

Backdoors/webshells

1. Usando GREP

- Guardar en el archivo pattern.txt

```
eval($_REQUEST
eval($_GET
eval($_POST
eval(
$GLOBALS[
$strrev('dedoce
base64_decode
str_replace
preg_replace
gzinflate
$f53[
hacked
FilesMan
\x73\x74\x72\x5f
str_rot13
Location:
google.com
bing.com
```

- Ejecutar al comando

```
fgrep -rf pattern.txt folderInstalacion | egrep -iv "\.js|.css|.po|.html|Binary" > resultado.txt
```

- Eliminar los falsos positivos
- Otros patrones sospechosos (Ejecutar dentro del directorio principal)

```
grep -r '\\x' * | egrep -iv "\.gif|.js|.png|#|entities"
grep -r '\\057' * | egrep -iv "\.gif|.js|.png|#|binary|Crypto|zip|case|elseif|ChaCha|\\x00|pie|escaper"
```

2. Usando la herramienta webshell-scanner-client

- Descargar e instalar webshell-scanner-client

```
wget https://github.com/baidu-security/webshell-scanner-client/releases/download/v1.0/webdir-linux32.bin
sudo mv webdir-linux32.bin /usr/bin/webshell-scanner-client
sudo chmod a+x /usr/bin/webshell-scanner-client
```

- Escanear un archivo

```
webshell-scanner-client.bin archivo.php- Solicitar al RSI que mueva los archivos de la instalacion wordpress a otra
ruta que no sea accesible desde el servidor web. Ej: /home/{usuario}
```

3. Usando la herramienta webshell-scan

- Descargar e instalar webshell-scan

```
git clone https://github.com/tstillz/webshell-scan
go build main.go
sudo mv main /usr/bin/webshell-scan
```

- Escanear en busca de webshells con extensión en php

```
webshell-scan -dir . -exts php
```

4. Usando findbot

- Instalar

```
wget https://raw.githubusercontent.com/wellr00t3d/findbot.pl/master/findbot.pl
chmod a+x findbot.pl
sudo mv findbot.pl /usr/bin
```

- Buscar archivos maliciosos

```
findbot.pl directorio
```

