Mysql中Load Data语句在phpadminer中的利用

小透明yo / 2019-09-26 09:25:06 / 浏览数 4507 渗透测试 渗透测试 顶(0) 踩(0)

起因：

和师傅们在群里面进行了一番学术性探讨，突然想起来有这么个东西，还是和领导偷的。

LOAD DATA语句介绍：

> MySQL 中提供了LOAD DATA INFILE语句来插入数据。 以下实例中将从当前目录中读取文件 dump.txt ，将该文件中的数据插入到当前数据库的 mytbl 表中。

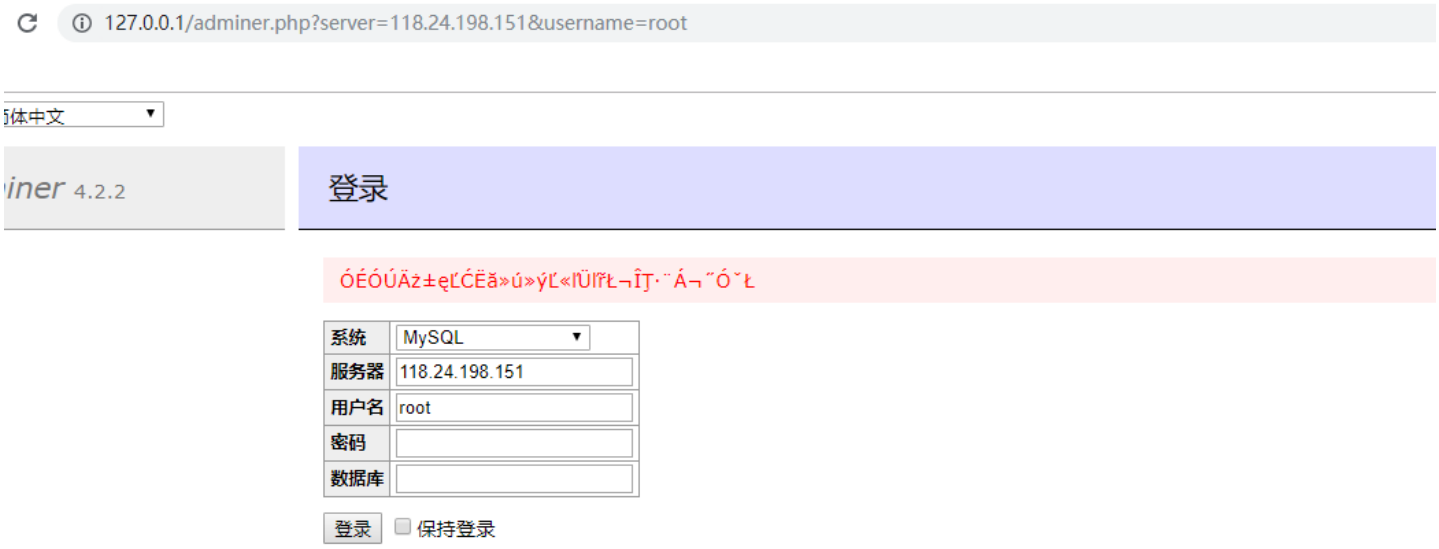
也就是说将客户端文件读入到mysql表中，phpadminer可以连接远程数据库，那么这样就可以在远程数据库中读到本地文件。

环境搭建：

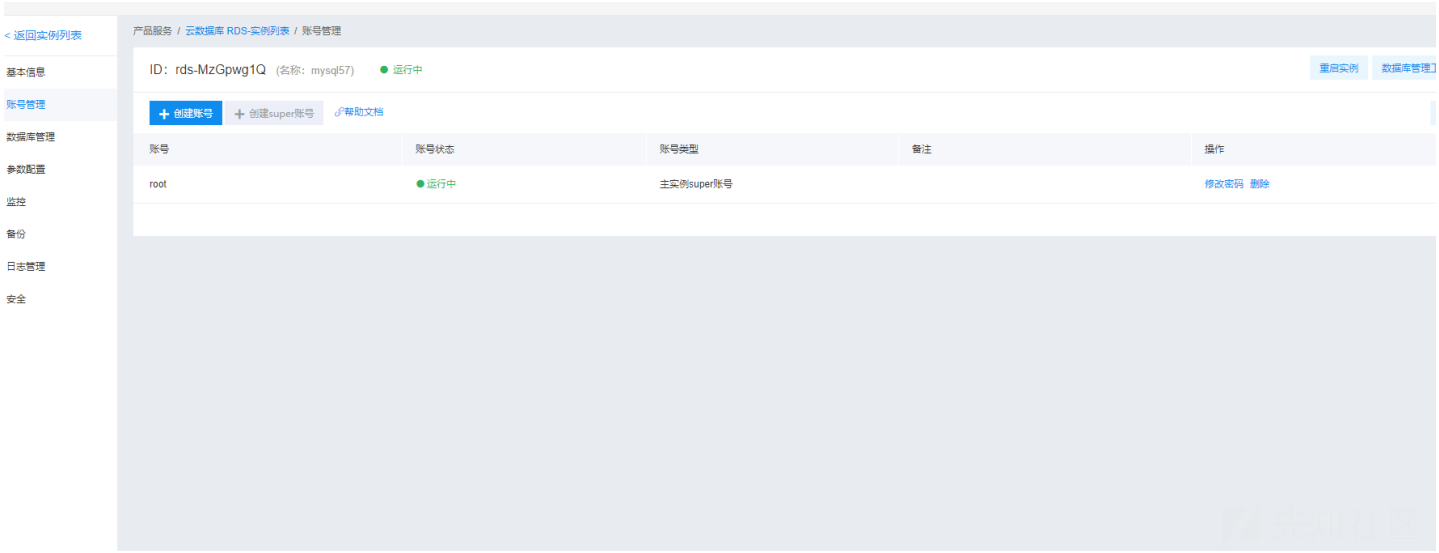
1. adminer
2. 远程服务器搭建mysql
3. 开启mysql外链

环境搭建：

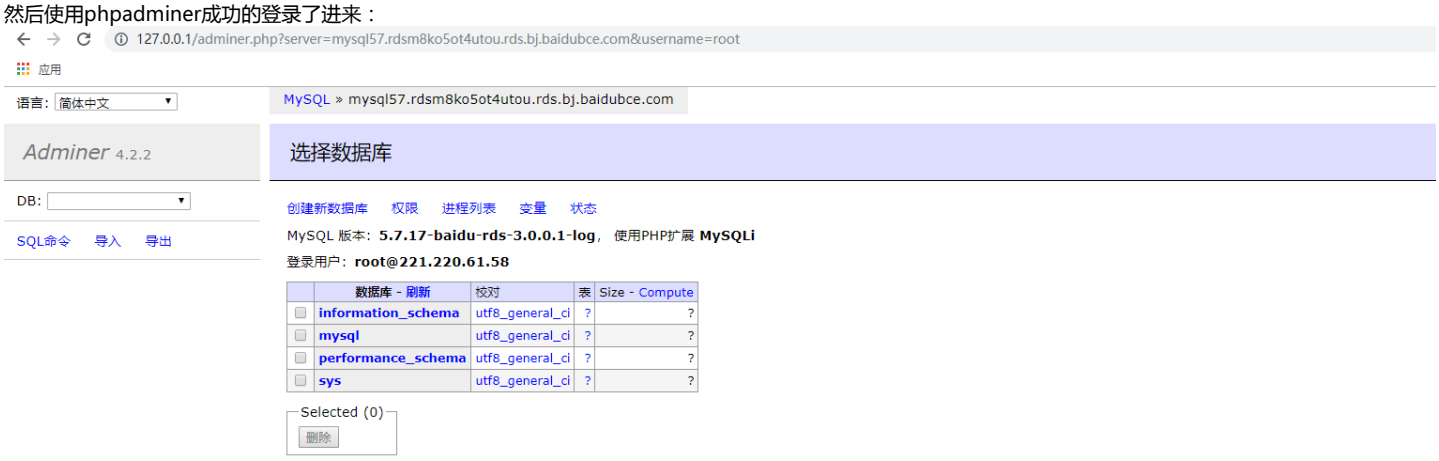
打开phpmyadminer页面，可以发现他允许链接远程数据：



这里我在百度云申请了一个免费的mysql云服务器：



然后使用phpadminer成功的登录了进来：

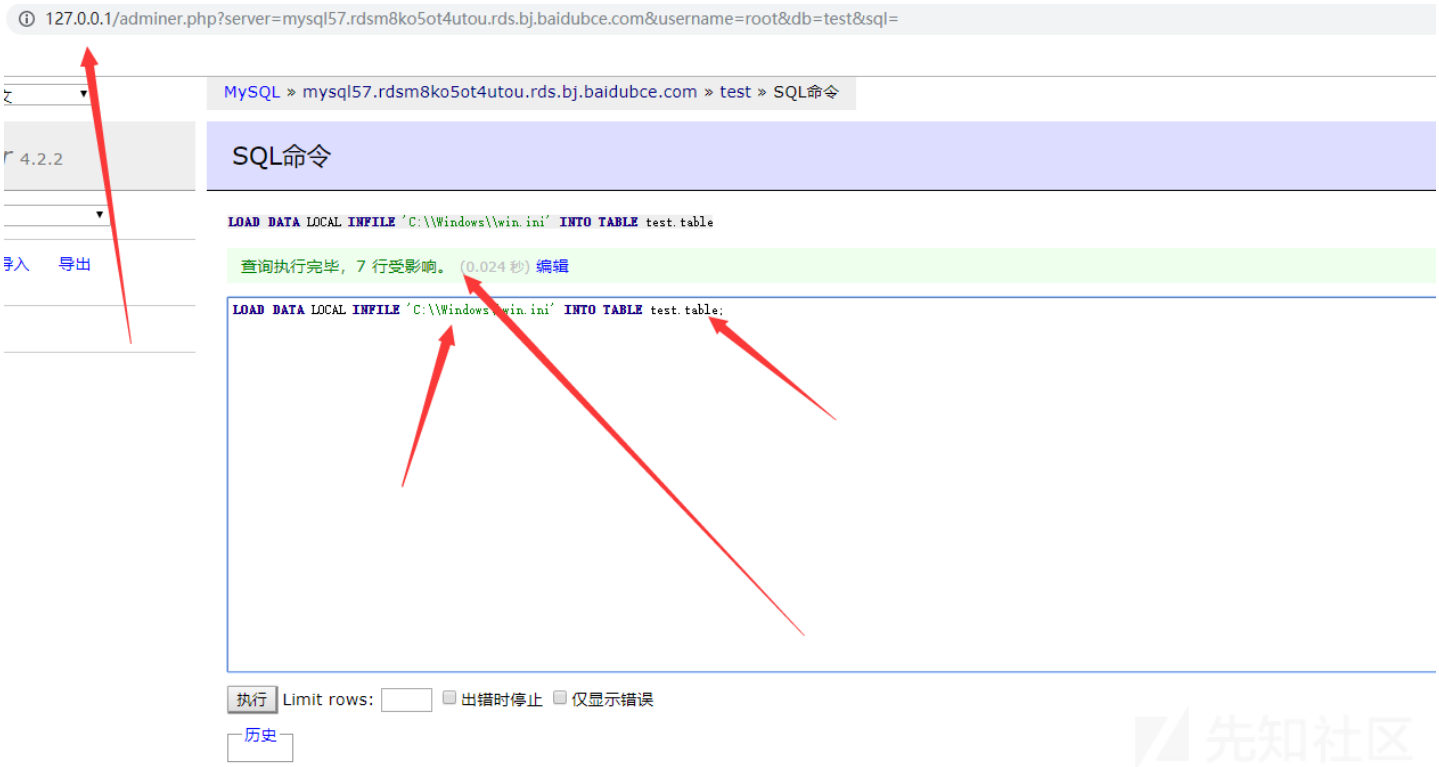


然后创建了一个test数据库以及name字段：

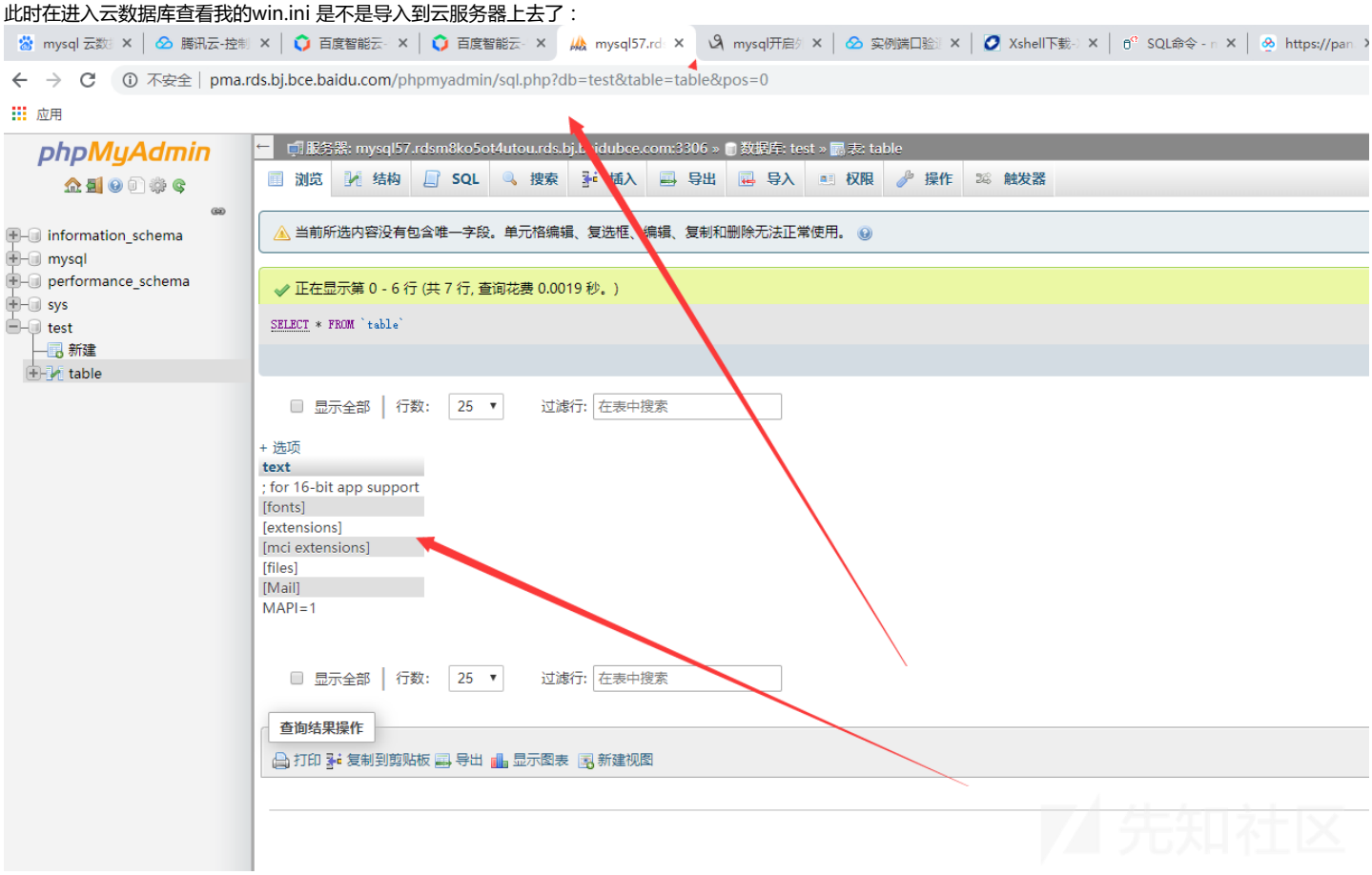
LOAD DATA读取数据:

SQL语句：

```
LOAD DATA LOCAL INFILE 'C:\\Windows\\win.ini' INTO TABLE table;
```



此时在进入云数据库查看我的win.ini 是不是导入到云服务器上去了：



小结:

也就是说，当目标使用phpadminner进行数据管理时，我们可以直接连接自己的数据库来达到读取客户端文件的目的。这样就可以直接读取到目标的数据库配置文件，在使

上一篇：pwn堆入门系列教程6 下一篇：[红日安全]Web安全Day6 -...

1. 0 条回复
   - 动动手指，沙发就是你的了！