

UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN
CICLO I - 2023



CÁTEDRA:

Seguridad Informática

TEMA:

ModSecurity

DOCENTE:

Lic.Eduardo Chachagua

ESTUDIANTES:

Marilyn Stephanie Salinas Torres

Edwin Alexander Bautista López

José Alexander Soriano Parada

Javier Antonio Cerna Cornejo

CARNET:

ST01136888

BL01137083

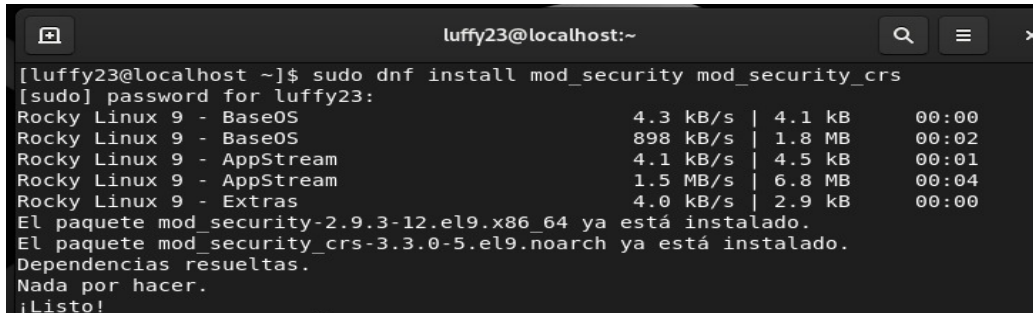
SP01137048

CC01136887

Instalación de Mod Security

Se instalará ModSecurity y los paquetes necesarios con el siguiente comando:

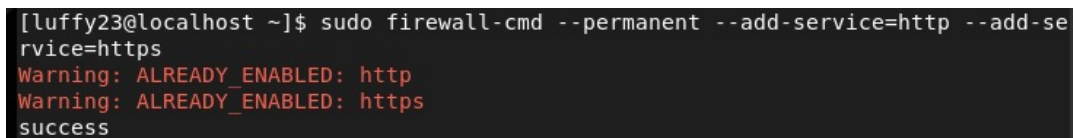
```
sudo dnf install mod_security mod_security_crs
```



```
luffy23@localhost:~  
[luffy23@localhost ~]$ sudo dnf install mod_security mod_security_crs  
[sudo] password for luffy23:  
Rocky Linux 9 - BaseOS          4.3 kB/s | 4.1 kB      00:00  
Rocky Linux 9 - BaseOS          898 kB/s | 1.8 MB      00:02  
Rocky Linux 9 - AppStream       4.1 kB/s | 4.5 kB      00:01  
Rocky Linux 9 - AppStream       1.5 MB/s | 6.8 MB      00:04  
Rocky Linux 9 - Extras          4.0 kB/s | 2.9 kB      00:00  
El paquete mod_security-2.9.3-12.el9.x86_64 ya está instalado.  
El paquete mod_security_crs-3.3.0-5.el9.noarch ya está instalado.  
Dependencias resueltas.  
Nada por hacer.  
¡Listo!
```

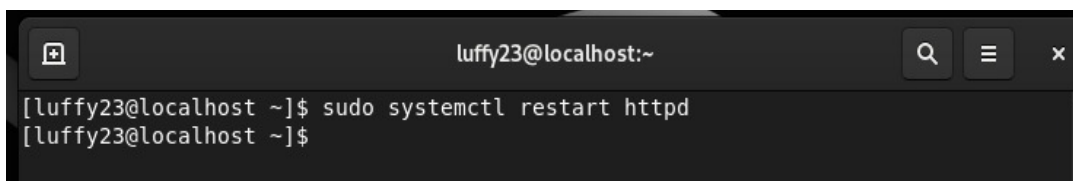
Habilitar el mod_security en Apache y abrir los puertos HTTP Y HTTPS en el firewall con el siguiente comando:

```
sudo firewall-cmd --permanent --add-service=http --add-service=https
```



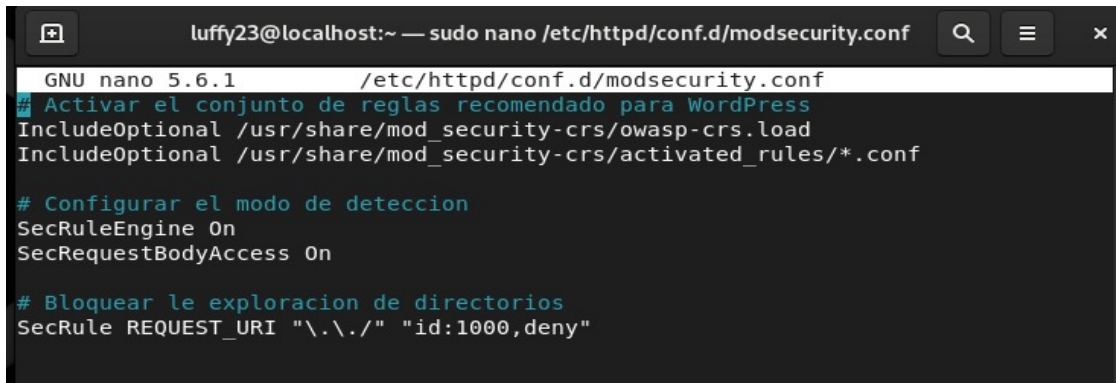
```
luffy23@localhost ~]$ sudo firewall-cmd --permanent --add-service=http --add-service=https  
Warning: ALREADY_ENABLED: http  
Warning: ALREADY_ENABLED: https  
success
```

Reiniciar el servidor Apache para aplicar los cambios.



```
luffy23@localhost:~  
[luffy23@localhost ~]$ sudo systemctl restart httpd  
[luffy23@localhost ~]$
```

Se editará el directorio `/etc/httpd/conf.d/` para configurar ModSecurity para que funcione con WordPress. Para ello se pegara todo el siguiente contenido.

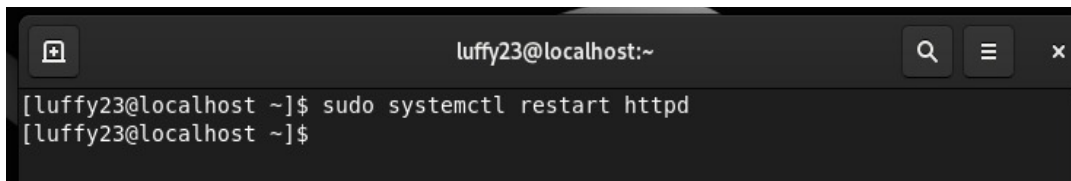


```
GNU nano 5.6.1 /etc/httpd/conf.d/modsecurity.conf
# Activar el conjunto de reglas recomendado para WordPress
IncludeOptional /usr/share/mod_security-crs/owasp-crs.load
IncludeOptional /usr/share/mod_security-crs/activated_rules/*.conf

# Configurar el modo de deteccion
SecRuleEngine On
SecRequestBodyAccess On

# Bloquear la exploracion de directorios
SecRule REQUEST_URI "\.\/" "id:1000,deny"
```

Reiniciamos nuevamente el servidor Apache para aplicar los cambios.



```
luffy23@localhost:~
[luffy23@localhost ~]$ sudo systemctl restart httpd
[luffy23@localhost ~]$
```

Acceso al FQDN del sitio

Se editará este archivo de configuración de Apache para el sitio WordPress con el siguiente comando.

```
Sudo nano /etc/httpd/conf.d/wordpress.conf
```

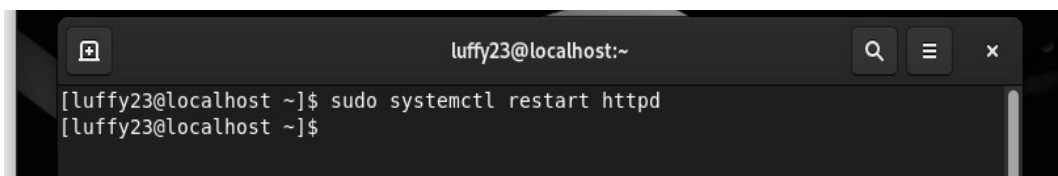
```
sudo nano /etc/httpd/conf.d/wordpress.conf
```

Se le agregara la sección 'ServerName' en la cual se colocara el FQDN de nuestro sitio de WordPress.

```
<VirtualHost *:80>
  ServerName example.com
  ServerAlias www.example.com
  DocumentRoot /var/www/html/wordpress
  # Resto de la configuración
</VirtualHost>
```

Reiniciar el servidor Apache para aplicar los cambios con el siguiente comando.

```
Sudo systemctl restart httpd
```



```
luffy23@localhost:~
[luffy23@localhost ~]$ sudo systemctl restart httpd
[luffy23@localhost ~]$
```

Accederemos al navegador con localhost/wordpress/wp-admin/



Luego nos vamos al apartado de ajustes para poder ingresar la respectiva información que se requiere.

Ajustes generales

Warning: Ha ocurrido un error inesperado. Puede que algo vaya mal con WordPress.org o la configuración de tu sitio no ha podido establecer una conexión segura con WordPress.org. Por favor, contacta con el administrador de tu sitio.

Título del sitio

Descripción corta
En pocas palabras, explica de qué va este sitio.

Dirección de WordPress (URL)

Dirección del sitio (URL)

Dirección de correo electrónico de administración
Esta dirección se usa para propósitos administrativos. Si la cambias, se activará hasta que la confirmes.

Miembros Cualquiera puede registrarse

Perfil por defecto para los nuevos usuarios

Idioma del sitio

Warning: Ha ocurrido un error inesperado. Puede que algo vaya mal con WordPress.org o la configuración de tu sitio no ha podido establecer una conexión segura con WordPress.org. Por favor, prueba en los [foros de soporte](#). (WordPress no ha podido establecer una conexión segura con el servidor). in `/var/www/wordpress/wp-admin/includes/transla`

Por último ingresamos en el navegador con `http://localhost/wordpress/` y podremos ver nuestro sitio web WordPress.

Prueba de Wordpress Página de entrada

¡Integrantes!

Marilyn Stephanie Salinas Torres Edwin Alexander Bautista López José Alexander Soriano Parada Javier Antonio Cerna Cornejo

Acceso de Ips

Editaremos el siguiente el siguiente archivo para poder dar permiso a ciertas IPs y para bloquear las IPs que no deseemos que tengan acceso:

```
sudo gedit /etc/httpd/modsecurity.d/modsecurity.conf
```

Para darle permiso de acceso se digitara la siguiente línea con las IPs:

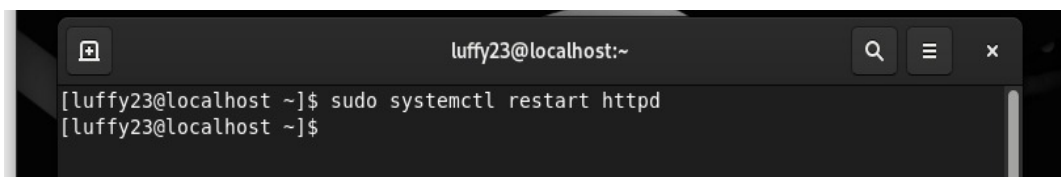
```
SecRule REMOTE_ADDR "@ipMatch x.x.x.x/xx,x.x.x.x/xx" "phase:1,id:100,allow"
```

Para denegar acceso se digitara la siguiente línea con las IPs:

```
SecRule REMOTE_ADDR "@ipMatch x.x.x.x/xx,x.x.x.x/xx" "phase:1,id:101,deny,status:403"
```

Después se guarda la configuración y se reinicia el servidor Apache para aplicar cambios.

```
Sudo systemctl restart httpd
```



Configuración del certificado SSL al FQDN

Primero vamos a instalar OpenSSL con:

```
sudo dnf install openssl
```

```
alex@localhost:~$ sudo dnf install openssl
sudo] password for alex:
ltima comprobación de caducidad de metadatos hecha hace 1:14:05, el vie 12 may 2023 09:59:05.
l paquete openssl-1:3.0.1-47.el9_1.x86_64 ya está instalado.
ependencias resueltas.
ada por hacer.
Listo!
```

Vamos a generar una clave privada y un certificado para el dominio 'localhost'

```
alex@localhost ~]$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/pki/tls/private/localhost.key -out /etc/pki/tls/certs/localhost.crt -subj "/C=US/ST=State/L=City/O=Organization/OU=Department/CN=localhost"
```

Configurar el Apache para utilizar el certificado SSL con el siguiente contenido

```
sudo nano /etc/httpd/conf/httpd.conf
```

```
GNU nano 5.6.1 /etc/httpd/conf/httpd.conf
<VirtualHost *:80>
  ServerName localhost
  DocumentRoot /var/www/html

  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

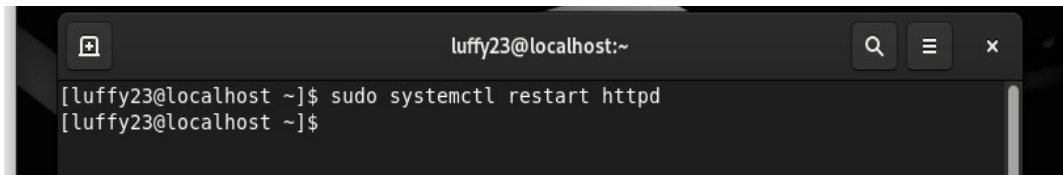
  <Directory "/var/www/html">
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
  </Directory>
</VirtualHost>
<VirtualHost *:443>
  ServerName localhost
  DocumentRoot /var/www/html

  SSLEngine on
  SSLCertificateFile /etc/pki/tls/certs/localhost.crt
  SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

  <Directory "/var/www/html">
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
  </Directory>
</VirtualHost>
^G Ayuda          ^O Guardar      ^W Buscar      ^X Cortar      ^T Ejecutar    ^G Ubicación   M-U Deshacer  M-A Poner marca M-J A llave
^H Salir          ^R Leer fich.  ^M Reemplazar  ^U Pegar       ^D Justificar  ^_ Ir a línea   M-E Rehacer    M-G Copiar     ^Q Buscar atrás
```

Reiniciamos nuevamente el servidor para aplicar los cambios.

Sudo systemctl restart httpd

A terminal window with a dark background. The title bar shows 'luffy23@localhost:~'. The terminal content shows the command '[luffy23@localhost ~]\$ sudo systemctl restart httpd' being entered and executed, followed by the prompt '[luffy23@localhost ~]\$'.

NOTA: Para la creación del segundo sitio de Wordpress lo único que se necesita hacer es volver a instalar Wordpress y crear una nueva base de datos para el nuevo sitio.