



**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**



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

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

## Índice

<b>Instalación</b>	<b>2</b>
PHP	2
Apache	4
PostgreSQL	5
Drupal	7
<b>Configuración PostgreSQL</b>	<b>9</b>
<b>Creación Base de datos</b>	<b>11</b>
<b>Configuración sitio</b>	<b>11</b>
<b>Certificado</b>	<b>14</b>
<b>Referencias</b>	<b>14</b>



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

**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
```

```
Removing php-mysql (2:8.1+92) ...

└─(user㉿kali)-[~]
$ sudo apt install php libapache2-mod-php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  libapache2-mod-php php php-mysql
0 upgraded, 3 newly installed, 0 to remove and 1097 not upgraded.
Need to get 0 B/21.7 kB of archives.
After this operation, 47.1 kB of additional disk space will be used.
Selecting previously unselected package libapache2-mod-php.
(Reading database ... 335680 files and directories currently installed.)
Preparing to unpack .../libapache2-mod-php_2%3a8.1+92_all.deb ...
Unpacking libapache2-mod-php (2:8.1+92) ...
Selecting previously unselected package php.
Preparing to unpack .../php_2%3a8.1+92_all.deb ...
Unpacking php (2:8.1+92) ...
Selecting previously unselected package php-mysql.
Preparing to unpack .../php-mysql_2%3a8.1+92_all.deb ...
Unpacking php-mysql (2:8.1+92) ...
Setting up php (2:8.1+92) ...
Setting up php-mysql (2:8.1+92) ...
Setting up libapache2-mod-php (2:8.1+92) ...
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No user sessions are running outdated binaries.

└─(user㉿kali)-[~]
$ █
```

Validamos la instalación



Programa de Becas de Formación en Seguridad Informática

Coordinación de Seguridad de la Información

UNAM-CERT

Seguridad en aplicaciones web

Macias Gomez Jorge

Lara López Martha Leticia

Mendez Gallegos Ligia Natalia

Patiño Maza Ismael Zinedine

```
No containers need to be restarted.  
No user sessions are running outdated binaries.  
└─(user㉿kali)-[~]  
└─$ php -v  
PHP 8.1.2 (cli) (built: Apr 24 2022 08:36:32) (NTS)  
Copyright (c) The PHP Group  
Zend Engine v4.1.2, Copyright (c) Zend Technologies  
with Zend OPcache v8.1.2, Copyright (c), by Zend Technologies  
└─$ ┌─
```

## Apache

Instalamos Apache2 con el comando

```
sudo apt install apache2
```

```
File Actions Edit View Help

└─(user㉿kali)-[~]
$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libldap2-2.5-0 libldap-common libsasl2-2 libsasl2-dev
  libsasl2-modules-db
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Recommended packages:
  libsasl2-modules
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils libldap2-2.5-0 libldap-common
The following packages will be upgraded:
  apache2-bin libsasl2-2 libsasl2-dev libsasl2-modules-db
4 upgraded, 5 newly installed, 0 to remove and 1093 not upgraded.
Need to get 2,770 kB of archives.
After this operation, 2,594 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 libsasl2-dev amd64 2.1.28+dfsg-4 [249 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libsasl2-modules-db amd64 2.1.28+dfsg-4 [38.0 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 libsasl2-2 amd64 2.1.28+dfsg-4 [76.8 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libldap2-2.5-0 amd64 2.5.11+dfsg-1 [226 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 apache2-bin amd64 2.4.53-2 [1,417 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 apache2-data all 2.4.53-2 [160 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 apache2-utils amd64 2.4.53-2 [259 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 apache2 amd64 2.4.53-2 [273 kB]
Get:9 http://http.kali.org/kali kali-rolling/main amd64 libldap-common all 2.5.11+dfsg-1 [71.5 kB]
Fetched 2,770 kB in 21s (130 kB/s)
(Reading database ... 335689 files and directories currently installed.)
Preparing to unpack .../0-libsasl2-dev_2.1.28+dfsg-4_amd64.deb ...
Unpacking libsasl2-dev (2.1.28+dfsg-4) over (2.1.27+dfsg2-3) ...
Preparing to unpack .../1-libsasl2-modules-db_2.1.28+dfsg-4_amd64.deb ...
Unpacking libsasl2-modules-db:amd64 (2.1.28+dfsg-4) over (2.1.27+dfsg2-3) ...
Preparing to unpack .../2-libsasl2-2_2.1.28+dfsg-4_amd64.deb ...
Unpacking libsasl2-2:amd64 (2.1.28+dfsg-4) over (2.1.27+dfsg2-3) ...
Selecting previously unselected package libldap2-2.5-0:amd64.
Preparing to unpack .../3-libldap2-2.5-0_2.5.11+dfsg-1_amd64.deb ...
Unpacking libldap2-2.5-0:amd64 (2.5.11+dfsg-1) ...
Preparing to unpack .../4-apache2-bin_2.4.53-2_amd64.deb ...
Unpacking apache2-bin (2.4.53-2) over (2.4.52-1) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../5-apache2-data_2.4.53-2_all.deb ...
Unpacking apache2-data (2.4.53-2) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../6-apache2-utils_2.4.53-2_amd64.deb ...
Unpacking apache2-utils (2.4.53-2) ...
Selecting previously unselected package apache2.
Preparing to unpack .../7-apache2_2.4.53-2_amd64.deb ...
Unpacking apache2 (2.4.53-2) ...
```

## PostgreSQL

Para la instalación, es necesario instalar algunos paquetes:

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

```
[root@kali ~]# 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 ~]# sudo apt install postgresql
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]
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**

```
(root㉿kali)-[~/var/www/proyecto]
# systemctl start postgresql.service
```

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

## Drupal

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

Instalar el módulo compatible de php-postgres

```
[user@kali)-[~] postgres | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
$ sudo apt-get install php-pgsql | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
[sudo] password for user: | UTF8 | en_US.UTF-8 | en_US.UTF-8 | *c/postgres |
Reading package lists ... Done | UTF8 | en_US.UTF-8 | en_US.UTF-8 | postgres=CTc/postgres |
Building dependency tree ... Done | UTF8 | en_US.UTF-8 | en_US.UTF-8 | =c/postgres |
Reading state information ... Done | UTF8 | en_US.UTF-8 | en_US.UTF-8 | postgres=CTc/postgres |
The following additional packages will be installed:
php8.1-pgsql | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
The following NEW packages will be installed:
php-pgsql php8.1-pgsql | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
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 ...

List of databases
Running kernel seems to be up-to-date. | Encoding | Collate | Ctype | Access privileges
No services need to be restarted. | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
No containers need to be restarted. | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
No user sessions are running outdated binaries. | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
```

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

```
[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 ... EXECUTE REVOKE
Scanning linux images ... EXPLAIN ROLLBACK
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.
```

```
└─(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 php8.1-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.
```

```
└─(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>



## Download Drupal

Drupal allows you to create a unique space in a world of cookie-cutter solutions.

### Use the Drupal Quickstart command

You'll need [php](#) and [composer](#), and then can run these two commands:

```
composer create-project drupal/recommended-project drupal
cd drupal php -d memory_limit=256M web/core/scripts/drupal quick-start demo_umami
```

For more options when installing drupal from the command line, consult the [quickstart docs](#), or how to start your site using [composer](#).

### Download a composer-ready package

[Download Drupal zip](#)

[download tar.gz](#)

[read release notes](#)

### Looking for Drupal hosting?

[Try a hosted demo](#)

[Explore Hosting](#)

### Enjoying Drupal?

[Give your support](#)

```
(user@kali)-[~/Downloads] gres
$ ls
drupal-9.3.12.zip
```

Descomprimimos el archivo y lo renombramos a drupal

```
(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
  inflating: drupal-9.3.12/vendor/composer/semver/src/Interval.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
```

```
[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.

```
root@kali: /etc/apache2/mods-available
File Actions Edit View Help
LogFormat "%{Referer}i → %U" referer
LogFormat "%{User-agent}i" agent

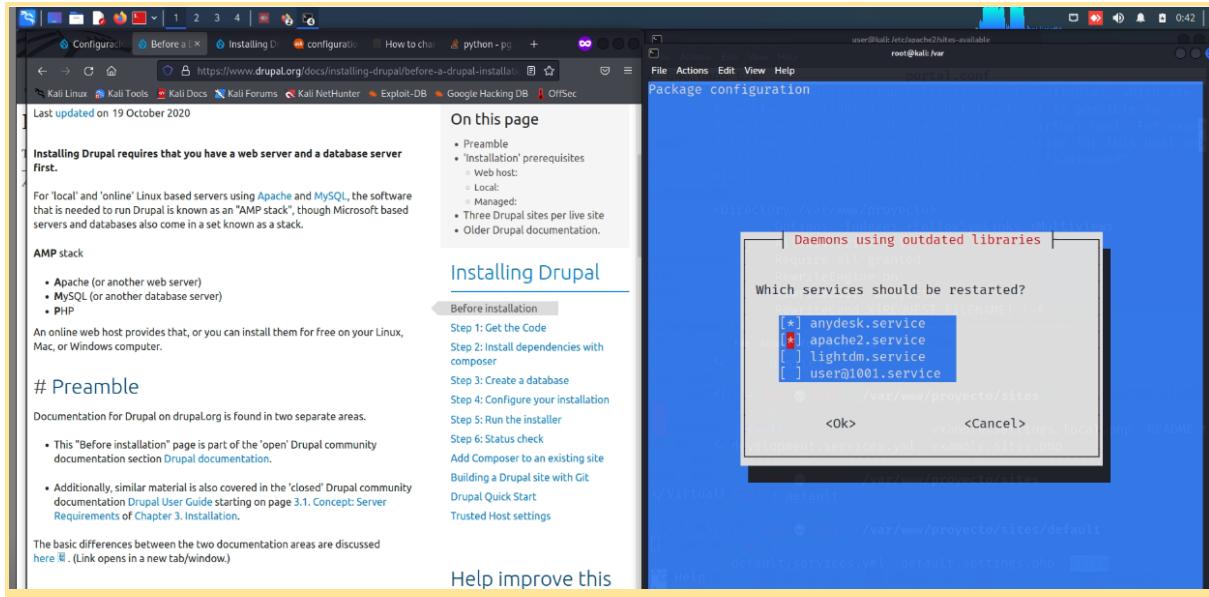
# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

<Directory /var/www/proyecto/>
RewriteEngine on
RewriteBase /
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_URI} !=/favicon.ico
RewriteRule ^(.*)$ index.php?q=$1
[L,QSA]
</Directory>
"/etc/apache2/apache2.conf" 238L, 7457B           237,7          Bot
```



## Configuración PostgreSQL

Cambiamos la contraseña del usuario postgres

```
(root㉿kali)-[~/var/www/proyecto]
# sudo -i -u postgres
postgres@kali:~$ psql
psql (14.1 (Debian 14.1-5))
Type "help" for help.

postgres=# ALTER USER postgres PASSWORD 'Password123.';
ALTER ROLE
postgres# \q
```

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

```
└─(root㉿kali)-[~/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)-[~/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)-[~/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=#
```

## Creación Base de datos

```
└─(root㉿kali)-[~/var]
# sudo apt install postgresql postgresql-contrib ━

└─(root㉿kali)-[/var/lib/postgresql/14]
# sudo -i -u postgres
(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/

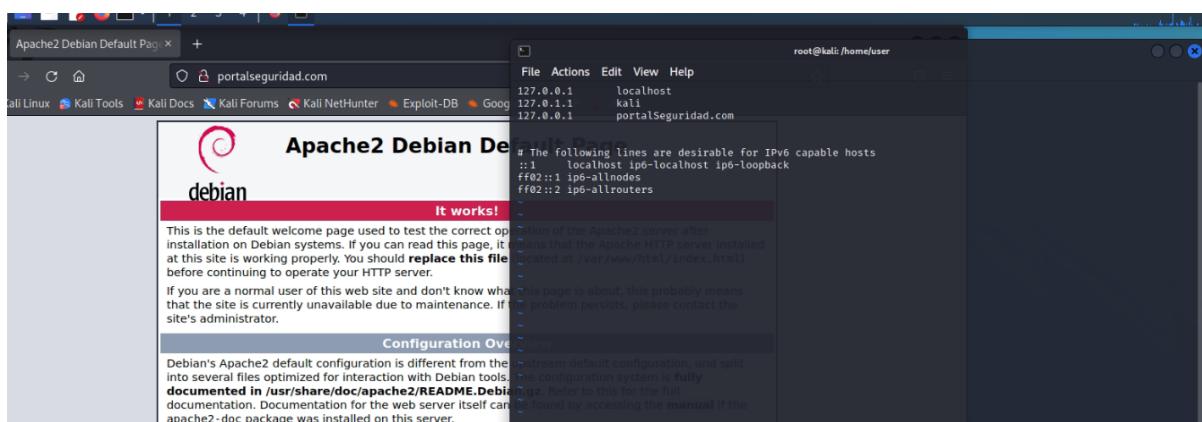
(Run: "touch ~/.hushlogin" to hide this message)
postgres@kali:~$ createuser --interactive
Enter name of role to add: proyect_owner
Shall the new role be a superuser? (y/n) y
postgres@kali:~$ createdb proyect_owner
postgres@kali:~$ exit
logout
```

```
psql (14.2 (Debian 14.2-1+b3))
Type "help" for help.

postgres=# \l
                                         List of databases
   Name    | Owner | Encoding | Collate | Ctype | Access privileges
-----+-----+-----+-----+-----+-----+
 postgres | postgres | UTF8      | en_US.UTF-8 | en_US.UTF-8 |
 proyecto_owner | postgres | UTF8      | en_US.UTF-8 | en_US.UTF-8 |
 template0 | postgres | UTF8      | en_US.UTF-8 | en_US.UTF-8 | =c/o
 postgres |          +-----+-----+-----+-----+-----+
 res=CTc/postgres
 template1 | postgres | UTF8      | en_US.UTF-8 | en_US.UTF-8 | =c/o
 postgres |          +-----+-----+-----+-----+-----+
 res=CTc/postgres
 postgres@kali:~$ psql
 postgres=# ALTER USER proyecto_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.





Editamos el VirtualHost de nuestro sitio:

/etc/apache2/sites-available/portal.conf

```
File Actions Edit View Help
<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.portalseguridad.com

    DocumentRoot /var/www/proyecto

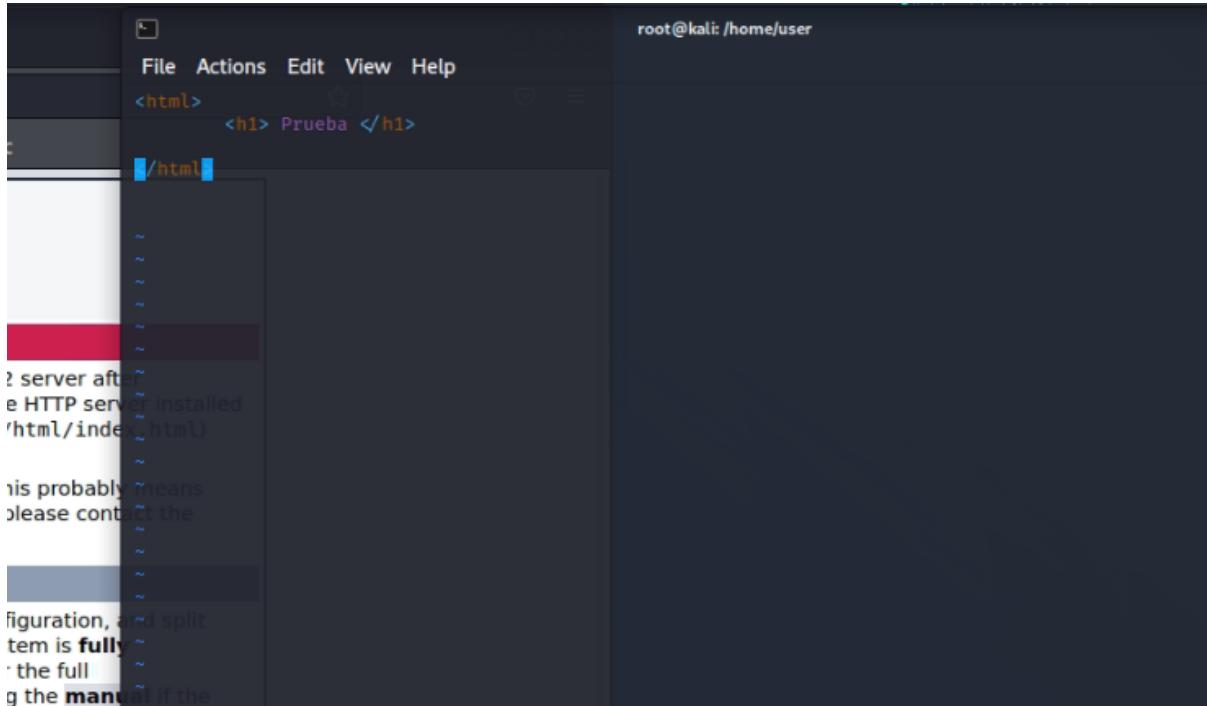
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/proyecto_error.log
    CustomLog ${APACHE_LOG_DIR}/proyecto_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>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

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



A screenshot of a terminal window titled "root@kali: /home/user". The window shows a file editor with the content of index.html. The file contains the following code:

```
<html>
    <h1> Prueba </h1>
```

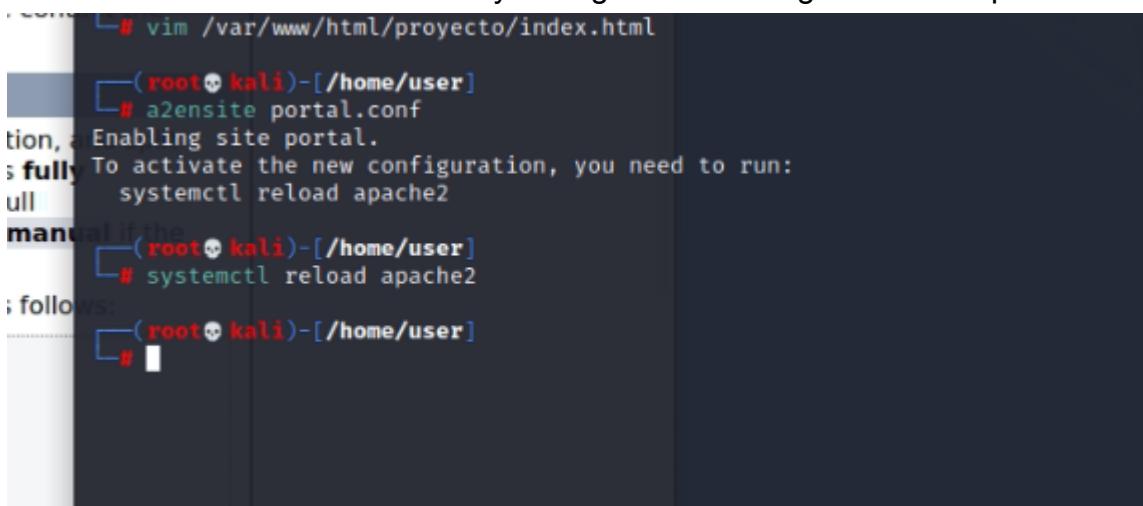
Below the code, there is a large block of text from the Apache error log:

```
? server after installed
e HTTP server installed
'html/index.html'

his probably means
please cont

figuration, and split
tem is fully
the full
g the man if the
```

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



```
# vim /var/www/html/proyecto/index.html
  ↵(root㉿kali)-[~/home/user]
  ↵# a2ensite portal.conf
tion, a Enabling site portal.
s fully To activate the new configuration, you need to run:
ull      systemctl reload apache2
manual if the
  ↵(root㉿kali)-[~/home/user]
  ↵# systemctl reload apache2
; follows:
  ↵(root㉿kali)-[~/home/user]
  ↵#
```

## 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 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*

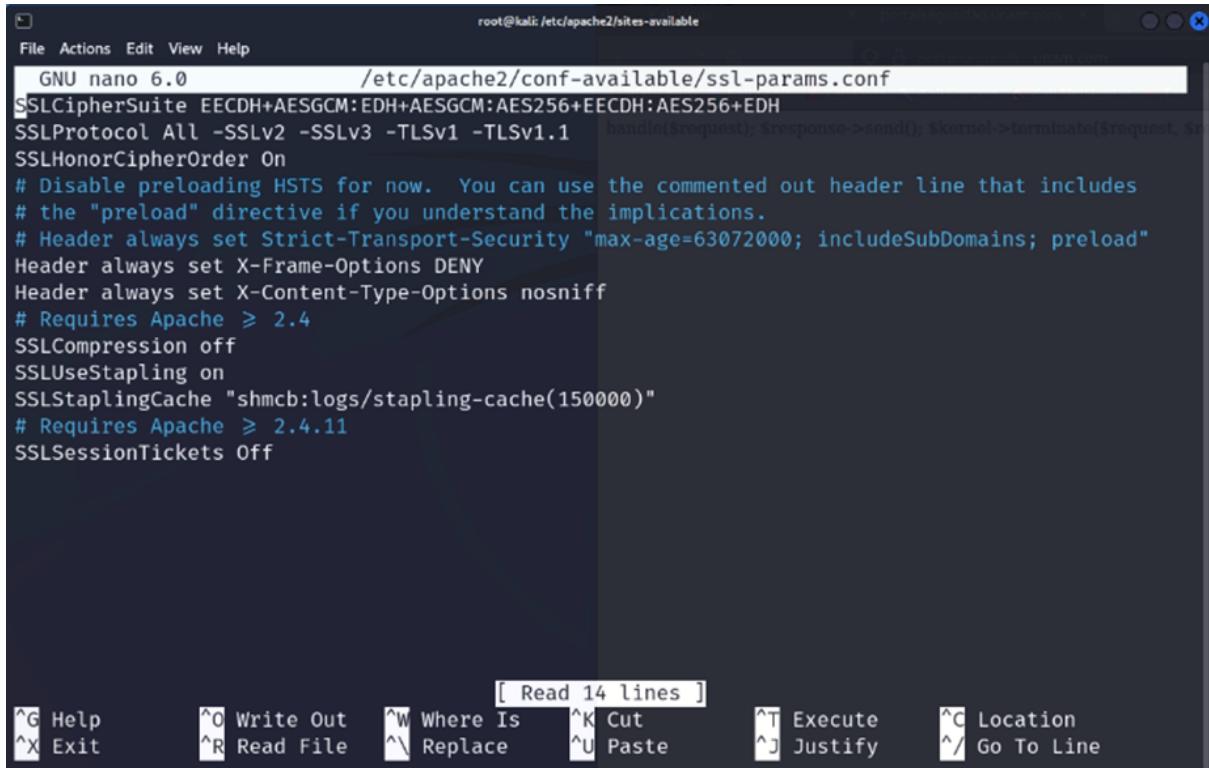
*-keyout: ruta del archivo de clave privada*

*-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:



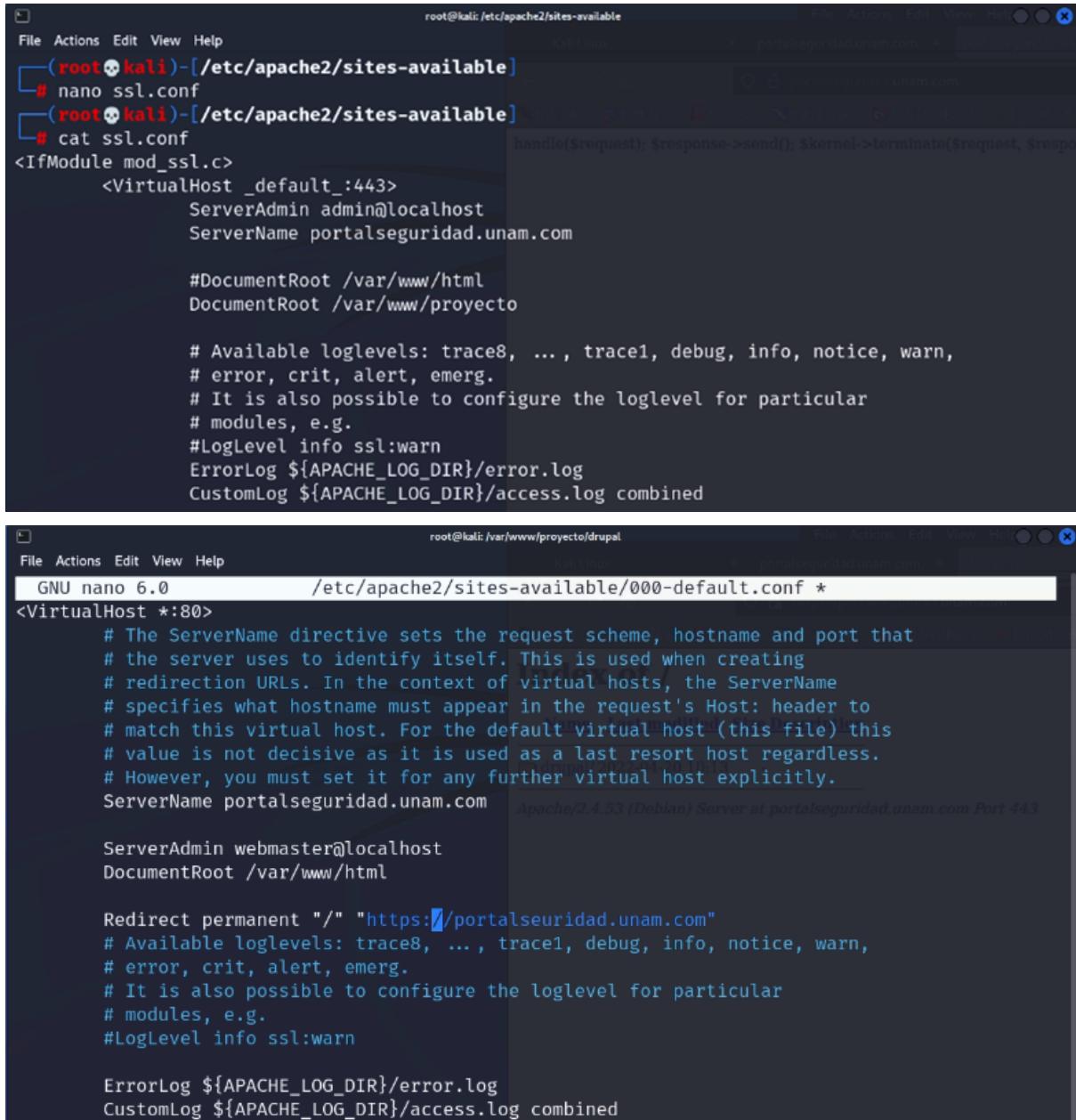
```
root@kali: /etc/apache2/sites-available
File Actions Edit View Help
GNU nano 6.0          /etc/apache2/conf-available/ssl-params.conf
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
# Disable preloading HSTS for now. You can use the commented out header line that includes
# the "preload" directive if you understand the implications.
# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
# Requires Apache ≥ 2.4
SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
# Requires Apache ≥ 2.4.11
SSLSessionTickets Off

[ Read 14 lines ]
^G Help      ^O Write Out    ^W Where Is     ^K Cut        ^T Execute     ^C Location
^X Exit      ^R Read File     ^\ Replace      ^U Paste       ^J Justify     ^/ Go To Line
```

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



```
root@kali:/etc/apache2/sites-available
File Actions Edit View Help
[root@kali ~]# nano ssl.conf
[root@kali ~]# cat ssl.conf
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin admin@localhost
        ServerName portalseguridad.unam.com

        #DocumentRoot /var/www/html
        DocumentRoot /var/www/proyecto

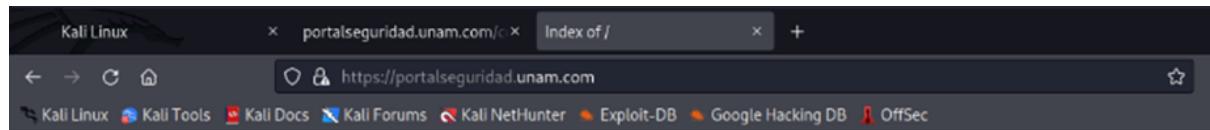
        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

root@kali:/var/www/proyecto/drupal
File Actions Edit View Help
GNU nano 6.0          /etc/apache2/sites-available/000-default.conf *
<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 portalseguridad.unam.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    Redirect permanent "/" "https://portalseguridad.unam.com"
    # 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
```



## Index of /

Name	Last modified	Size	Description
------	---------------	------	-------------

drupal/	2022-04-20 10:13	-	
---------	------------------	---	--

Apache/2.4.53 (Debian) Server at portalseguridad.unam.com Port 443

```
(root💀kali㉿kali)-[~/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
└─# systemctl restart apache2

(root💀kali㉿kali)-[~/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
```

```
root@kali: /var/www/html/proyecto
File Actions Edit View Help
Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256      DHE 2048 bits
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384      Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA      Curve 25519 DHE 253
Accepted TLSv1.2 256 bits DHE-RSA-AES256-CCM8      DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-CCM      DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256      DHE 2048 bits
Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA      DHE 2048 bits

Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.3 224 bits x448
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519
TLSv1.2 224 bits x448

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: 127.0.0.1
Issuer: 127.0.0.1

Not valid before: May 8 15:54:28 2022 GMT
Not valid after: May 8 15:54:28 2023 GMT
└─(root💀kali㉿kali)-[/var/www/html/proyecto]
```

## Configuración Drupal

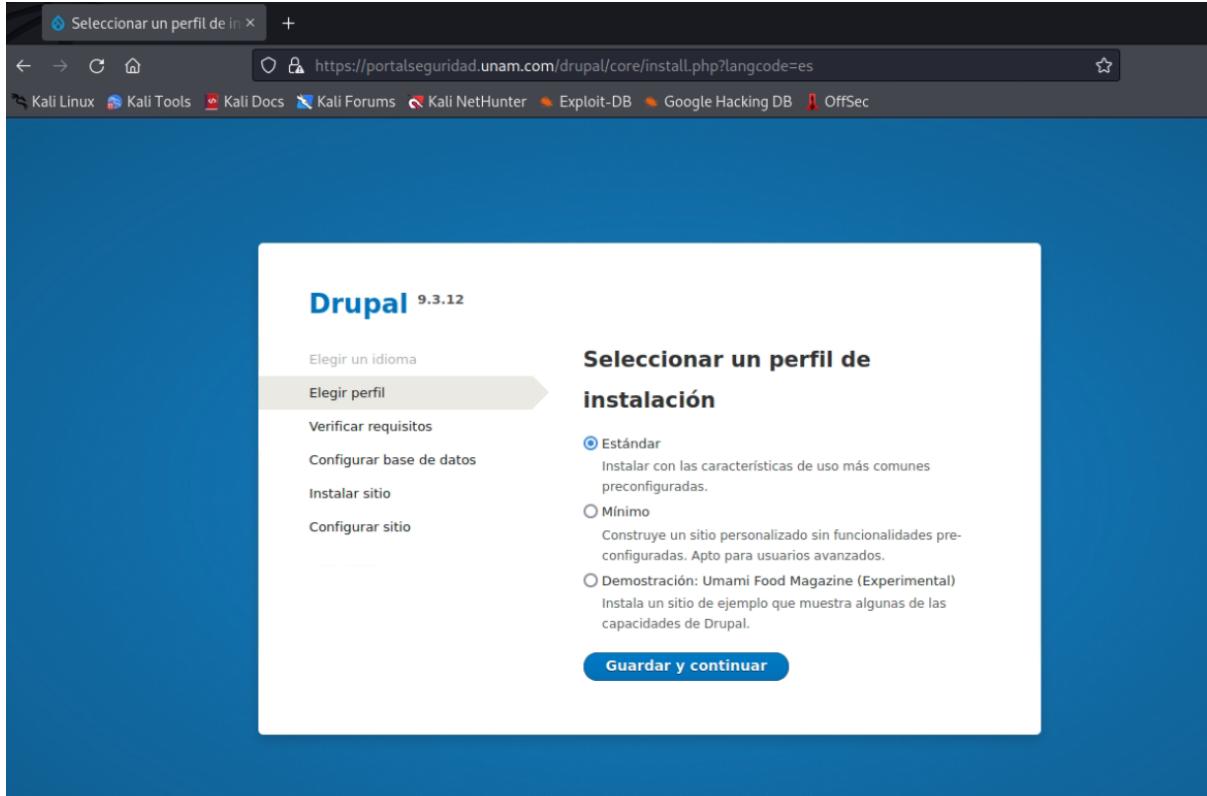
Con el usuario project\_owner creamos una base de datos llamada “drupal”

Esto es con el comando

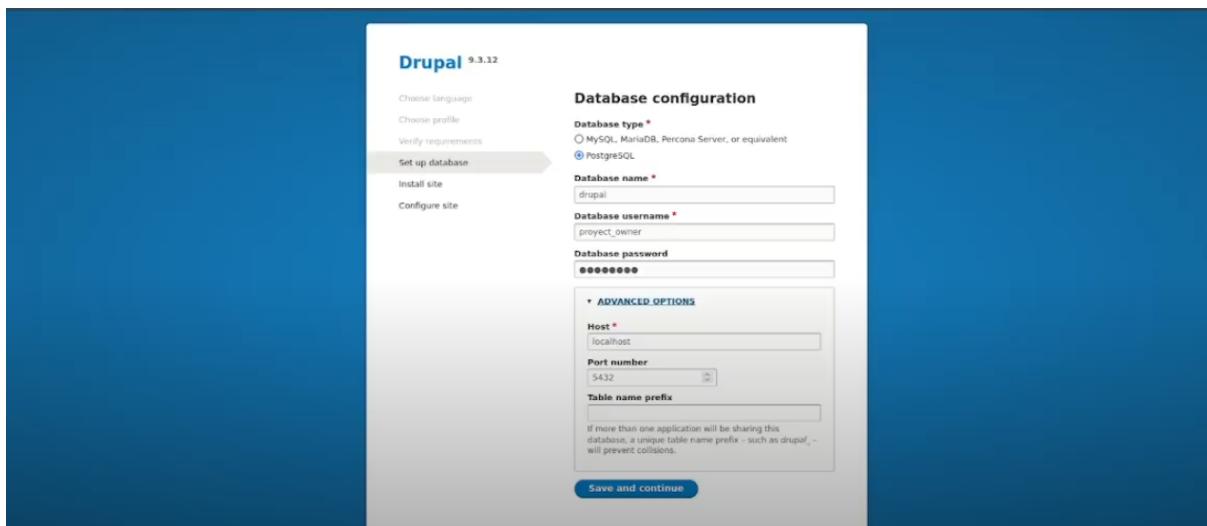
```
createdb --encoding=UNICODE --owner=project_owner drupal
```

```
─(project_owner㉿kali)-[~]
└─$ createdb --encoding=UNICODE --owner=project_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.



The screenshot shows the 'Drupal 9.3.12' installation interface. On the left, a sidebar lists steps: 'Elegir un idioma', 'Elegir perfil' (which is selected), 'Verificar requisitos', 'Configurar base de datos', 'Instalar sitio', and 'Configurar sitio'. The main area is titled 'Seleccionar un perfil de instalación'. It shows three options: 'Estándar' (selected), 'Mínimo', and 'Demostración: Umami Food Magazine (Experimental)'. A 'Guardar y continuar' button is at the bottom.

The screenshot shows the 'Database configuration' step of the Drupal 9.3.12 installation. The sidebar now includes 'Set up database' (selected), 'Install site', and 'Configure site'. The main area is titled 'Database configuration' and contains fields for 'Database type' (PostgreSQL selected), 'Database name' (drupal), 'Database username' (project\_owner), and 'Database password' (\*\*\*\*\*). Advanced options for 'Host' (localhost), 'Port number' (5432), and 'Table name prefix' are shown below. A note states: 'If more than one application will be sharing this database, a unique table name prefix - such as drupal\_ - will prevent collisions.' A 'Save and continue' button is at the bottom.

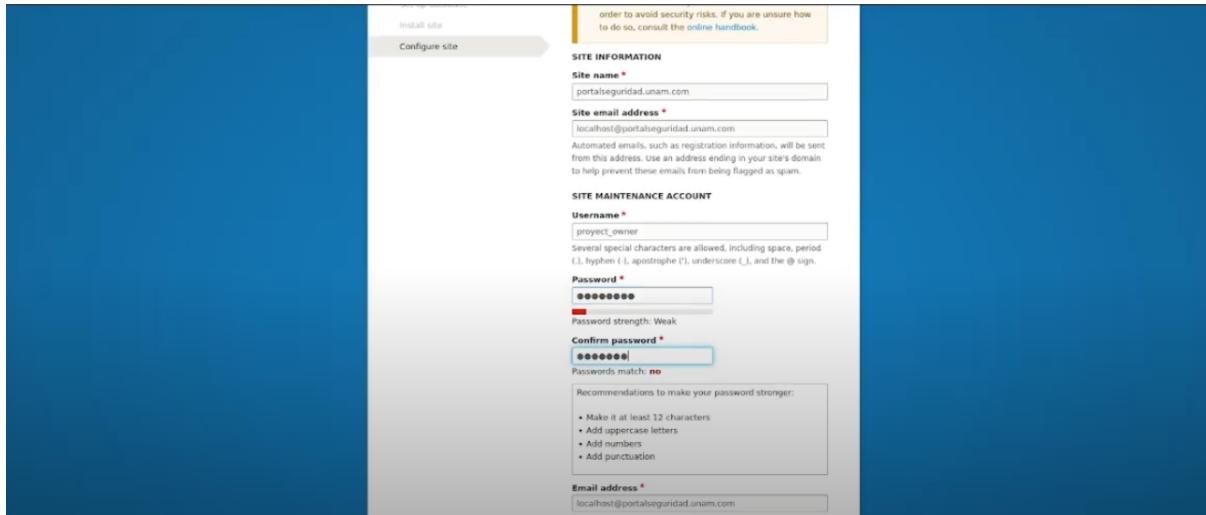
# Programa de Becas de Formación en Seguridad Informática

Coordinación de Seguridad de la Información

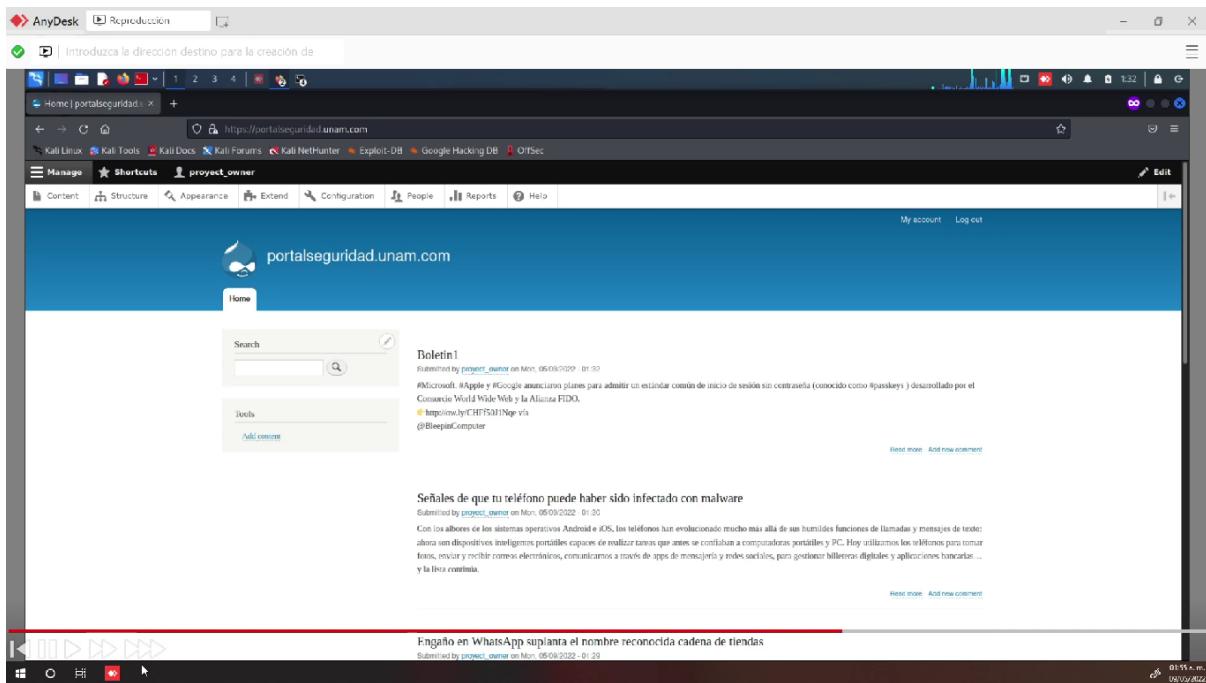
UNAM-CERT

Seguridad en aplicaciones web

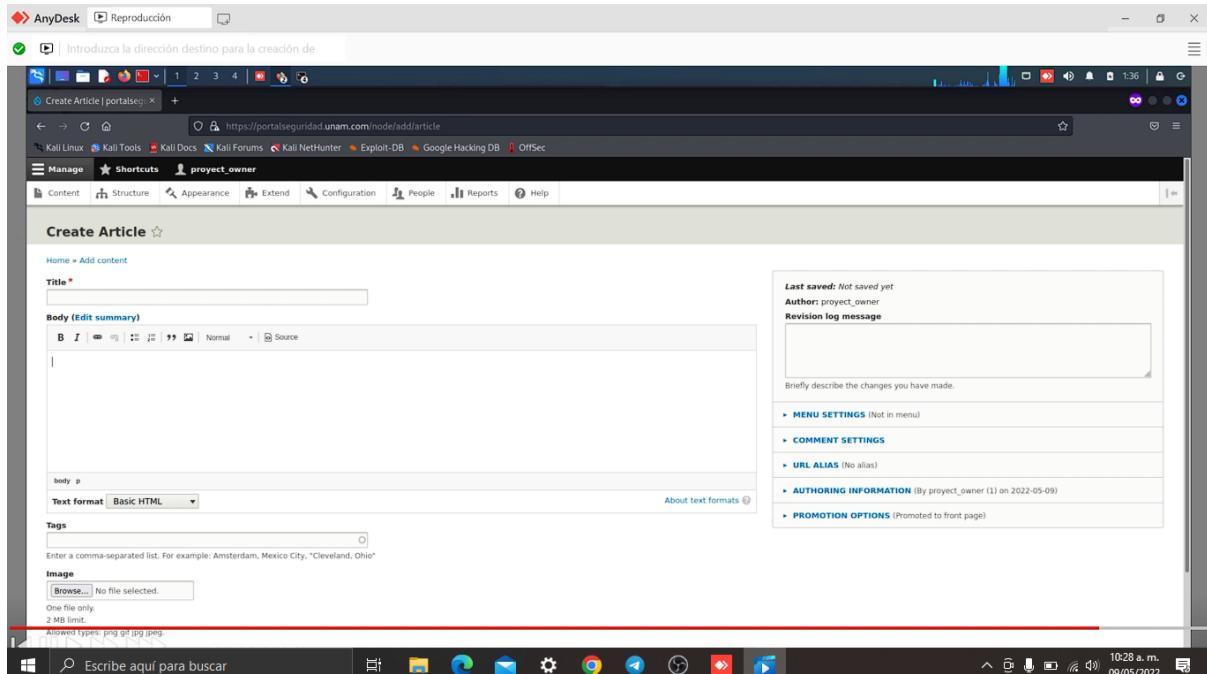
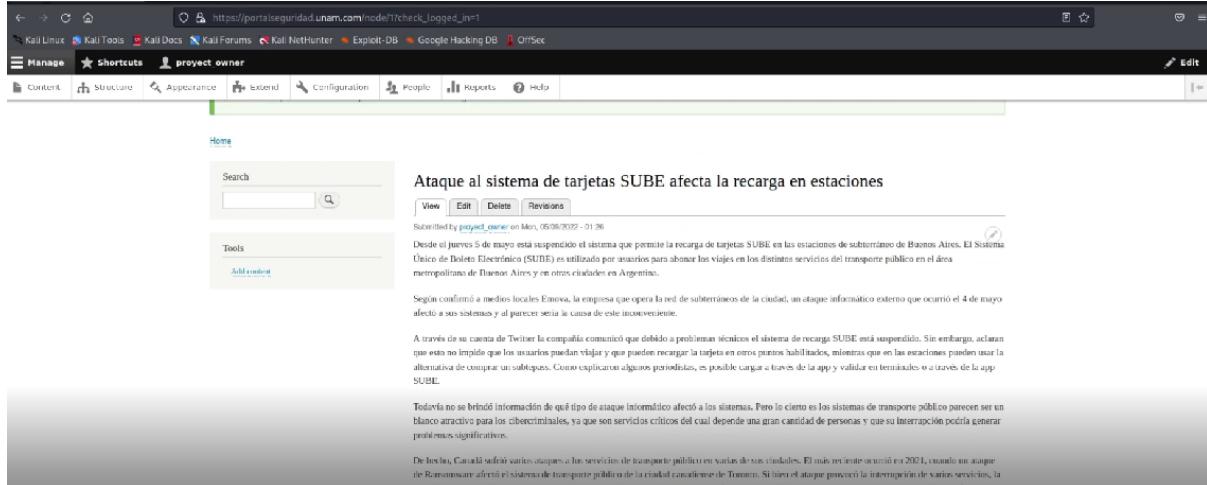
**Macias Gomez Jorge**  
**Lara López Martha Leticia**  
**Mendez Gallegos Ligia Natalia**  
**Patiño Maza Ismael Zinedine**



The screenshot shows the 'Configure site' interface. In the 'SITE INFORMATION' section, the 'Site name' is set to 'portalseguridad.unam.com' and the 'Site email address' is 'localhost@portalseguridad.unam.com'. In the 'SITE MAINTENANCE ACCOUNT' section, the 'Username' is 'project\_mener' and the 'Password' is '\*\*\*\*\*'. A note indicates that automated emails from this address will be sent to help prevent them from being flagged as spam. Below the password fields, there is a 'Confirm password' field and a note that they do not match. A 'Password strength' indicator shows 'Weak'. A 'Recommendations to make your password stronger' box lists: 'Make it at least 12 characters', 'Add uppercase letters', 'Add numbers', and 'Add punctuation'. An 'Email address' field is also present.



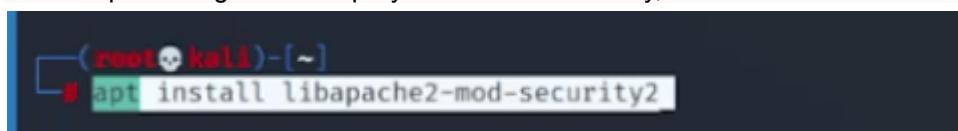
The screenshot shows a web browser window displaying a news article from 'portalseguridad.unam.com'. The article title is 'Boletín 1' and it was submitted by 'project\_mener' on Mon, 05/09/2022, 01:30. The content discusses Microsoft, Apple, and Google's plans to implement a standard passwordless login method called 'passwordless' developed by the Consorcio World Wide Web and the Alliance FIDO. It includes a link to 'https://www.w3.org/FIDO/passwordless' and a note about Bleepin Computer. Below the article is another news item titled 'Señales de que tu teléfono puede haber sido infectado con malware' submitted by 'project\_mener' on Mon, 05/09/2022, 01:30. The content notes that modern smartphones have evolved beyond basic calling and messaging functions, now featuring intelligent devices capable of performing tasks like connecting to computers and PCs. It highlights the use of phones for making calls, sending and receiving emails, communicating via messaging apps and social networks, managing bills, and more. The bottom of the screen shows a video player interface with a red play button.

## 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 eligió en este proyecto fue mod security, el cual se instaló mediante apt.



Ya instalado se habilita el modulo de seguridad.

```
[root@kali]# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
```

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

```
[root@kali]# cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.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
# 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:requestBodyProcessor=XML"
```

```
(root💀kali)-[~]
└─# vim /etc/modsecurity/modsecurity.conf

(root💀kali)-[~]
└─# systemctl restart apache2
```

## 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>