Programa de Becas de Formación en Seguridad Informática
Coordinación de Seguridad de la Información
Investigación
UNAM-CERT

Seguridad en aplicaciones web

Proyecto

Macias Gomez Jorge
Lara López Martha Leticia
Méndez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

Índice

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

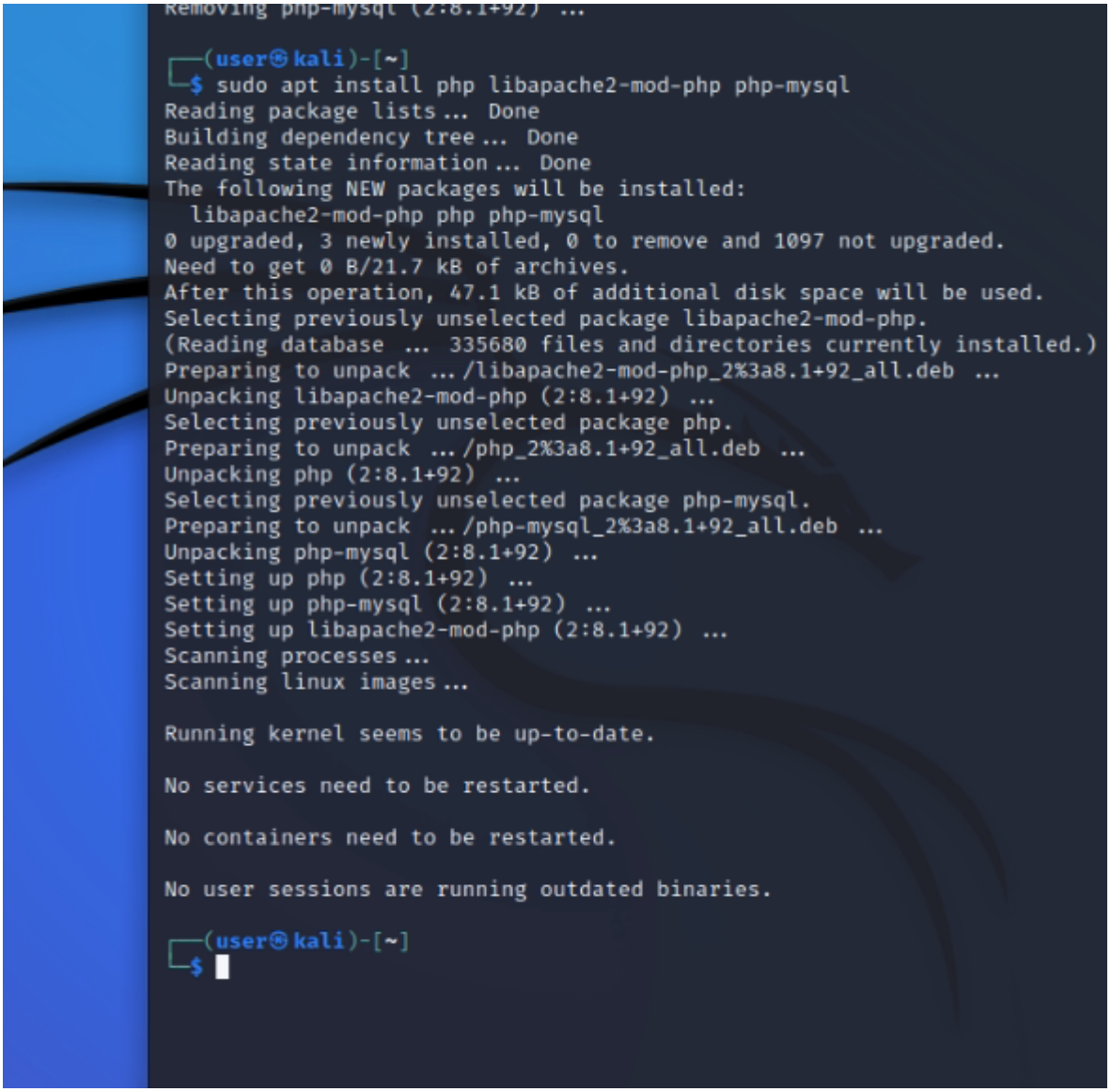
Instalación

PHP

Instalamos php con

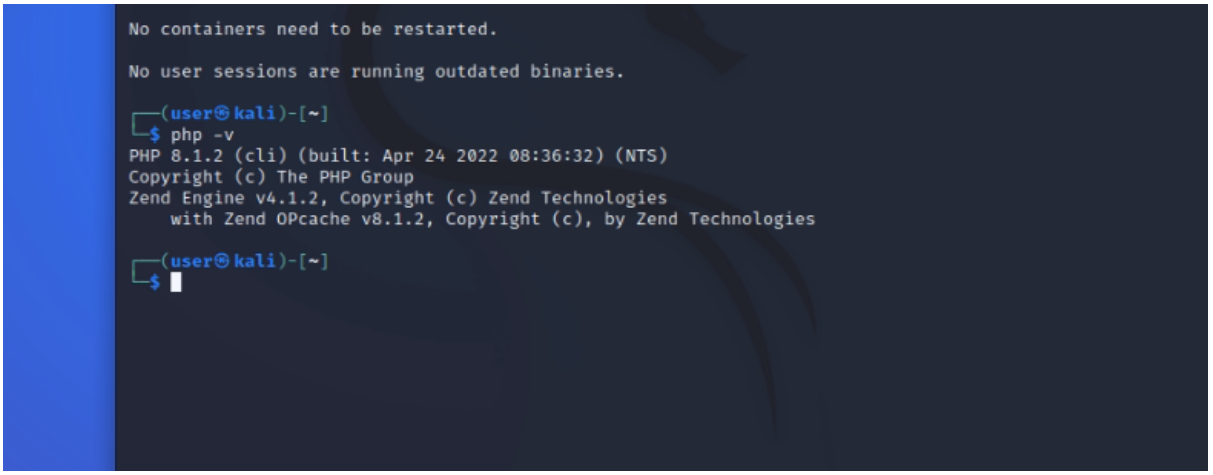
```
sudo apt install php libapache2-mod-php php-mysql
```

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine



Validamos la instalación

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

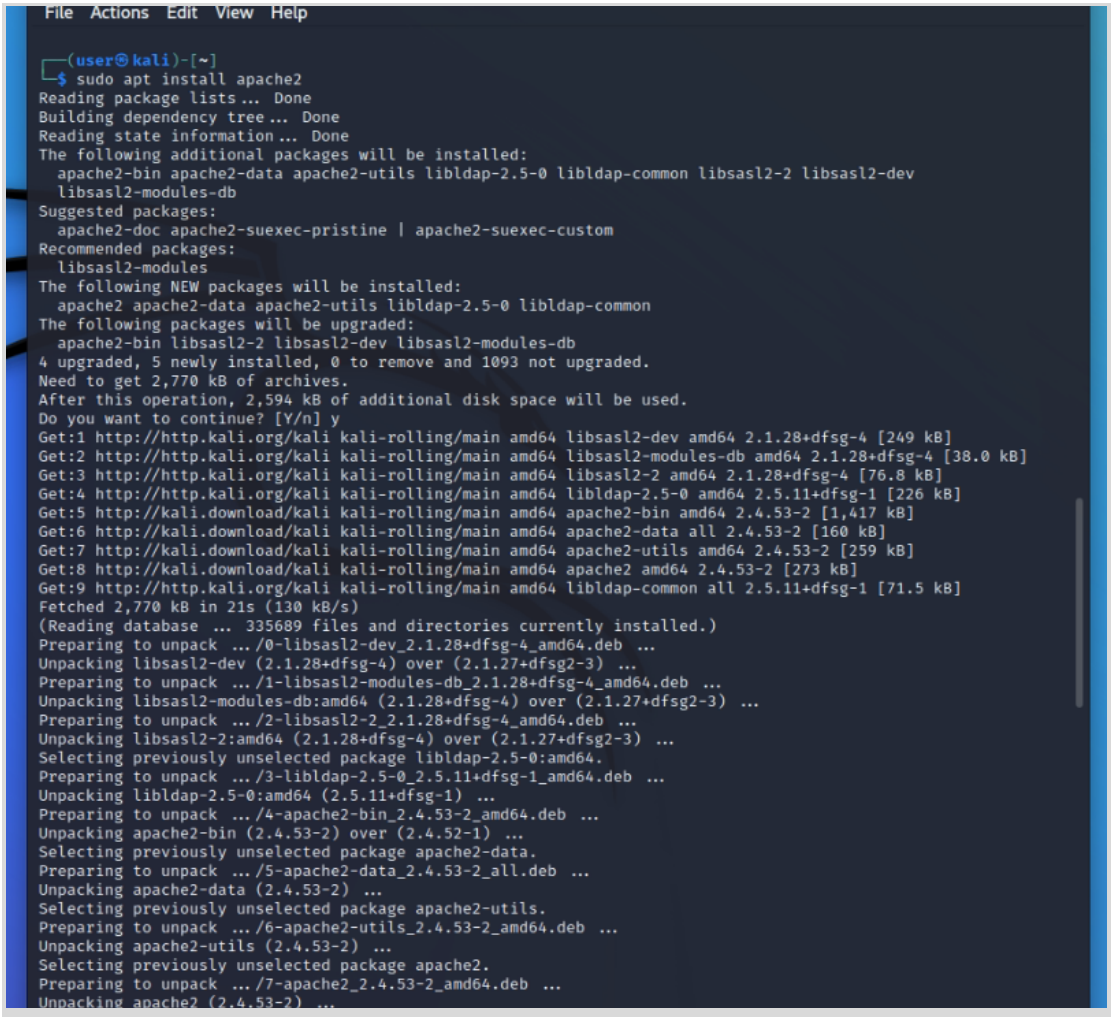


Apache

Instalamos Apache2 con el comando

```
sudo apt install apache2
```

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine



PostgreSQL

Para la instalación, es necesario instalar algunos paquetes:

```
sudo apt install postgresql-contrib
```

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(root💀kali)-[/var/www/proyecto]
└─# sudo apt install postgresql-contrib
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  postgresql-contrib
0 upgraded, 1 newly installed, 0 to remove and 1093 not upgraded.
Need to get 66.5 kB of archives.
After this operation, 71.7 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 postgresql-contrib all 14+240 [66.5 kB]
Fetched 66.5 kB in 11s (6,076 B/s)
Selecting previously unselected package postgresql-contrib.
(Reading database ... 336233 files and directories currently installed.)
Preparing to unpack .../postgresql-contrib_14+240_all.deb ...
Unpacking postgresql-contrib (14+240) ...
Setting up postgresql-contrib (14+240) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

`sudo apt install postgresql`

```
┌──(root💀kali)-[/var/www/proyecto]
└─# sudo apt install postgresql                                                                    100
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Suggested packages:
  postgresql-doc
The following packages will be upgraded:
  postgresql
1 upgraded, 0 newly installed, 0 to remove and 1092 not upgraded.
Need to get 66.5 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 postgresql all 14+240 [66.5 kB]B^[[B^[[B^[[B^[[B
Fetched 66.5 kB in 11s (6,311 B/s)
(Reading database ... 336236 files and directories currently installed.)
Preparing to unpack .../postgresql_14+240_all.deb ...
Unpacking postgresql (14+240) over (14+237) ...
Setting up postgresql (14+240) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

Podemos confirmar la instalación al revisar la versión, pero antes que nada, hay que iniciar el servicio de postgres.

`systemctl start postgresql.service`

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(root💀kali)-[/var/www/proyecto]
└─# systemctl start postgresql.service
```

```
sudo -u postgres psql -c "SELECT version();"
```

```
┌──(root💀kali)-[/var/www/proyecto]
└─# sudo -u postgres psql -c "SELECT version();"
                                                  version
-----------------------------------------------------------------------------------------------------------
 PostgreSQL 14.1 (Debian 14.1-5) on x86_64-pc-linux-gnu, compiled by gcc (Debian 11.2.0-13) 11.2.0, 64-bit
(1 row)
```

Drupal

Para la instalación de drupal, es necesario seguir una serie de pasos:

Instalar el módulo compatible de php-postgres

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(user㉿kali)-[~]
└─$ sudo apt-get install php-pgsql
[sudo] password for user:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  php8.1-pgsql
The following NEW packages will be installed:
  php-pgsql php8.1-pgsql
0 upgraded, 2 newly installed, 0 to remove and 1092 not upgraded.
Need to get 64.5 kB of archives.
After this operation, 240 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 php8.1-pgsql amd64 8.1.2-1+b3 [57.3 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php-pgsql all 2:8.1+92 [7,212 B]
Fetched 64.5 kB in 11s (5,805 B/s)
Selecting previously unselected package php8.1-pgsql.
(Reading database ... 336236 files and directories currently installed.)
Preparing to unpack .../php8.1-pgsql_8.1.2-1+b3_amd64.deb ...
Unpacking php8.1-pgsql (8.1.2-1+b3) ...
Selecting previously unselected package php-pgsql.
Preparing to unpack .../php-pgsql_2%3a8.1+92_all.deb ...
Unpacking php-pgsql (2:8.1+92) ...
Setting up php8.1-pgsql (8.1.2-1+b3) ...

Creating config file /etc/php/8.1/mods-available/pgsql.ini with new version

Creating config file /etc/php/8.1/mods-available/pdo_pgsql.ini with new version
Setting up php-pgsql (2:8.1+92) ...
Processing triggers for libapache2-mod-php8.1 (8.1.2-1+b3) ...
Processing triggers for php8.1-cli (8.1.2-1+b3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

Y el módulo de php gp, pgp-xml y php mbstring

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(user㉿kali)-[/var/www/proyecto/drupal]
└─$ sudo apt-get install php-gd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  php8.1-gd
The following NEW packages will be installed:
  php-gd php8.1-gd
0 upgraded, 2 newly installed, 0 to remove and 1091 not upgraded.
Need to get 35.8 kB of archives.
After this operation, 154 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 php8.1-gd amd64 8.1.2-1+b3 [28.6 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php-gd all 2:8.1+92 [7,204 B]
Fetched 35.8 kB in 11s (3,388 B/s)
Selecting previously unselected package php8.1-gd.
(Reading database ... 336456 files and directories currently installed.)
Preparing to unpack .../php8.1-gd_8.1.2-1+b3_amd64.deb ...
Unpacking php8.1-gd (8.1.2-1+b3) ...
Selecting previously unselected package php-gd.
Preparing to unpack .../php-gd_2%3a8.1+92_all.deb ...
Unpacking php-gd (2:8.1+92) ...
Setting up php8.1-gd (8.1.2-1+b3) ...

Creating config file /etc/php/8.1/mods-available/gd.ini with new version
Setting up php-gd (2:8.1+92) ...
Processing triggers for libapache2-mod-php8.1 (8.1.2-1+b3) ...
Processing triggers for php8.1-cli (8.1.2-1+b3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

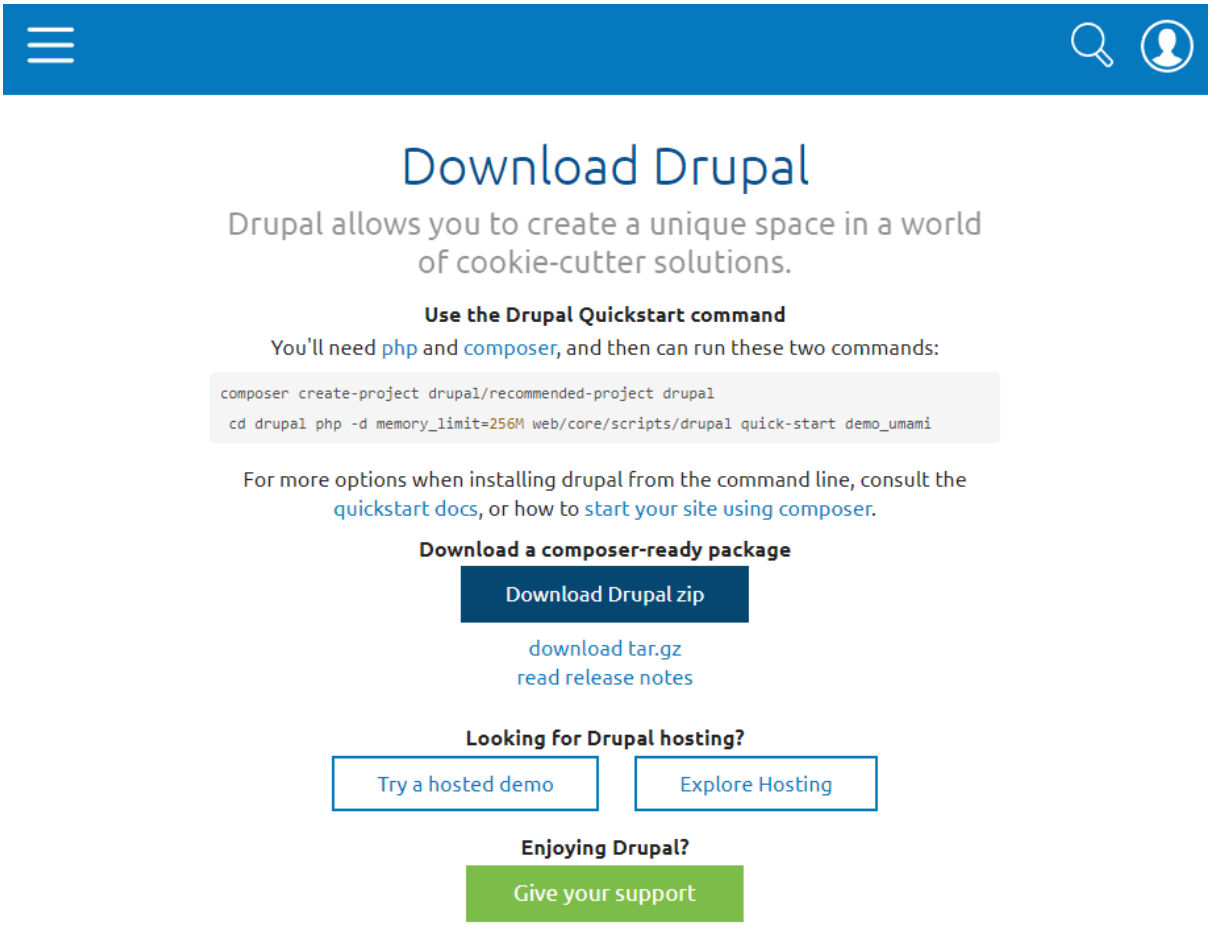
```
┌──(user㉿kali)-[/var/www/proyecto/drupal]
└─$ sudo apt-get install php-mbstring
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  libonig5 php8.1-mbstring
The following NEW packages will be installed:
  libonig5 php-mbstring php8.1-mbstring
0 upgraded, 3 newly installed, 0 to remove and 1091 not upgraded.
Need to get 589 kB of archives.
After this operation, 1,772 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 libonig5 amd64 6.9.7.1-2 [186 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php8.1-mbstring amd64 8.1.2-1+b3 [395 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 php-mbstring all 2:8.1+92 [7,216 B]
Fetched 589 kB in 11s (55.5 kB/s)
Selecting previously unselected package libonig5:amd64.
(Reading database ... 336468 files and directories currently installed.)
Preparing to unpack .../libonig5_6.9.7.1-2_amd64.deb ...
Unpacking libonig5:amd64 (6.9.7.1-2) ...
Selecting previously unselected package php8.1-mbstring.
Preparing to unpack .../php8.1-mbstring_8.1.2-1+b3_amd64.deb ...
Unpacking php8.1-mbstring (8.1.2-1+b3) ...
Selecting previously unselected package php-mbstring.
Preparing to unpack .../php-mbstring_2%3a8.1+92_all.deb ...
Unpacking php-mbstring (2:8.1+92) ...
Setting up libonig5:amd64 (6.9.7.1-2) ...
Setting up php8.1-mbstring (8.1.2-1+b3) ...

Creating config file /etc/php/8.1/mods-available/mbstring.ini with new version
Setting up php-mbstring (2:8.1+92) ...
Processing triggers for libc-bin (2.33-1) ...
Processing triggers for libapache2-mod-php8.1 (8.1.2-1+b3) ...
Processing triggers for php8.1-cli (8.1.2-1+b3) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

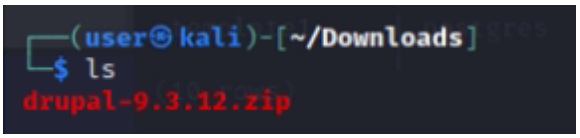
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(user㉿kali)-[/var/www/proyecto/drupal]
└─$ sudo apt install php-xml
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  php8.1-xml
The following NEW packages will be installed:
  php-xml php8.1-xml
0 upgraded, 2 newly installed, 0 to remove and 1092 not upgraded.
Need to get 114 kB of archives.
After this operation, 490 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 php8.1-xml amd64 8.1.2-1+b3 [106 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php-xml all 2:8.1+92 [7,228 B]
Fetched 114 kB in 11s (10.8 kB/s)
Selecting previously unselected package php8.1-xml.
(Reading database ... 336326 files and directories currently installed.)
Preparing to unpack .../php8.1-xml_8.1.2-1+b3_amd64.deb ...
Unpacking php8.1-xml (8.1.2-1+b3) ...
Selecting previously unselected package php-xml.
Preparing to unpack .../php-xml_2%3a8.1+92_all.deb ...
Unpacking php-xml (2:8.1+92) ...
Setting up php8.1-xml (8.1.2-1+b3) ...

Creating config file /etc/php/8.1/mods-available/dom.ini with new version

Creating config file /etc/php/8.1/mods-available/simplexml.ini with new version

Creating config file /etc/php/8.1/mods-available/xml.ini with new version

Creating config file /etc/php/8.1/mods-available/xmlreader.ini with new version

Creating config file /etc/php/8.1/mods-available/xmlwriter.ini with new version

Creating config file /etc/php/8.1/mods-available/xsl.ini with new version
Setting up php-xml (2:8.1+92) ...
Processing triggers for libapache2-mod-php8.1 (8.1.2-1+b3) ...
Processing triggers for php8.1-cli (8.1.2-1+b3) ...
Scanning processes ...
Scanning linux images ...
```

Descargamos la última versión de Drupal en la liga: https://www.drupal.org/download

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine





Descomprimimos el archivo y lo renombramos a drupal

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(user㉿kali)-[~/Downloads]
└─$ unzip drupal-9.3.12.zip
Archive:  drupal-9.3.12.zip
   creating: drupal-9.3.12/
   creating: drupal-9.3.12/vendor/
   creating: drupal-9.3.12/vendor/composer/
   creating: drupal-9.3.12/vendor/composer/semver/
  inflating: drupal-9.3.12/vendor/composer/semver/CHANGELOG.md
  inflating: drupal-9.3.12/vendor/composer/semver/LICENSE
  inflating: drupal-9.3.12/vendor/composer/semver/README.md
  inflating: drupal-9.3.12/vendor/composer/semver/composer.json
   creating: drupal-9.3.12/vendor/composer/semver/src/
  inflating: drupal-9.3.12/vendor/composer/semver/src/Comparator.php
  inflating: drupal-9.3.12/vendor/composer/semver/src/CompilingMatcher.php
   creating: drupal-9.3.12/vendor/composer/semver/src/Constraint/
  inflating: drupal-9.3.12/vendor/composer/semver/src/Constraint/Bound.php
  inflating: drupal-9.3.12/vendor/composer/semver/src/Constraint/Constraint.php
  inflating: drupal-9.3.12/vendor/composer/semver/src/Constraint/ConstraintInterface.php
  inflating: drupal-9.3.12/vendor/composer/semver/src/Constraint/MatchAllConstraint.php
  inflating: drupal-9.3.12/vendor/composer/semver/src/Constraint/MatchNoneConstraint.php
  inflating: drupal-9.3.12/vendor/composer/semver/src/Constraint/MultiConstraint.php
```

```
┌──(user㉿kali)-[~/Downloads]
└─$ mv drupal-9.3.12 drupal
```

Cambiamos los permisos a la carpeta para que el grupo y usuario www-data tenga permisos.

```
└─$ sudo chown www-data:www-data -R drupal
```

```
┌──(user㉿kali)-[~/Downloads]
└─$ ls -la .
total 33008
drwxr-xr-x  3 user     user         4096 May  6 17:48 .
drwxr-xr-x 17 user     user         4096 May  5 23:03 ..
drwxr-xr-x  8 www-data www-data     4096 Apr 20 10:13 drupal
-rw-r--r--  1 user     user     33784914 May  6 17:34 drupal-9.3.12.zip
```

Lo movemos a /var/www/proyecto

```
┌──(user㉿kali)-[~/Downloads]
└─$ sudo mv drupal /var/www/proyecto/
```

Desactivamos el módulo mpm_event y activamos el de mpm_fork para evitar conflictos con php.

```
┌──(user㉿kali)-[/var/www/proyecto/drupal]
└─$ sudo a2dismod mpm_event
Module mpm_event disabled.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(user㉿kali)-[/var/www/proyecto/drupal]
└─$ sudo a2enmod mpm_prefork
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Enabling module mpm_prefork.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

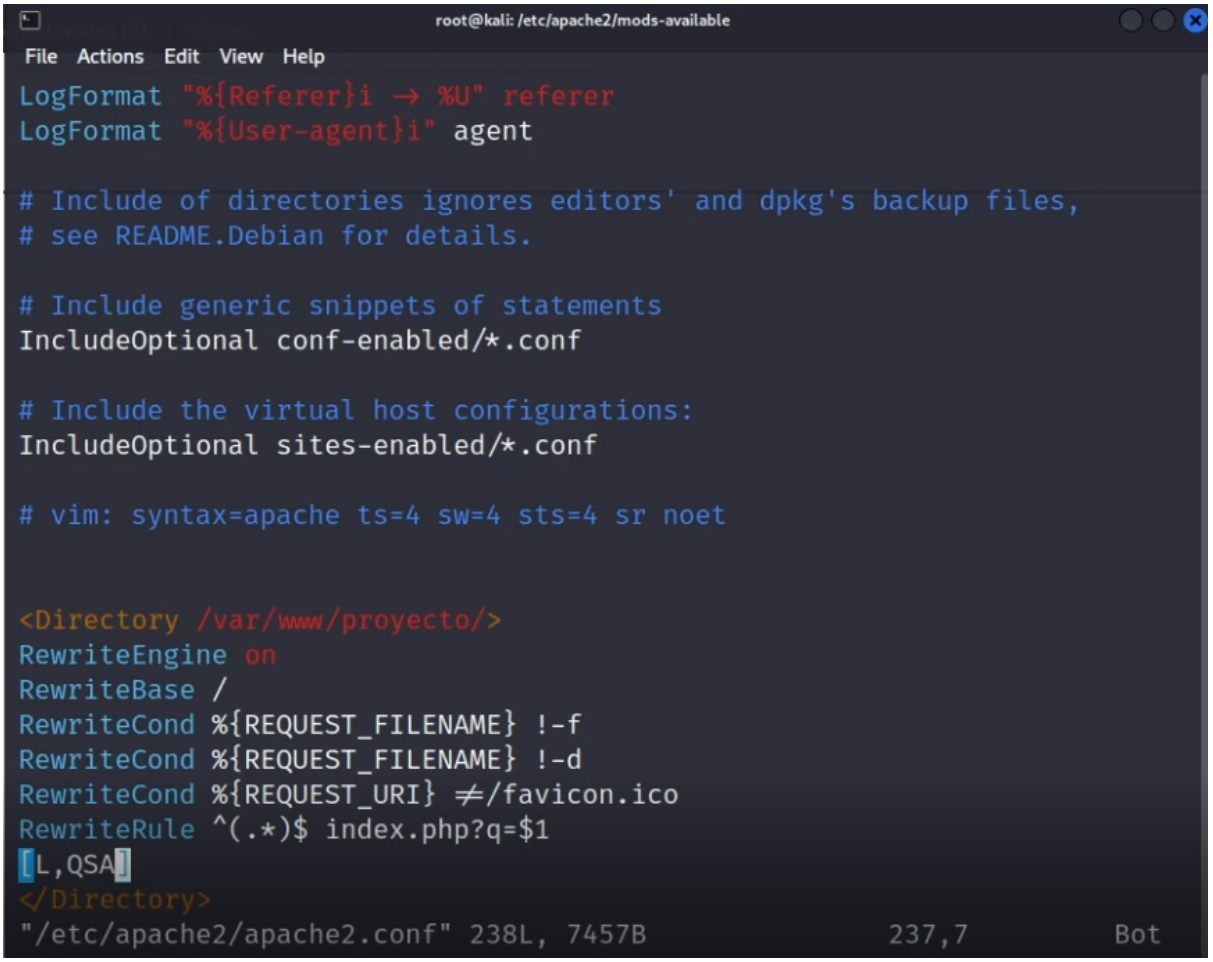
Y habilitamos el módulo de php

```
┌──(user㉿kali)-[/var/www/proyecto/drupal]
└─$ sudo a2enmod php8.1
Considering dependency mpm_prefork for php8.1:
Considering conflict mpm_event for mpm_prefork:
Considering conflict mpm_worker for mpm_prefork:
Module mpm_prefork already enabled
Considering conflict php5 for php8.1:
Enabling module php8.1.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

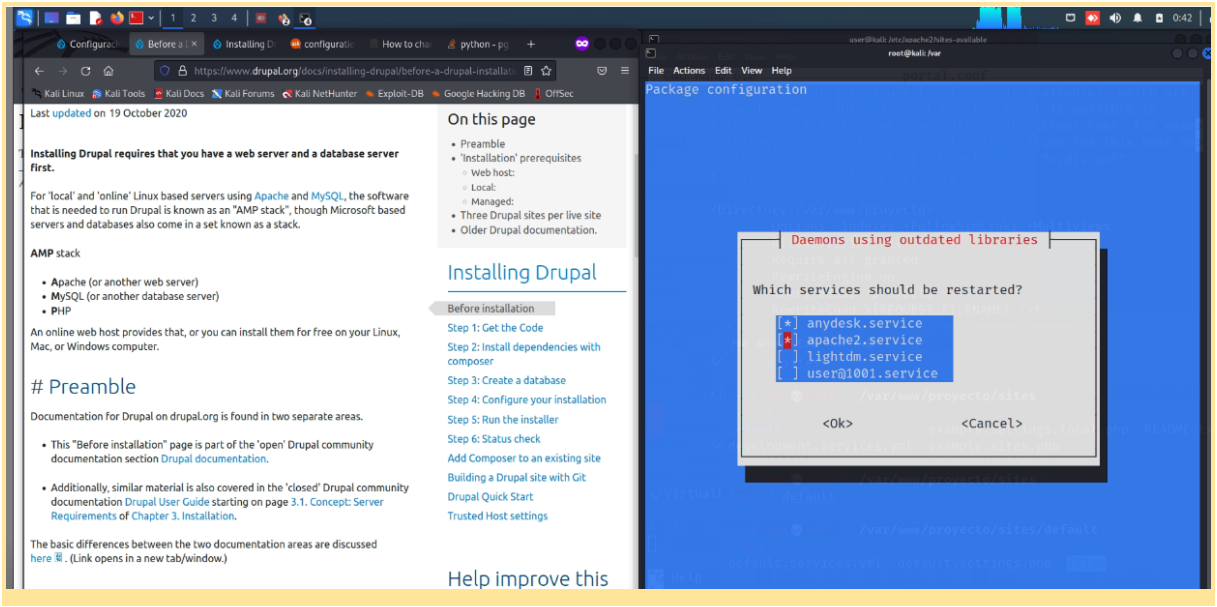
```
┌──(user㉿kali)-[/var/www/proyecto/drupal]
└─$ sudo systemctl restart apache2
```

Finalmente editamos el archivo de configuración de apache, /etc/apache2/apache2.conf para que haya redireccionamiento limpio en las url.

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

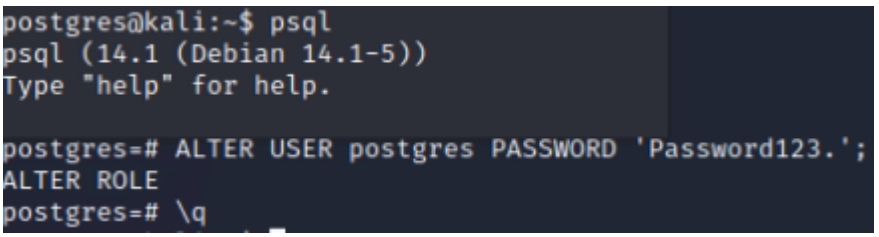


Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine



Configuración PostgreSQL

Cambiamos la contraseña del usuario postgres



Crearemos un rol llamado “proyect_owner” quien será dueño de la base de datos para nuestra página.

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
┌──(root💀kali)-[/var/www/proyecto]
└─# sudo -i -u postgres
┌──(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
postgres@kali:~$ createuser --interactive
Enter name of role to add: proyect_owner
Shall the new role be a superuser? (y/n) y
```

```
┌──(root💀kali)-[/var/www/proyecto]
└─# adduser proyect_owner
Adding user `proyect_owner' ...
Adding new group `proyect_owner' (1002) ...
Adding new user `proyect_owner' (1002) with group `proyect_owner' ...
Creating home directory `/home/proyect_owner' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for proyect_owner
Enter the new value, or press ENTER for the default
        Full Name []: Proyect_owner
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
```

Y ahora podemos iniciar sesión con el usuario proyect_owner

```
┌──(root💀kali)-[/var/www/proyecto]
└─# sudo -i -u proyect_owner
┌──(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(proyect_owner㉿kali)-[~]
└─$ psql
psql (14.1 (Debian 14.1-5))
Type "help" for help.

proyect_owner=#
```

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

Creación Base de datos

```
┌──(root💀kali)-[/var]
└─# sudo apt install postgresql postgresql-contrib
```

```
┌──(root💀kali)-[/var/lib/postgresql/14]
└─# sudo -i -u postgres                                          1 ✘
┌──(Message from Kali developers)
│
│ This is a minimal installation of Kali Linux, you likely
│ want to install supplementary tools. Learn how:
│ ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
postgres@kali:~$ createuser --interactive
Enter name of role to add: proyect_owner
Shall the new role be a superuser? (y/n) y
postgres@kali:~$ createdb proyect_owner
postgres@kali:~$ exit
logout
```

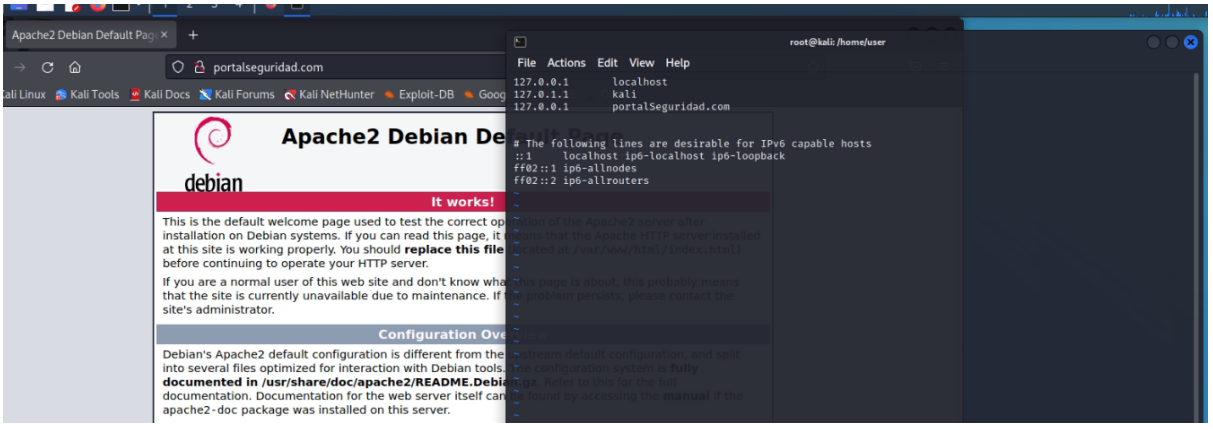
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

```
                                                List of databases
    Name     |  Owner   | Encoding |   Collate   |    Ctype    |   Acc
ess privileges
-------------+----------+----------+-------------+-------------+------
-------------
 postgres    | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 proyect_owner | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/po
stgres          +
             |          |          |             |             | postg
res=CTc/postgres
 template1   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/po
stgres          +
             |          |          |             |             | postg
res=CTc/postgres
```

```
postgres@kali:~$ psql
psql (14.2 (Debian 14.2-1+b3))
Type "help" for help.

postgres=# ALTER USER proyect_owner WITH PASSWORD 'Password123.'
```

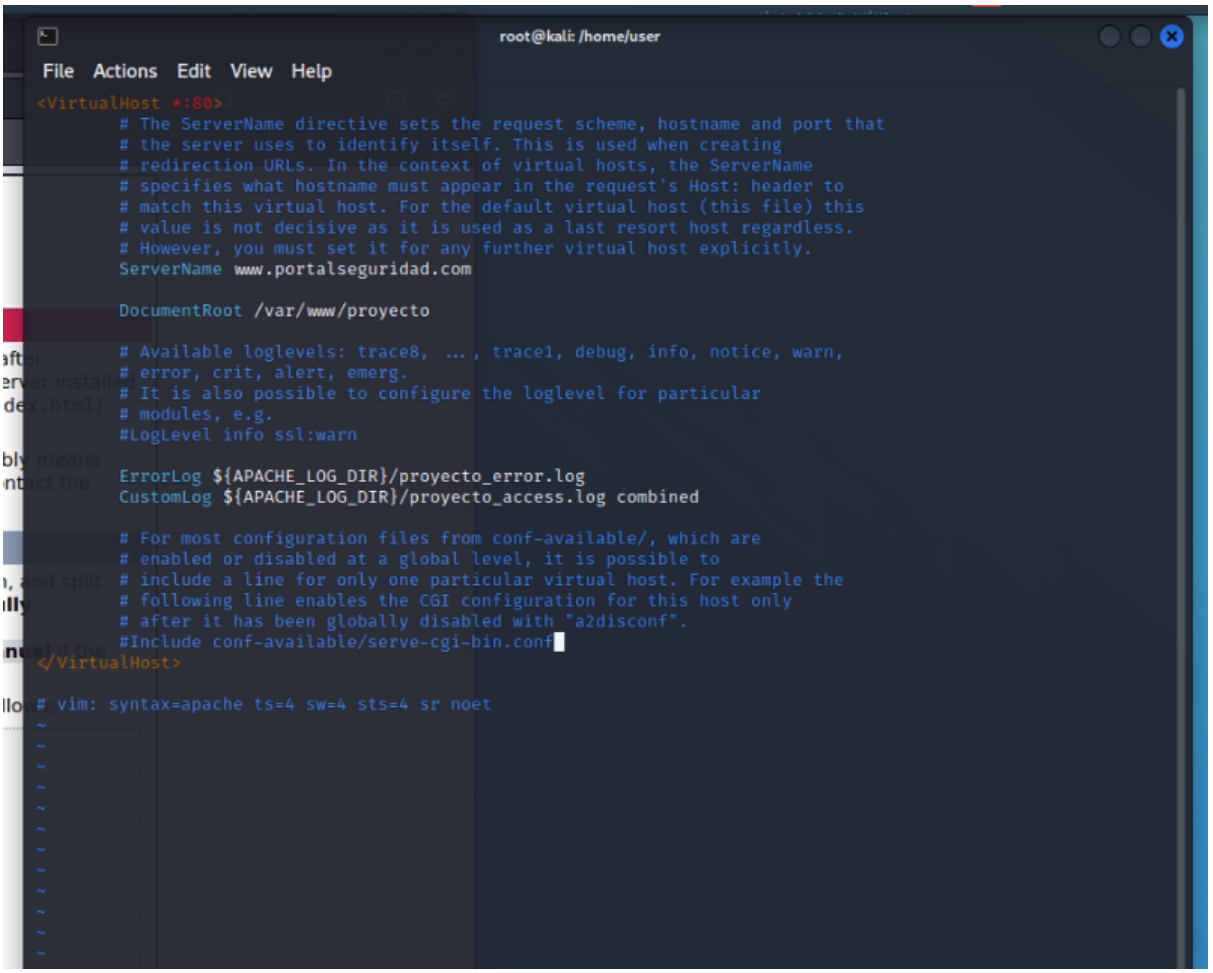
Configuración sitio

Para validar la correcta instalación de apache2, editamos el archivo `/etc/hosts` para agregar una URL asociada a localhost. Usaremos el nombre de portalSeguridad.com para la creación de nuestro sitio.



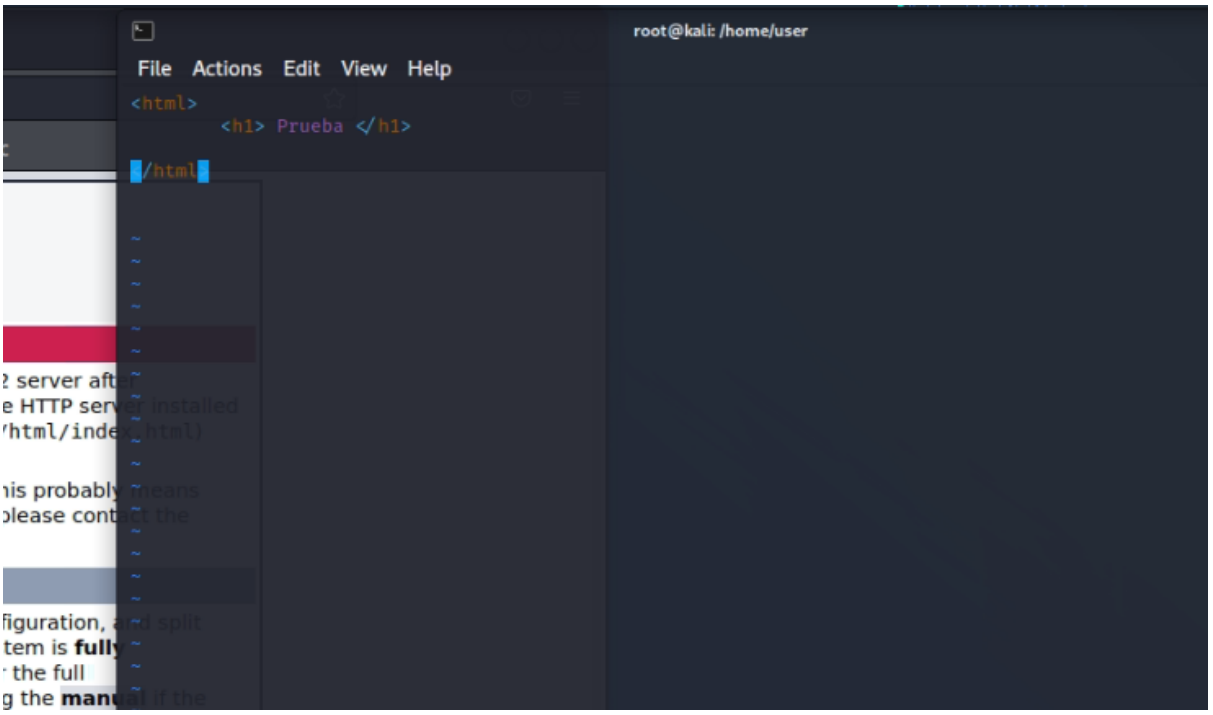
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

Editamos el VirtualHost de nuestro sitio:
`/etc/apache2/sites-available/portal.conf`

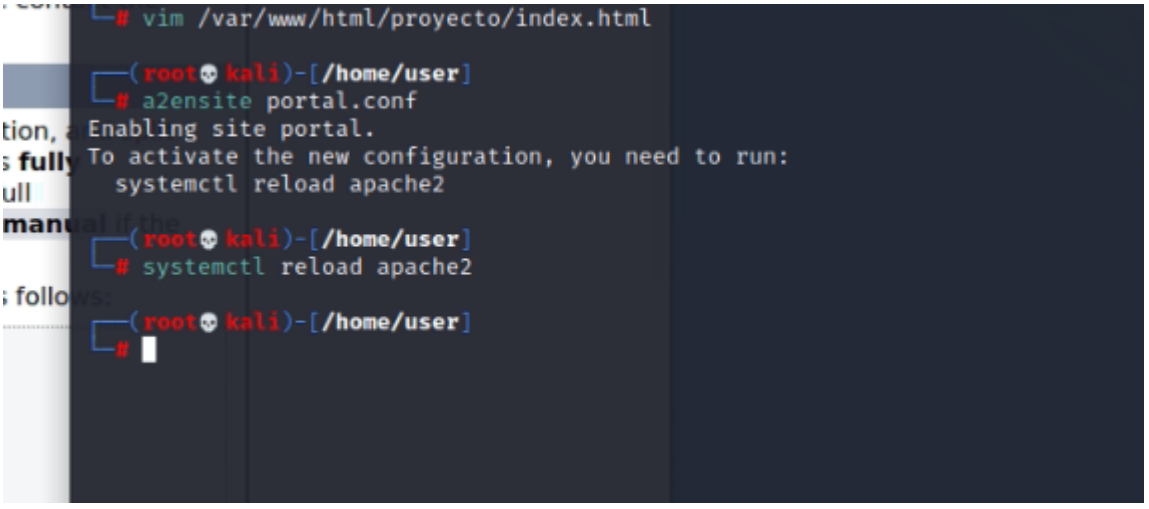


Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

Dentro de la carpeta `/var/www/proyecto` editamos el archivo `index.html`



Y habilitamos el nuevo virtualHost y recargamos la configuración de apache2.



Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

Certificado

Los certificados SSL funcionan garantizando que los datos transferidos entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. Utiliza algoritmos de cifrado para cifrar los datos en tránsito, lo que evita a los hackers interceptar la información que se envía a través de la conexión.

Para el certificado autofirmado utilizamos el siguiente comando:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt

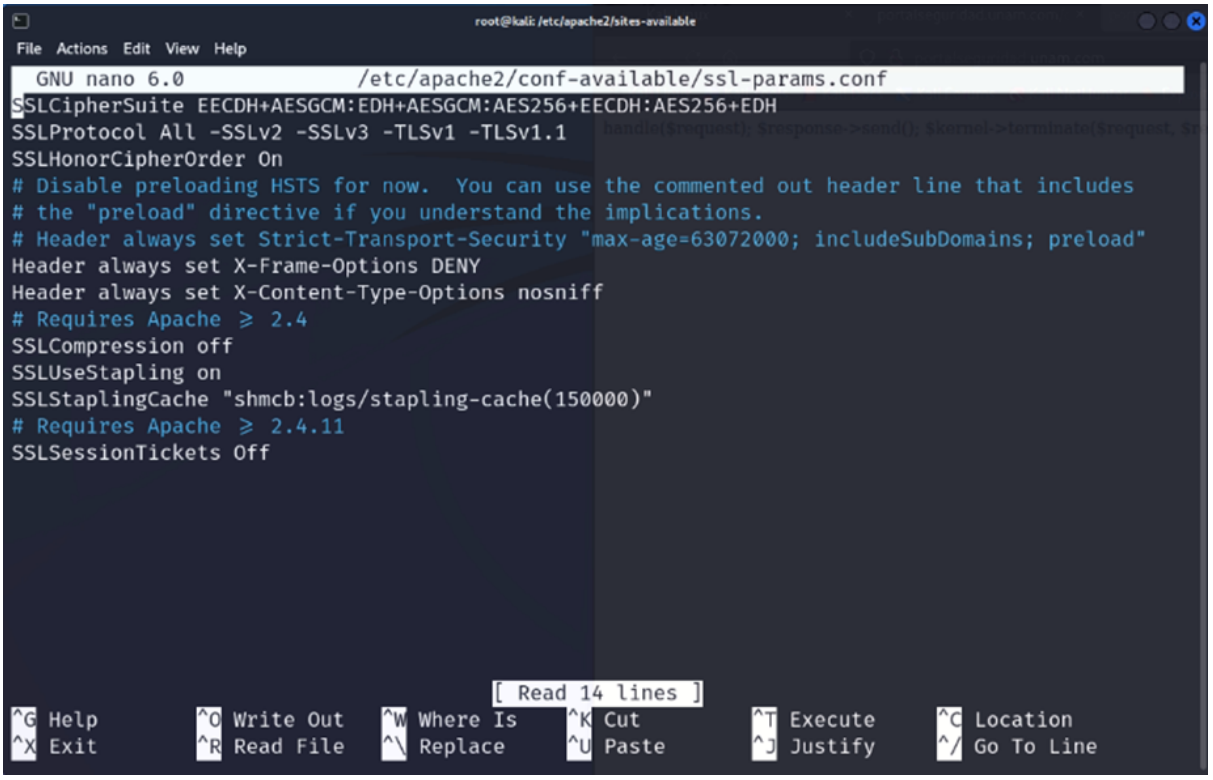
Explicado por partes:
openssl: herramienta para crear y administrar certificados
req -x509: estándar para la infraestructura de claves públicas
-nodes: omite la opción para proteger nuestro certificado con una frase de contraseña
-newkey rsa:2048: generar clave y certificado al mismo tiempo, usando una clave de 2048 bits de extensión
-keyout: ruta del archivo de clave privada
-out: ruta del certificado

Después de esto se debe llenar la ficha con las solicitudes, entre ellos país, estado, nombre de la organización, el nombre del servidor y correo del administrador.

Lo siguiente es modificar el archivo de host virtual de Apache SSL incluido para apuntar a los certificados SSL que generamos.

Cree un nuevo fragmento en el directorio /etc/apache2/conf-available. Daremos el nombre ssl-params.conf al archivo para que quede claro su propósito:

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

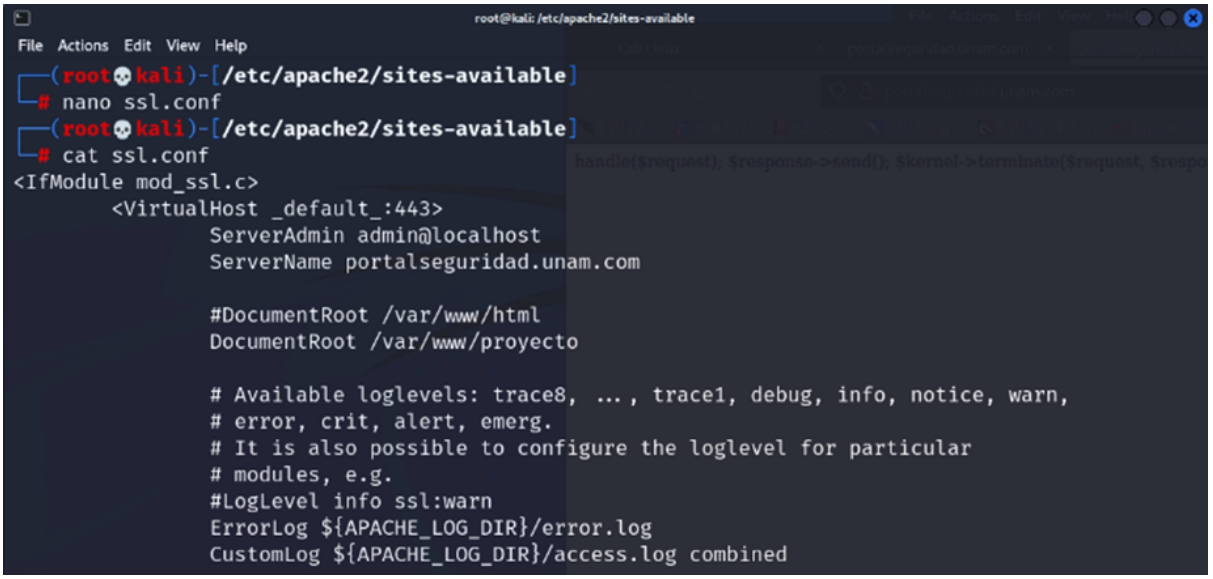


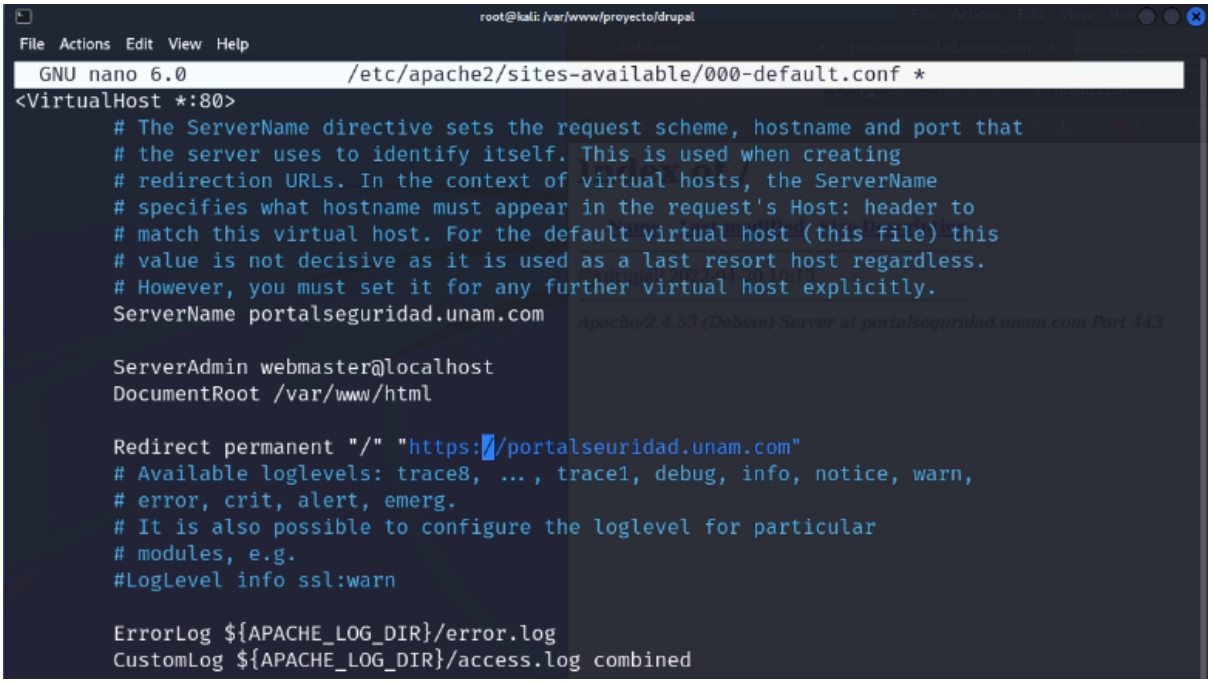
Copiar archivo de configuración del Virtual Host ssl-default.conf a ssl.conf
cp ssl-default.conf ssl.conf

*Trabajar lo de ssl-default.conf en "ssl.conf"

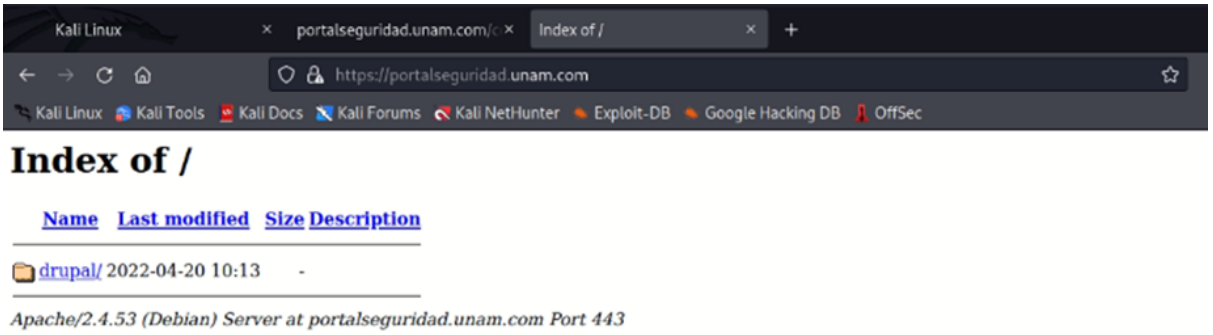
Copa seguridad: cp /etc/apache2/sites-available/ssl.conf
/etc/apache2/sites-available/ssl.conf.bak

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine





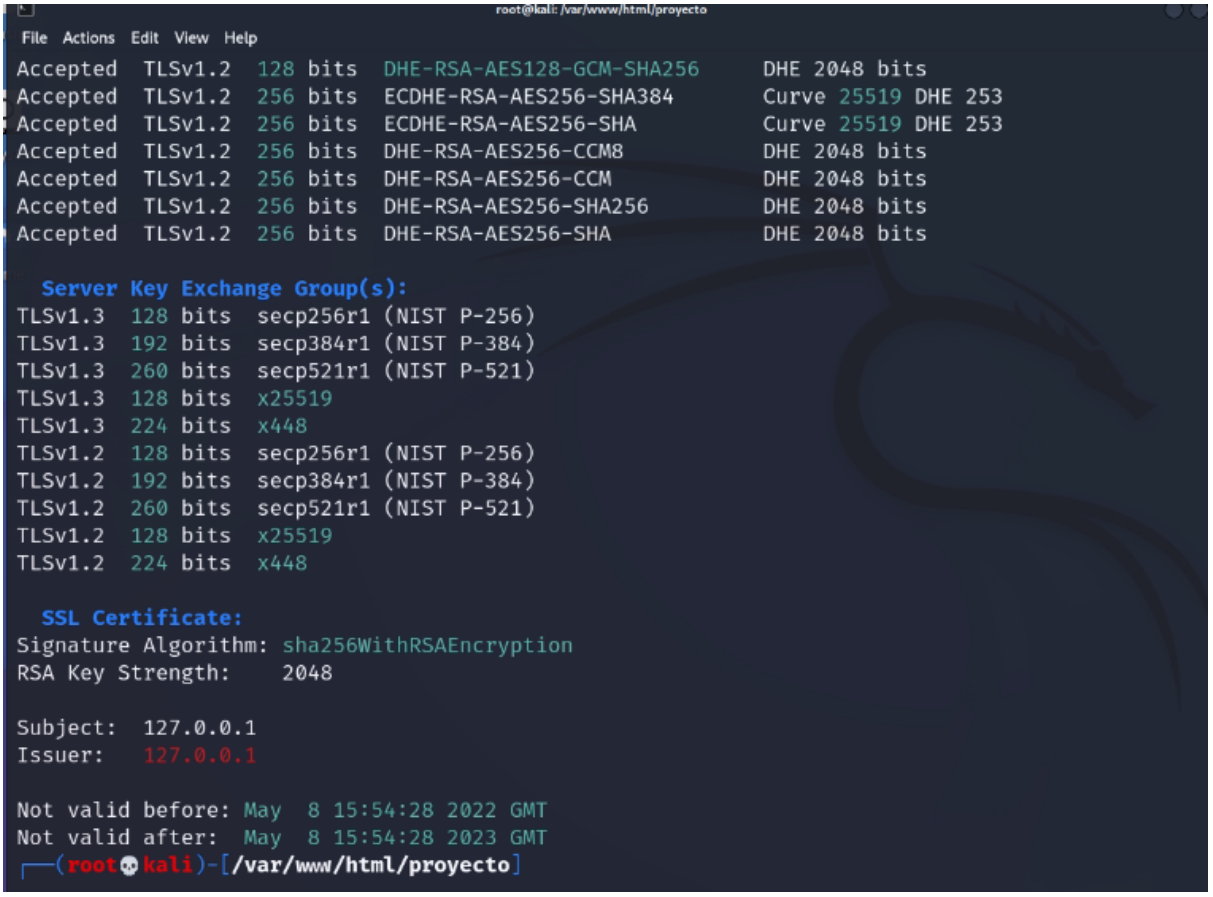
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine




```
┌──(root💀kali)-[/var/www/proyecto/drupal]
└─# apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using
127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
┌──(root💀kali)-[/var/www/proyecto/drupal]
└─# systemctl restart apache2
```

```
┌──(root💀kali)-[/var/www/html/proyecto]
└─# sslscan portalseguridad.unam.com
Version: 2.0.12-static
OpenSSL 1.1.1n-dev  xx XXX xxxx

Connected to 127.0.0.1

Testing SSL server portalseguridad.unam.com on port 443 using SNI name portalseguridad.unam.com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled
```

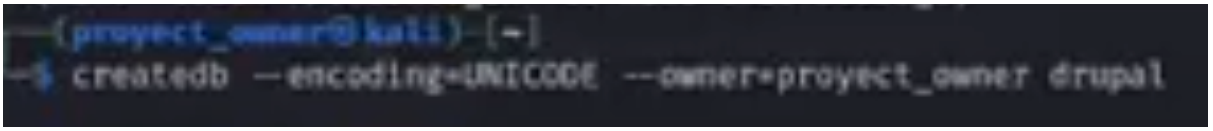
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine



Configuración Drupal

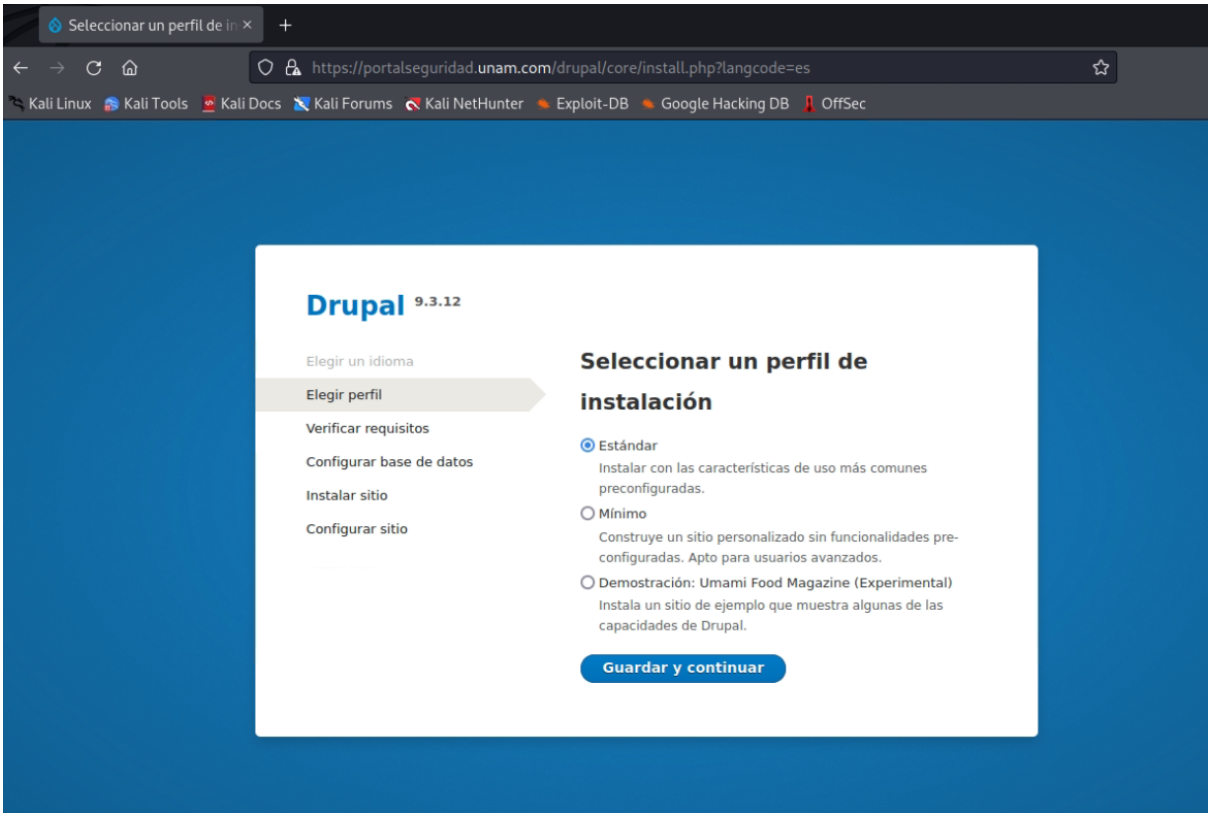
Con el usuario proyect_owner creamos una base de datos llamada “drupal”
Esto es con el comando

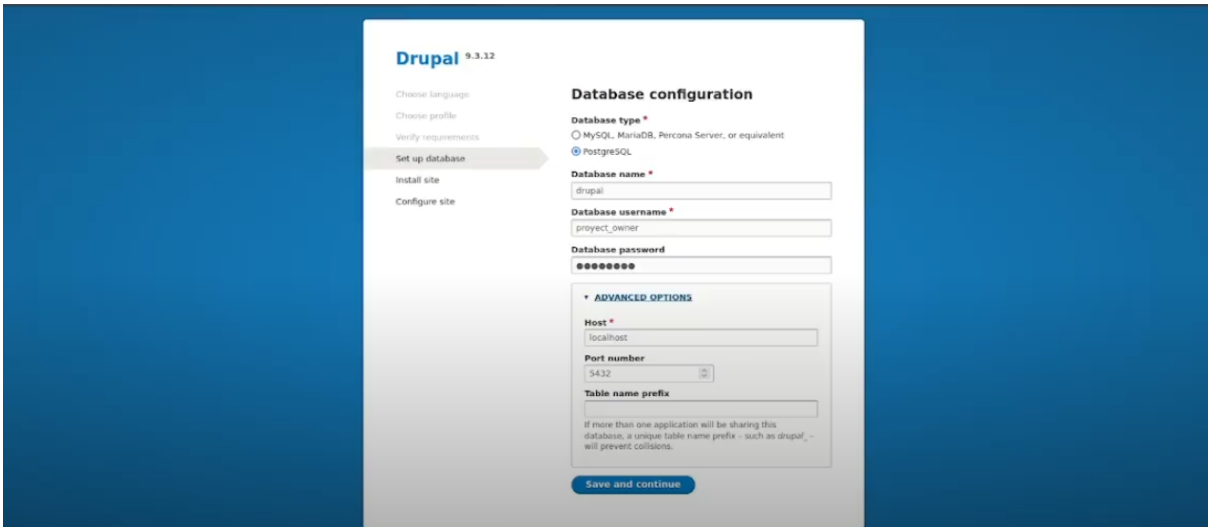
```
createdb --encoding=UNICODE --owner=proyect_owner drupal
```



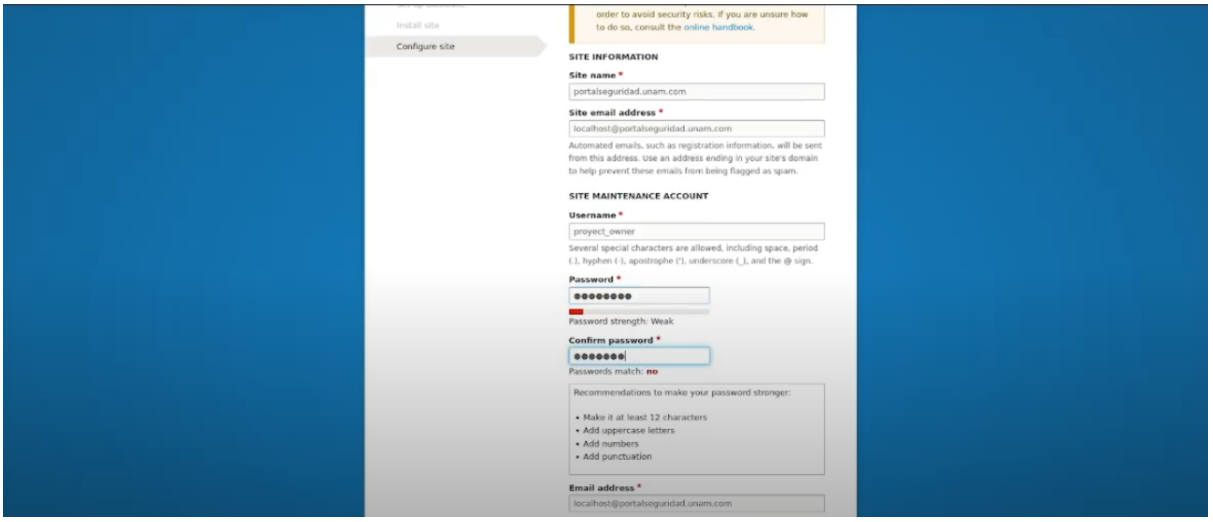
Accedemos a la liga https://portalseguridad.unam.com/drupal/core/install.php y seleccionamos el idioma español. Después elegimos el perfil de instalación, que será estándar.

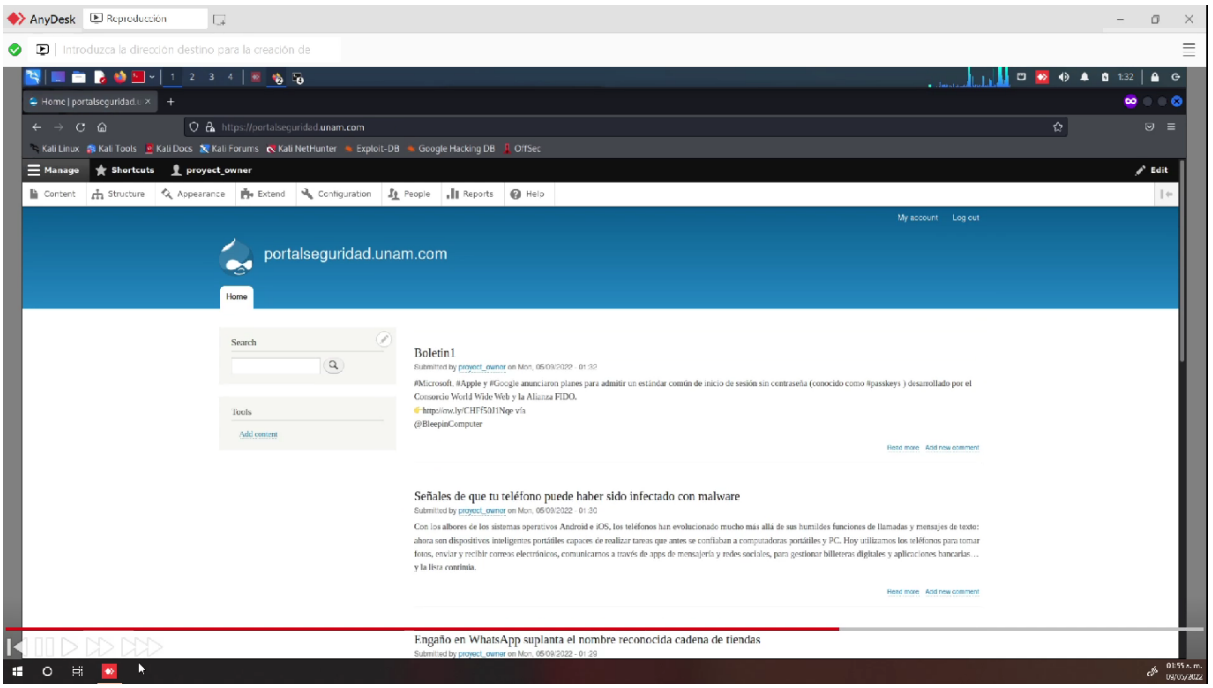
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine



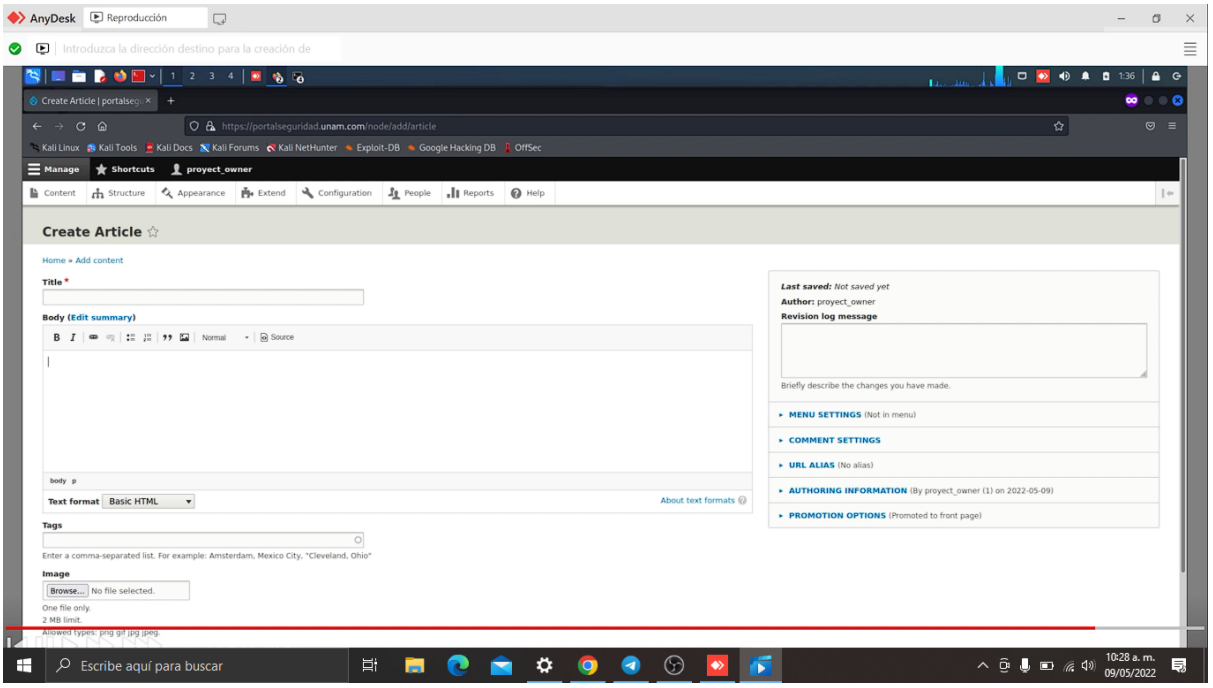


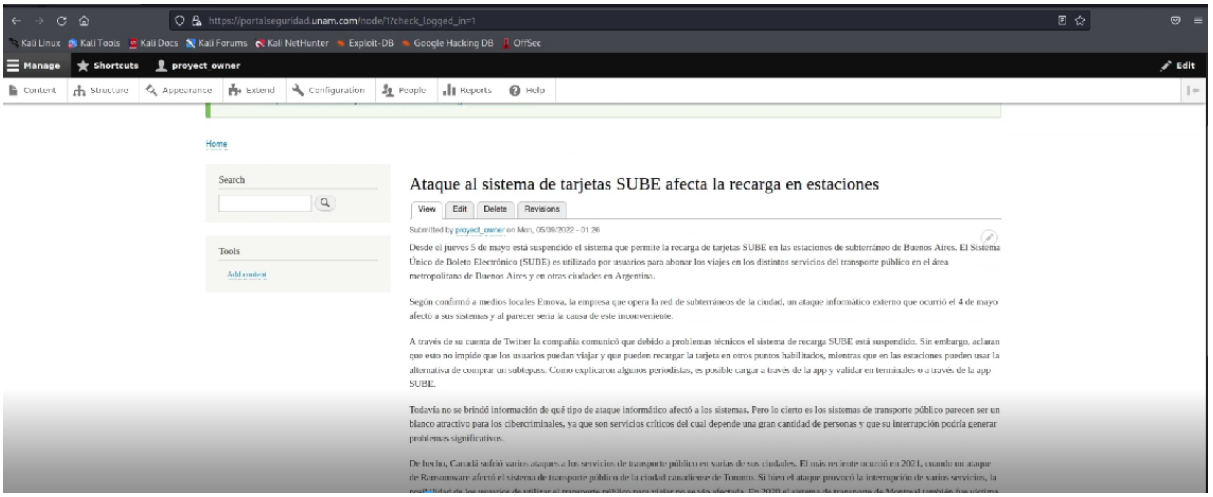
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine





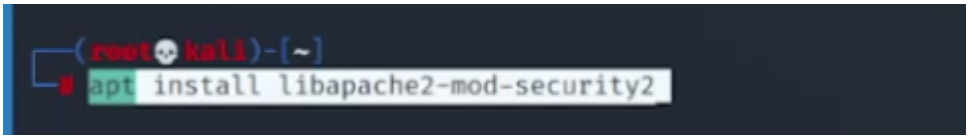
Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine





WAF

Un Web Application Firewall (WAF) protege de múltiples ataques al servidor de aplicaciones web en el backend. La función del WAF es garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico.
El WAF que se eligio en este proyecto fue mod security, el cual se instalo mediante apt.



Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine

Ya instalado se habilita el modulo de sguridad.

```
┌──(root💀kali)-[~]
└─# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
```

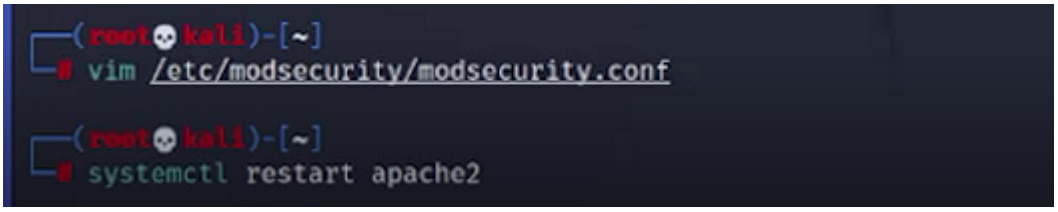
Se copia el archvo de configuración y se edita el correspondiente para habilitar la configuracion.

```
┌──(root💀kali)-[~]
└─# cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/mo
dsecurity.conf
```

En la opcion de SecRuleEngine On se habilitan las reglas

```
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-install
ation
# disruption.
#
SecRuleEngine On


# -- Request body handling ---------------------------------------------
------


# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On


# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "(?:application(?:/soap\+|/)|text/)
xml" \
     "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyP
rocessor=XML"
```

Macias Gomez Jorge
Lara López Martha Leticia
Mendez Gallegos Ligia Natalia
Patiño Maza Ismael Zinedine



Referencias

https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-18-04-es

https://www.digitalocean.com/community/tutorials/como-instalar-y-utilizar-postgresql-en-ubuntu-18-04-es

https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04-es

https://waf.io/apidocs/tutorial.html