadmin incluida

Acceder al estado del servidor

vps612581.ovh.net/server.status //o /estado

http://vps612581.ovh.net/estado?refresh=10 //tiempo

//hacer la peticion desde nuestro servidor

openssl passwd -apr1 -salt salt\_de\_8\_caracteres murcia | diff - <(cat .htpasswd | cut -d: -f2)

Creamos otro usuario:

sudo htpasswd .htpasswd robin

cadiz

nos dirigimos a:

cd mods\_enabled

sudo nano info.conf

Añadimos:

AuthType Basic

Authname "Acceso a la informacion del servidor restringida"

AuthUserFile /etc(apache2/.htpasswd

Require user batman

sudo apache2ctl graceful

sudo a2enmod info //Habilitar modulo info

FORMATO URL CON USUARIO Y CONTRASEÑA:

Dos formas:

1-http://usuario:contraseña@vps612581.ovh.net/server-info

Actividad:

Escribir una url para acceder al fichero osito.png que esta en /img

en la maquina vps... por el puerto 81.

http://vps612581.ovh.net:81/img/osito.png

http://batman:murcia@vps612581.ovh.net/img/osito.png

Cabecera de peticion Authorization: Codificacion usuario y pass

sudo tcpflow port 80

DESCODIFICAR:

el fichero de tcpflow

echo -n autorization... | base64 -d

ESTE SERIA EL PROCESO DE AUTORIZACION

ACTIVIDADES:

-OBESERVAR PETICIONES Y RESPUESTAS PARA AUTORIZACIONES CORRECTAS E INCORR.

-EVITAR QUE EL NAVEGADOR ENVIE AUTOMATICAMENTE

(RECUERDE EL USUARIO Y LA CONTRASEÑA USADO EN LA ULTIMA "SESION"

DE ACCESO A LA INFORMACION DEL SERVIDOR

ontroles de acceso:

Directivas que nos interesan:<Directory><Files><Location>

Terminos para describir directivas:

Directiva AllowOverride //valor por defecto AllowOverride None

nos conectamos al vps:

cd /etc/apache2/sites-ennabled

sudo nano vps.conf

desactivamos 000-default.conf

AllowOverride su contexto es directory no server config (apache2.conf)

añadimos en vps.conf

<Directory /var/www/vps/img>

AllowOverride AuthConfig

AuthType Basic

AuthName "Acceso a las imagenes restrigido"

AuthUserFile /etc/apache2/.htpasswd

Require user batman robin

</Directory>

Contenedor directory:

sites-enabled/vps.conf

.htaccess

Permite el acesso a cada directorio de la conf de apache siempre que este tambien establecido en AllowOverride

cd /etc/apache2

sudo nano apache2.comf

AllowOverride None //Ya lo incluye apache

nano sites-enabled/vps.conf

Directiva options nos permite estableces politicas asignando indices de cara al contenido que pueda ver el usuario.

Debemos restringirlo

Directiva Options en DAWEB DOCUMENTACION //Usamos: Indexes

diferencias -Indexes y +Indexes -> se aplican a subdirectorios

-Indexes +FollowSk...

HTTPS Y CERTIFICADOS DIGITALES

X.509.

(Certificados. nos interesa entender que es el formato que vamos a usar de clave pública)

RSA.

(clave publica y privada. Asimetrico)

AES.

(simetrico, )

funcion hash.

(obtenemos una longitud fija, se aplica en ciptografia)

funcion hash criptografica

(Caso particular. caracateristicas ideales:

1. Es determinista: un mismo mensaje siempre resulta en el mismo hash

2. La computación del valor hash es rapida para cualquier mensaje.

3. Es inviable generar un mensaje a partir de su valor hash.

4. Un pequeño cambio en un mensaje debria cambiar el valor hash de tal manera que el nuevo valor no parezca que tenga correlación con el valor hash antiguo.

5. Es inviable encontrar 2 mensajes diferentes con el mismo valor hash.

)

MD5.

Es un algoritmo que aplica una funcion de hash.

SHA.

Familia de funciones criptográficas.

Usamos sha256.

OpenSSL.

Un paquete de herramientas relacionadas con la ciptografia.

man openssl

Funcionalidades que ofrece en lineas de comando:

1-Creacion y administracion de claves privadas, claves publicas y parametros.

2-Operaciones criptograficas de clave publica.

3-Creacion de certificados X509, CSRs y CRLs.

4-Calculo de resumen de mensajes.

5-Encriptacion y desencriptacion.

6-Pruebas SSL/TLS cliente-servidor.

7-Gestion de S/MIME firmado o correo encriptado.

8-Petición de marcas horarias, generación y verificación.

Formato PEM.

Claves criptograficas y certificados.

PEM es un formato de ficheros para almacenar y enviar claves criptograficas, certificados y otros datos.

Base64.

Codificacion cabezeras authorization

CERTIFIACDOS DIGITALES: Contienen la clave publica

-AUTOFIRMADO.

Lo podemos usar pero el cliente no lo conoce.

habilitar modulo ssl: sudo a2enmod ssl

restart

sudo mkdir /etc/apache2/ssl

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

/etc/apache2/ssl/apache.crt //fichero de certificado digital

como se genera:

nos conectamenos al vps

mkdir demo

cd demo

sudo opensll req-x509 -nodes -days 365 -newkey rsa:2048 -keyout...

ES, Cadiz, Sanl, Doñana, 2DAW, --IMPORTANTE-- vps612581.ovh.net, arturo.barba@iesdonana.org

//debemos configurar apache para que use estos ficheros

mkdir /etc/apache2/sll

cp . /etc/apache2/ssl

sudo a2enmod ssl //si no esta habilitado

graceful

apache2ctl -M | grep ssl

cd /etc/apache2/sites-available

cp sudo a2ensite ...

-GRATUITO (AUTORIZATOPOR CA)

Nos permiten obtener un certificado.

3)Comodo es una de las mas importantes a nivel mundial.

Ofrece certificados gratuitos

|  |  |
| --- | --- |
|  | 1) DirectoryIndex: |
|  | La DirectoryIndex directiva establece la lista de recursos a buscar, cuando el cliente solicita un índice del directorio al especificar un / al final del nombre del directorio. Local-url es la URL (codificada en%) de un documento en el servidor en relación con el directorio solicitado; suele ser el nombre de un archivo en el directorio. Se pueden proporcionar varias URL, en cuyo caso el servidor devolverá la primera que encuentre. Si no existe ninguno de los recursos y la Indexesopción está establecida, el servidor generará su propia lista del directorio. |
|  | <Directory "/foo"> |
|  | DirectoryIndex index.html index.php |
|  | </Directory> |
|  |  |
|  |  |
|  | 2) Documentroot: |
|  | Esta directiva establece el directorio desde el cual httpd servirán los archivos. A menos que coincida con una directiva como Alias, el servidor agrega la ruta desde la URL solicitada a la raíz del documento para hacer la ruta al documento. |
|  | DocumentRoot /usr/web |
|  |  |
|  | 3) Include: |
|  | Esta directiva permite la inclusión de otros archivos de configuración dentro de los archivos de configuración del servidor. |
|  | Include /usr/local/apache2/conf/ssl.conf |
|  | Include /usr/local/apache2/conf/vhosts/\*.conf |
|  | o |
|  | Include conf/ssl.conf |
|  | Include conf/vhosts/\*.conf |
|  |  |
|  | Los fnmatch()caracteres comodín de estilo Shell ( ) se pueden usar en el nombre del archivo o en las partes del directorio de la ruta para incluir varios archivos a la vez, en orden alfabético. Además, si Includeapunta a un directorio, en lugar de a un archivo, Apache httpd leerá todos los archivos en ese directorio y cualquier subdirectorio. Sin embargo, no se recomienda incluir directorios completos, ya que es fácil dejar accidentalmente los archivos temporales en un directorio que puede hacer httpdque falle. En su lugar, le recomendamos que utilice la sintaxis de comodines que se muestra a continuación para incluir archivos que coincidan con un patrón en particular, como \* .conf, por ejemplo. |
|  |  |
|  | La Includedirectiva fallará con un error si una expresión de comodín no coincide con ningún archivo. La IncludeOptional directiva se puede utilizar si se deben ignorar los comodines no coincidentes. |
|  |  |
|  | La ruta del archivo especificada puede ser una ruta absoluta o puede ser relativa al ServerRootdirectorio. |
|  |  |
|  | 4) IncludeOptional: |
|  | Esta directiva permite la inclusión de otros archivos de configuración dentro de los archivos de configuración del servidor. Funciona de manera idéntica a la Includedirectiva, pero se ignorará silenciosamente (en lugar de causar un error) si se usan comodines y no coinciden con ningún archivo o directorio o si no existe una ruta de archivo en el sistema de archivos. |
|  | IncludeOptional conf/ssl.conf |
|  | IncludeOptional conf/vhosts/\*.conf |
|  |  |
|  | 5) Listen: |
|  | La Listendirectiva le indica a Apache httpd que solo escuche direcciones IP o puertos específicos; de forma predeterminada, responde a las solicitudes en todas las interfaces IP. Listen Ahora es una directiva obligatoria. Si no está en el archivo de configuración, el servidor no podrá iniciarse. Este es un cambio de las versiones anteriores de Apache httpd. |
|  | Listen 80 |
|  | Listen 192.170.2.1:80 |
|  |  |
|  | La Listendirectiva le dice al servidor que acepte las solicitudes entrantes en el puerto especificado o la combinación de dirección y puerto. Si solo se especifica un número de puerto, el servidor escucha el puerto dado en todas las interfaces. Si se proporciona una dirección IP y un puerto, el servidor escuchará en el puerto y la interfaz dados. |
|  |  |
|  | Se Listenpueden usar varias directivas para especificar un número de direcciones y puertos para escuchar. El servidor responderá a las solicitudes de cualquiera de las direcciones y puertos listados. |
|  |  |
|  | 6) PidFile: |
|  | La PidFiledirectiva establece el archivo en el que el servidor registra el ID de proceso del daemon. Si el nombre del archivo no es absoluto, entonces se asume que es relativo al ServerRoot. |
|  | PidFile /var/run/apache.pid |
|  |  |
|  | 7) ServerAdmin: https://httpd.apache.org/docs/2.4/mod/core.html#serveradmin |
|  | Los ServerAdminconjuntos de la dirección de contacto que el servidor incluye en los mensajes de error se devuelve al cliente. Si el httpdno reconoce el argumento suministrado como una URL, asume que es una dirección de correo electrónico y la añade mailto:en los destinos de hipervínculo. Sin embargo, se recomienda usar una dirección de correo electrónico, ya que hay muchos scripts CGI que hacen esa suposición. Si desea utilizar una URL, debería apuntar a otro servidor bajo su control. De lo contrario, los usuarios no podrán contactarlo en caso de errores. |
|  | ServerAdmin www-admin@foo.example.com |
|  |  |
|  | 8) ServerName: https://httpd.apache.org/docs/2.4/mod/core.html#servername |
|  | La ServerName directiva establece el esquema de solicitud, el nombre de host y el puerto que el servidor utiliza para identificarse. ServerName [scheme://]domain-name|ip-address[:port] |
|  | ServerName se utiliza (posiblemente junto con ServerAlias) para identificar de forma única un host virtual, cuando se usan hosts virtuales basados ​​en nombres . |
|  | Además, esto se usa cuando se crean direcciones URL de redireccionamiento autorreferenciales cuando UseCanonicalNamese establece en un valor no predeterminado. |
|  | ServerName server.domain.com |
|  |  |
|  | 9) ServerRoot: https://httpd.apache.org/docs/2.4/mod/core.html#serverroot |
|  | La ServerRootdirectiva establece el directorio en el que vive el servidor. Normalmente contendrá los subdirectorios conf/y logs/. Las rutas relativas en otras directivas de configuración (como Includeo LoadModule, por ejemplo) se toman como relativas a este directorio. |
|  | ServerRoot /home/httpd |
|  |  |
|  | 10) <VirtualHost>: https://httpd.apache.org/docs/2.4/mod/core.html#virtualhost |
|  | <VirtualHost>y </VirtualHost>se utilizan para incluir un grupo de directivas que se aplicarán solo a un host virtual en particular. Se puede utilizar cualquier directiva permitida en un contexto de host virtual. Cuando el servidor recibe una solicitud de un documento en un host virtual en particular, utiliza las directivas de configuración adjuntas en la <VirtualHost> sección. Addr puede ser cualquiera de los siguientes, opcionalmente seguido de dos puntos y un número de puerto (o \*): |
|  | <VirtualHost 10.1.2.3> |
|  | ServerAdmin webmaster@host.example.com |
|  | DocumentRoot /www/docs/host.example.com |
|  | ServerName host.example.com |
|  | ErrorLog logs/host.example.com-error\_log |
|  | TransferLog logs/host.example.com-access\_log |
|  | </VirtualHost> |
|  |  |
|  |  |
|  | La dirección IP del host virtual; |
|  | Un nombre de dominio completo para la dirección IP del host virtual (no recomendado); |
|  | El carácter \*, que actúa como un comodín y coincide con cualquier dirección IP. |
|  | La cadena \_default\_, que es un alias para\* |
|  |  |
|  | 11) ServerAlias: https://httpd.apache.org/docs/2.4/mod/core.html#serveralias |
|  | La ServerAlias directiva establece los nombres alternativos para un host, para su uso con hosts virtuales basados ​​en nombres. El ServerAlias puede incluir comodines, si es apropiado. |
|  | Los hosts virtuales basados ​​en el nombre para el conjunto de <virtualhost>s de mejor coincidencia se procesan en el orden en que aparecen en la configuración. La primera coincidencia ServerNameo ServerAliasse usa, sin una prioridad diferente para los comodines (ni para ServerName vs. ServerAlias). |
|  | La lista completa de nombres en la <VirtualHost> directiva se trata como un (no comodín) ServerAlias. |
|  | <VirtualHost \*:80> |
|  | ServerName server.domain.com |
|  | ServerAlias server server2.domain.com server2 |
|  | ServerAlias \*.example.com |
|  | UseCanonicalName Off |
|  | # ... |
|  | </VirtualHost> |
|  |  |
|  | 12) Alias: https://httpd.apache.org/docs/2.4/mod/mod\_alias.html#alias |
|  | La Alias directiva permite que los documentos se almacenen en el sistema de archivos local que no sea bajo el DocumentRoot. Las URL con una ruta (% -decoded) que comienza con la ruta URL se asignarán a los archivos locales que comienzan con la ruta del directorio . La ruta de la URL distingue entre mayúsculas y minúsculas, incluso en sistemas de archivos que no distinguen entre mayúsculas y minúsculas. |
|  | Alias "/image" "/ftp/pub/image" |
|  |  |
|  | 13) Directiva <Directory>: https://httpd.apache.org/docs/2.4/mod/core.html#directory |
|  | <Directory>y </Directory>se utilizan para incluir un grupo de directivas que se aplicarán solo al directorio nombrado, a los subdirectorios de ese directorio y a los archivos dentro de los directorios respectivos. Se puede utilizar cualquier directiva permitida en un contexto de directorio. La ruta del directorio es la ruta completa a un directorio o una cadena de comodines que utiliza la coincidencia de estilo de shell de Unix. En una cadena de comodines, ?coincide con cualquier carácter individual y \*coincide con cualquier secuencia de caracteres. También puede utilizar []rangos de caracteres. Ninguno de los comodines coincide con un carácter `/ ', por <Directory "/\*/public\_html">lo que no coincidirá /home/user/public\_html, pero <Directory "/home/\*/public\_html">sí coincidirá. |
|  |  |
|  | <Directory /usr/local/httpd/htdocs> |
|  | Options Indexes FollowSymLinks |
|  | AllowOverride None |
|  | </Directory> |
|  |  |
|  |  |
|  |  |
|  |  |