



Dirección General de Cómputo y de
Tecnologías de Información y Comunicación

UNAM-CERT
Plan de Becarios en Seguridad Informática



Seguridad en aplicaciones web

Mini Proyecto

“Portal de vulnerabilidades”

Pedro Bautista Garcia
Sofía Colín López
Ivan Daniel Galindo
Erick Gómez

Profesora Angie Aguilar

09/05/2022

Contenido

Introducción	3
Desarrollo	4
Instalación de apache2	4
HTTPS	4
Instalación de Drupal	7
Creación de usuarios	8
WAF	15

Introducción

En el presente proyecto se desarrollará un sitio web con PHP, Apache y PostgreSQL en el sistema operativo Debian. Adicionalmente, se implementará el sistema de gestión de contenidos Drupal y el firewall de aplicaciones Web de Apache ModSecurity.

Se expondrá todo el procedimiento y las configuraciones realizadas.

El principal objetivo de este proyecto es implementar prácticas de seguridad en el sitio web, como el uso de certificados autofirmados que permitan establecer una conexión segura mediante el protocolo HTTPS, la implementación de un firewall que permita monitorear y bloquear el tráfico malicioso, el uso de directivas que permitan limitar la información del servidor a los usuarios, entre otras.

Los conocimientos adquiridos durante el Plan de Becarios en Seguridad Informática nos han permitido poder hacer una implementación más real, por lo que se realizarán las configuraciones necesarias para poder realizar el proyecto en un ambiente productivo.

Sitio: <https://www.proyectopbsi.cf/>

Desarrollo

Instalación de apache2

1. Para instalar apache es necesario ejecutar el siguiente comando.

```
sudo apt install apache2
```

```
admin@ip-172-31-14-213:~$ sudo apt install apache2
Reading package lists... Done
```

2. Después en el archivo de configuración /etc/apache2/apache2.conf tenemos que agregar las siguientes líneas para evitar que se muestran datos del servidor web.

```
ServerTokens ProductOnly
ServerSignature off
```

HTTPS

1. Para configurar HTTPS es necesario crear el certificado y la llave privada, ambos emitidos por Let's Encrypt, para ello usaremos la herramienta de cerbot y ejecutaremos los siguientes comandos.

```
sudo snap install --classic certbot
sudo ln -s /snap/bin/certbot /usr/bin/certbot
sudo snap set certbot trust-plugin-with-root=ok
sudo certbot certonly --apache
```

```
admin@ip-172-31-14-213:~$ sudo snap install --classic certbot
certbot 1.27.0 from Certbot Project (certbot-eff@) installed
admin@ip-172-31-14-213:~$ sudo ln -s /snap/bin/certbot /usr/bin/certbot
admin@ip-172-31-14-213:~$ sudo snap set certbot trust-plugin-with-root=ok
admin@ip-172-31-14-213:~$ sudo certbot certonly --apache
```

2. Se debe editar el archivo /etc/apache2/sites-available/ssl.conf agregando las siguientes líneas.

```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        ServerName www.proyectopbsi.cf

        DocumentRoot /var/www/proyecto/drupal
        LogLevel warn
```

```

        ErrorLog ${APACHE_LOG_DIR}/proyectopbsi_error.log
        CustomLog ${APACHE_LOG_DIR}/proyectopbsi_access.log combined
        SSLEngine on
        SSLCertificateFile
/etc/letsencrypt/live/www.proyectopbsi.cf/fullchain.pem
        SSLCertificateKeyFile
/etc/letsencrypt/live/www.proyectopbsi.cf/privkey.pem
        <FilesMatch "\.(cgi|shtml|phtml|php)$">
            SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
            SSLOptions +StdEnvVars
        </Directory>

        ErrorDocument 400 /error/error.html
        ErrorDocument 401 /error/error.html
        ErrorDocument 402 /error/error.html
        ErrorDocument 403 /error/error.html
        ErrorDocument 404 /error/error.html
        ErrorDocument 500 /error/error.html
        ErrorDocument 502 /error/error.html
        ErrorDocument 503 /error/error.html
        ErrorDocument 504 /error/error.html
    </VirtualHost>
</IfModule>

<VirtualHost *:80>
    ServerName www.proyectopbsi.cf
    Redirect / https://www.proyectopbsi.cf
</VirtualHost>

```

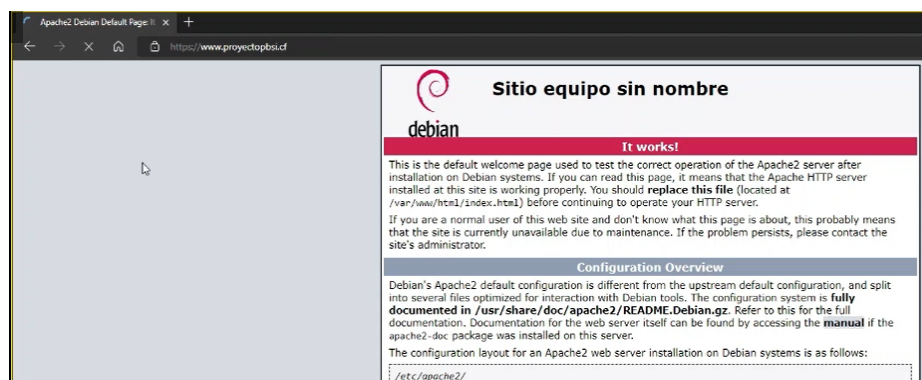
```
ServerName www.proyectopbsi.cf
```

```
SSLCertificateFile /etc/letsencrypt/live/www.proyectopbsi.cf/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/www.proyectopbsi.cf/privkey.pem
```

```
<VirtualHost *:80>
    ServerName www.proyectopbsi.cf
    Redirect / https://www.proyectopbsi.cf
</VirtualHost>
```

```
ErrorDocument 400 /error/error.html
ErrorDocument 401 /error/error.html
ErrorDocument 402 /error/error.html
ErrorDocument 403 /error/error.html
ErrorDocument 404 /error/error.html
ErrorDocument 500 /error/error.html
ErrorDocument 502 /error/error.html
ErrorDocument 503 /error/error.html
ErrorDocument 504 /error/error.html
```

3. Así es como se ve el sitio con apache instalado y agregando la configuración de HTTPS.



Instalación de Drupal

Primero se instalarán Postgres, Apache y PHP. Se obtendrá la versión de PHP para instalar ciertos módulos necesarios que requiere Drupal. Se habilitarán los módulos “rewrite” y “ssl”, se reiniciará el servicio de Apache

```
sudo apt install postgresql apache2 php
php --version
sudo apt install libapache2-mod-php7.4 php7.4-gd php7.4-xml php7.4-pgsql
sudo a2enmod rewrite ssl
sudo systemctl restart apache2
```

Posteriormente, se descargará el último drupal disponible, se descomprime el archivo y se moverá a la carpeta indicada como “DocumentRoot”. Se cambiarán los permisos y el dueño para que no existan problemas y se editará el .conf del sitio disponible de Apache. Se probará la configuración y, si no hay problemas, volveremos a cargar el servicio de Apache.

```
sudo wget https://www.drupal.org/download-latest/tar.gz -O drupal.tar.gz
sudo tar -xvf drupal.tar.gz
sudo mkdir /var/www/proyecto/
sudo mv drupal-9.3.12 /var/www/proyecto/drupal
ls -l /var/www/proyecto/drupal
sudo chown -R www-data:www-data /var/www/proyecto/drupal/
sudo chmod -R 755 /var/www/proyecto/drupal/
sudo nano /etc/apache2/sites-available/ssl.conf
sudo a2ensite ssl
sudo a2dissite 000-default
apachectl configtest
sudo systemctl reload apache2
```

Una vez terminado este proceso, se instalará un módulo adicional que, de no hacerlo ahora, Drupal lo pedirá posteriormente. Se habilitará y reiniciará el sistema.

```
sudo apt install php-mbstring
sudo phpenmod -s apache2 mbstring
sudo systemctl reload apache2
```

Ahora, se cambiará al usuario postgres, se creará el usuario “drupal” y una base de datos también llamada “drupal” con la intención de ser utilizada posteriormente por Drupal.

```

su - postgres
psql
    CREATE USER drupal WITH password 'XXXXXXXXXXXXXXXXXXXX';
    CREATE DATABASE drupal OWNER drupal;
    GRANT ALL privileges ON DATABASE drupal TO drupal;
exit
psql -h localhost drupal drupal
    ALTER DATABASE "drupal" SET bytea_output = 'escape';

```

Ahora ya podemos ingresar desde el navegador a www.proyectopbsi.cf donde se seguirán las instrucciones del asistente para configurar, se termina cambiando None por All en apache2.conf como se muestra a continuación y se reiniciará el servicio.

```

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

sudo systemctl reload apache2

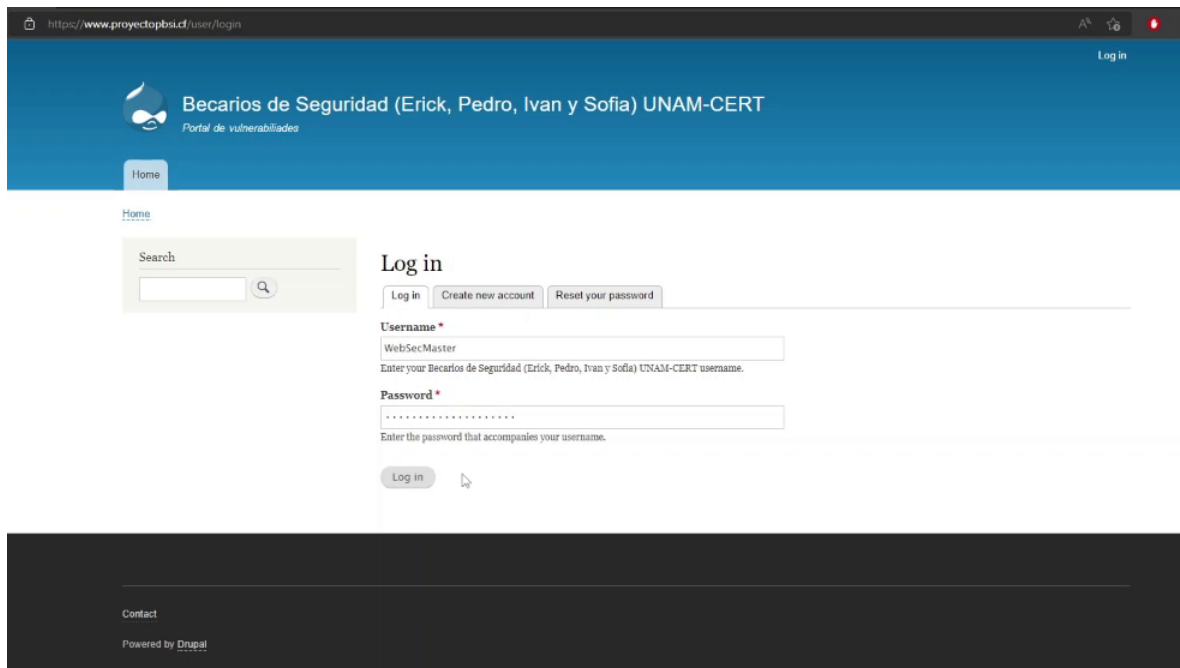
```

Portal web principal

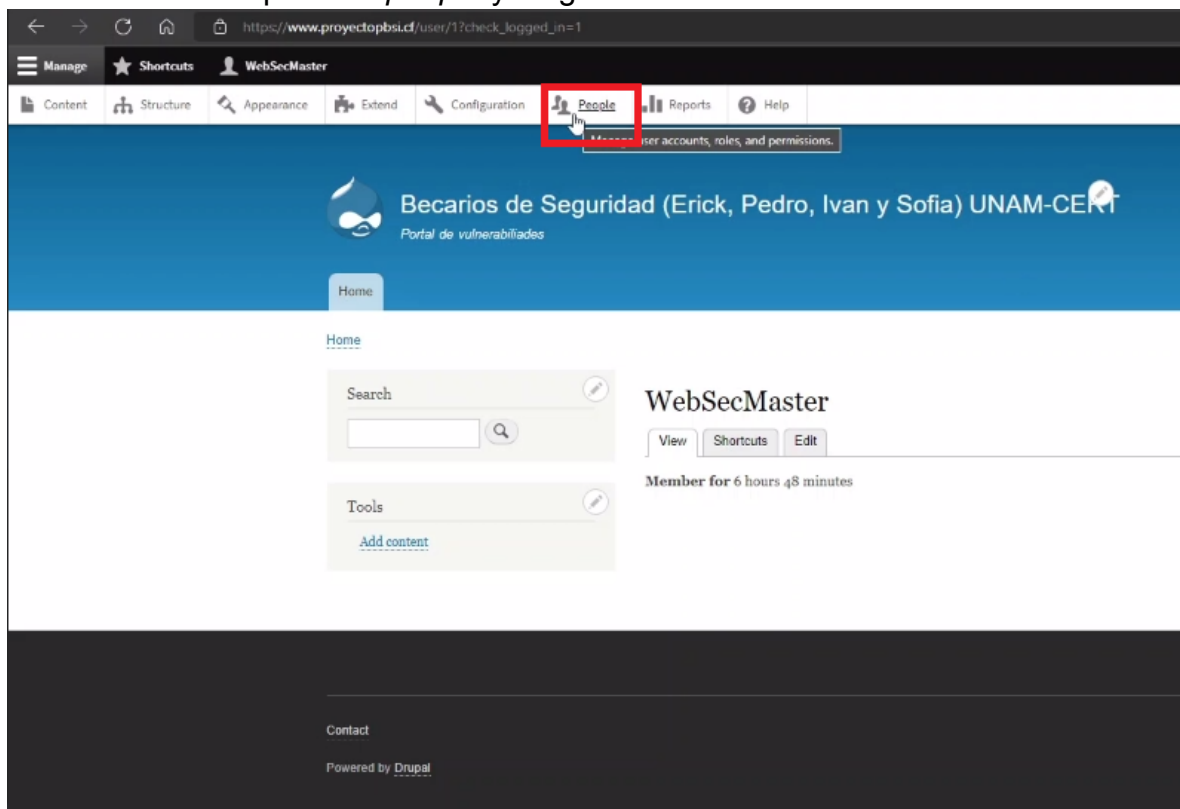


Creación de usuarios

Primero ingresamos al portal como usuario administrador:



Damos click en la pestaña *people* y luego en *Add user*



Back to site Manage Shortcuts WebSecMaster

Content Structure Appearance Extend Configuration People Reports Help

People

List Permissions Roles Role settings

Home » Administration

+ Add user

Name or email contains Status Role Permission

Filter

Action
Add the Administrator role to the selected user(s)

Apply to selected items

<input type="checkbox"/>	USERNAME	STATUS	ROLES	MEMBER FOR
<input type="checkbox"/>	sofia	Active	• Content editor	2 hours 33 minutes
<input type="checkbox"/>	WebSecMaster	Active	• Administrator	12 hours 16 minutes

Apply to selected items

Rellenamos los campos requeridos y damos click en *Create new account*

Back to site Manage Shortcuts WebSecMaster

Content Structure Appearance Extend Configuration People Reports Help

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

Username*

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

Password*

Password strength: Strong

Confirm password*

Passwords match: yes

Recommendations to make your password stronger:

- Add uppercase letters

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

[Choose File](#) 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 privileged users such as site administrators are still able to contact you even if you choose to disable this feature.

LOCALE SETTINGS


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

[Create new account](#)

Comprobamos que se pueda ingresar con la nueva cuenta.

https://www.proyectopbsi.cf/user/login

Log in

 **Becarios de Seguridad (Erick, Pedro, Ivan y Sofia) UNAM-CERT**
Portal de vulnerabilidades

Home

Home

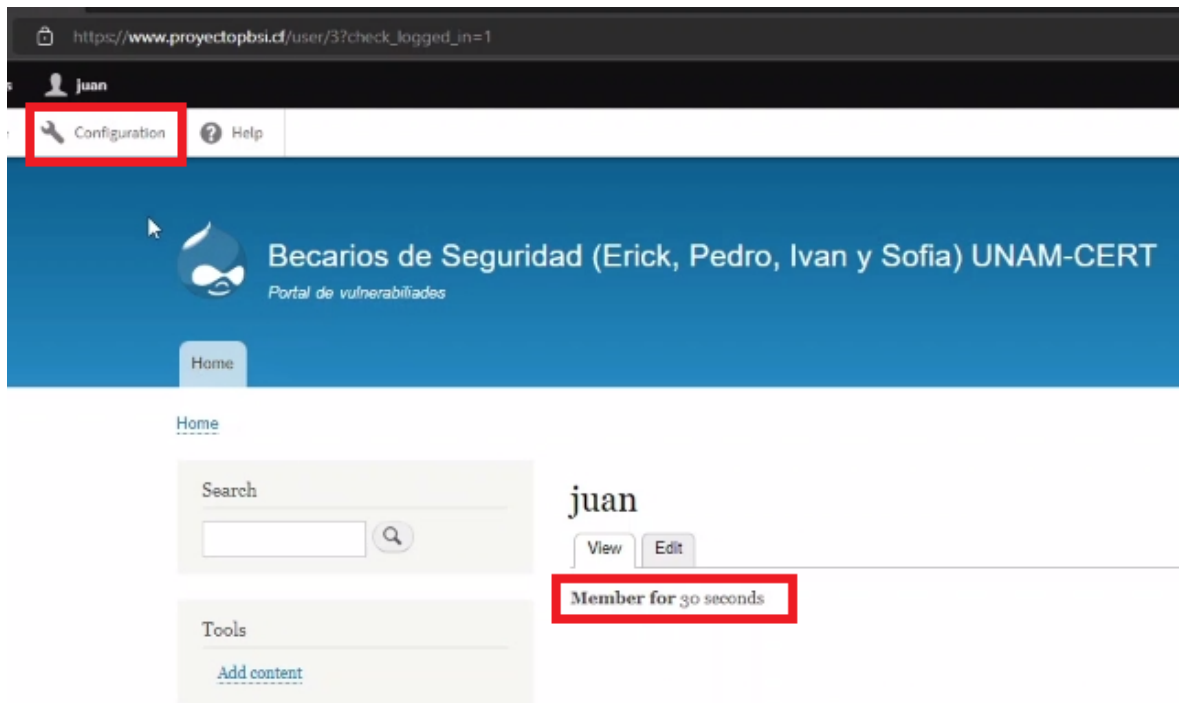
Search

Log in

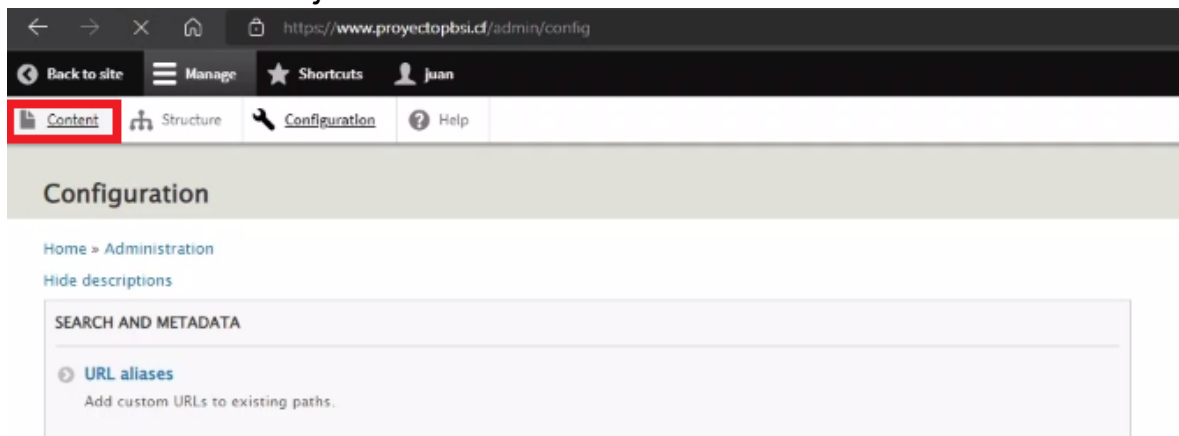
Username *
Enter your Becarios de Seguridad (Erick, Pedro, Ivan y Sofia) UNAM-CERT username.
juan

Password *
Enter the password that accompanies your username.
.....

Log in



Al dar click en *Configuration* y luego en *Content* verificamos el rol de editor de contenido del usuario *juan*.



← → ↻ 🏠 <https://www.proyectopbsi.d/admin/content>

🔙 Back to site 🗑️ Manage ⭐ Shortcuts 👤 **Juan**

📄 Content 🏠 Structure ⚙️ Configuration ? Help

Content

Content Files

Home » Administration

[+ Add content](#)

Title Content type Published status Language

[Filter](#)

Action

[Apply to selected items](#)

<input type="checkbox"/>	TITLE	CONTENT TYPE	AUTHOR
<input type="checkbox"/>	Escalación de privilegios local en la utilidad pkexec de polkit	Vulnerabilidades	WebSecMaster
<input type="checkbox"/>	Fallo en la verificación de zonas secundarias de DNSSEC	Vulnerabilidades	WebSecMaster
<input type="checkbox"/>	Envenenamiento de caché en BIND	Vulnerabilidades	WebSecMaster
<input type="checkbox"/>	Desbordamiento de búfer en productos SonicWall	Vulnerabilidades	WebSecMaster

[Apply to selected items](#)

Creamos un segundo usuario *maria* con el rol de administrador.

Username *

maria

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

Password *

.....

Password strength: Strong

Confirm password *

.....

Passwords match: yes

Recommendations to make your password stronger:

- Add uppercase letters

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 privi

▼ LOCALE SETTINGS

Time zone

Mexico City

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

[Create new account](#)

WAF

Primero se debe instalar el módulo de ModSecurity con el comando

```
sudo apt install libapache2-mod-security2
```

```
admin@ip-172-31-14-213:~$ sudo apt install libapache2-mod-security2
```

Se tiene que habilitar el módulo con el comando

```
sudo a2enmod security2
```

```
admin@ip-172-31-14-213:~$ sudo a2enmod security2
```

Copiar el archivo de configuración de ModSecurity recomendado a un archivo nuevo

```
sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

```
admin@ip-172-31-14-213:~$ sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

Editar el archivo que se acaba de crear cambiar la línea `SecRuleEngine DetectionOnly` por `SecRuleEngine On`

```
sudo nano /etc/modsecurity/modsecurity.conf
```

```
admin@ip-172-31-14-213:~$ sudo nano /etc/modsecurity/modsecurity.conf
```

```
# -- 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
```

Recargar la configuración de Apache

```
sudo systemctl restart apache2
```

```
admin@ip-172-31-14-213:~$ sudo systemctl restart apache2
```