

# Practica09

---

En esta práctica vamos a crear una auditoria de seguridad para wordpress usando la herramienta WPscan en una máquina de Vagrant.

## Paso 1

Creamos una carpeta donde guardaremos los archivos de la máquina.

```
mkdir practica-09
```

## Paso 2

Una vez creada la máquina ejecutamos el comando vagrant init, el cual nos creara el archivo Vagrantfile.

```
vagrant init
```

## Paso 3

Una vez tengamos el archivo Vagrantfile, lo abrimos y añadiremos las siguientes lineas que son necesarias.

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

Vagrant.configure("2") do |config|

  config.vm.box = "ubuntu/bionic64"

  config.vm.provision "shell", inline: <<-SHELL

  #Actualizamos los repositorios
  apt-get update

  #Instalamos git y ruby-bundler
  apt-get install -y git
  apt-get install -y ruby-bundler

  #Instalamos las dependencias para instalar las gemas de nokogiri
  apt-get install -y build-essential
  apt-get install -y patch
  apt-get install -y ruby-dev
  apt-get install -y zlib1g-dev
  apt-get install -y liblzma-dev

  #Instalamos las gemas necesarias de ruby
```

```
gem install nokogiri
cd /vagrant

#Clonamos el repositorio de wpscan
git clone https://github.com/wpscanteam/wpscan --depth 1
cd wpscan/

#Compilamos el codigo de wpscan
bundle install && rake install

SHELL
end
```

Una vez tengamos el Vagrantfile configurado ya estara todo listo para empezar con la auditoria.

## Paso 4

Iniciamos la máquina.

```
vagrant up
```

## Paso 5

Una vez esta levantada la máquina nos conectamos a ella.

```
vagrant ssh
```

## Paso 6

Cuando estemos dentro de nuestra máquina para usar WPScan pondremos el siguiente comando.

```
wpsacn --url http://35.175.193.94 -enumerate p
```

Donde pone 35.175.193.94 ponemos la IP de nuestro balanceador web en caso de tener y sino tenemos ponemos la IP de nuestro sitio web.