



Curso Seguridad aplicaciones web

Proyecto Final

Alumnos:

Molina Zepeda Natalia Elizeth
Martinez Hernandez Luis Eduardo
Olivera Trejo Luis David
Reynoso Gálvez Ana Laura

Profesora: Angie Aguilar

Fecha de entrega: 09 de mayo de 2022

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

ÍNDICE

- 1. En una máquina virtual con Debian ('10 u 11), realizar la instalación por paquetes de: PHP, Apache HTTP y PostgreSQL. DocumentRoot en /var/www/proyecto.** 3
- 2. Dar de alta un VH para su sitio: realizar las configuraciones necesarias para que el sitio funcione con HTTPS, tenga su propia bitácora y configuraciones de seguridad (considerar los archivos empleados y requeridos en el paso 3).** 4
- 3. Realizar la instalación de Drupal 9. Dar de alta 2 tipos de usuarios: admin (todos los privilegios en el sitio), contenidos (dar de alta contenidos -alta, edición, borrado y consulta-, pero sin acceso de administración del CMS). Verificar la documentación del CMS o algún tutorial para la instalación y puesta en marcha.** 4
- 4. Implementar su propio "Portal de Seguridad" con contenido de: noticias de seguridad, boletines y vulnerabilidades (recientes, al menos 5 elementos de cada uno).** 4
- 5. Implementar un WAF para proteger el CMS (verificar antes y después con algún ataque).** 4
- 6. Realizar la documentación correspondiente con capturas de pantalla, así como grabar un vídeo de la implementación y funcionamiento.** 4
- 7. Se entrega: ruta al repositorio de GitHub, documentación y vídeo, en equipos de máximo 4 personas.** 4

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

1. En una máquina virtual con Debian ('10 u 11), realizar la instalación por paquetes de: PHP, Apache HTTP y PostgreSQL. DocumentRoot en /var/www/proyecto.

Instalación de PHP.

```
debian@debian:~$ sudo apt install php
[sudo] password for debian:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2 apache2-data apache2-utils libapache2-mod-php7.4 php-common php7.4 php7.4-cli php7.4-common php7.4-json
  php7.4-opcache php7.4-readline
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils libapache2-mod-php7.4 php php-common php7.4 php7.4-cli php7.4-common php7.4-json
  php7.4-opcache php7.4-readline
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,818 kB of archives.
After this operation, 20.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

Instalación de Apache2.

```
debian@debian:~$ sudo apt reinstall apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 1 reinstalled, 0 to remove and 0 not upgraded.
Need to get 273 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 apache2 amd64 2.4.53-1-deb11u1 [273 kB]
Fetched 273 kB in 0s (703 kB/s)
(Reading database ... 163527 files and directories currently installed.)
Preparing to unpack .../apache2_2.4.53-1-deb11u1_amd64.deb ...
Unpacking apache2 (2.4.53-1-deb11u1) over (2.4.53-1-deb11u1) ...
Setting up apache2 (2.4.53-1-deb11u1) ...
Progress: [ 60%] [########################################.....]
```

Instalación de PostgreSQL.

```
debian@debian:~$ sudo apt install postgresql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpq5 postgresql-13 postgresql-client-13 postgresql-client-common postgresql-common sysstat
Suggested packages:
  postgresql-doc postgresql-doc-13 libjson-perl isag
The following NEW packages will be installed:
  libpq5 postgresql postgresql-13 postgresql-client-13 postgresql-client-common postgresql-common sysstat
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 17.8 MB of archives.
After this operation, 59.5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://deb.debian.org/debian bullseye/main amd64 libpq5 amd64 13.5-0+deb11u1 [179 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 postgresql-client-common all 225 [89.3 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 postgresql-client-13 amd64 13.5-0+deb11u1 [1,513 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 postgresql-common all 225 [237 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 postgresql-13 amd64 13.5-0+deb11u1 [15.1 MB]
80% [5 postgresql-13 13.3 MB/15.1 MB 88%] ■
```

En la ruta /etc/hosts debemos editarla de la siguiente forma:

```
debian@debian:~$ sudo nano /etc/hosts
127.0.0.1      localhost
127.0.1.1      debian
127.0.0.1      www.proyecto.unam.mx  proyecto.unam.mx■
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Creamos el directorio en la ruta /var/www y en el paso 2 redirigiremos el DocumentRoot a esta ruta.

```
debian@debian:~$ sudo mkdir /var/www/proyecto  
debian@debian:~$ cd /var/www/proyecto  
debian@debian:/var/www/proyecto$ █
```

2. Dar de alta un VH para su sitio: realizar las configuraciones necesarias para que el sitio funcione con HTTPS, tenga su propia bitácora y configuraciones de seguridad (considerar los archivos empleados y requeridos en el paso 3).

Nos dirigimos a la ruta /etc/apache2/sites-available.

```
└─(root💀 kali)-[~]  
└─# cd /etc/apache2/sites-available
```

Vamos a copiar el VH que da apache2 por default con el nombre de proyecto.conf.

```
└─(root💀 kali)-[/etc/apache2/sites-available]  
└─# cp 000-default.conf proyecto.conf
```

Ahora con vi editaremos proyecto.conf con los requerimientos del proyecto.

Primero realizaremos la configuración para que el sitio funcione con HTTPS así que debemos hacer un update y descargar el paquete de openssl.

```
└─(root💀 kali)-[~]  
└─# apt-get update  
Obj:1 http://kali.download/kali kali-rolling InRelease  
Obj:2 https://download.docker.com/linux/debian bullseye InRelease  
Leyendo lista de paquetes ... Hecho
```

Instalación del paquete.

```
└─(root💀 kali)-[~]  
└─# apt-get install apache2 openssl  
Leyendo lista de paquetes ... Hecho  
Creando árbol de dependencias ... Hecho  
Leyendo la información de estado ... Hecho  
apache2 ya está en su versión más reciente (2.4.53-2).  
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.  
  criu libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processstable-perl libsort-naturally-perl  
  needrestart tini  
Utilice «apt autoremove» para eliminarlos.
```

Si es la primera vez que instalamos el módulo nos preguntará si queremos continuar, podemos poner S/s o sólo dar Enter.

```
Se necesita descargar 853 kB de archivos.  
Se utilizarán 0 B de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] s
```

Habilitaremos los módulos de ssl y rewrite.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

```
[root💀kali]-[~]
└─# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2

[root💀kali]-[~]
└─# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
```

Nos pedirá reiniciar apache2 así que lo reiniciamos.

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

Después editaremos el archivo de configuración de Apache.

```
[root💀kali]-[~]
└─# vi /etc/apache2/apache2.conf
```

Colocaremos esta línea debajo del archivo.

```
<Directory /var/www/html>
    AllowOverride All
</Directory>
```

Ahora crearemos una clave privada y el certificado de nuestro sitio web.

Creación del directorio.

```
[root💀kali]-[~]
└─# mkdir /etc/apache2/certificate
```

Nos dirigimos al directorio.

```
[root💀kali]-[~]
└─# cd /etc/apache2/certificate
```

Creación de la llave privada y el certificado, los datos son de manera opcional pero al tratarse del proyecto final decidimos incluirlos.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT

PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

```
└─(root㉿kali)-[/etc/apache2/certificate]
  # openssl req -new -newkey rsa:4096 -x509 -sha256 -days 365 -nodes -out apache-certificate.crt -keyout apache.key
  Generating a RSA private key
  .....+++++
  .....+++++
writing new private key to 'apache.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:CDMX
Locality Name (eg, city) []:CDMX
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNAM
Organizational Unit Name (eg, section) []:cCERT
Common Name (e.g. server FQDN or YOUR name) []:PROYECTO
Email Address []:naelmoze@outlook.com
```

Pasamos a editar el VH, esta es su configuración inicial:

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

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

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

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

Editado quedaría así:

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

```
<VirtualHost *:80>
    RewriteEngine ON
    RewriteCond %{HTTPS} ≠on
    RewriteRule ^/?(.*) https:// %{SERVER_NAME}/$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
    # 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.proyecto.unam.mx

    ServerAdmin webmaster@localhost
    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
    SSLEngine ON
    SSLCertificateFile /etc/apache2/certificate/apache-certificate.crt
    SSLCertificateKeyFile /etc/apache2/certificate/apache.key
```

Y reiniciamos apache2.

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

Para la bitácora se necesitará el módulo ModSecurity.

Primero realizamos un update.

```
└─(root💀 kali)-[~]
  # sudo apt update
Obj:1 https://download.docker.com/linux/debian bullseye InRelease
Obj:2 http://kali.download/kali kali-rolling InRelease
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Se pueden actualizar 1205 paquetes. Ejecute «apt list --upgradable» para verlos.
```

Descargamos el módulo.

```
└─(root💀 kali)-[~]
  # sudo apt install libapache2-mod-security2
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
libapache2-mod-security2 ya está en su versión más reciente (2.9.5-1).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  criu libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl libsort-naturally-perl
  needrestart tini
Utilece «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 1205 no actualizados.
```

Habilitamos el módulo.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

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

Y hacemos un restart a apache2.

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

Ahora para configurarlo vamos a copiar su configuración.

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

Y con vi vamos a editarla.

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

En este parte cambiaremos la instrucción:

```
# -- Rule engine initialization

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

Por ON

```
# -- Rule engine initialization

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

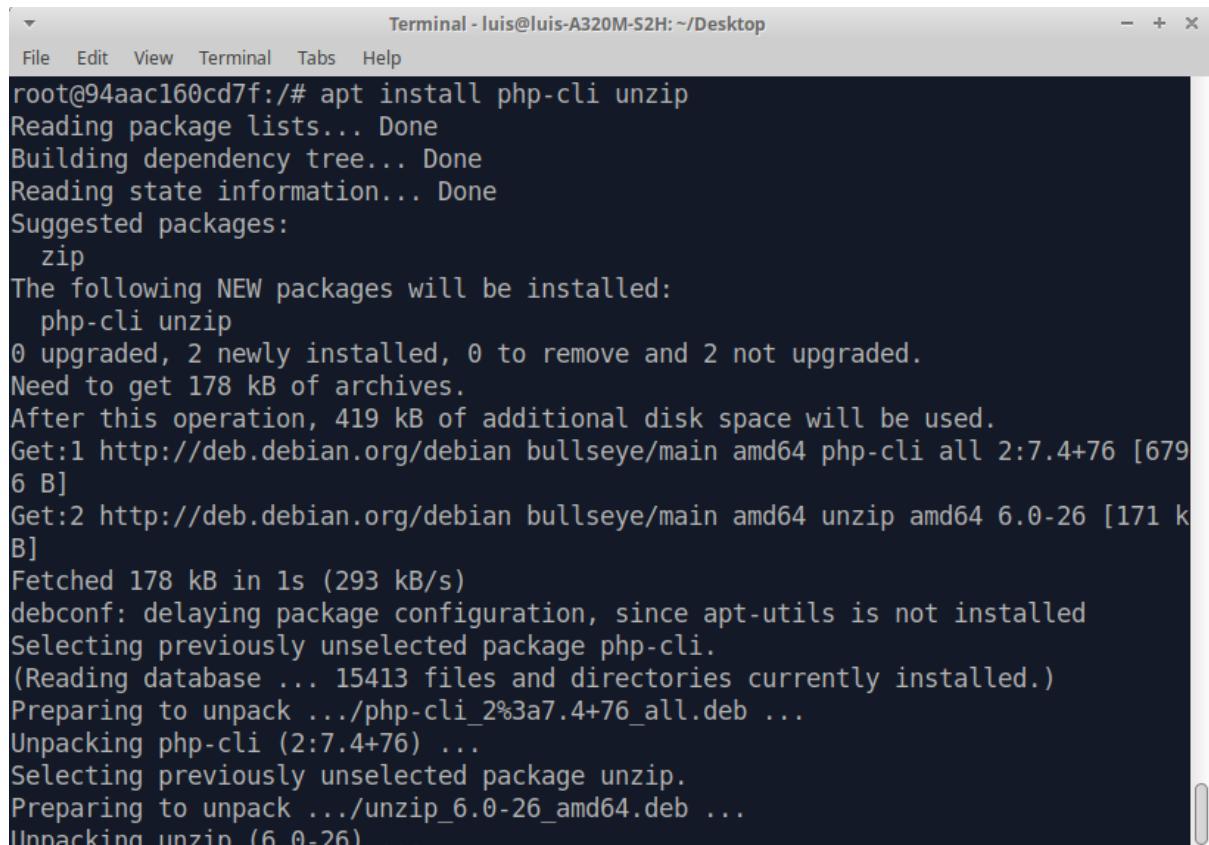
Y para finalizar reiniciamos el servicio de apache2.

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

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

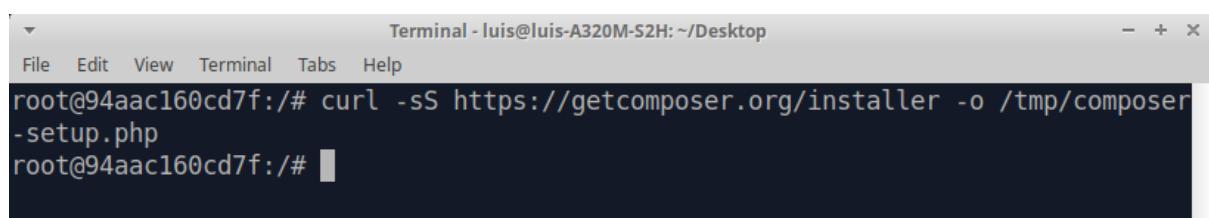
3. Realizar la instalación de Drupal 9. Dar de alta 2 tipos de usuarios: admin (todos los privilegios en el sitio), contenidos (dar de alta contenidos -alta, edición, borrado y consulta-, pero sin acceso de administración del CMS). Verificar la documentación del CMS o algún tutorial para la instalación y puesta en marcha.

Primero descargamos php-cli para que podamos ejecutar composer que es la herramienta que nos permitirá instalar drupal.



```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/# apt install php-cli unzip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  zip
The following NEW packages will be installed:
  php-cli unzip
0 upgraded, 2 newly installed, 0 to remove and 2 not upgraded.
Need to get 178 kB of archives.
After this operation, 419 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 php-cli all 2:7.4+76 [679
6 B]
Get:2 http://deb.debian.org/debian bullseye/main amd64 unzip amd64 6.0-26 [171 k
B]
Fetched 178 kB in 1s (293 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package php-cli.
(Reading database ... 15413 files and directories currently installed.)
Preparing to unpack .../php-cli_2%3a7.4+76_all.deb ...
Unpacking php-cli (2:7.4+76) ...
Selecting previously unselected package unzip.
Preparing to unpack .../unzip_6.0-26_amd64.deb ...
Unpacking unzip (6.0-26) ...
```

Después ejecutamos el siguiente curl para bajar los archivos de composer

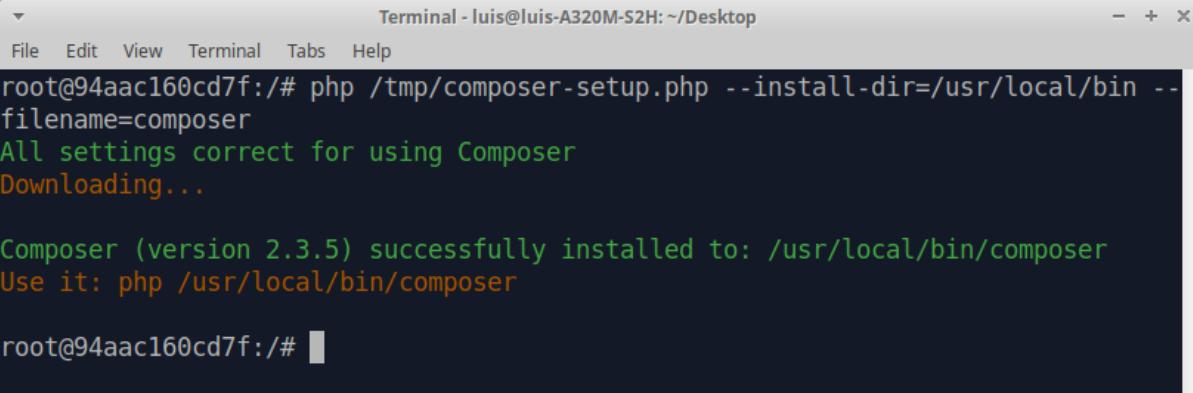


```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/# curl -sS https://getcomposer.org/installer -o /tmp/composer
-setup.php
root@94aac160cd7f:/#
```

Después ejecutamos el setup usando php como se muestra en la imagen.

Nota: se está usando la versión de PHP 7.4.21

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA



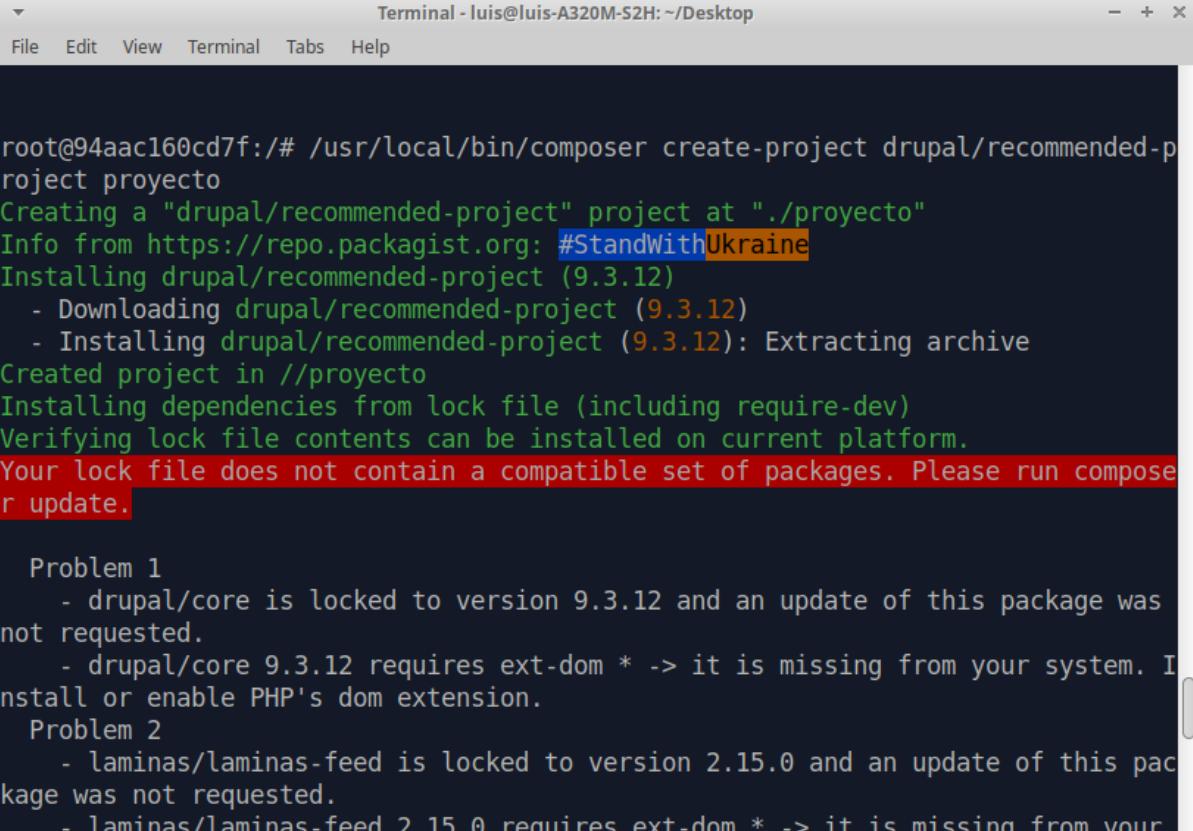
```
Terminal - luis@luis-A320M-S2H:~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/# php /tmp/composer-setup.php --install-dir=/usr/local/bin --filename=composer
All settings correct for using Composer
Downloading...

Composer (version 2.3.5) successfully installed to: /usr/local/bin/composer
Use it: php /usr/local/bin/composer

root@94aac160cd7f:/#
```

En caso de tener problemas con el comando anterior, cambiar a la versión 7 de PHP.

Después ejecutamos el siguiente comando para que nuestro recién instalado composer cree un proyecto de drupal que se va a llamar proyecto.



```
Terminal - luis@luis-A320M-S2H:~/Desktop
File Edit View Terminal Tabs Help

root@94aac160cd7f:/# /usr/local/bin/composer create-project drupal/recommended-project proyecto
Creating a "drupal/recommended-project" project at "./proyecto"
Info from https://repo.packagist.org: #StandWithUkraine
Installing drupal/recommended-project (9.3.12)
- Downloading drupal/recommended-project (9.3.12)
- Installing drupal/recommended-project (9.3.12): Extracting archive
Created project in //proyecto
Installing dependencies from lock file (including require-dev)
Verifying lock file contents can be installed on current platform.
Your lock file does not contain a compatible set of packages. Please run composer update.

Problem 1
- drupal/core is locked to version 9.3.12 and an update of this package was not requested.
- drupal/core 9.3.12 requires ext-dom * -> it is missing from your system. Install or enable PHP's dom extension.

Problem 2
- laminas/laminas-feed is locked to version 2.15.0 and an update of this package was not requested.
- laminas/laminas-feed 2.15.0 requires ext-dom * -> it is missing from your
```

Después nos movemos a la carpeta del proyecto que acaba de crear composer.



```
root@94aac160cd7f:/# cd proyecto
root@94aac160cd7f:/proyecto#
```

Ahora necesitamos instalar un par de dependencias como se muestran en la imagen.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/proyecto# apt search ext-dom
Sorting... Done
Full Text Search... Done
root@94aac160cd7f:/proyecto#
root@94aac160cd7f:/proyecto# apt install php-xml
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  php7.4-xml
The following NEW packages will be installed:
  php-xml php7.4-xml
0 upgraded, 2 newly installed, 0 to remove and 2 not upgraded.
Need to get 105 kB of archives.
After this operation, 453 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 php7.4-xml amd64 7.4.28-1+deb11u1 [98.4 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 php-xml all 2:7.4+76 [6384 B]
Fetched 105 kB in 1s (172 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package php7.4-xml.
(Reading database ... 15440 files and directories currently installed.)
```

```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/proyecto# apt install php-gd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config fonts-dejavu-core libdeflate0 libfontconfig1 libfreetype6
  libgd3 libjbig0 libjpeg62-turbo libpng16-16 libtiff5 libwebp6 libx11-6
  libx11-data libxau6 libxcb1 libxdmcp6 libxpm4 php7.4-gd
Suggested packages:
  libgd-tools
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core libdeflate0 libfontconfig1 libfreetype6
  libgd3 libjbig0 libjpeg62-turbo libpng16-16 libtiff5 libwebp6 libx11-6
  libx11-data libxau6 libxcb1 libxdmcp6 libxpm4 php-gd php7.4-gd
0 upgraded, 19 newly installed, 0 to remove and 2 not upgraded.
Need to get 4681 kB of archives.
After this operation, 11.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

Después de instalar las dependencias tenemos que actualizar nuestro proyecto de drupal ejecutando el comando que se muestra en la imagen.

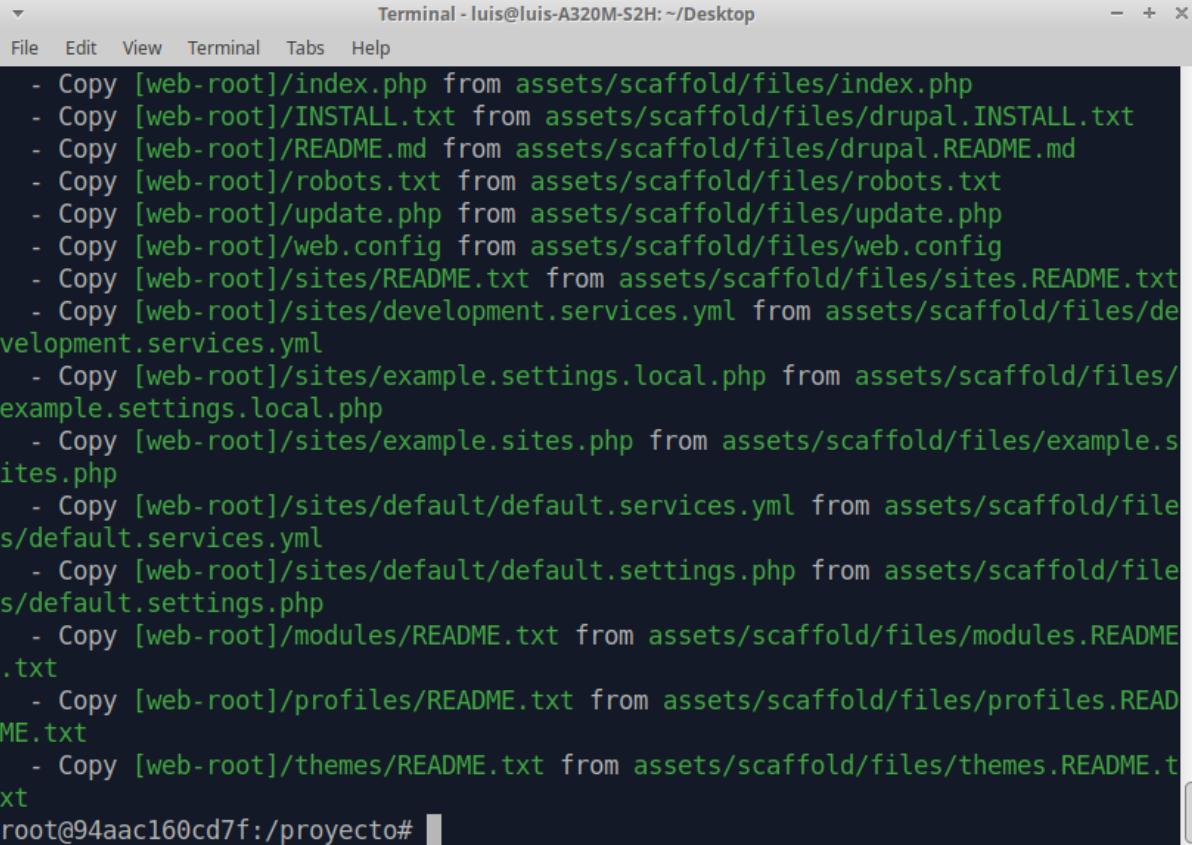
COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/proyecto# /usr/local/bin/composer update
Composer is operating significantly slower than normal because you do not have t
he PHP curl extension enabled.
Loading composer repositories with package information
Updating dependencies
Nothing to modify in lock file
Writing lock file
Installing dependencies from lock file (including require-dev)
Package operations: 62 installs, 0 updates, 0 removals
- Downloading composer/installers (v1.12.0)
- Downloading drupal/core-composer-scaffold (9.3.12)
- Downloading drupal/core-project-message (9.3.12)
- Downloading typo3/phar-stream-wrapper (v3.1.7)
- Downloading symfony/polyfill-php72 (v1.25.0)
- Downloading symfony/polyfill-mbstring (v1.23.1)
- Downloading symfony/polyfill-ctype (v1.23.0)
- Downloading twig/twig (v2.14.11)
- Downloading symfony/yaml (v4.4.34)
- Downloading symfony/polyfill-php80 (v1.23.1)
- Downloading symfony/var-dumper (v5.4.0)
- Downloading symfony/translation-contracts (v2.5.0)
- Downloading symfony/validator (v4.4.35)
- Downloading symfony/translation (v4.4.34)
- Downloading symfony/deprecation-contracts (v2.5.0)
```

En algún punto de la actualización nos preguntará si confiamos en los módulos que vamos a instalar y le damos que si a cada uno.

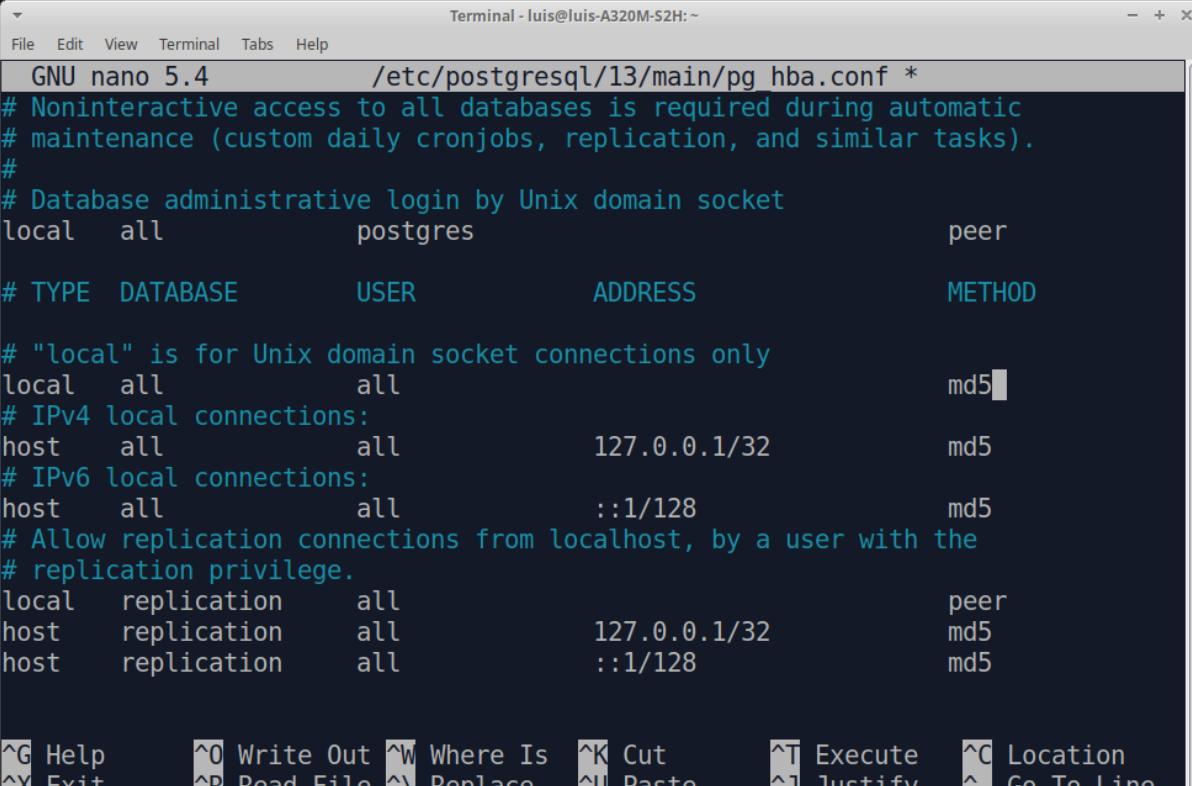
```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
- Downloading pear/pear_exception (v1.0.2)
- Downloading pear/console_getopt (v1.4.3)
- Downloading pear/pear-core-minimal (v1.10.11)
- Downloading pear/archive_tar (1.4.14)
- Downloading masterminds/html5 (2.7.5)
- Downloading laminas/laminas-stdlib (3.6.1)
- Downloading laminas/laminas-escaper (2.9.0)
- Downloading laminas/laminas-feed (2.15.0)
- Downloading laminas/laminas-diactoros (2.8.0)
- Downloading guzzlehttp/psr7 (1.8.5)
- Downloading guzzlehttp/promises (1.5.1)
- Downloading guzzlehttp/guzzle (6.5.5)
- Downloading doctrine/lexer (1.2.1)
- Downloading egulias/email-validator (3.1.2)
- Downloading doctrine/annotations (1.13.2)
- Downloading doctrine/reflection (1.2.2)
- Downloading composer/semver (3.2.6)
- Downloading asm89/stack-cors (1.3.0)
- Downloading drupal/core (9.3.12)
- Installing composer/installers (v1.12.0): Extracting archive
composer/installers contains a Composer plugin which is currently not in your al
low-plugins config. See https://getcomposer.org/allow-plugins
Do you trust "composer/installers" to execute code and wish to enable it now? (w
rites "allow-plugins" to composer.json) [y,n,d,?] y
```

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA



```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
- Copy [web-root]/index.php from assets/scaffold/files/index.php
- Copy [web-root]/INSTALL.txt from assets/scaffold/files/drupal.INSTALL.txt
- Copy [web-root]/README.md from assets/scaffold/files/drupal.README.md
- Copy [web-root]/robots.txt from assets/scaffold/files/robots.txt
- Copy [web-root]/update.php from assets/scaffold/files/update.php
- Copy [web-root]/web.config from assets/scaffold/files/web.config
- Copy [web-root]/sites/README.txt from assets/scaffold/files/sites.README.txt
- Copy [web-root]/sites/development.services.yml from assets/scaffold/files/development.services.yml
- Copy [web-root]/sites/example.settings.local.php from assets/scaffold/files/example.settings.local.php
- Copy [web-root]/sites/example.sites.php from assets/scaffold/files/example.sites.php
- Copy [web-root]/sites/default/default.services.yml from assets/scaffold/files/default.services.yml
- Copy [web-root]/sites/default/default.settings.php from assets/scaffold/files/default.settings.php
- Copy [web-root]/modules/README.txt from assets/scaffold/files/modules.README.txt
- Copy [web-root]/profiles/README.txt from assets/scaffold/files/profiles.README.txt
- Copy [web-root]/themes/README.txt from assets/scaffold/files/themes.README.txt
root@94aac160cd7f:/proyecto#
```

Ahora necesitamos configurar la base de datos. Primero necesitamos configurar el archivo pg_hba.conf para que autentique usuarios por md5 cuando están en local. Para eso modificamos la linea que dice **local all all peer** por la linea **local all all md5**



```
Terminal - luis@luis-A320M-S2H: ~
File Edit View Terminal Tabs Help
GNU nano 5.4          /etc/postgresql/13/main/pg_hba.conf *
# Noninteractive access to all databases is required during automatic
# maintenance (custom daily cronjobs, replication, and similar tasks).
#
# Database administrative login by Unix domain socket
local  all      postgres                      peer
# TYPE   DATABASE        USER            ADDRESS                 METHOD
#
# "local" is for Unix domain socket connections only
local  all      all                           md5
# IPv4 local connections:
host    all      all      127.0.0.1/32        md5
# IPv6 local connections:
host    all      all      ::1/128             md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local  replication all                      peer
host    replication all      127.0.0.1/32        md5
host    replication all      ::1/128             md5

^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
```

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Después de eso nos tenemos que conectar a la base de datos. Esto lo hacemos cambiandonos al usuario postgres y despues ejecutando psql.

```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/proyecto# su postgres
postgres@94aac160cd7f:/proyecto$ psql
psql (13.5 (Debian 13.5.0+deb11u1))
Type "help" for help.

postgres=#
```

Una vez dentro creamos la base de datos proyecto y al usuario drupal.

```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
postgres=# CREATE DATABASE proyecto;
CREATE DATABASE
postgres=# create user drupal with encrypted password 'password';
CREATE ROLE
postgres=#

```

Ponemos que el output lo escape.

```
Terminal - luis@luis-A320M-S2H: ~
File Edit View Terminal Tabs Help
postgres=# ALTER DATABASE "proyecto" SET bytea_output = 'escape';
ALTER DATABASE
postgres=#

```

Después nos conectamos a la base de datos.

```
Terminal - luis@luis-A320M-S2H: ~
File Edit View Terminal Tabs Help
postgres=# \c proyecto
You are now connected to database "proyecto" as user "postgres".
proyecto=#

```

Después le damos permisos a nuestro usuario drupal.

```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
proyecto=# GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA public TO drupal;
GRANT
proyecto=#

```

Después ponemos una extensión a la base de datos como se muestra en la imagen.

```
Terminal - luis@luis-A320M-S2H: ~
File Edit View Terminal Tabs Help
proyecto=# CREATE EXTENSION pg_trgm;
CREATE EXTENSION
proyecto=#

```

Después nos desconectamos de la base y salimos de la sesión del usuario postgres.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
proyecto=# \q
postgres@94aac160cd7f:/ proyecto$
```

```
postgres@94aac160cd7f:/ proyecto/web$ exit
exit
```

Después copiamos el archivo de configuración de drupal como se muestra en la imagen y muy importante, **le damos la carpeta a www-data** con el comando chown.

```
Terminal - luis@luis-A320M-S2H: ~
File Edit View Terminal Tabs Help
root@94aac160cd7f:/ proyecto# cp ./web/sites/default/default.settings.php ./web/sites/default/settings.php
root@94aac160cd7f:/ proyecto# chown -R www-data ./web/
root@94aac160cd7f:/ proyecto#
```

Después de esto debemos de configurar nuestro virtualhost desde donde va a estar escuchando nuestro servidor. Lo que hay que configurar sea cual sea el virtualhost es cambiar el DocumentRoot a donde está la carpeta de la instalación de drupal y agregar la directiva de directory para la carpeta de instalación de drupal como se muestra en la imagen.

```
File Edit View Search Terminal Help
GNU nano 5.4                                     proyecto.conf
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /home/debian/proyecto/web
        ServerName proyecto.unam.mx
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
        SSLCertificateKeyFile  /etc/ssl/private/apache-selfsigned.key
        <FilesMatch "\.(cgi|html|php)$">
            SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
            SSLOptions +StdEnvVars
        </Directory>
        <Directory /home/debian/proyecto/web>
            Options Indexes followSymLinks
            AllowOverride All
            Require all granted
        </Directory>
    </VirtualHost>
</IfModule>
```

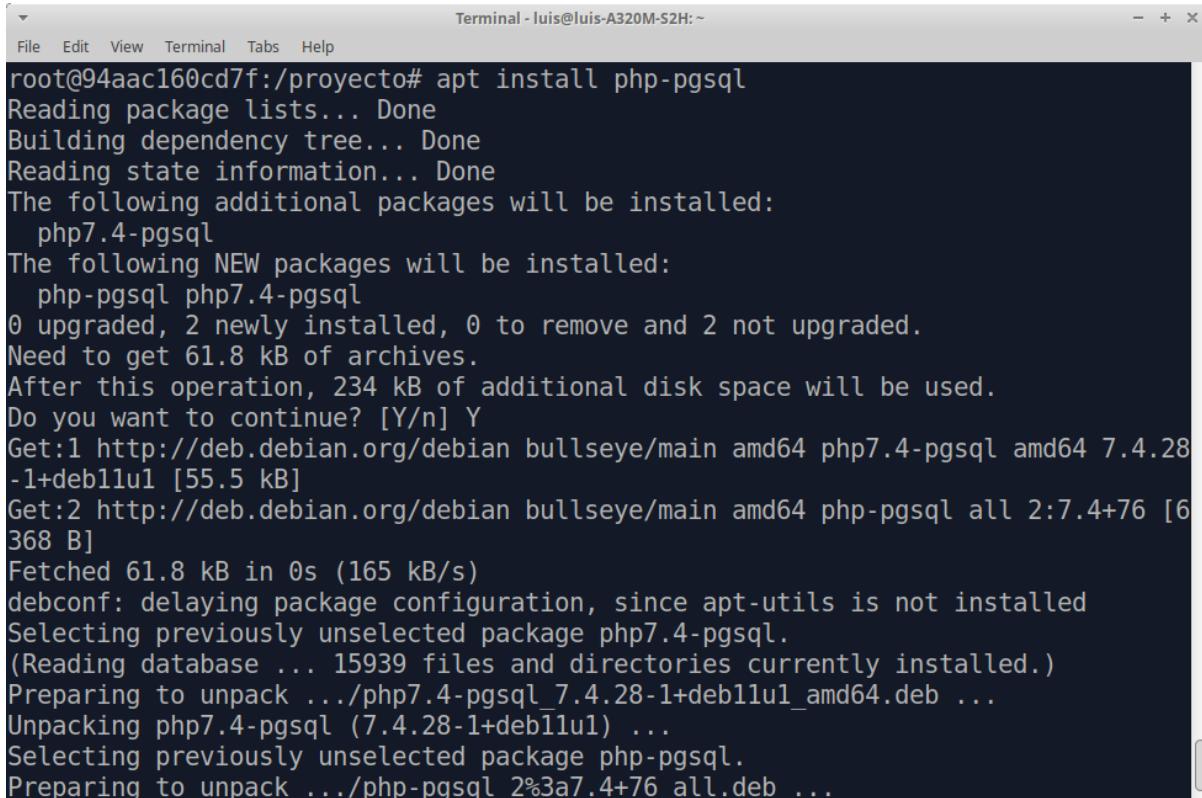
Terminando esto reiniciamos nuestro apache.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA



```
Terminal - luis@luis-A320M-S2H: ~/Desktop
File Edit View Terminal Tabs Help
root@94aac160cd7f:/proyecto/web# service apache2 restart
Restarting Apache httpd web server: apache2AH00558: apache2: Could not reliably
determine the server's fully qualified domain name, using 172.17.0.2. Set the 'S
erverName' directive globally to suppress this message
.
root@94aac160cd7f:/proyecto/web#
```

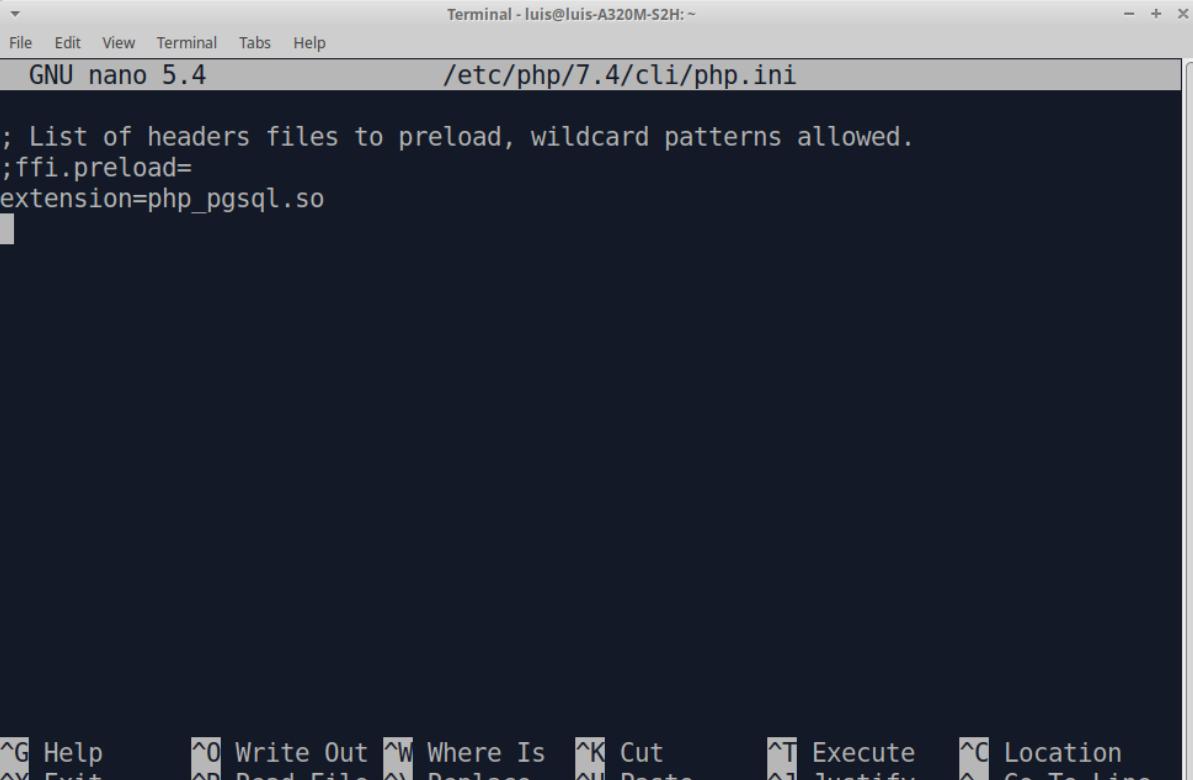
Adicionalmente debemos de instalar algunas dependencias para la conexión de php con postgres.



```
Terminal - luis@luis-A320M-S2H: ~
File Edit View Terminal Tabs Help
root@94aac160cd7f:/proyecto# apt install php-pgsql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  php7.4-pgsql
The following NEW packages will be installed:
  php-pgsql php7.4-pgsql
0 upgraded, 2 newly installed, 0 to remove and 2 not upgraded.
Need to get 61.8 kB of archives.
After this operation, 234 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 php7.4-pgsql amd64 7.4.28
-1+deb11u1 [55.5 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 php-pgsql all 2:7.4+76 [6
368 B]
Fetched 61.8 kB in 0s (165 kB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package php7.4-pgsql.
(Reading database ... 15939 files and directories currently installed.)
Preparing to unpack .../php7.4-pgsql_7.4.28-1+deb11u1_amd64.deb ...
Unpacking php7.4-pgsql (7.4.28-1+deb11u1) ...
Selecting previously unselected package php-pgsql.
Preparing to unpack .../php-pgsql_2%3a7.4+76_all.deb ...
```

Después debemos de agregar la siguiente línea al final del archivo(extension=php...) php.ini como se muestra en la imagen.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

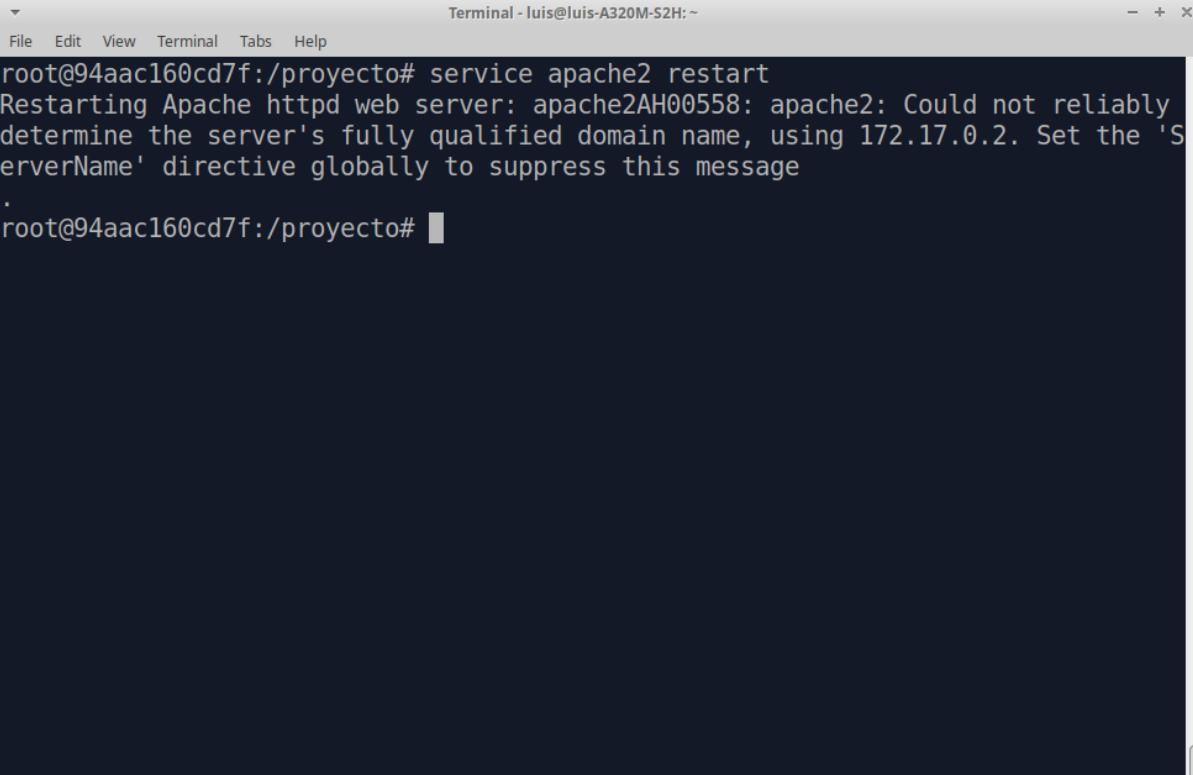


```
GNU nano 5.4          /etc/php/7.4/cli/php.ini

; List of headers files to preload, wildcard patterns allowed.
; ffi.preload=
extension=php_pgsql.so
```

^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

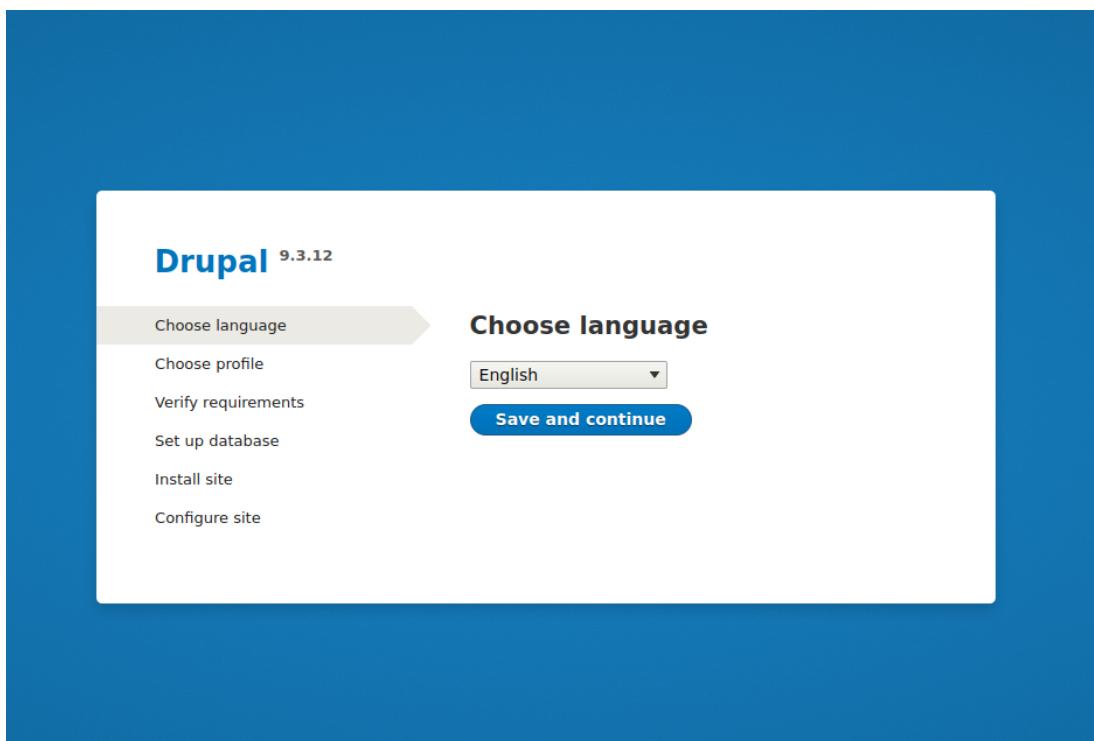
Y volvemos a reiniciar apache.



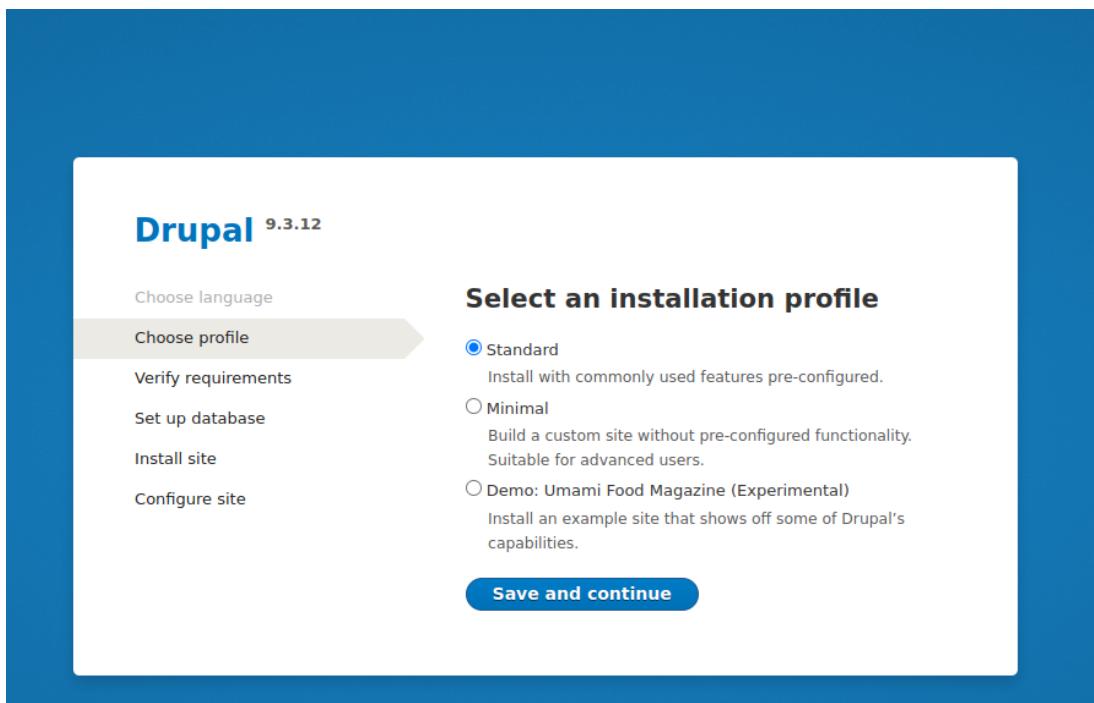
```
Terminal - luis@luis-A320M-S2H:~  
File Edit View Terminal Tabs Help  
root@94aac160cd7f:/proyecto# service apache2 restart  
Restarting Apache httpd web server: apache2AH00558: apache2: Could not reliably  
determine the server's fully qualified domain name, using 172.17.0.2. Set the 'S  
erverName' directive globally to suppress this message  
.root@94aac160cd7f:/proyecto#
```

Una vez hecho esto nos dirigimos al navegador en la ruta: **/core/install.php**. En la primera ventana seleccionamos el lenguaje con el que queremos continuar.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA



Después seleccionamos que queremos la instalación estándar.



Después nos saldrán un par de warnings así como el resumen de lo que tenemos.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

The screenshot shows the Drupal 9.3.12 Requirements review page. On the left, a sidebar lists steps: Choose language, Choose profile, Verify requirements (which is highlighted in grey), Set up database, Install site, and Configure site. The main content area has two sections: 'Requirements review' and 'Warnings found'. Under 'Requirements review', it says 'OK'. Under 'Warnings found', there are two items: 'CLEAN URLs' (disabled) and 'UNICODE LIBRARY' (Standard PHP). Both have detailed descriptions and links to enable them. Below these, under 'OK', there are several sections: WEB SERVER (Apache/2.4.53 (Debian)), PHP (7.4.28), PHP EXTENSIONS (Enabled), PHP OPCODE CACHING (Enabled), RANDOM NUMBER GENERATION (Successful), and DATABASE SUPPORT (Enabled).

Drupal 9.3.12

Choose language

Choose profile

Verify requirements

Set up database

Install site

Configure site

Requirements review

Warnings found

CLEAN URLs
Disabled
Your server is capable of using clean URLs, but it is not enabled. Using clean URLs gives an improved user experience and is recommended. [Enable clean URLs](#)

UNICODE LIBRARY
Standard PHP
Operations on Unicode strings are emulated on a best-effort basis. Install the [PHP mbstring extension](#) for improved Unicode support.

OK

WEB SERVER
Apache/2.4.53 (Debian)

PHP
7.4.28

PHP EXTENSIONS
Enabled

PHP OPCODE CACHING
Enabled

RANDOM NUMBER GENERATION
Successful

DATABASE SUPPORT
Enabled

Si vamos al final podremos continuar dando click en continue anyway.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT

PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Operations with Unicode strings are emulated on a best-effort basis. Install the [PHP mbstring extension](#) for improved Unicode support.

OK

WEB SERVER
Apache/2.4.53 (Debian)

PHP
7.4.28

PHP EXTENSIONS
Enabled

PHP OPCODE CACHING
Enabled

RANDOM NUMBER GENERATION
Successful

DATABASE SUPPORT
Enabled

PHP MEMORY LIMIT
128M

FILE SYSTEM
Writable (*public* download method)

SETTINGS FILE
The `./sites/default/settings.php` exists.

SETTINGS FILE
The Settings file is writable.

Check the messages and [retry](#), or you may choose to [continue anyway](#).

Después nos pedirá los datos de conexión a la base de datos. Introducimos los datos del usuario que creamos: **drupal** con clave **password**. Todo para la base de datos **proyecto**.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Drupal 9.3.12

Choose language
Choose profile
Verify requirements
Set up database
Install site
Configure site

Database configuration

Database type *
 PostgreSQL

Database name *
projecto

Database username *
drupal

Database password

► ADVANCED OPTIONS

Save and continue

Después nos saldrá una ventana de que se está instalando drupal.

Drupal 9.3.12

Choose language
Choose profile
Verify requirements
Set up database
Install site
Configure site

Installing Drupal

Installed *Image* module.
Completed 31 of 39. 79%

Una vez hecho esto tendremos que crear a nuestro administrador con la información que queramos.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Drupal 9.3.12

Choose language

Choose profile

Verify requirements

Set up database

Install site

Configure site

Configure site

SITE INFORMATION

Site name *
proyecto

Site email address *
proyecto@localhost

Automated emails, such as registration information, will be sent from this address. Use an address ending in your site's domain to help prevent these emails from being flagged as spam.

SITE MAINTENANCE ACCOUNT

Username *
admin

Several special characters are allowed, including space, period (.), hyphen (-), apostrophe ('), underscore (_), and the @ sign.

Password *
.....

Password strength: Strong

Confirm password *
.....

Passwords match: yes

Email address *
proyecto@localhost

REGIONAL SETTINGS

Default country
Mexico

Default time zone
Mexico City

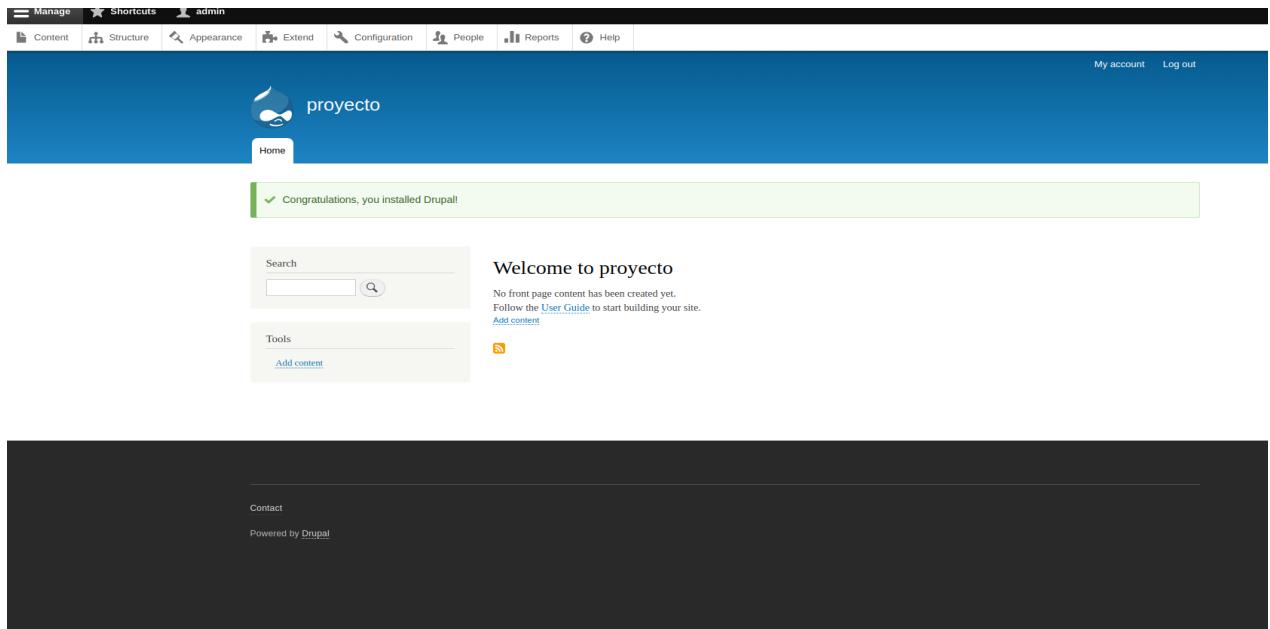
UPDATE NOTIFICATIONS

Check for updates automatically

Una vez introducida la información nos redirigirá a la página principal del sitio proyecto.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT

PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA



NUEVOS USUARIOS

Para agregar nuevos usuarios debemos de ir al navbar en la parte de people. Como podemos apreciar ya hay un administrador agregado por lo que solo agregaremos al usuario de contenidos. Para eso damos click en **add user**.

USERNAME	STATUS	ROLES	MEMBER FOR	LAST ACCESS	OPEN
admin	Active	• Administrator	5 minutes 52 seconds	56 seconds ago	

Llenamos el formulario con los datos que queramos para nuestro usuario. Es importante remarcar que para que se cree como un usuario de contenidos se debe de especificar está opción en **Roles**.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Add user ★

[Home](#) » [Administration](#) » [People](#)

This web page allows administrators to register new users. Users' email addresses and usernames must be unique.

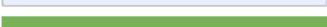
Email address

A valid email address. All emails from the system will be sent to this address. The email address is not made public and will only be used by site administrators.

Username *

Several special characters are allowed, including space, period (.), hyphen (-), apostrophe ('), underscore (_), and the @ sign.

Password *



Password strength: Strong

Confirm password *

Passwords match: **yes**

Provide a password for the new account in both fields.

Status

- Blocked
 Active

Roles

- Authenticated user
 Content editor
 Administrator
 Notify user of new account

Picture

No file chosen

Your virtual face or picture.

One file only.

2 MB limit.

Allowed types: png gif jpg jpeg.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT

PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA



Confirm password*

Passwords match: yes

Provide a password for the new account in both fields.

Status

- Blocked
 Active

Roles

- Authenticated user
 Content editor
 Administrator
 Notify user of new account

Picture

 No file chosen

Your virtual face or picture.

One file only.

2 MB limit.

Allowed types: png gif jpg jpeg.

▼ CONTACT SETTINGS

- Personal contact form

Allow other users to contact you via a personal contact form which keeps your email address hidden. Note that some privileg

▼ LOCALE SETTINGS

Time zone

Select the desired local time and time zone. Dates and times throughout this site will be displayed using this time zone.

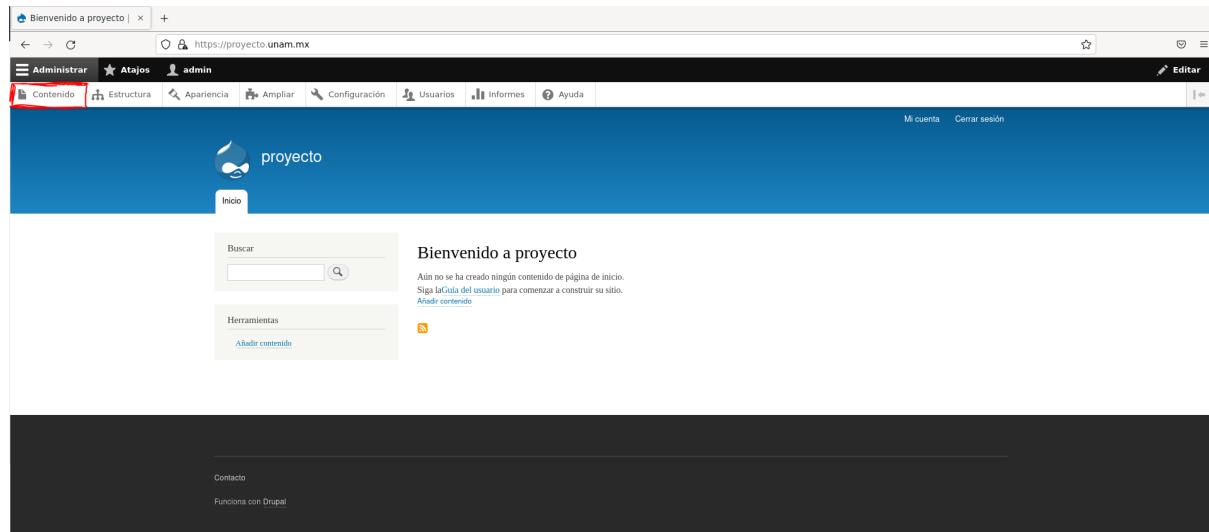
[Create new account](#)

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

4. Implementar su propio "Portal de Seguridad" con contenido de: noticias de seguridad, boletines y vulnerabilidades (recientes, al menos 5 elementos de cada uno).

Ingresamos al CMS drupal y nos logueamos.

Después en la página de Inicio seleccionamos el apartado de Contenido



Luego seleccionamos Añadir contenido



Ahora podemos desarrollar el artículo que se desea publicar, para este caso se realizará el ejemplo de una noticia de seguridad informática.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Crear Artículo

Inicio » Añadir contenido

Título *

Señales de que tu teléfono puede haber sido infectado con malware

Cuerpo (Editar resumen)

B I         | Normal | 

Autor: Amer Owala

Con los altos de los sistemas operativos Android e iOS, los teléfonos han evolucionado mucho más allá de sus humildes funciones de llamadas y mensajes de texto: ahora son dispositivos inteligentes portátiles capaces de realizar tareas que antes se confiaban a computadoras portátiles y PC. Hoy utilizamos los teléfonos para tomar fotos, enviar y recibir correos electrónicos, comunicarnos a través de apps de mensajería y redes sociales, para gestionar billetes digitales y aplicaciones bancarias... y la lista continúa. Toda esa riqueza de datos también atrae a actores de amenazas que quieren usarsela para sus propios fines, ya sea desde venderlos en la dark web hasta usarlos para cometer robo de identidad y fraude.

Los últimos años han proporcionado mucha evidencia de que incluso tu confiable teléfono podría verse comprometido por malware. Con Android como el sistema operativo que ocupa la mayor parte del mercado de smartphones, nos centremos en esta plataforma y aprovecharemos los conocimientos de Lukas Stefanko, investigador de malware de ESET, quien tiene un largo recorrido descubriendo y analizando distintas amenazas dirigidas a usuarios de Android.

Cómo puede infectarse tu teléfono

De muchas maneras, en realidad. Una de las tácticas más comunes utilizadas para comprometer el dispositivo de una víctima es el uso de correos electrónicos de phishing que contienen enlaces o archivos adjuntos maliciosos. Una vez que la víctima hace clic en el archivo adjunto o el enlace (que luego descarga malware a su dispositivo), ese malware permite a los actores maliciosos llevar a cabo sus acciones maliciosas.

Otra estrategia que utilizan son los sitios fraudulentos, donde los cibercriminales se hacen pasar sitios de marcas u organizaciones conocidas e incluyen enlaces maliciosos que descargan malware en el dispositivo.

Por otra parte, no es extraño que los cibercriminales recurran al uso de aplicaciones falsas que se hacen pasar por apps legítimas. De hecho, es algo que ocurre de forma frecuente. De esta manera los atacantes logran que víctimas desprevenidas descarguen en sus equipos programas maliciosos como keyloggers, ransomware o spyware disfrazados de apps de seguimiento de fitness o aplicaciones de criptomonedas. Estas aplicaciones generalmente se difunden a través de tiendas de aplicaciones no oficiales.

Cómo comprobar si tu teléfono ha sido comprometido

<https://projecteonamix/admin/content> de que tu smartphone puede haber sido infectado con algún tipo de malware:

1. Aparecerá un anuncio emergente a pantalla completa
2. Al tocar el botón/menú de aplicaciones recientes, se muestra la aplicación responsable de mostrar el anuncio.
3. En este caso, la aplicación tiene un ícono negro sólido, lo que hace que sea menos obvio dónde hacer clic.
4. Luego de mantener presionado ese ícono, vamos a la información de la aplicación, inspeccionamos sus permisos, etc. y la desinstalamos.

body ol li

Formato de texto HTML básico ▾

Acerca de formatos de texto 

Etiquetas

Noticias 

Especifique una lista separada por comas. Por ejemplo: Amsterdam, Mexico City, "Cleveland, Ohio"

Imagen

No file selected.

Máximo 1 fichero.

Límite de 2 MB.

Tipos permitidos: png gif jpg jpeg.

Publicado

Después de terminarlo, lo guardamos. Y ahora podemos verlo

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT

PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Inicio

✓ Artículo [Señales de que tu teléfono puede haber sido infectado con malware](#) se ha creado.

Inicio

Buscar

Ver Editar Eliminar Revisiones

Enviado por admin el Dom, 08/05/2022 - 15:08

Autor: Amer Owaida

Con los albores de los sistemas operativos Android e iOS, los teléfonos han evolucionado mucho más allá de sus humildes funciones de llamadas y mensajes de texto: ahora son dispositivos inteligentes portátiles capaces de realizar tareas que antes se confiaban a computadoras portátiles y PC. Hoy utilizamos los teléfonos para tomar fotos, enviar y recibir correos electrónicos, comunicarnos a través de apps de mensajería y redes sociales, para gestionar billeteras digitales y aplicaciones bancarias... y la lista continúa. Toda esa riqueza de datos también atrae a actores de amenazas que quieren usarlos para sus propios fines, ya sea desde [venderlos en la dark web](#) hasta usarlos para cometer [robo de identidad y fraude](#).

Los últimos años han proporcionado mucha evidencia de que incluso tu confiable teléfono podría verse comprometido por malware. Con Android como el sistema operativo que ocupa la mayor parte del mercado de smartphones, nos centraremos en esta plataforma y aprovecharemos los conocimientos de [Lucas Stefanko](#), investigador de malware de ESET, quien tiene un largo recorrido descubriendo y analizando distintas amenazas dirigidas a usuarios de Android.

Cómo puede infectarse tu teléfono

De muchas maneras, en realidad. Una de las tácticas más comunes utilizadas para comprometer el dispositivo de una víctima es el uso de correos electrónicos de phishing que contienen enlaces o archivos adjuntos maliciosos. Una vez que la víctima hace clic en el archivo adjunto o el enlace (que luego descarga malware a su dispositivo), ese malware permite a los actores maliciosos llevar a cabo sus acciones maliciosas.

Otra estrategia que utilizan son los sitios fraudulentos, donde los cibercriminales se hacen pasar sitios de marcas u organizaciones conocidas e incluyen enlaces maliciosos para desviar a los usuarios a las páginas falsas.

Lo mismo aplicamos para agregar un boletín, solo que ahora la etiqueta será diferente.

Título *

Top tres de estafas en redes sociales

Cuerpo ([Editar resumen](#))

B I Formato | Fuente HTML

Resumen

Si bien las redes sociales son una forma fantástica de comunicarse, compartir y divertirse con los demás, también son una forma económica para que los cibercriminales engañen y se aprovechen de millones de personas. No seas víctima de las tres estafas más comunes en redes sociales.

Estafas de inversión

¿Alguna vez has visto una publicación sobre una oportunidad de inversión que promete un gran retorno en poco tiempo con un riesgo supuestamente mínimo o nulo? La realidad es que estas promesas son en realidad estafas de inversión. Los estafadores simplemente robarán tu dinero después de que les pagues. Estas estafas usualmente incluyen anuncios o historias de éxito de clientes anteriores para promover dichas inversiones, pero son solo testimonios falsos para aumentar tu confianza. A menudo, estas estafas de inversión tienen que ver con invertir en criptomonedas o bienes raíces, y el pago se suele realizar en este u otros métodos de pago no estándares. Si una inversión parece demasiado buena para ser verdad, lo más probable es que no lo sea. Recuerda, no existen las inversiones garantizadas de alto rendimiento. Solo invierte tu dinero instrumentos financieros conocidos y regulados, no en extraños que conozcas en línea que impulsan un plan para hacerse rico rápidamente.

Estafas amorosas

Cuando los delincuentes establecen una relación en línea con alguien que han identificado como solitario o vulnerable para engañarlos y sacarles dinero, esto se conoce como una estafa amorosa. Los delincuentes utilizarán todas las tácticas que puedan para generar confianza, incluido el envío de fotos falsas u obsequios, y luego compartirán una historia trágica sobre la necesidad de dinero para pagar gastos como las facturas del hospital o los costos de viaje para visitar a la víctima en persona. Para evitar reunirse en persona, estos delincuentes pueden decir que trabajan en una industria que les impide hacerlo, como la construcción, la medicina internacional o el ejército. Frecuentemente solicitan dinero mediante transferencias bancarias o tarjetas de regalo para obtener efectivo rápidamente y permanecer anónimos. Estos tipos de estafas no solo son comunes en las redes sociales, sino también en las apps de citas en línea. Ten cuidado con las personas que conoces en línea, toma las cosas con calma y nunca envíes dinero a alguien con quien solo te ha comunicado por ese medio.

Además, si crees que alguien que conoces puede ser vulnerable a un ataque de este tipo o tiene una relación en línea que genera estas alertas, ofrece tu ayuda. A veces puede ser muy difícil para alguien con una conexión emocional darse cuenta de lo peligrosa que se ha vuelto la situación.

Estafas de compras en línea

Las estafas de compras en línea ocurren cuando compras artículos en línea a precios extremadamente bajos o increíbles, pero nunca los recibes. Los anuncios tentadores en las redes sociales promoverán

Formato de texto HTML básico

Etiquetas

Biletin

Imagen

Browse... No file selected.

Máximo 1 fichero.
Límite de 2 MB.
Tipos permitidos: png gif jpg jpeg.

Publicado

Guardar Vista previa Eliminar

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT

PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

Por último, finalizado el llenado de los artículos, podemos revisar que estos se muestran en la página principal cuando entramos al sitio. Incluso se muestran las etiquetas que les asignamos.

The screenshot shows the website's main page with three articles listed:

- Descubren vulnerabilidades de alto impacto en UEFI de laptops Lenovo**
Envío por [admin](#) el Dom, 08/05/2022 - 16:25
Autor: [Martin Smolár](#)
Etiquetas: [Vulnerabilidades](#)
[Lee más](#) [Añadir nuevo comentario](#)
- Top tres de estafas en redes sociales**
Envío por [admin](#) el Dom, 08/05/2022 - 16:21
Resumen
Si bien las redes sociales son una forma fantástica de comunicarse, compartir y divertirse con los demás, también son una forma económica para que los ciberdelincuentes engañen y se aprovechen de millones de personas. No seas víctima de las tres estafas más comunes en redes sociales.
Etiquetas: [Buletín](#)
[Lee más](#) [Añadir nuevo comentario](#)
- Señales de que tu teléfono puede haber sido infectado con malware**
Envío por [admin](#) el Dom, 08/05/2022 - 15:08
Autor: [Amer Owaida](#)
Etiquetas: [Noticias](#)
[Lee más](#) [Añadir nuevo comentario](#)

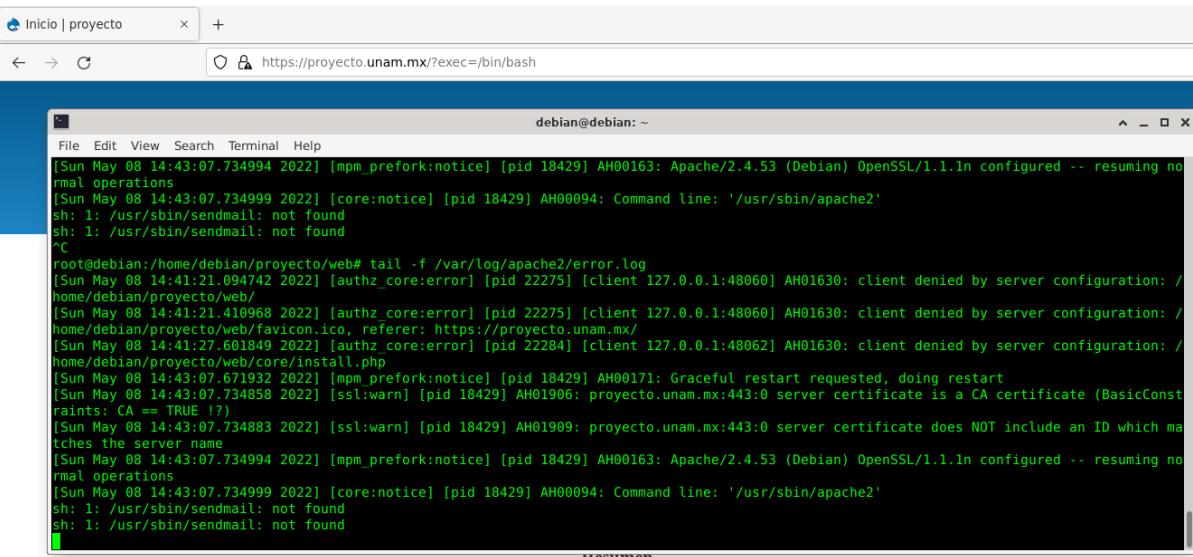
In the second article, the "Etiquetas" section and the "Buletín" tag are highlighted with a red box. In the third article, the "Etiquetas" section and the "Noticias" tag are highlighted with a red box.

COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA

5. Implementar un WAF para proteger el CMS (verificar antes y después con algún ataque).

Para la implementación del WAF haremos uso de modSecurity. Este es un firewall de aplicaciones Web embedible bajo licencia GNU que se ejecuta como módulo del servidor web Apache, provee protección contra diversos ataques hacia aplicaciones Web y permite monitorizar tráfico HTTP, así como realizar análisis en tiempo real sin necesidad de hacer cambios a la infraestructura existente.

Primero hacemos una prueba con la petición: <https://proyecto.unam.mx/?exec=/bin/bash>



```
[Sun May 08 14:43:07.734994 2022] [mpm_prefork:notice] [pid 18429] AH00163: Apache/2.4.53 (Debian) OpenSSL/1.1.1n configured -- resuming normal operations
[Sun May 08 14:43:07.734994 2022] [core:notice] [pid 18429] AH00094: Command line: '/usr/sbin/apache2'
sh: 1: /usr/sbin/sendmail: not found
sh: 1: /usr/sbin/sendmail: not found
^C
root@debian:/home/debian/proyecto/web# tail -f /var/log/apache2/error.log
[Sun May 08 14:41:21.094742 2022] [authz_core:error] [pid 22275] [client 127.0.0.1:48060] AH01630: client denied by server configuration: /home/debian/proyecto/web/
[Sun May 08 14:41:21.410968 2022] [authz_core:error] [pid 22275] [client 127.0.0.1:48060] AH01630: client denied by server configuration: /home/debian/proyecto/web/favicon.ico, referer: https://proyecto.unam.mx/
[Sun May 08 14:41:27.601849 2022] [authz_core:error] [pid 22284] [client 127.0.0.1:48062] AH01630: client denied by server configuration: /home/debian/proyecto/web/core/install.php
[Sun May 08 14:43:07.671932 2022] [mpm_prefork:notice] [pid 18429] AH00171: Graceful restart requested, doing restart
[Sun May 08 14:43:07.734858 2022] [ssl:warn] [pid 18429] AH01906: proyecto.unam.mx:443:0 server certificate is a CA certificate (BasicConstraints: CA == TRUE !?)
[Sun May 08 14:43:07.734883 2022] [ssl:warn] [pid 18429] AH01909: proyecto.unam.mx:443:0 server certificate does NOT include an ID which matches the server name
[Sun May 08 14:43:07.734994 2022] [mpm_prefork:notice] [pid 18429] AH00163: Apache/2.4.53 (Debian) OpenSSL/1.1.1n configured -- resuming normal operations
[Sun May 08 14:43:07.734999 2022] [core:notice] [pid 18429] AH00094: Command line: '/usr/sbin/apache2'
sh: 1: /usr/sbin/sendmail: not found
sh: 1: /usr/sbin/sendmail: not found
```

Instalamos modSecurity.

```
root@debian:/home/debian# apt install libapache2-mod-security2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  liblua5.1-0 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby python
The following NEW packages will be installed:
  libapache2-mod-security2 liblua5.1-0 modsecurity-crs
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 526 kB of archives.
After this operation, 2,395 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Editamos el archivo modSecurity.conf en /etc/modsecurity/modsecurity.conf

```
GNU nano 5.4                                     modsecurity.conf-recommended *
# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
#SecRuleEngine DetectionOnly
SecRuleEngine On
# -- Request body handling -----
```

**COORDINACIÓN DE SEGURIDAD DE LA INFORMACIÓN / UNAM-CERT
PLAN DE BECARIOS DE SEGURIDAD INFORMÁTICA**

Por último habilitamos el modulo con el comando:

```
root@debian:/etc/modsecurity# sudo a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
```

Volemos a realizar la prueba y revisamos las bitácoras:



The screenshot shows a browser window with the URL <https://proyecto.unam.mx/?exec=/bin/bash>. The page displays a large red "Forbidden" header and the message "You don't have permission to access this resource."

```
root@debian:/etc/modsecurity# tail -f /var/log/apache2/error.log
[Sun May 08 17:49:15 2022] [:notice] [pid 24718] ModSecurity: PCRE compiled version="8.39 "; loaded version="8.39 2016-06-14"
[Sun May 08 17:49:15 2022] [:notice] [pid 24718] ModSecurity: LUA compiled version="Lua 5.1"
[Sun May 08 17:49:15 2022] [:notice] [pid 24718] ModSecurity: YAJL compiled version="2.1.10"
[Sun May 08 17:49:15 2022] [:notice] [pid 24718] ModSecurity: LIBXML compiled version="2.9.10"
[Sun May 08 17:49:15 2022] [:notice] [pid 24718] ModSecurity: StatusEngine v2.9.3,Apache/2.4.53 (Debian),1.7.0/1.7.0.8.39/8.39 2016-06-14,Lua 5.1,2.9.10,86
[Sun May 08 17:49:15 2022] [:notice] [pid 24719] ModSecurity: StatusEngine call failed. Query: GIX0SLRTFRAXAYLDNB556MR0G0X0KMZA.FBCGKYTJMFX5LBRY354MBPGEXDOLQ.F04C4MZ
F44C4MZEEZDAMJWFYDMLR.GOMEYSLBEA254WJMGI0XLSRRGAN0W1.1652050155 status:modsecurity.org
[Sun May 08 17:49:23 170848 2022] [ssl:warn] [pid 24721] AH01906: projecto.unam.mx:443:0 server certificate is a CA certificate (BasicConstraints: CA == TRUE !)
[Sun May 08 17:49:23 170848 2022] [ssl:warn] [pid 24721] AH01909: projecto.unam.mx:443:0 server certificate does NOT include an ID which matches the server name
[Sun May 08 17:49:23 185023 2022] [mpm_prefork:notice] [pid 24721] AH00163: Apache/2.4.53 (Debian) OpenSSL/1.1.1n configured -- resuming normal operations
[Sun May 08 17:49:23 185059 2022] [core:notice] [pid 24721] AH00094: Command line: '/usr/sbin/apache2'
[Sun May 08 17:50:11 182615 2022] [error] [pid 24721] [client 127.0.0.1:49314] (client 127.0.0.1) ModSecurity: Warning, Matched phrase "bin/bash" at ARGS:exec, [file "/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "500"] [id "932160"] [msg "Remote Command Execution: Unix Shell Code Found"] [data "Matched Data: bin/bash found within ARGS:exec: '/bin/bash'" [severity "CRITICAL"] [ver "OWASP CRS/3.0.0"] [tag "application-multi"] [tag "language-shell"] [tag "attack-rce"] [tag "paranoia-level"] [tag "OWASP CRS"] [tag "capec/1090/152/248/89"] [tag "platform-unix"] [uri "/"] [unique_id "YnhjIBXOVyj2NhIBq3bkogAAAE"]
[Sun May 08 17:50:11 183266 2022] [error] [pid 24723] [client 127.0.0.1:49314] [client 127.0.0.1] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 5) [severity "CRITICAL"] [ver "OWASP CRS/3.0.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "projecto.unam.mx"] [uri "/"] [unique_id "YnhjIBXOVyj2NhIBq3bkogAAAE"]
[Sun May 08 17:50:11 183913 2022] [error] [pid 24723] [client 127.0.0.1:49314] [client 127.0.0.1] ModSecurity: Warning. Operator GE matched 5 at TX:inbound anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "91"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=0,XSS=0,RFI=0,LEI=0,RCE=5,PHP=0,HTTP=0,SESS=0): individual paranoia level scores: 5, 0, 0, 0" [ver "OWASP CRS/3.0.0"] [tag "event-correlation"] [hostname "projecto.unam.mx"] [uri "/"] [unique_id "YnhjIBXOVyj2NhIBq3bkogAAAE"]
root@debian:/etc/modsecurity# tail -f /var/log/apache2/
access.log           error.log          modsec_audit.log      other_vhosts_access.log
root@debian:/etc/modsecurity# tail -f /var/log/apache2/modsec_audit.log
Action: Intercepted (phase 2)
Stopwatch: 1652050211180471 3690 (- - -)
Stopwatch2: 1652050211180471 3690; combined=2263, p1=580, p2=1447, p3=0, p4=0, p5=236, sr=71, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.3 (http://www.modsecurity.org/); OWASP CRS/3.3.0.
Server: Apache/2.4.53 (Debian)
Engine-Mode: "ENABLED"

--1426931f-Z--
```

6. Realizar la documentación correspondiente con capturas de pantalla, así como grabar un vídeo de la implementación y funcionamiento.

La grabación se encontrará en un link de drive.

El documento se encontrará tanto en nuestro repositorio de Github así como en la carpeta de drive.

7. Se entrega: ruta al repositorio de GitHub, documentación y vídeo, en equipos de máximo 4 personas.

Link del repositorio de GitHub: <https://github.com/D4vidd/ProyectoSegWeb>

Link de la carpeta de Google Drive:

https://drive.google.com/drive/folders/1cLQFzoZybUyjbmhZh4Wm8WY_YtB6y--S?usp=sharing