**Default ServerConfig**: /etc/httpd/conf.d/httpd.conf

**Default ServerRoot:** /etc/httpd

**Default DocumentRoot:** /var/www/html/

**Quick Commands:**

$ apachectl {restart|start|stop}

$ service httpd{restart|stop|start}

$ systemctl {restart|stop|start} httpd.service

## Installing LAMP Wordpress Stack (On empty Apache):

$ sudo yum install php-gd mariadb-server mariadb php php-mysql php-fpm httpd

$ sudo systemctl start mariadb.service #this is necessary for the next step

$ sudo mysql\_secure\_installation # Run through these steps. Disable root remote!

$ sudo systemctl enable mariadb.service

Create a dedicated user for the database.

$ mysql -u root -p #This password is set to whatever you set in mysql\_secure\_installation

CREATE DATABASE wordpress;

CREATE USER wordpressuser@localhost IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON wordpress.\* TO wordpressuser@localhost IDENTIFIED BY 'password';

FLUSH PRIVILEGES;

Setup Wordpress:

1. Download tar from wordpress.org
2. Untar the file
3. Copy all wordpress contents to /var/www/html/

$ wget https://wordpress.org/latest.tar.gz

$ tar xzvf latest.tar.gz

# Preserve Permissions via rsync

$ sudo cp -Rp ~/wordpress/ /var/www/html/

$ sudo mkdir /var/www/html/wordpress/wp-content/uploads

$ sudo chown -R apache:apache /var/www/html/\* #Ubuntu user: www-data

$ cd /var/www/html && cp wp-config-sample.php wp-config.php

$ emacs wp-config.php

# Make File look like dah

# /var/www/html/wp-config.php

// \*\* MySQL settings - You can get this info from your web host \*\* //

/\*\* The name of the database for WordPress \*/

define('DB\_NAME', 'wordpress');

/\*\* MySQL database username \*/

define('DB\_USER', 'wordpressuser');

/\*\* MySQL database password \*/

define('DB\_PASSWORD', 'password');

$ service httpd restart

MOD\_SEC

sudo mkdir /etc/httpd/crs

sudo cd /etc/httpd/crs

git clone https://github.com/SpiderLabs/owasp-modsecurity-crs

This will create a new **owasp-modsecurity-crs** folder.

5. Move the crs-setup.conf.example file to crs-setup.conf.

Please take the time to go through this file and customize the settings

for your local environment. Failure to do so may result in false

negatives and false positives. See the section entitled OWASP CRS

Configuration for more detail.

6. Rename rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example and

rules/RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf.example to remove the '.example' extension. This will allow you to add exclusions without updates

overwriting them in the future.

7. Add the following line to your httpd.conf/apache2.conf (the following

assumes you've cloned CRS into **modsecurity.d/owasp-modsecurity-crs**). You can alternatively place these in any config file included by Apache: