



Programa de Becas de Formación en Seguridad Informática

Coordinación de Seguridad de la Información

UNAM-CERT

Seguridad en aplicaciones web

Proyecto: Drupal

Integrantes:

- Andrés Martínez López
- Billy Diaz De Luis
- César Alejandro Varela Cruz
- Emmanuel Julián José

Requisitos	3
Instalación	4
Instalación de apache	4
Instalación de PHP	4
Instalación PostgreSQL	5
Configuración Sitio	5
Habilitación de módulos	5
Crearemos un certificado autofirmado	5
Instalacion Drupal	7
Configuración de Drupal	12
Usuario Contenido	13
Contenido	16
Configuración para administración de contenido	16
Noticias	19
Boletín	22
Vulnerabilidades	24
WAF	27
Implementación de un WAF	27
Pruebas del WAF	29

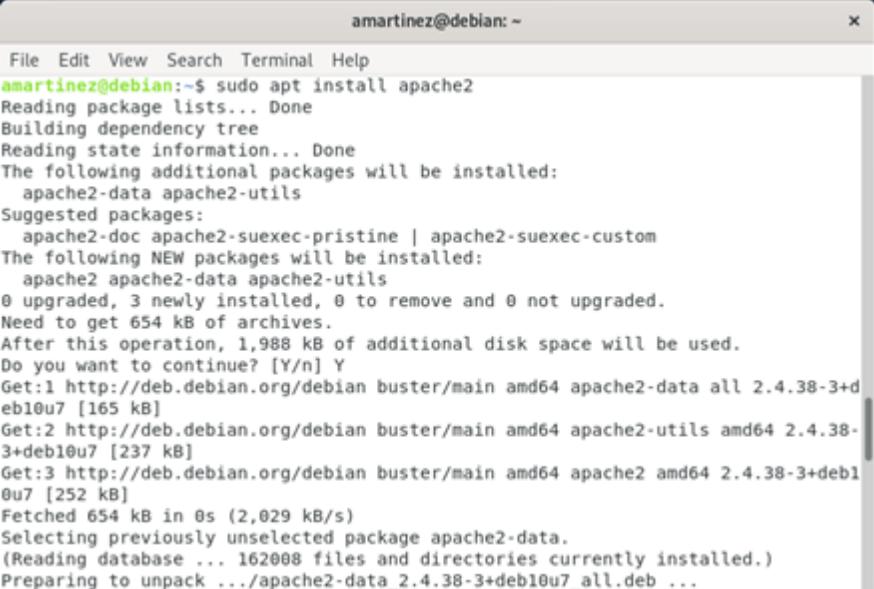
Requisitos

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.
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).
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. Implementar su propio "Portal de Seguridad" con contenido de: noticias de seguridad, boletines y vulnerabilidades (recientes, al menos 5 elementos de cada uno).
5. Implementar un WAF para proteger el CMS (verificar antes y después con algún ataque).
6. Realizar la documentación correspondiente con capturas de pantalla, así como grabar un vídeo de la implementación y funcionamiento.
7. Se entrega: ruta al repositorio de GitHub, documentación y vídeo, en equipos de máximo 4 personas.

Instalación

Instalación de apache

```
sudo apt install apache2
```

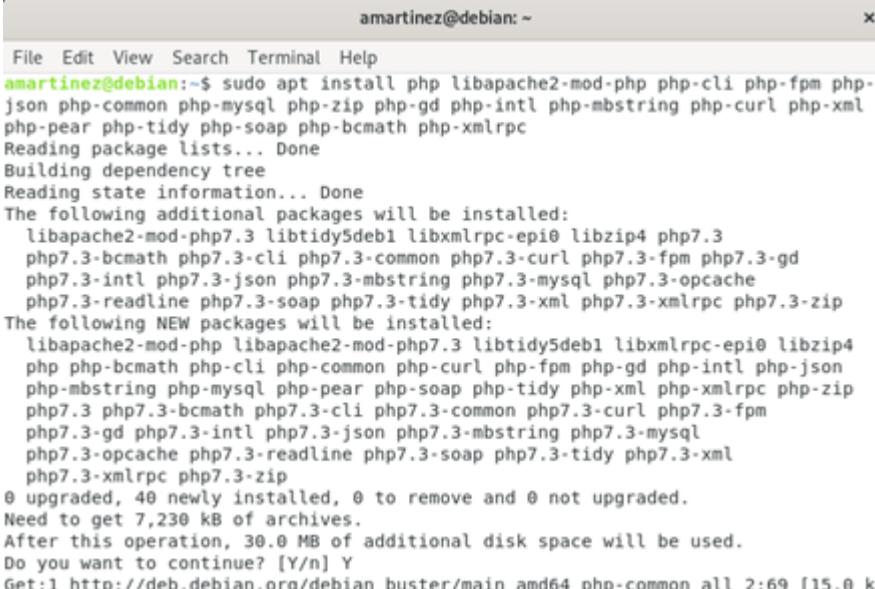


```
amartinez@debian:~
```

```
File Edit View Search Terminal Help
amartinez@debian:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 654 kB of archives.
After this operation, 1,988 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian buster/main amd64 apache2-data all 2.4.38-3+deb10u7 [165 kB]
Get:2 http://deb.debian.org/debian buster/main amd64 apache2-utils amd64 2.4.38-3+deb10u7 [237 kB]
Get:3 http://deb.debian.org/debian buster/main amd64 apache2 amd64 2.4.38-3+deb10u7 [252 kB]
Fetched 654 kB in 0s (2,029 kB/s)
Selecting previously unselected package apache2-data.
(Reading database ... 162008 files and directories currently installed.)
Preparing to unpack .../apache2-data_2.4.38-3+deb10u7_all.deb ...
```

Instalación de PHP

```
sudo apt install php libapache2-mod-php php-cli php-fpm php-json php-common
php-pgsql php-zip php-gd php-intl php-mbstring php-curl php-xml php-pear php-tidy
php-soap php-bcmath php-xmlrpc
```

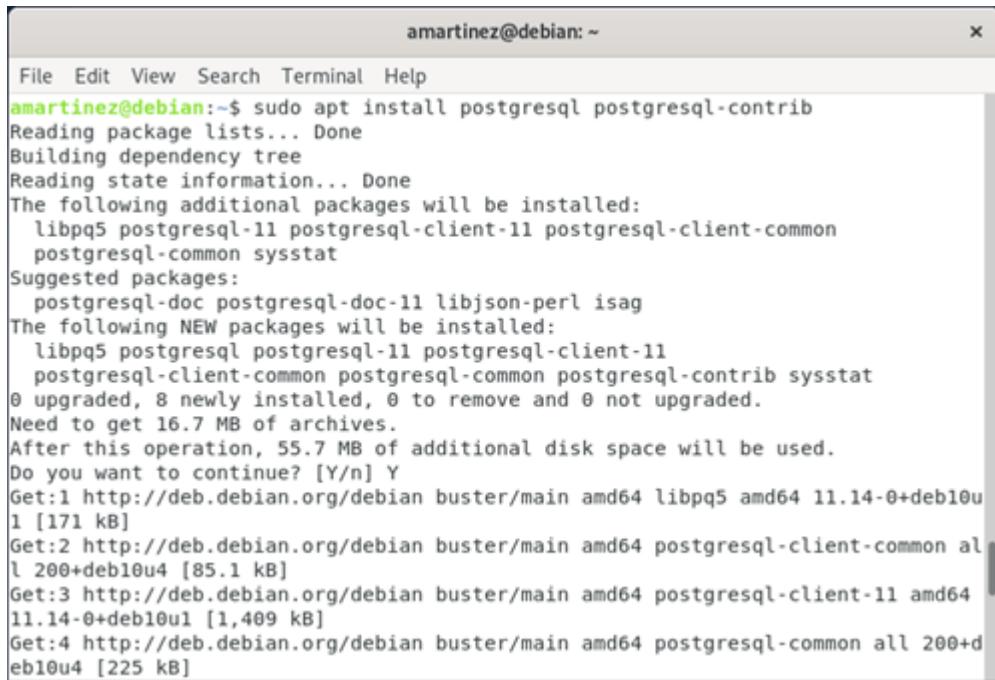


```
amartinez@debian:~
```

```
File Edit View Search Terminal Help
amartinez@debian:~$ sudo apt install php libapache2-mod-php php-cli php-fpm php-
json php-common php-mysql php-zip php-gd php-intl php-mbstring php-curl php-xml
php-pear php-tidy php-soap php-bcmath php-xmlrpc
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php7.3 libtidy5deb1 libxmlrpc-epi0 libzip4 php7.3-
php7.3-bcmath php7.3-cli php7.3-common php7.3-curl php7.3-fpm php7.3-gd
php7.3-intl php7.3-json php7.3-mbstring php7.3-mysql php7.3-opcache
php7.3-readline php7.3-soap php7.3-tidy php7.3-xml php7.3-xmlrpc php7.3-zip
The following NEW packages will be installed:
  libapache2-mod-php libapache2-mod-php7.3 libtidy5deb1 libxmlrpc-epi0 libzip4
php php-bcmath php-cli php-common php-curl php-fpm php-gd php-intl php-json
php-mbstring php-mysql php-pear php-soap php-tidy php-xml php-xmlrpc php-zip
php7.3 php7.3-bcmath php7.3-cli php7.3-common php7.3-curl php7.3-fpm
php7.3-gd php7.3-intl php7.3-json php7.3-mbstring php7.3-mysql
php7.3-opcache php7.3-readline php7.3-soap php7.3-tidy php7.3-xml
php7.3-xmlrpc php7.3-zip
0 upgraded, 48 newly installed, 0 to remove and 0 not upgraded.
Need to get 7,230 kB of archives.
After this operation, 30.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian buster/main amd64 php-common all 2:69 [15.0 k]
```

Instalación PostgreSQL

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



```
amartinez@debian:~$ sudo apt install postgresql postgresql-contrib
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpq5 postgresql-11 postgresql-client-11 postgresql-client-common
  postgresql-common sysstat
Suggested packages:
  postgresql-doc postgresql-doc-11 libjson-perl isag
The following NEW packages will be installed:
  libpq5 postgresql postgresql-11 postgresql-client-11
  postgresql-client-common postgresql-common postgresql-contrib sysstat
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 16.7 MB of archives.
After this operation, 55.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian buster/main amd64 libpq5 amd64 11.14-0+deb10u1 [171 kB]
Get:2 http://deb.debian.org/debian buster/main amd64 postgresql-client-common all 200+deb10u4 [85.1 kB]
Get:3 http://deb.debian.org/debian buster/main amd64 postgresql-client-11 amd64 11.14-0+deb10u1 [1,409 kB]
Get:4 http://deb.debian.org/debian buster/main amd64 postgresql-common all 200+deb10u4 [225 kB]
```

Configuración Sitio

Habilitación de módulos

```
sudo a2enmod rewrite
sudo systemctl restart apache2
```

```
amartinez@debian:~$ sudo a2enmod rewrite
[sudo] password for amartinez:
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
amartinez@debian:~$ sudo systemctl restart apache2
amartinez@debian:~$ sudo apache2ctl -M |grep rewrite
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
  rewrite_module (shared)
amartinez@debian:~$
```

Crearemos un certificado autofirmado

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

```

amartinez@debian:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -ke
yout /etc/ssl/private/proyecto.key -out /etc/ssl/certs/proyecto.crt
[sudo] password for amartinez:
Generating a RSA private key
+++++
.....+++++
writing new private key to '/etc/ssl/private/proyecto.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]:Mexico
Locality Name (eg, city) []:CU
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNAM
Organizational Unit Name (eg, section) []:DGTIC
Common Name (e.g. server FQDN or YOUR name) []:www.portalseguridad.unam.mx
Email Address []:

```

Creamos el archivo de configuración del sitio www.portalseguridad.unam.mx de la siguiente forma

```
sudo nano /etc/apache2/sites-available/proyecto.conf
```

```

GNU nano 3.2                               /etc/apache2/sites-available/proyecto.conf

<VirtualHost *:80>
    ServerName      www.portalseguridad.unam.mx
    RedirectMatch 301 (.*) https://www.portalseguridad.unam.mx$1
</VirtualHost>

<VirtualHost _default_:443>
    ServerName      www.portalseguridad.unam.mx
    ServerAlias     portalseguridad.unam.mx
    DocumentRoot   /var/www/proyecto
    <Directory /var/www/proyecto/>
        Options FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
    SSLEngine On
    SSLCertificateFile    /etc/ssl/certs/proyecto.crt
    SSLCertificateKeyFile /etc/ssl/private/proyecto.key

    LogLevel info ssl:warn
    ErrorLog ${APACHE_LOG_DIR}/proyecto-error.log
    CustomLog ${APACHE_LOG_DIR}/proyecto-access.log combined
</VirtualHost>
```

Posteriormente creamos el directorio en el cual se alojarán los archivos de nuestro sitio

```
sudo mkdir -p /var/www/proyecto
```

Creación de base de datos para Drupal 9

```

sudo -u postgres createuser -P drupal
sudo -u postgres createdb drupal -O drupal
```

```

amartinez@debian:~$ sudo -u postgres createuser -P drupal
Enter password for new role:
Enter it again:
amartinez@debian:~$ sudo -u postgres createdb drupal -O drupal
```

Instalacion Drupal

Ahora Descargamos la versión 9 de Drupal

```
DRUPAL_VERSION="9.2.7"
```

```
wget https://ftp.drupal.org/files/projects/drupal-${DRUPAL_VERSION}.tar.gz
```

```
amartinez@debian:~$ DRUPAL_VERSION="9.2.7"
amartinez@debian:~$ sudo wget https://ftp.drupal.org/files/projects/drupal-${DRUPAL_V
ERSION}.tar.gz
[sudo] password for amartinez:
--2022-05-06 16:56:56-- https://ftp.drupal.org/files/projects/drupal-9.2.7.tar.gz
Resolving ftp.drupal.org (ftp.drupal.org)... 151.101.50.217
Connecting to ftp.drupal.org (ftp.drupal.org)|151.101.50.217|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18863167 (18M) [application/octet-stream]
Saving to: 'drupal-9.2.7.tar.gz'

drupal-9.2.7.tar.gz    100%[=====] 17.99M  9.43MB/s   in 1.9s

2022-05-06 16:56:59 (9.43 MB/s) - 'drupal-9.2.7.tar.gz' saved [18863167/18863167]
```

Y descomprimimos el archivo con el siguiente comando

```
tar xvf drupal-${DRUPAL_VERSION}.tar.gz
```

Ahora movemos los archivos generados a la carpeta creada anteriormente para el sitio
www/var/proyecto

```
amartinez@debian:~$ sudo mv drupal-9.2.7 /var/www/proyecto
amartinez@debian:~$ ls /var/www/proyecto/
autoload.php  core          INSTALL.txt  profiles    sites      vendor
composer.json example.gitignore LICENSE.txt  README.md  themes    web.config
composer.lock index.php       modules      robots.txt update.php
amartinez@debian:~$
```

Y cambiamos al usuario y grupo dueño de los archivos

```
Sudo chown -R www-data:www-data /var/www/proyecto/
```

```
amartinez@debian:~$ sudo chown -R www-data:www-data /var/www/proyecto/
-----
```

Activamos el módulo de apache ssl

```
sudo a2enmod ssl
```

```
amartinez@debian:~$ sudo 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
```

Y algunos otros módulos que podría llegar a ocupar drupal

```
amartinez@debian:~$ sudo a2enmod expires headers rewrite
Enabling module expires.
Enabling module headers.
Module rewrite already enabled
To activate the new configuration, you need to run:
    systemctl restart apache2
amartinez@debian:~$ sudo systemctl restart apache2
```

Ahora habilitamos el sitio y reiniciamos el servicio de apache

```
sudo a2ensite Proyecto.conf
sudo systemctl reload apache2
```

```
amartinez@debian:~$ sudo a2ensite proyecto.conf
Enabling site proyecto.
To activate the new configuration, you need to run:
    systemctl reload apache2
amartinez@debian:~$ sudo systemctl reload apache2
```

Modificamos el archivo hosts para poder acceder al sitio web

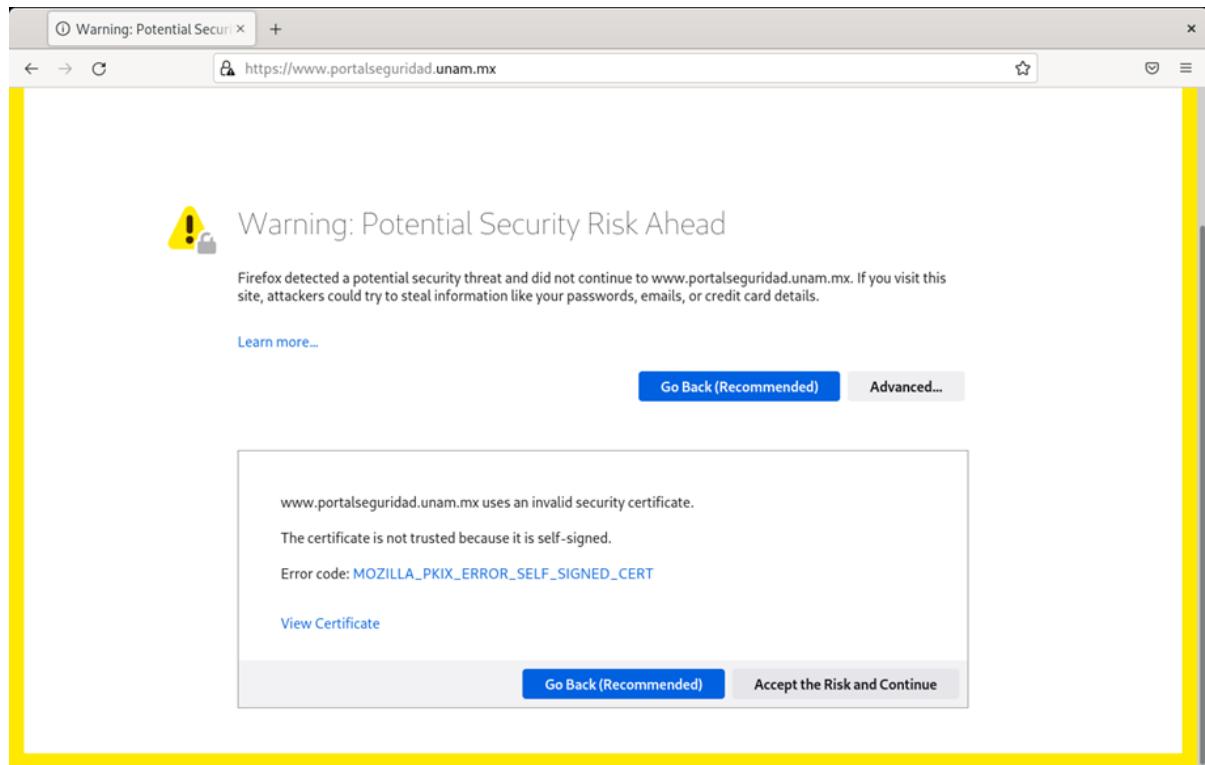
```
GNU nano 3.2                               /etc/hosts

127.0.0.1      localhost
127.0.1.1      debian

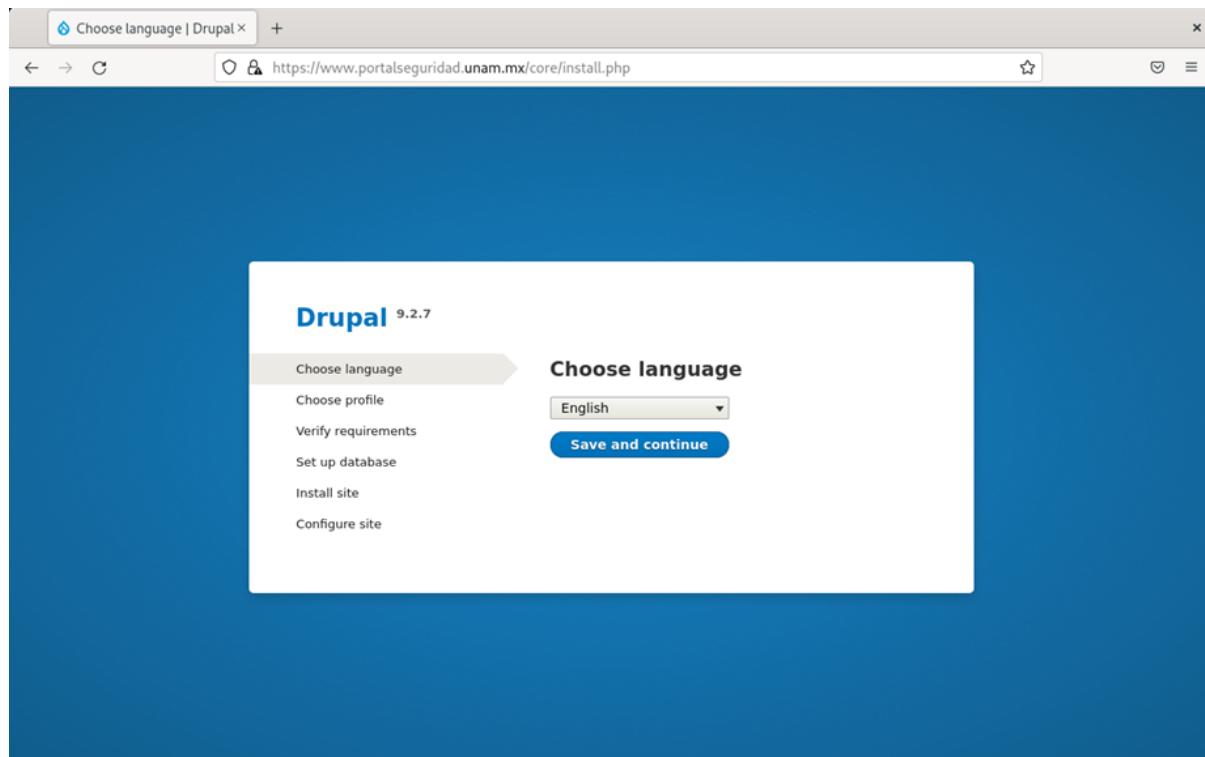
127.0.0.1      www.portalseguridad.unam.mx

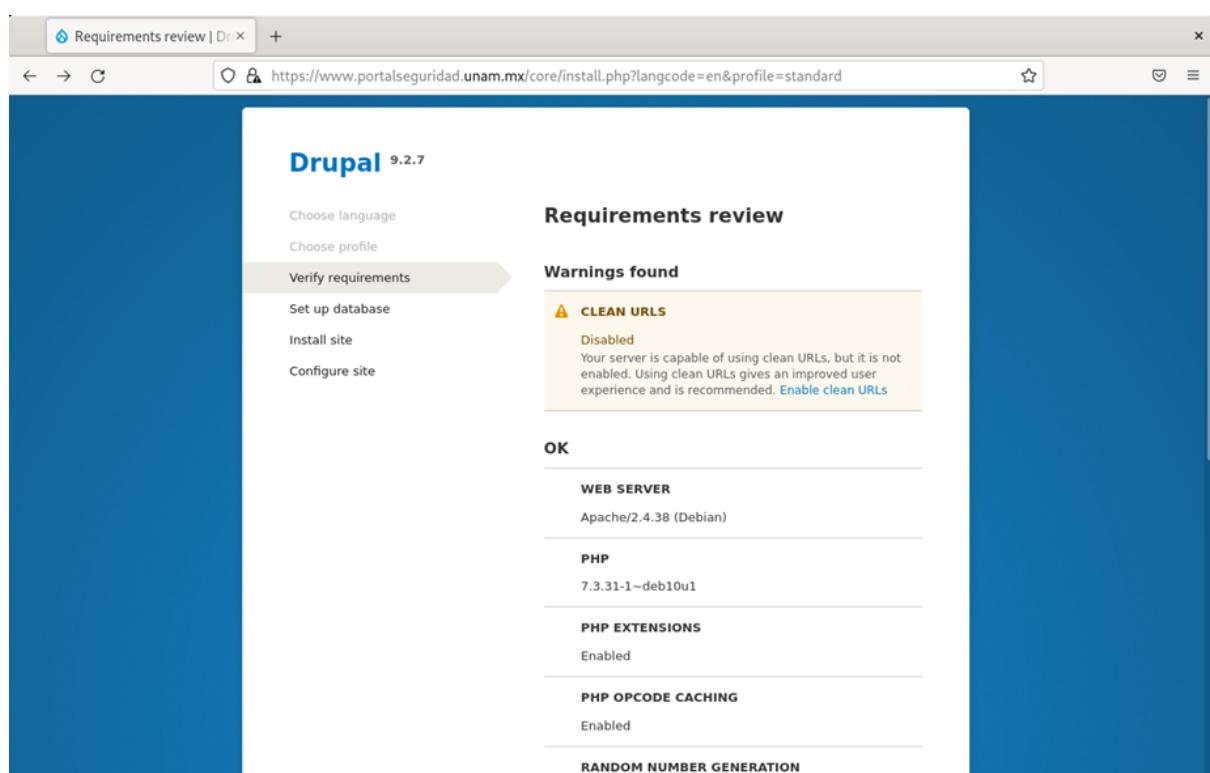
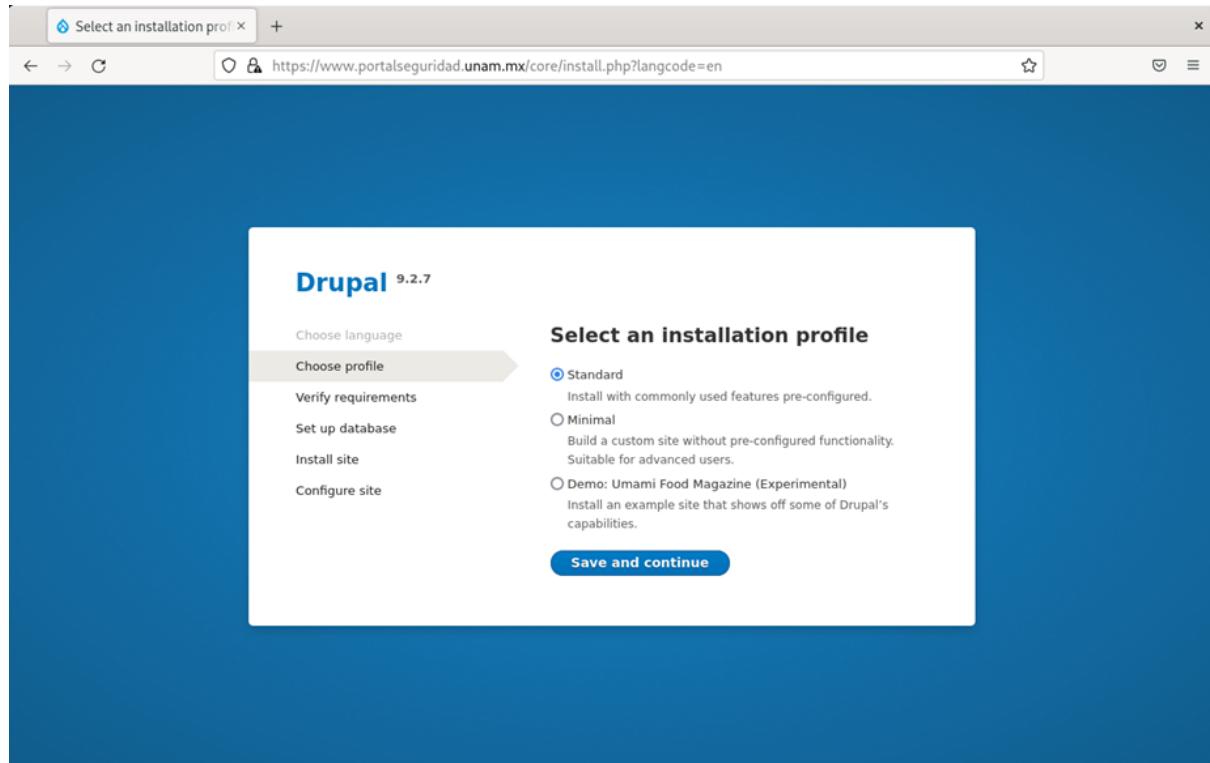
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

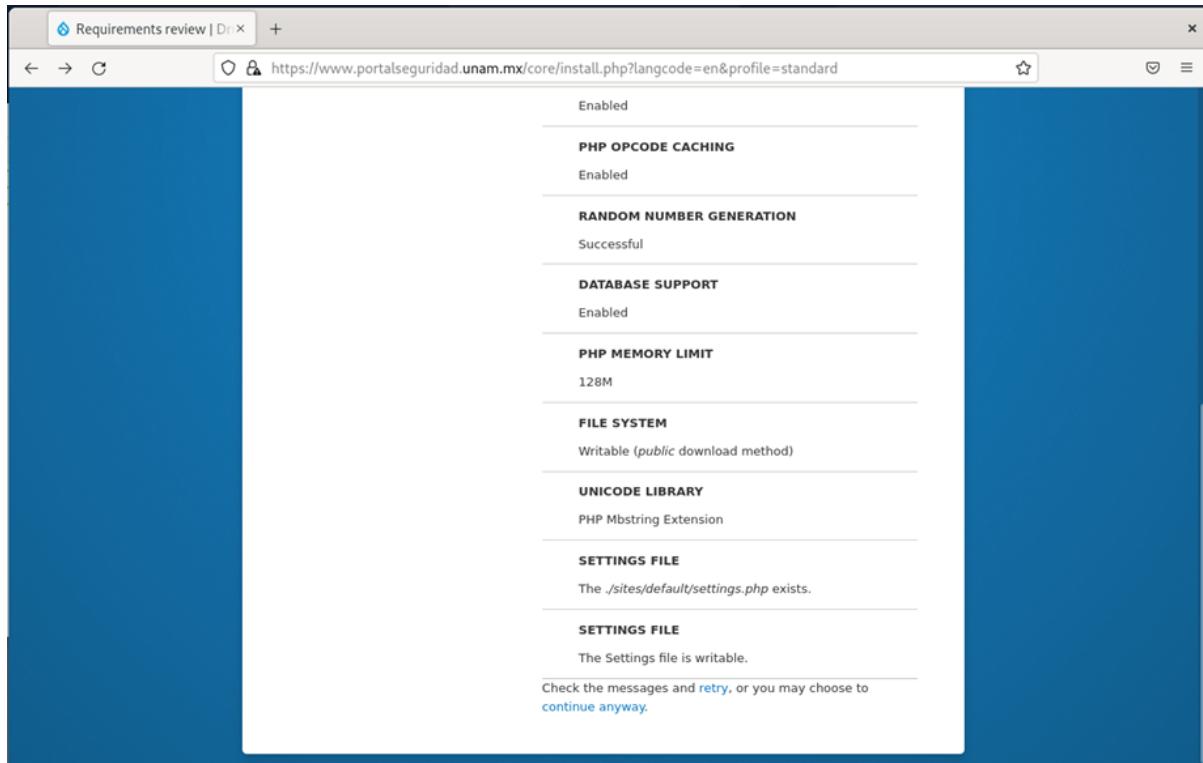
Ahora a través de un navegador ingresamos a www.portalseguridad.unam.mx y aceptamos los riesgos del certificado



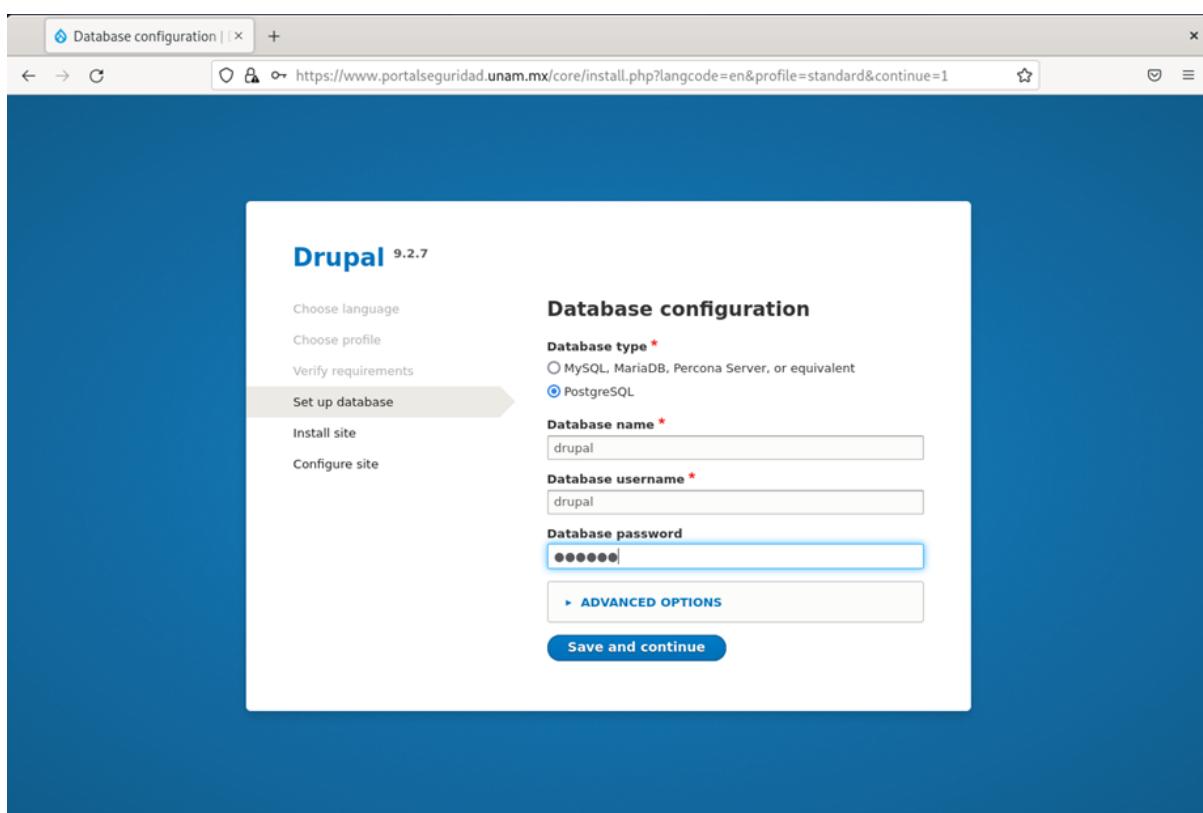
Posteriormente se nos muestra la interfaz de Drupal en el que acabaremos la configuración como se muestra a continuación

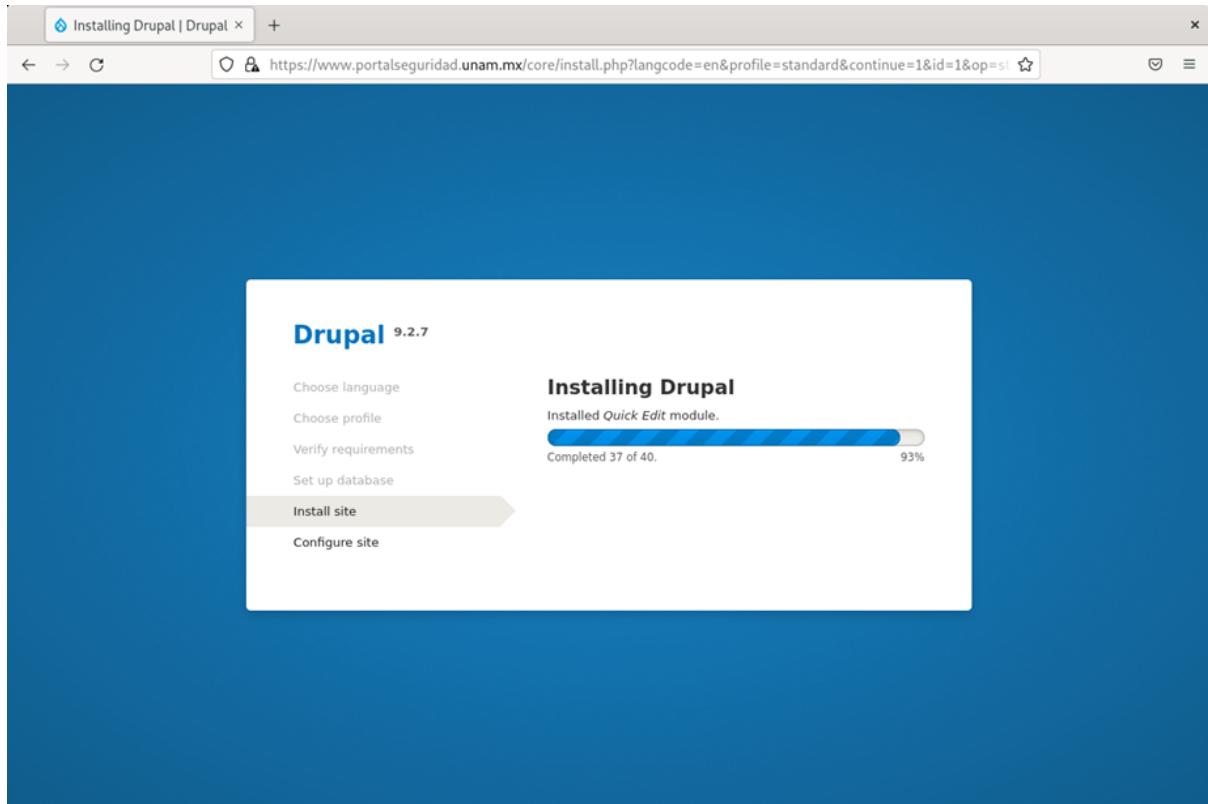






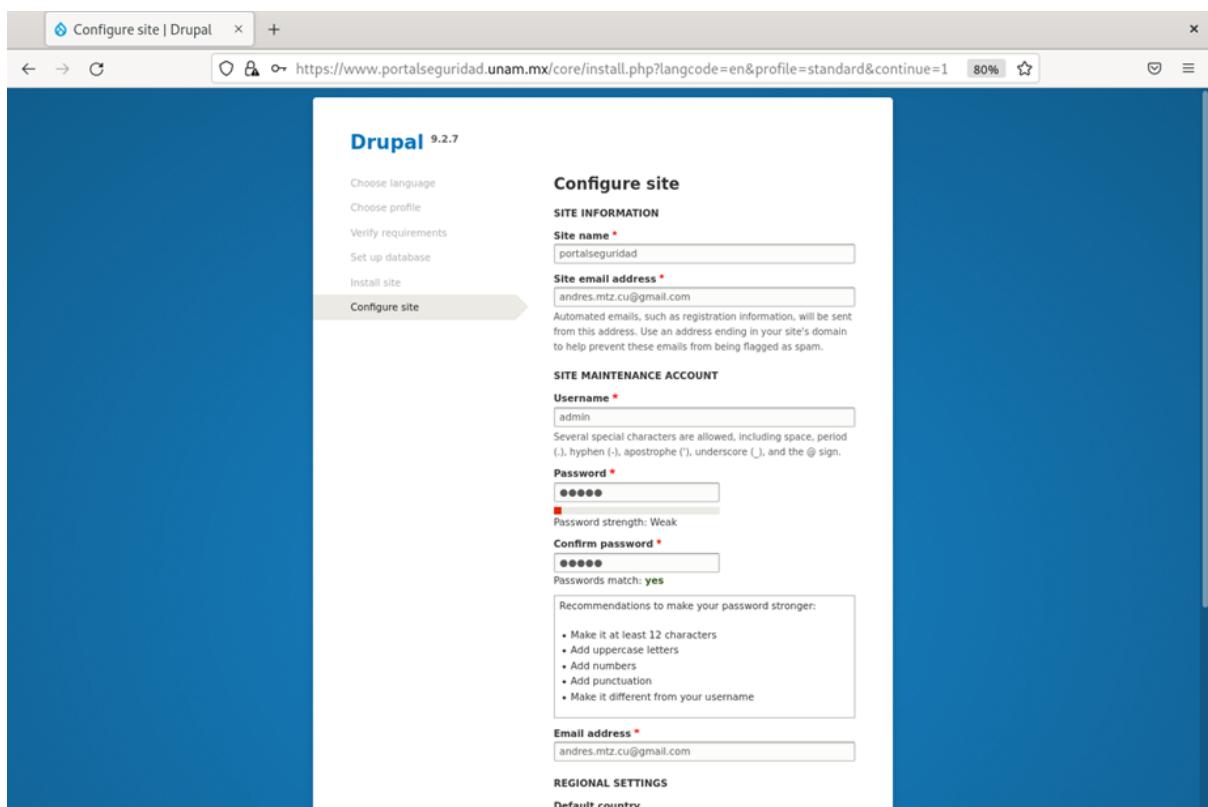
Para la configuración de la base de datos elegimos Postgresql.

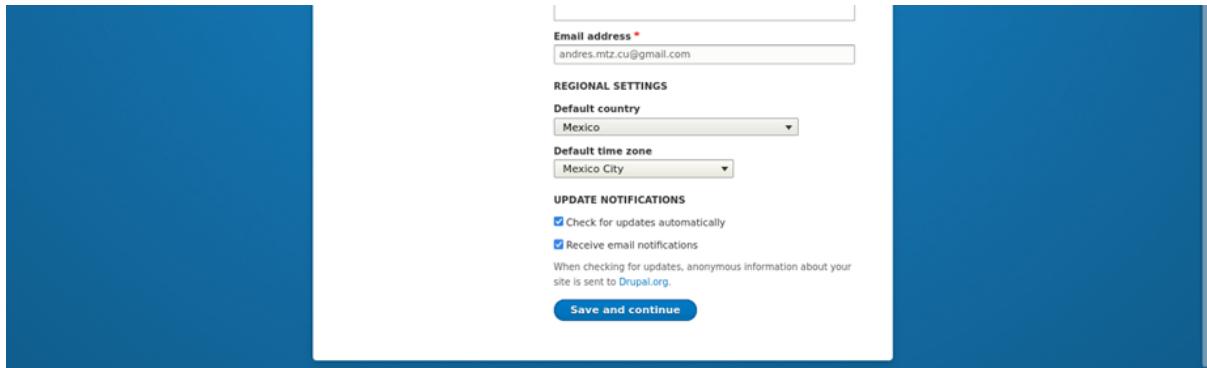




Configuración de Drupal

Configuramos el sitio www.portalseguridad.unam.mx





A continuación se muestra el funcionamiento e instalación correcta de drupal.

A screenshot of a web browser showing the Drupal 7 homepage. The URL in the address bar is 'https://www.portalseguridad.unam.mx'. The page has a dark blue header with the site logo 'portalseguridad' and a navigation menu with links like 'Content', 'Structure', 'Appearance', 'Extend', 'Configuration', 'People', 'Reports', and 'Help'. On the right, there are links for 'My account' and 'Log out'. The main content area has a green banner at the top with the text 'Congratulations, you installed Drupal!'. Below it is a search bar with placeholder text 'Search' and a magnifying glass icon. To the right of the search bar is a 'Welcome to portalseguridad' message. It says 'No front page content has been created yet. Follow the [User Guide](#) to start building your site.' There is also a link 'Add content' and a small orange RSS feed icon. In the bottom left corner of the content area, there is a link 'Contact'.

Usuario Contenido

Ahora crearemos el usuario contenido, este usuario se encargara de administrar el contenido de la pagina.

The screenshot shows the 'Roles' page in the Drupal administration interface. At the top, there is a message box stating: 'There is a security update available for your version of Drupal. To ensure the security of your server, you should update immediately! See the available updates page for more information and to install your missing updates.' Below this, a note explains that a role defines a group of users with certain privileges. A blue button '+ Add role' is visible. The main area displays a table with columns 'NAME' and 'OPERATIONS'. The table lists several roles, including 'Anonymous user', 'Authenticated user', 'Content author', 'Content moderator', 'Content reviewer', 'Content manager', 'Editor', 'Administrator', and 'Guest'. The 'OPERATIONS' column contains icons for each role.

Asignaremos únicamente todos los permisos de Node

The screenshot shows the 'Permissions' page for the 'Node' role in the Drupal administration interface. The left sidebar shows the 'PERMISSION' section, and the right sidebar shows the 'CONTENIDO' section. The table lists various permissions, all of which are checked (indicated by a blue checkmark). The permissions listed include: Article: Create new content, Basic page: Create new content, Article: Delete any content, Basic page: Delete any content, Article: Delete own content, Basic page: Delete own content, Article: Delete revisions, Basic page: Delete revisions, Article: Edit any content, Basic page: Edit any content, Article: Edit own content, Basic page: Edit own content, and Article: Revert revisions.

Ahora asignaremos ese Rol al nuevo usuario llamado contenidos

https://www.portalseguridad.unam.mx/admin/people

Back to site Manage Shortcuts admin

Content Structure Appearance Extend Configuration People Reports Help

People ☆

List Permissions Roles

Home » Administration

There is a security update available for your version of Drupal. To ensure the security of your server, you should update immediately! See the [available updates](#) page for more information and to install your missing updates.

+ Add user

Name or email contains Status Role Permission

contenidos Active contenido - Any -

Filter

Action

Add the Administrator role to the selected user(s)

Content Structure Appearance Extend Configuration People Reports Help

Add user ☆

Home » Administration » People

There is a security update available for your version of Drupal. To ensure the security of your server, you should update immediately! See the [available updates](#) page for more information and to install your missing updates.

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 if you wish to receive a new password or wish to receive certain news or notifications by email.

Username *

contenidos

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

Password *

••••••••••
Password strength: Weak

Confirm password *

••••••••••
Passwords match: yes

Recommendations to make your password stronger:

- Make it at least 12 characters
- Add uppercase letters
- Add numbers
- Add punctuation

Contenido

Configuración para administración de contenido

Status
 Blocked
 Active

Roles
 Authenticated user
 Administrator
 contenido

Picture
 No file selected.
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 privileged users such as site administrators are still able to contact you even if you choose to disable this feature.

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

A continuación se muestran los usuarios existentes en drupal.

Usuarios						
Listado		Permisos	Roles	Role settings		
Inicio > Administración						
<input type="button" value="+ Anadir usuario"/>	Nombre o correo electrónico contiene	Estado	Rol	Permiso		
	<input type="text"/>	<input type="button" value="- Cualquiera -"/>	<input type="button" value="- Cualquiera -"/>	<input type="button" value="- Cualquiera -"/>		
<input type="button" value="Filtro"/>						
Acción	<input type="button" value="Add the Administrator role to the selected user(s)"/>					
<input type="button" value="Aplicar a los elementos seleccionados"/>						
<input type="checkbox"/> NOMBRE DE USUARIO ESTADO ROLES MIEMBRO DESDE HACE ÚLTIMO ACCESO OPERACIONES						
<input type="checkbox"/>	contenidos	Activo	• Content editor	1 minuto 11 segundos	32 segundos ago	<input type="button" value="Editar"/>
<input type="checkbox"/>	admin	Activo	• Administrador	9 minutos 6 segundos	3 minutos 58 segundos ago	<input type="button" value="Editar"/>
<input type="button" value="Aplicar a los elementos seleccionados"/>						

Inicio de sesión utilizando el usuario contenidos.

Iniciar sesión | Portal seguridad

Portal seguridad

Inicio

Buscar

Iniciar sesión | Crear nueva cuenta | Reiniciar su contraseña

Nombre de usuario *

contenidos

Escriba su nombre de usuario en Portal seguridad.

Contraseña *

Escriba la contraseña asignada a su nombre de usuario.

Iniciar sesión

Contacto

Funciona con Drupal

Podemos observar los permisos del usuario contenidos y administrador.

Permisos | Portal seguridad

Regresar al sitio Administrar Atajos admin

Contenido Estructura Apariencia Ampliar Configuración Usuarios Informes Ayuda

Permisos

Listado Permisos Roles Role settings

Inicio > Administración > Usuarios

Los permisos les permiten controlar lo que los usuarios pueden hacer y ver en su sitio. Puede definir un conjunto específico de permisos para cada rol. (Consulte la página Roles para crear un rol.) Cualquier permiso concedido al rol de usuario registrado será dado a cualquier usuario que haya iniciado sesión en su sitio. Desde la página Opciones de la cuenta, puede cambiar cualquier rol en un rol de Administrador para el sitio, lo que significa que pueden conceder nuevos permisos automáticamente. Deberá tener cuidado de asegurar que solo los usuarios en los que confíe se le conceda este acceso y nivel de control de su sitio.

Ocultar las descripciones

PERMISO	USUARIO ANÓNIMO	USUARIO AUTENTICADO	CONTENT EDITOR	ADMINISTRADOR
Block				<input checked="" type="checkbox"/>
Administrar bloques	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Comment				
Administrar tipos de comentarios y sus opciones	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Advertencia: Proporcionar sólo a los roles de confianza. Este permiso implica riesgos de seguridad.				
Administrar comentarios y opciones de comentarios	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Editar comentarios propios	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Publicar comentarios	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Omitir aprobación de comentario	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
Ver comentarios	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Configuration Manager				

Habilitamos la creación de vistas al usuario de los contenidos.

Permisos | Portal seguridad

Regresar al sitio Administrar Atajos admin

Contenido Estructura Apariencia Ampliar Configuración Usuarios Informes Ayuda

Permisos

Listado Permisos Roles Role settings

Este incluye métodos de cancelación de cuentas, contenido de correos para usuarios y campos adjuntos a usuarios.

Administrar roles y permissions

Advertencia: Proporcionar sólo a los roles de confianza. Este permiso implica riesgos de seguridad.

Administrar usuarios

Advertencia: Proporcionar sólo a los roles de confianza. Este permiso implica riesgos de seguridad. Gestiona todas las cuentas de usuario. Esto incluye edición de toda la información de usuarios, cambios de direcciones de email y contraseña, avisos a los usuarios por correo electrónico y bloqueo y borrado de cuentas de usuarios.

Cancelar cuenta propia

Nota: el contenido puede ser mantenido, despublicado, eliminado o transferido al usuario anónimo dependiendo de la configuración del usuario activo.

Cambiar nombre de usuario propio

Seleccionar el método para cancelar la cuenta.

Advertencia: Proporcionar sólo a los roles de confianza. Este permiso implica riesgos de seguridad.

View user email addresses

Users without this permission will not have access to email addresses on user pages or other places where they might be shown, such as Views and JSON:API responses.

Ver información del usuario

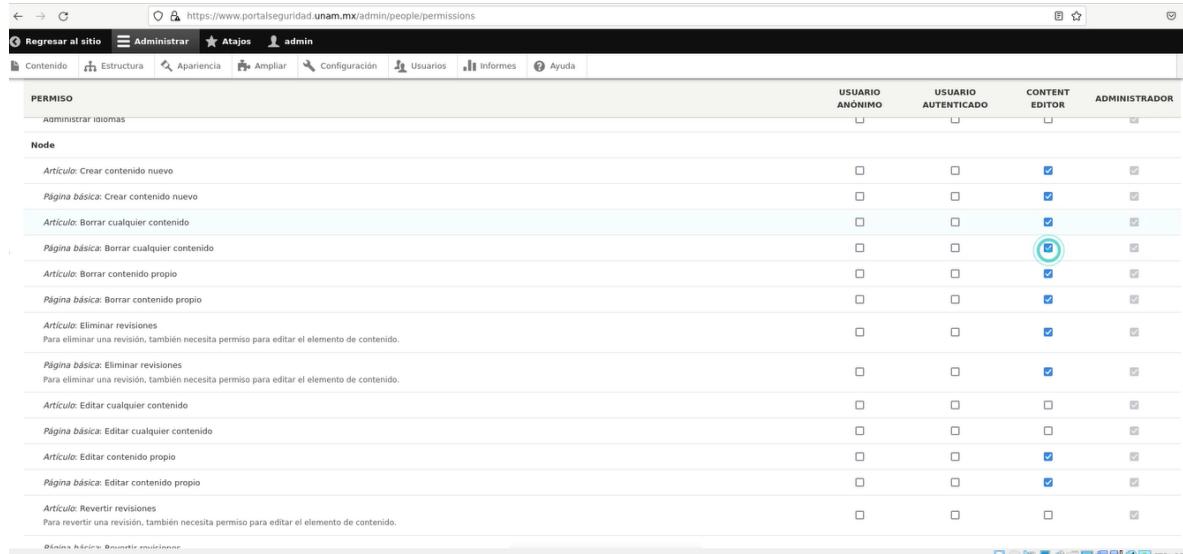
Views UI

Administrarse vistas

Advertencia: Proporcionar sólo a los roles de confianza. Este permiso implica riesgos de seguridad.

Guardar permisos

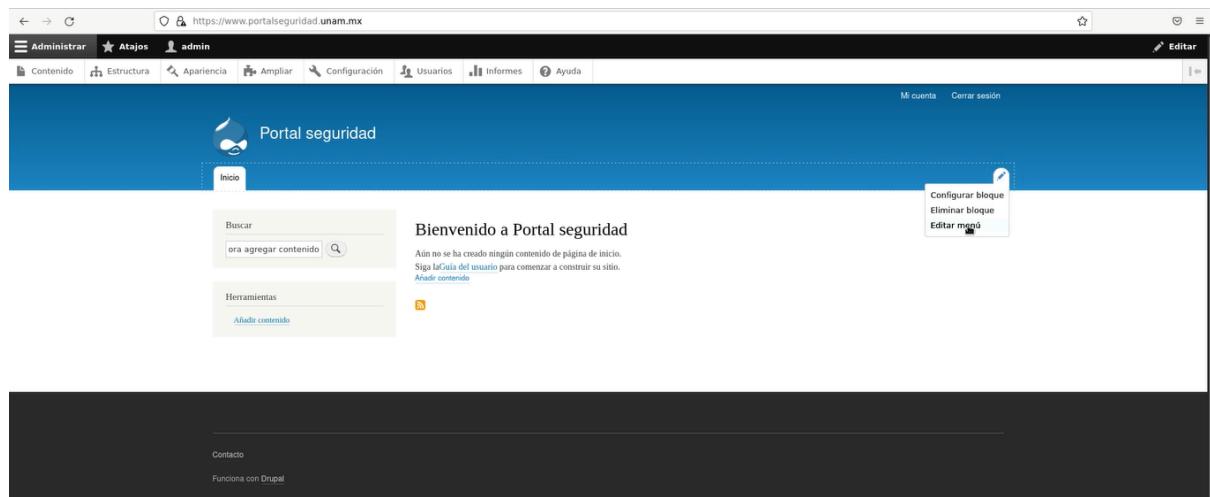
Al usuario de contenidos le agregamos los permisos administrar, crear y borrar contenido. Guardamos los cambios.



PERMISO	USUARIO ANÓNIMO	USUARIO AUTENTICADO	CONTENT EDITOR	ADMINISTRADOR
Administrador idiomas	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Node				
Artículo: Crear contenido nuevo	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Página básica: Crear contenido nuevo	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Artículo: Borrar cualquier contenido	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Página básica: Borrar cualquier contenido	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Artículo: Borrar contenido propio	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Página básica: Borrar contenido propio	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Artículo: Eliminar revisiones	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Para eliminar una revisión, también necesita permiso para editar el elemento de contenido.				
Página básica: Eliminar revisiones	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Para eliminar una revisión, también necesita permiso para editar el elemento de contenido.				
Artículo: Editar cualquier contenido	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Página básica: Editar cualquier contenido	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Artículo: Editar contenido propio	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Página básica: Editar contenido propio	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Artículo: Revertir revisiones	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Para revertir una revisión, también necesita permiso para editar el elemento de contenido.				

Agregamos contenido.

Abrimos la herramienta de configuración y seleccionamos editar menú.



Editamos el menú de Navegación principal.

Editar menú Navegación principal

Título *
Navegación principal

Resumen Administrativo
Enlaces de secciones del sitio

Idioma del menú Spanish

ENLACE DEL MENU

ACTIVADO OPERACIONES

+ Inicio Editar

Guardar

Noticias

Añadimos enlace Noticias del Menú y completamos los datos requeridos y guardamos.

Añadir enlace de menú

Título del enlace del menú *
Noticias

El texto que se usará en el menú para este enlace.

Enlace *
Noticias

• La ubicación a la que este enlace de menú apunta.
• Start typing the title of a piece of content to select it. You can also enter an internal path such as /node/add or an external URL such as http://example.com. Enter <front> to link to the front page. Enter <nolink> to display link text only. Enter <button> to display keyboard-accessible link text only.

Activado

Una bandera para si un enlace debe ser activado o ocultado en los menús.

Descripción

Mostrar cuando se pase el cursor por encima del enlace de menú.

Mostrar expandido

Si se selecciona y este enlace de menú tiene hijos, el menú siempre aparecerá expandido. Esta opción se puede anular para todo el árbol de menú al colocar un bloque de menú.

ENLACE PADRE
<Navegación principal>

La profundidad máxima de un enlace y todos sus hijos es fija. Es posible que algunos enlaces del menú no estén disponibles como padres si al seleccionarlos se excede este límite.

Peso
0

El peso del enlace entre los enlaces del mismo menú y a la misma profundidad. En el menú, los enlaces con un peso alto se desplazarán hacia abajo, y los enlaces con un peso bajo se posicionaran más cerca de la parte superior.

Guardar

Ahora se logra visualizar el nuevo enlace “Noticias” en nuestra página principal.

Página no encontrada | Portal seguridad — Mozilla Firefox

Administrador Atajos admin

Contenido Estructura Apariencia Ampliar Configuración Usuarios Informes Ayuda

Portal seguridad

Inicio Noticias

Inicio

Buscar

Herramientas

Noticias

Página no encontrada

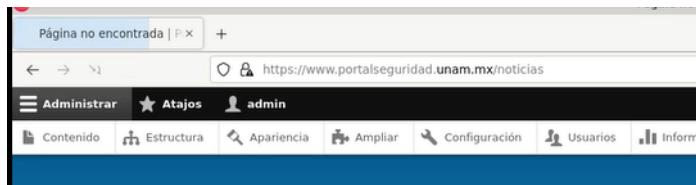
No se ha encontrado la página solicitada.

Contacto

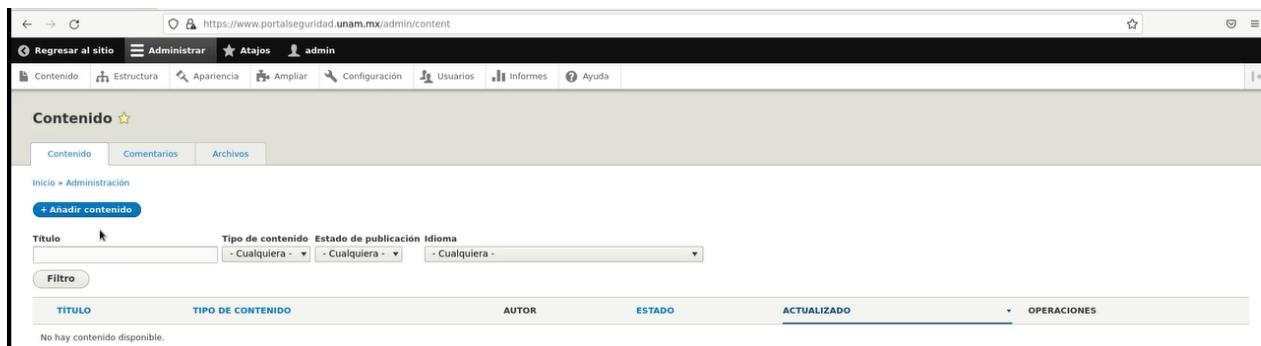
Funciona con Drupal

El enlace de noticias no muestra información por el momento, agregamos contenido al nuevo enlace con los siguientes pasos.

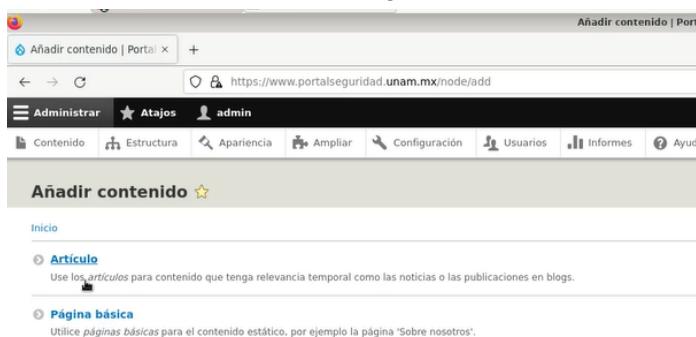
En la barra de herramientas de drupal elegimos la opción contenido.



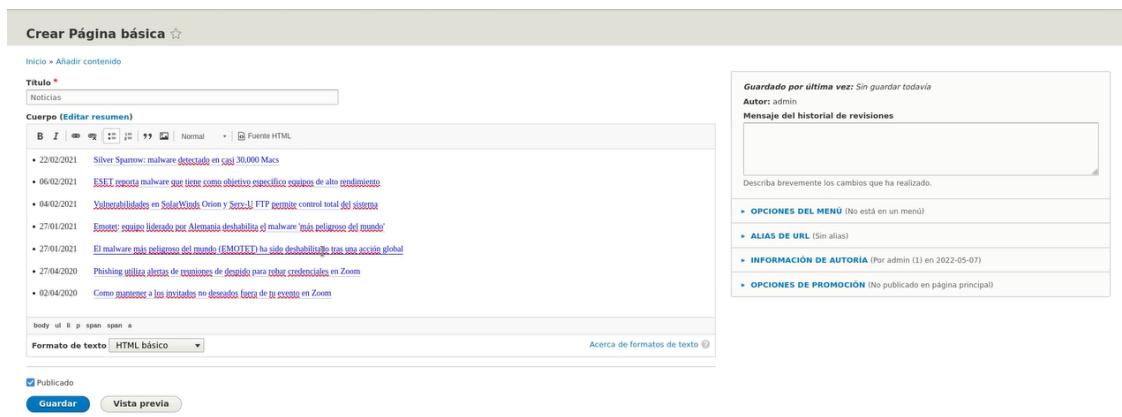
mostrará la siguiente página y añadimos contenido.



Seleccionamos crear una página básica.



Agregamos un título y contenido a la nueva página.



Drupal cuenta con la herramienta de vista previa de la nueva página.

The screenshot shows the Joomla administrator dashboard. In the top navigation bar, 'Administrador' is selected. Below it, there are tabs for 'Contenido', 'Estructura', 'Apariencia', 'Configuración', 'Usuarios', 'Informes', and 'Ayuda'. A breadcrumb trail indicates 'Volver a la edición del contenido' and 'Modo de vista: Completo'. The main content area is titled 'Portal seguridad' and has two tabs: 'Inicio' and 'Noticias'. On the left, there's a sidebar with 'Noticias' selected under 'Contenido', a search bar, and a 'Herramientas' section with a 'Nuevo' button. The right side displays a list of news items:

- 22/02/2021 Silver Sparrow: malware detectado en casi 30.000 Macs
- 06/02/2021 ESET reporta malware que tiene como objetivo específico equipos de alto rendimiento
- 04/02/2021 Vulnerabilidades en SolarWinds Orion y Serv-U FTP permite control total del sistema
- 27/01/2021 Emotet: equipo liderado por Alemania deshabilita el malware 'más peligroso del mundo'
- 27/01/2021 El malware más peligroso del mundo (EMOTET) ha sido deshabilitado tras una acción global
- 27/04/2020 Phishing utiliza alertas de reuniones de despidos para robar credenciales en Zoom
- 02/04/2020 Cómo mantener a los invitados no deseados fuera de tu evento en Zoom

Agregamos un alias de url para la nueva página de contenido noticias.Guardamos y visitamos la nueva sección de noticias.

This screenshot shows the Joomla editor for the 'Noticias' article. The title is 'Noticias'. The 'Body' tab is active, containing the article content and a list of news items. The 'Formato de texto' dropdown is set to 'HTML básico'. The 'Guardado por última vez' field shows 'Sin guardar todavía'. The 'Autor' field is 'admin'. The 'Mensaje del historial de revisiones' field is empty. The 'OPCIONES DEL MENÚ' section is expanded, showing 'Noticias' assigned to the 'Noticias' menu item. The 'ALIAS DE URL' field contains '/noticias'. The 'INFORMACIÓN DE AUTORÍA' and 'OPCIONES DE PROMOCIÓN' sections are also visible.

La vista de la nueva página de noticias se muestra de la siguiente manera para el usuario contenidos. note que existen las herramientas de editar, eliminar y revisión de contenido.

This screenshot shows the published news page at the URL https://www.portalseguridad.unam.mx/noticias. The page title is 'Noticias'. It features a search bar and a toolbar with 'Ver', 'Editar', 'Eliminar', and 'Revisões' buttons. The main content area lists the same news items as the administrator view:

- 22/02/2021 Silver Sparrow: malware detectado en casi 30.000 Macs
- 06/02/2021 ESET reporta malware que tiene como objetivo específico equipos de alto rendimiento
- 04/02/2021 Vulnerabilidades en SolarWinds Orion y Serv-U FTP permite control total del sistema
- 27/01/2021 Emotet: equipo liderado por Alemania deshabilita el malware 'más peligroso del mundo'
- 27/01/2021 El malware más peligroso del mundo (EMOTET) ha sido deshabilitado tras una acción global
- 27/04/2020 Phishing utiliza alertas de reuniones de despidos para robar credenciales en Zoom
- 02/04/2020 Cómo mantener a los invitados no deseados fuera de tu evento en Zoom

Boletín

Añadimos una nueva página de contenido llamada boletines.

The screenshot shows the 'Edit enlace de menú' (Edit menu link) page. The 'Título del enlace del menú' (Menu link title) field contains 'Boletines'. The 'Enlace' (Link) field contains '/boletines'. The 'Activado' (Enabled) checkbox is checked. The 'Descripción' (Description) field is empty. The 'Mostrar cuando se pase el cursor por encima del enlace de menú.' (Show when hovering over the menu link) checkbox is unchecked. The 'Mostrar expandido' (Show expanded) checkbox is unchecked. The 'Enlace padre' (Parent link) dropdown is set to 'Navegación principal'. The 'Peso' (Weight) input field has a value of 0. At the bottom are 'Guardar' (Save) and 'Eliminar' (Delete) buttons.

Editamos el enlace de menú, agregamos contenido a la pagina boletín y asignamos un alias de URL.

The screenshot shows the 'Editar Página básica Boletines' (Edit basic page Boletines) page. The 'Título' (Title) field contains 'Boletines'. The 'Cuadro' (Body) contains a large block of HTML code representing a list of security bulletins. On the right side, there is a sidebar with sections for 'Publicado' (Published), 'Opciones del menú' (Menu options), 'Alias de URL' (Alias), 'Información de autoría' (Author information), and 'Opciones de promoción' (Promotion options). The 'Publicado' section shows the page was last saved on 07/05/2022 at 19:55 by 'contenidos'. The 'Alias de URL' section shows the alias is '/boletines'.

La nueva sección de contenido boletín se muestra a continuación.

The screenshot shows the UNAM Security Portal homepage. At the top, there are navigation links for 'Administrador', 'Atajos', and 'admin'. Below this is a header with the UNAM logo, 'DGTC' (DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN), and 'Seguridad de la Información'. A search bar and a login link ('Mi cuenta') are also present. The main content area is titled 'Portal seguridad' and contains a 'Boletines' section. This section includes a search bar, a toolbar with 'Ver', 'Editar', 'Eliminar', and 'Revisores' buttons, and a list of recent bulletins:

- 04/04/2022 Boletín de Seguridad UNAM-CERT-2022-020 Actualizaciones de seguridad liberadas para productos VMware
- 30/03/2022 Boletín de Seguridad UNAM-CERT-2022-019 Actualizaciones de seguridad liberadas para Joomla
- 29/03/2022 Boletín de Seguridad UNAM-CERT-2022-018 Actualizaciones de seguridad liberadas para productos VMware
- 21/03/2022 Boletín de Seguridad UNAM-CERT-2022-017 Actualizaciones de seguridad liberadas para productos HP
- 16/03/2022 Boletín de Seguridad UNAM-CERT-2022-014 Actualizaciones de seguridad liberadas para Drupal (SA-CORE-2022-005)
- 16/03/2022 Boletín de Seguridad UNAM-CERT-2022-015 Actualizaciones de seguridad liberadas para BIND
- 11/03/2022 Boletín de Seguridad UNAM-CERT-2022-016 Actualizaciones de seguridad liberadas para WordPress

At the bottom left, a link to 'Noticias' is visible.

Creamos una nueva página para cada link de la sección de contenido boletín, bajo la dirección de “boletín/”, de la siguiente manera, empleando el el nombre del boletín como alias de la URL, por ejemplo:

`boletin_20_05_2022_boletin_de_seguridad_actualizaciones_de_vmware.`

The screenshot shows the UNAM CMS interface for creating a new page. The title is 'Boletín de Seguridad UNAM-CERT-2022-020 Actualizaciones de seguridad liberadas para productos vmware'. The content area contains the following text:

Título *
2022 020 actualizaciones de seguridad liberadas para productos vmware

Cuerpo (Editar resumen)

Criticó

Descripción

VMware libera actualizaciones de seguridad que corrigen una vulnerabilidad de ejecución de código remoto en Spring Framework (CVE-2022-22965) en algunos de sus productos.

Productos afectados

- VMware Tanzu Application Service for VMs
- VMware Tanzu Operations Manager
- VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

Solución

Aplicar el parche de acuerdo con el producto y versión que publique VMware (ver columna Fixed Version)

Nota: La Coordinación de Seguridad de la Información UNAM-CERT agradece el aporte en la elaboración o traducción y revisión de este Documento a:

- Alberto Valyavide Martínez (alberto.valyavide@cert.unam.mx)

The right side of the screen shows the 'Guardado por última vez' (Saved last time) section, which is empty. It also includes sections for 'OPCIONES DEL MENÚ' (Menu options), 'ALIAS DE URL' (Alias), 'INFORMACIÓN DE AUTORÍA' (Author information), and 'OPCIONES DE PROMOCIÓN' (Promotion options).

Logramos de esta manera visualizar los nuevos boletines creados.

The screenshot shows a web browser window with the URL <https://www.portalseguridad.unam.mx/boletin/2022-020-actualizaciones-de-seguridad-liberadas-para-productos-vmware>. The page title is "Boletín de Seguridad UNAM". The header includes the UNAM logo and the text "DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN". The main content area is titled "Portal seguridad" and shows a green success message: "Página básica 2022 020 actualizaciones de seguridad liberadas para productos vmware se ha creado." Navigation links include "Inicio", "Noticias", and "Boletines".

The screenshot shows a news item titled "2022 020 actualizaciones de seguridad liberadas para productos vmware". The item has a "Ver" button, a date of "04/04/2022", and a link to "https://www.vmware.com/security/advisories/MSA-2022-0010.html". It also includes fields for "Fecha liberación", "Fuente", "Riesgo", and "Descripción". A sidebar on the left shows a search bar and a "Herramientas" section with a "Añadir contenido" button.

Vulnerabilidades

Añadimos nuevo contenido para la sección vulnerabilidades, agregando el enlace de menú y los datos solicitados.

The screenshot shows the "Añadir enlace de menú" (Add menu link) form. The title is "Vulnerabilidades". The "Enlace" field contains the URL "/vulnerabilidades". The "Activado" checkbox is checked. The "Descripción" field is empty. The "Peso" field is set to 0. The "Guardar" button is visible at the bottom.

Creamos la página que aloja el contenido de la sección del sitio llamada vulnerabilidades.

Título *
Vulnerabilidades

Cuerpo (Editar resumen)

Vulnerabilidades

Fecha	Título
24/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-009 Desbordamiento de búfer en productos SonicWall
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-008 Envenenamiento de caché en BIND
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-007 Fallo en la verificación de zonas secundarias de DNSSEC
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-006 Fallo en el componente DNSSEC de BIND
25/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-005 Escalación de privilegios local en la utilidad pexec de polkit
11/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-003 Ejecución remota de código en Microsoft Exchange
11/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-004 Ejecución remota de código en HTTP Protocol Stack
07/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-002 XSS reflejado en servidor TFTP
04/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-001 Vulnerabilidad heap-overflow en productos VMware Workstation, Fusion y ESXi
10/12/2021	Vulnerabilidad de Seguridad UNAM-CERT-2021-001 Ejecución remota de código en Apache Log4j

Formato de texto: HTML, básico

Guardado por última vez: Sin guardar todavía
Autor: admin
Mensaje del historial de revisiones

Describa brevemente los cambios que ha realizado.

OPCIONES DEL MENÚ (No está en un menú)
ALIAS DE URL (Sin alias)
INFORMACIÓN DE AUTORÍA (Por admin (1) en 2022-05-07)
OPCIONES DE PROMOCIÓN (No publicado en página principal)

Agregamos su alias de URL.

Título *
Vulnerabilidades

Cuerpo (Editar resumen)

Vulnerabilidades

Fecha	Título
24/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-009 Desbordamiento de búfer en productos SonicWall
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-008 Envenenamiento de caché en BIND
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-007 Fallo en la verificación de zonas secundarias de DNSSEC
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-006 Fallo en el componente DNSSEC de BIND
25/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-005 Escalación de privilegios local en la utilidad pexec de polkit
11/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-003 Ejecución remota de código en Microsoft Exchange
11/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-004 Ejecución remota de código en HTTP Protocol Stack
07/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-002 XSS reflejado en servidor TFTP
04/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-001 Vulnerabilidad heap-overflow en productos VMware Workstation, Fusion y ESXi
10/12/2021	Vulnerabilidad de Seguridad UNAM-CERT-2021-001 Ejecución remota de código en Apache Log4j

Formato de texto: HTML, básico

Guardado por última vez: Sin guardar todavía
Autor: admin
Mensaje del historial de revisiones

Describa brevemente los cambios que ha realizado.

OPCIONES DEL MENÚ (No está en un menú)
ALIAS DE URL (Alias: /vulnerabilidades)
Alias de URL: /vulnerabilidades
Especifique una ruta alternativa por la que se pueda acceder a estos datos. Por ejemplo, escriba "í sobre" al escribir una página acerca de.

INFORMACIÓN DE AUTORÍA (Por admin (1) en 2022-05-07)
OPCIONES DE PROMOCIÓN (No publicado en página principal)

La nueva sección vulnerabilidades se muestra de la siguiente manera.

Vulnerabilidades | Portal seguridad — Mozilla Firefox

Vulnerabilidades | Portal seguridad | UNAM

Administrador | Atajos | admin

Contenido | Estructura | Apariencia | Ampliar | Configuración | Usuarios | Informes | Ayuda

UNAM DIRECCIÓN CENTRAL DE COMPUTO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN CERT la información

Portal seguridad

Inicio | Noticias | Boletines | Vulnerabilidades

Página básica Vulnerabilidades se ha creado.

Inicio

Buscar

Vulnerabilidades

Herramientas

Ver | Editar | Eliminar | Revisiones

Fecha	Título
24/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-009 Desbordamiento de búfer en productos SonicWall
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-008 Envenenamiento de caché en BIND
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-007 Fallo en la verificación de zonas secundarias de DNSSEC
16/03/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-006 Fallo en el componente DNSSEC de BIND
25/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-005 Escalación de privilegios local en la utilidad pexec de polkit
11/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-003 Ejecución remota de código en Microsoft Exchange
11/01/2022	Vulnerabilidad de Seguridad UNAM-CERT-2022-004 Ejecución remota de código en HTTP Protocol Stack

El sitio permite mejoras visuales para nuestra página principal.

Página inicio (Contenido) x Vulnerabilidades | UNAM x +

https://www.portalseguridad.unam.mx/admin/structure/views/view/frontpage/edit/page_1?destination=/node

Regresar al sitio Administrar Atajos admin

Contenido Estructura Apariencia Ampliar Configuración Usuarios Informes Ayuda

Página inicio (Contenido)

Inicio > Administración > Estructura > Vistas > Frontpage > Edit

Presentaciones

Página Canal de noticias Agregar

Nombre a mostrar: Página

Editar el nombre/descripción de la vista Vista Página

TÍTULO
Título: Ninguno

FORMATO
Formato: Lista sin formato | Configuración
Mostrar: Contenido | Resumen

CAMPOS
El estilo o formato de fila seleccionado no utiliza campos.

CRITERIOS DE FILTRADO
Contenido: Promocionado a la página principal (= Si)
Contenido: Publicado (= Sí)
Contenido: Translation language (= Idioma Contenido seleccionado para la página)

CRITERIO DE ORDENACIÓN
Contenido: Fijo al comienzo de las listas (desc)
Contenido: Fecha (desc)

Opciones de página
Ruta: /node
Menú: Sin menú
Acceso: Permitido | Ver contenido publicado

Encabezado

Pie de página

Comportamiento si no hay resultados
Global: Texto sin filtrar (Global: Texto sin filtrar)
Contenido: Comportamiento del Nodo Vacío de la página frontal (Contenido:
Comportamiento del Nodo Vacío de la página frontal)
Global: Sobrescribir el título (Global: Sobrescribir el título)

Paginador
Usar paginador: Completo | Paginado, 10 elementos
Enlace 'más...': No

AVANZADO

Guardar Cancelar

Agregamos un mensaje de bienvenida a los usuarios que visitan nuestro sitio.

The screenshot shows a web-based content management system for UNAM-CERT. The URL is https://www.portalseguridad.unam.mx/admin/structure/views/viewfrontpage/edit/page_1?destination=node. The interface includes a top navigation bar with links like Inicio | UNAM-CERT, Administrar, Ajustes, and Admin. Below this is a secondary navigation bar with Contento, Estructura, Apariencia, Ampliar, Configuración, Usuarios, Informes, Ayuda, and Campos. A sidebar on the left lists various content types and their counts. The main content area is titled 'Configurar Comportamiento si no hay resultados: Global: Texto sin filtrar'. It contains sections for 'Para' (set to 'Todas las presentaciones'), 'Provide markup for the area with minimal filtering.', and 'Utilice tokens de reemplazo de la primera fila'. Below this is a section titled 'REEMPLAZOS GLOBALES DE TOKEN DISPONIBLES' with a 'Contenido' field containing the text 'Hoy es: **viernes**, 7 de mayo de 2022'. Another section below it contains the text 'Buscamos mejorar la seguridad de la información en RedINAM e Internet al responder a incidentes, analizar amenazas e intercambiar información de ciberseguridad con otros equipos de respuesta'. At the bottom, there are buttons for 'Aplicar (todas las presentaciones)', 'Cancelar', and 'Eliminar'.

Agregamos una imagen a la página de inicio.

The screenshot shows a web-based content management interface for UNAM-CERT. The top navigation bar includes links for 'Crear Página básica | Por x', 'Inicio | UNAM-CERT', and a search bar. The main menu has sections like 'Administrador', 'Atajos', 'admin', 'Contenido', 'Estructura', 'Apariencia', 'Ampliar', 'Configuración', 'Usuarios', 'Informes', and 'Ayuda'. A sub-menu for 'Crear Página básica' is open. The main content area is titled 'Crear Página básica' and shows a preview of the page with the title 'OUCH MARZO'. The page content includes a banner image for 'OUCH! Marzo 2022' from SANS Security Awareness, a sub-headline 'Aprende una nueva habilidad de supervivencia: Detectando deepfakes', and some text in the body. On the right side, there's a sidebar with revision history, options for saving, and a link to the URL.

WAF

Implementación de un WAF

Instalación de módulo security, a continuación se muestra el comando y la ejecución del mismo.

```
Terminal - root@debian:~#
File Edit View Terminal Tabs Help
root@debian:~# apt install libxml2 libapache2-mod-security2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libxml2 is already the newest version (2.9.10+dfsg-6.7+deb11u1).
libxml2 set to manually installed.
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 liblLua5.1-0 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] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 liblLua5.1-0 amd64 5.1.5-8
.1+b3 [109 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 libapache2-mod-security2
amd64 2.9.3-3+deb11u1 [259 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 modsecurity-crs all 3.3.0
-1+deb11u1 [158 kB]
Fetched 526 kB in 1s (1,032 kB/s)
```

Habilitamos el módulo security2.

```
root@debian:~# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
root@debian:~#
```

Copiamos el archivo /etc/modsecurity/modsecurity-recommended.conf a /etc/modsecurity/modsecurity.conf

```
root@debian:~# cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity
/modsecurity.conf
root@debian:~#
```

Editamos el archivo /etc/modsecurity/modsecurity.conf, agregando las directivas SecDebugLog /var/log/apache2/debug.log y SecLogLevel 3.

```
GNU nano 5.4          /etc/modsecurity/modsecurity.conf *

# -- Debug log configuration -----
# The default debug log configuration is to duplicate the error, warning
# and notice messages from the error log.
#
SecDebugLog /var/log/apache2/debug.log
SecDebugLogLevel 3

# -- Audit log configuration -----
# Log the transactions that are marked by a rule, as well as those that
# trigger a server error (determined by a 5xx or 4xx, excluding 404,
# level response status codes).
#
SecAuditEngine RelevantOnly
SecAuditLogRelevantStatus "^(?:5|4(?:04))"

^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
```

guardamos y reiniciamos el servicio de apache.

```
root@debian:~# nano /etc/modsecurity/modsecurity.conf
root@debian:~# systemctl restart apache2
```

listamos con un ls -la la carpeta /var/log/apache2/ y observamos que se han generado los archivos debug.log u modsec_audit.log.

```
Terminal -
File Edit View Terminal Tabs Help
Processing triggers for libc-bin (2.31-13+deb11u3) ...
root@debian:~# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
root@debian:~# cp /etc/mod
modprobe.d/    modules      modules-load.d/
root@debian:~# cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity
/modsecurity.conf
root@debian:~# nano /etc/modsecurity/modsecurity.conf
root@debian:~# nano /etc/modsecurity/modsecurity.conf
root@debian:~# systemctl restart apache2
root@debian:~# ls -la /var/log/apache2/
total 488
drwxr-x---  2 root adm  4096 May  7 20:57 .
drwxr-xr-x 12 root root  4096 May  7 18:49 ..
-rw-r-----  1 root adm   1794 May  7 20:08 access.log
-rw-r-----  1 root root     0 May  7 20:57 debug.log
-rw-r-----  1 root adm   4793 May  7 20:57 error.log
-rw-r-----  1 root root     0 May  7 20:57 modsec_audit.log
-rw-r-----  1 root adm     0 May  7 18:47 other_vhosts_access.log
-rw-r--r--  1 root root 469681 May  7 20:51 proyecto_access.log
-rw-r--r--  1 root root   3090 May  7 20:57 proyecto_error.log
root@debian:~#
```

cambiamos de propietario a los anteriores archivos mencionados.

```
root@debian:~# chown :adm /var/log/apache2/debug.log
root@debian:~# chown :adm /var/log/apache2/modsec_audit.log
root@debian:~# ls -la /var/log/apache2/
total 488
drwxr-x--- 2 root adm 4096 May 7 20:57 .
drwxr-xr-x 12 root root 4096 May 7 18:49 ..
-rw-r---- 1 root adm 1794 May 7 20:08 access.log
-rw-r---- 1 root adm 0 May 7 20:57 debug.log
-rw-r---- 1 root adm 4793 May 7 20:57 error.log
-rw-r---- 1 root adm 0 May 7 20:57 modsec_audit.log
-rw-r---- 1 root adm 0 May 7 18:47 other_vhosts_access.log
-rw-r--r-- 1 root root 469681 May 7 20:51 proyecto_access.log
-rw-r--r-- 1 root root 3090 May 7 20:57 proyecto_error.log
root@debian:~#
```

Pruebas del WAF

Cuando activamos el módulo sin agregarlos al <Directory> del archivo de configuración solo nos marcará los errores de autenticación por injection en el debug.log pero no dará ningún otro aviso.

```
<Directory /var/www/proyecto/>
    SecRuleEngine On
    Options FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
```

Al agregarlo la configuración cambia del lado del navegador, en primer lugar tu como administrador o content user no te dejará subir imágenes directamente y cualquier autenticación por intento de injection se regirá automáticamente a un forbidden por parte del WAF.



Forbidden

You don't have permission to access this resource.

Cabe mencionar que Drupal ya tiene consigo métodos de seguridad contra injection sql, pero también se ha encontrado algunas fallas pero constan de script más avanzados en subida de archivos que WAF puede ayudar a detectar o no permitir el paso.

sitio www.portalseguridad.unam.mx