SQL INJECTION.

原创

will_chan_bowei 于 2017-01-01 21:05:33 发布 248 收藏
分类专栏： 个人教程 文章标签： sql sql注入 漏洞

这是一篇小白学习SQL注入的笔记

在2017年的第一天，小白决定要开始写笔记了，不然什么鬼东西一下子搞定完之后就又忘了。最近在某站上做题，没什么思路，只能边上网查WRITEUP边做了，2017要有所改变。

对于SQL注入是个常年的漏洞了吧，只是你后来发现想去注入的时候，发现现在的WAF太多，用工具像某MAP已经有点难满足各种强大的绕过，也可能因为我是小白不会用那工具，也许可以用机器学习来完善注入，我是不会啦。但是正所谓人才是安全环节中最重要的一环，所以没什么是可以难到人的，手工注入才是最厉害的，各种绕过只要你想得到就是可以绕过的。
本篇笔记还在完善中...

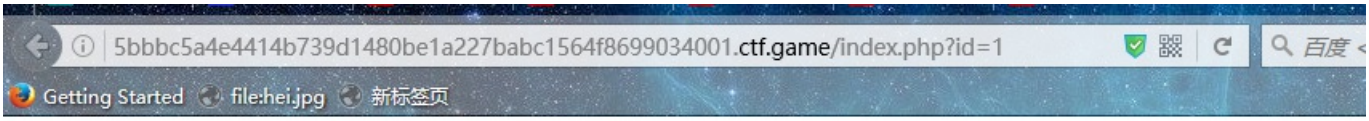
WAF绕过

注入尝试

题目例子演示

1. i春秋题目:SQL注入（百度杯9月第二场）

题目二话不说就是注入。

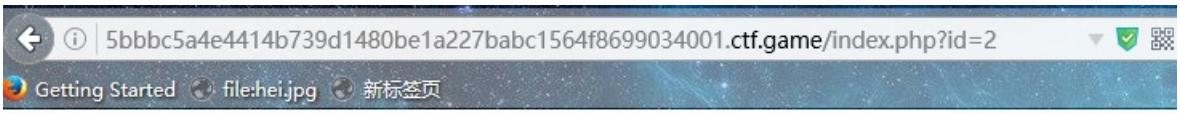


flag{在数据库中}

作为小白只能以我局限的的知识去解了。首先是想试一下order by，union select的，结果就给我显示了inj code。。。其他太明显的就是直接i春秋的WAF了吧，我都被405拦截了，你还要我怎样，我很绝望啊！

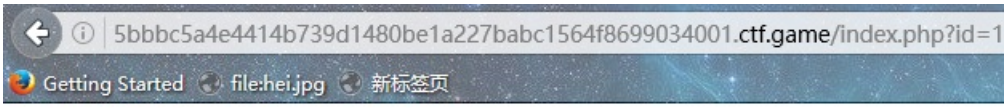
inj code!

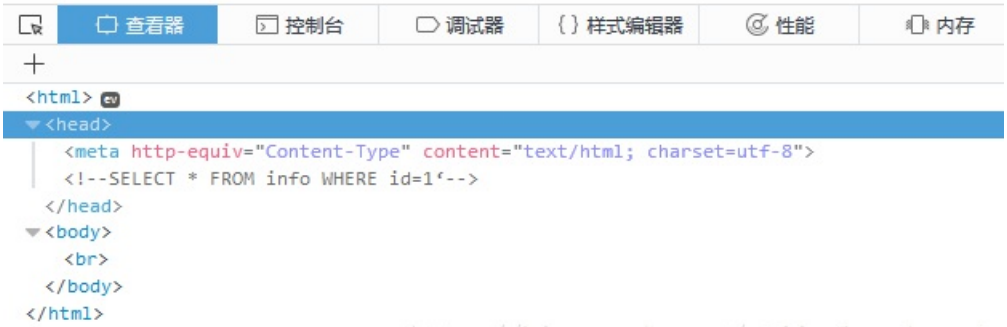
那么把id的值换一下会有什么？
发现id=1的时候会显示flag{在数据库中}，id=2的时候会显示test，id=3
或是其他的时候都是空白页。好像并没什么卵用。



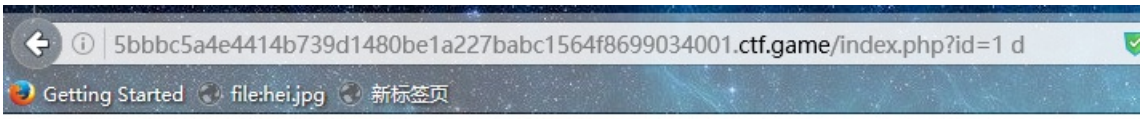
test

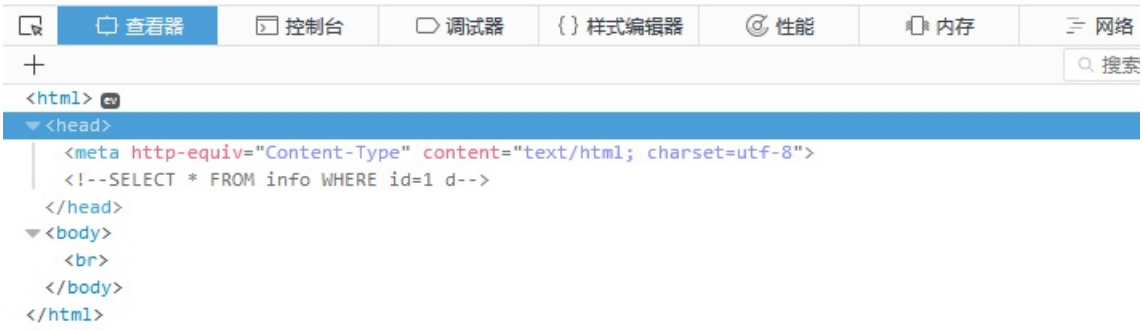
试了其他几个什么常见的注入绕过，毕竟作为小白的我了解还是太少了，只会大小写Unlon SeLecT,加注释/**/,等一些低级绕过，
没有特别大的脑洞又不知道要尝试什么，简直生不如死。毫无头绪之际，我只能去看WRITEUP先了。
危急关头居然说页面F12有提示。。。打开一看果然有sql语句





当我在id后书写什么，只要页面返回不是405的话，那句sql也会变，输入id=1 d



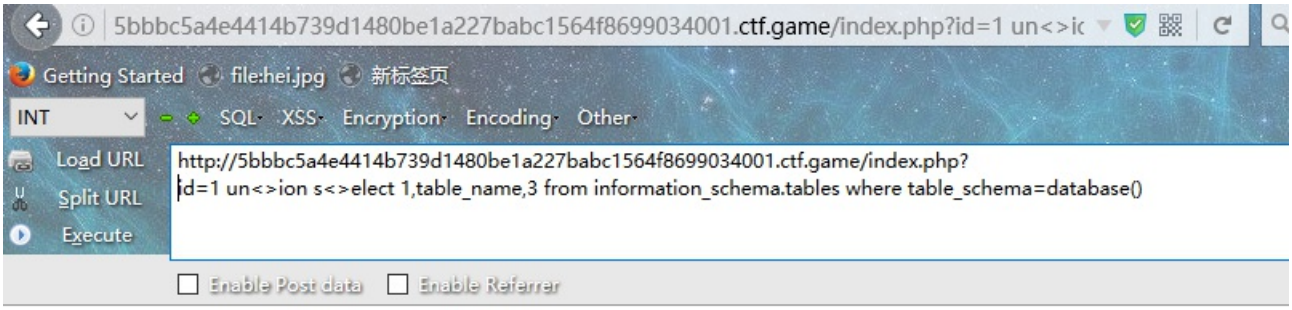


接着尝试了一些其他符号后，发现最后被过滤掉的<>可以用。

所以构造un<>ion sel<>ect 1,2,3来爆显位和猜子段数，其实子段数可以用order by来猜，可以知道子段数是3，只有1，2为显位。

然后爆表名:un<>ion s<>elect 1,table_name,3 from information_schema.tables where table_schema=database().

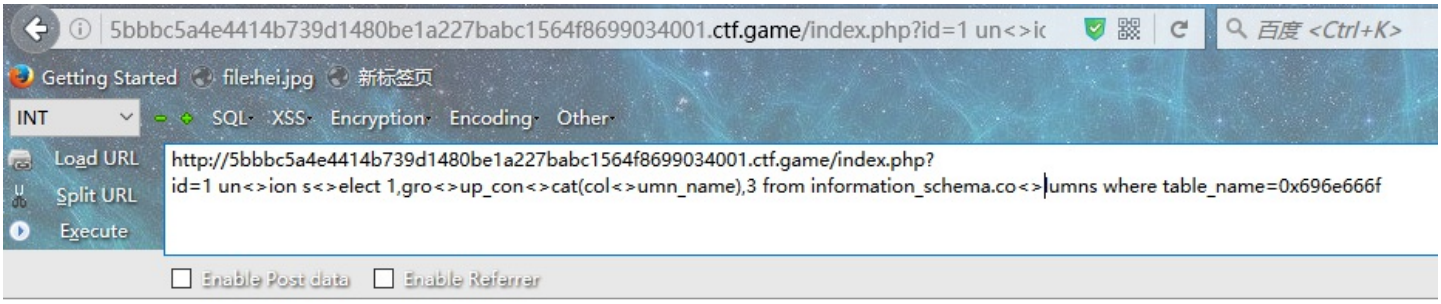
database()是个mysql函数，返回当前使用的数据库，利用的是mysql中的information_schma库中会存所有数据库的表，字段的信息。得出表明为info，其实这已经从那sql注释中就可以得出了。



flag{在数据库中}

info

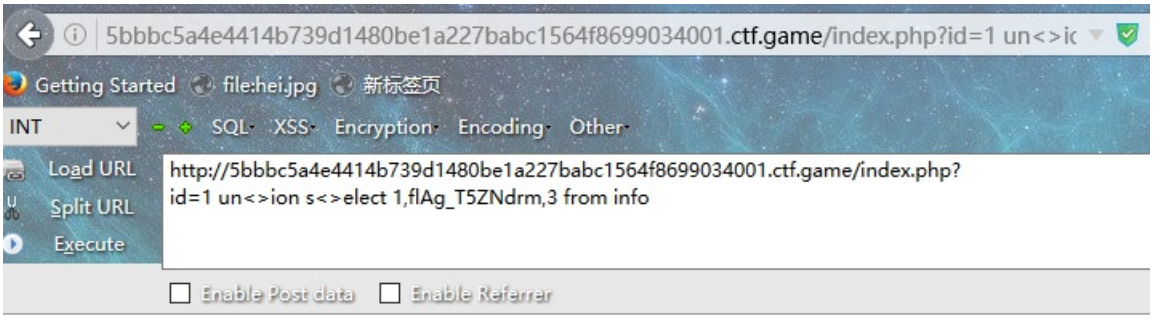
接下来就是看看有什么字段,un<>ion s<>elect 1,gro<>up_con<>cat(col<>umn_name),3 from information_schema.co<>lumns where table_name=0x696e666f



flag{在数据库中}

id,title,flAg_T5ZNdrm

看来哪个字段是我们想要的已经很清楚了。继续用union select语句来爆出flag，un<>ion s<>elect 1,flAg_T5ZNdrm,3 from info



flag{在数据库中}

flag{64dfabd6-4c76-4737-9886-d0e39529b896}

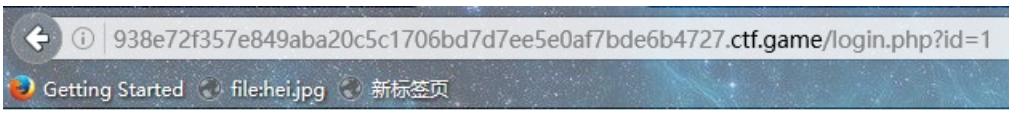
test

很好，flag拿到！（感谢ichunqiu的WRITEUP我就是记个笔记）

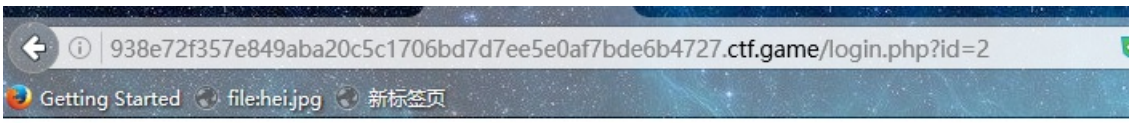
2.还是SQL注入，不过这次题目是SQLi(第三场)

创建完题目之后，访问一懵，这是什么鬼，php名字一大串，开始就想来个下马威。

所以我就小白脸的按下了F12,发现有个login.php?id=1，会有什么蹊跷，看看便知。

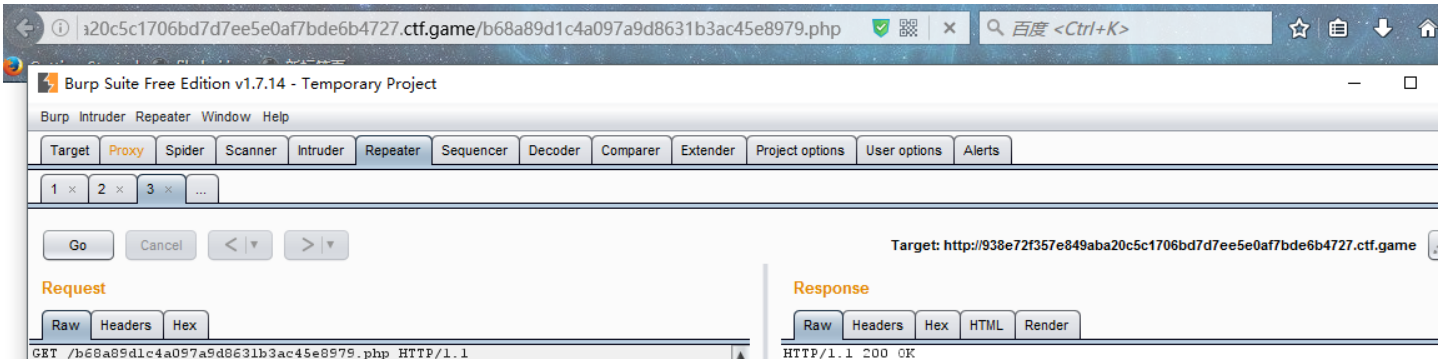


welcome admin~



something error~

看起来这里是注入点？于是尝试过上面的BYPASS思路，当主办方是傻的，两次题目的BYPASS能一样吗。好像没戏呀！情急之下，我又去搜索了一下，发现有思路。BURPSUITE抓包看一下。
第一次没有收获。没发现什么异常的。

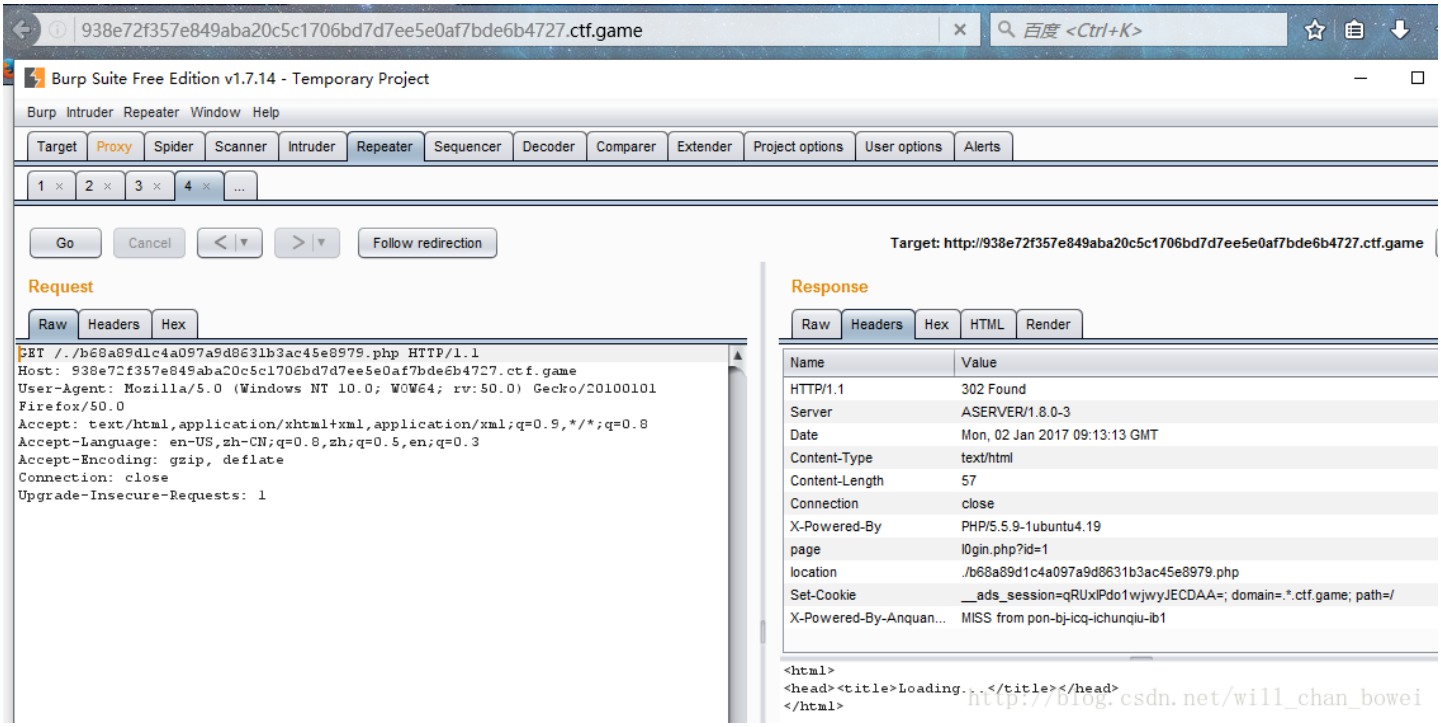


```
Host: 938e72f357e849aba20c5c1706bd7d7ee5e0af7bde6b4727.ctf.game
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101
Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,zh-CN;q=0.8,zh;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

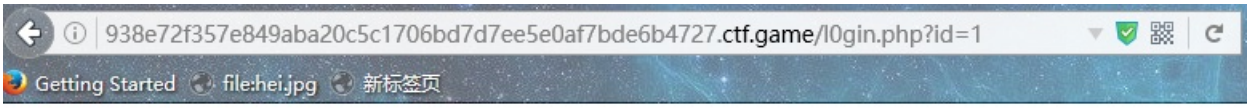
```
Server: ASERVER/1.8.0-3
Date: Mon, 02 Jan 2017 09:11:06 GMT
Content-Type: text/html
Content-Length: 98
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.19
Vary: Accept-Encoding
Set-Cookie: __ads_session=90e6MepolwhBx5ECDAA=; domain=.*.ctf.game; path=/
X-Powered-By-Anquanbao: MISS from pon-bj-icq-ichunqiu-ib1

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

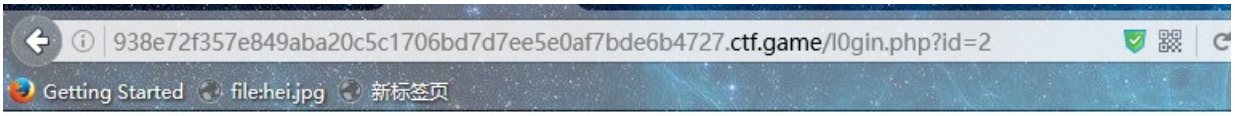

去掉php再来一次，发现有重定向header里面有个page，值是l0gin.php？id=1，是0不是o，看来刚才那个是个干扰。出题人真是伤心病狂这样欺负小白。



来吧，访问看看！



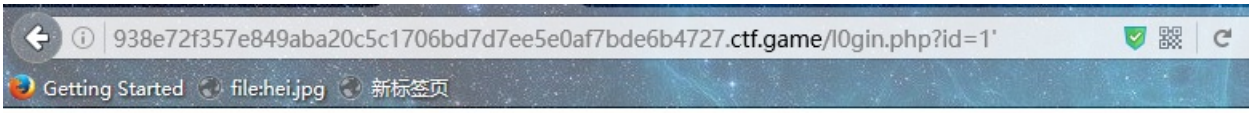
id	username
1	flag



id	username
2	test

id	username
3	

手贱加了个分号，结果发现下面也带上了分号



id	username
1'	

试试其他的，什么order by 啊，union 啊加上试试.最后发现原来逗号之后的内容会被截掉，好吧其实不是我发现，只是根据思路验证了一下。很好逗号被截了那我union select 还怎么加上1,2,3?