数据库操作有3中途径

1. 下载Mysql客户端

参数	内容
IP	200.200.209.9
USER	algo
PASSWORD	algo123
DATABASE	webshell_data
TABLE	webshell_total_data

2. 下载批处理代码

```
git clone git@code.sangfor.org:SRI/waf/webshell_3_0_code.git
```

3. 下载release包

```
http://code.sangfor.org/SRI/waf/webshell_3_0_code/raw/master/release/data_manager.exe
```

4. 脚本使用

> 脚本主入口 `release/data_manager.exe`

4.1 插入

> 数据库插入有两种模式, `file` 和 `csv` . `file` 模式直接传入待入库的文件夹，编辑标签配置文件，运行脚本，批量入库； `csv` 模式指定自己生成的 `csv` 文件，调用脚本，自动入库。脚本灰自动对比文件md5值，若库中已存在该文件，则跳过。

> 编辑配置文件

```
# cat insert_config.ini
```

```
# 批量插入操作
[insert]
# 文件类型(不填则自动解析文件后缀)
file_type = php
# 文件来源
file_source = 客户漏报样本
# -1 1 0 标志位  1 备注 是修改说明 用append方式
flag = -1
# 标签(标签 -2 白 -1灰白 0未知 1灰黑 2黑)
label = 2
# 审核人
checker = luojie19445
# 审核状态(-1未知 1已检测)
check_state = 1
# 是否符合语法(-1未知 0 不符合语法 1符合语法)
# correct_syntax = -1
# 备注
# remarks=
```

4.1.1 文件插入模式

参数	备注
--insert	插入模式 file
--sample_dir	待入库样本路径
--config_path	配置文件路径

```
data_manager.exe --insert file --sample_dir C:\Users\Sangfor\Desktop\webshell --config_path insert_config.ini
```

4.1.2 csv插入模式

参数	备注
--insert	csv 更新模式
--csv_path	csv 路径

```
data_manager.exe --insert csv --csv_path result_2019-07-02.csv
```

4.2 更新

> 数据库插入有两种模式, file ， vt , d_safe 和 csv , file 模式直接传入待入库的文件夹，编辑标签配置文件，运行脚本，批量入库；df 模式指定自己生成的csv文件，调用脚本，自动入库。脚本灰自动对比文件md5值，若库中已存在该文件，则跳过。

> 编辑配置文件，大开你需要更新的行

```
# cat update_config.ini
```

```
# 批量更新操作
[update]
# 文件类型
file_type = php
# 文件来源
file_source = 客户漏报样本
# D盾检测结果
# d_safe_2_1_4_9 = -1
# VT检测结果
# virus_total = -1
# wsk2_0检测结果
# wsk2_0 = -1
# wsk3_0_0检测结果
# wsk3_0_0 = -1
# -1 1 0 标志位  1 备注 是修改说明 用append方式
# flag = -1
# 标签
# label = -2
# 是否符合语法
# correct_syntax = -1
# 审核人
# checker = liudong
# 审核状态
# check_state = -1
# 备注
# remarks=
```

4.2.1 文件更新模式

参数	备注
--update	文件更新模式 file
--sample_dir	待入库样本路径
--config_path	配置文件路径

```
data_manager.exe --update file --sample_dir C:\Users\Sangfor\Desktop\webshell\客户测试数据\客户漏报\灰白样本 --config_path update_config.ini
```

4.2.2 csv更新模式

参数	备注
--update	csv 更新模式
--csv_path	csv 路径

```
data_manager.exe --update csv --csv_path result_2019-07-02.csv
```

4.2.3 vt 查杀结果更新

参数	备注
--update	vt 更新模式
--vt_dir	vt 结果文件夹路径

```
data_manager.exe --update vt --vt_dir C:\Users\Sangfor\Desktop\webshell\VT\task_20190621_8W#0_webshell.csv_1561081564947
```

4.2.4 d_safe 查杀结果更新

参数	备注
--update	d_safe 更新模式
--d_path	d盾结果文件路径

```
data_manager.exe --update d_safe --d_safe_dir C:\Users\Sangfor\Desktop\webshell\D盾_web扫描记录_2019070311.zip
```

4.3 批量查询

参数	备注
--query	file 查询模式
--sql	sql 语句data_manager.exe
--output_dir	输出路径

```
data_manager.exe --query file --sql "select * from webshell_total_data where file_type='php' and label=2 limit 50" --output_dir C:\Users\Sangfor\De
```