参考：

http://www.youknowi.xin/2018/06/sqlmap%e8%bf%9b%e9%98%b6%e7%af%87/
https://www.cnblogs.com/hongfei/p/3872156.html（相当于中文手册了）

二. 命令基础解析

sqlmap 支持五种不同的注入模式：
1、基于布尔的盲注，即可以根据返回页面判断条件真假的注入。
2、基于时间的盲注，即不能根据页面返回内容判断任何信息，用条件语句查看时间延迟语句是否执行（即页面返回时间是否增加）来判断。
3、基于报错注入，即页面会返回错误信息，或者把注入的语句的结果直接返回在页面中。
4、联合查询注入，可以使用 union 的情况下的注入。
5、堆查询注入，可以同时执行多条语句的执行时的注入。

通过一段命令来学习：
解析这段命令：sqlmap -u "" --dbms=mysql --batch --random-agent --ignore-proxy --tamper=space2comment --level=3 --timeout=30 --delay=1 --retries=5 --time-sec=5 -v 3 -p "id"　　（会很耗时，最好自己修改，只是学习命令，文末会有大佬写的手册）

–dbms-mysql　指定数据库为 mysql，一般 php 小站都是 mysql

–batch　自动填写

–random-agnet　参数来随机的从./txt/user-agents.txt 中获取 User-Agent 值

–ignore-proxy 拒绝使用本地局域网的 HTTP(S)代理(可以去掉)

–tamper=space2comment　使用/**/代替空格

–level=3　当–level 的值大于等于 2 的时候也会测试 HTTP Cookie 头的值，当大于等于 3 的时候也会测试 User-Agent 和 HTTP Referer 头的值（默认为 1）

–timeout:可以设定一个 HTTP(S)请求超过多久判定为超时，10.5 表示 10.5 秒，默认是 30 秒。设定重试超时

–delay　可以设定两个 HTTP(S)请求间的延迟，设定为 0.5 的时候是半秒，默认是没有延迟的。设定超时时间

–retries　　当 HTTP(S)超时时，可以设定重新尝试连接次数，默认是 3 次。
设定随机改变的参数值

–time-sec 当使用继续时间的盲注时，时刻使用–time-sec 参数设定延时时间，默认是 5 秒。设定 UNION 查询字段数

-p 指定测试参数

如果你想观察 sqlmap 对一个点是进行了怎样的尝试判断以及读取数据的，可以使用-v 参数。

共有七个等级，默认为 1：
0、只显示 python 错误以及严重的信息。
1、同时显示基本信息和警告信息。（默认）
2、同时显示 debug 信息。
3、同时显示注入的 payload。
4、同时显示 HTTP 请求。
5、同时显示 HTTP 响应头。
6、同时显示 HTTP 响应页面。
sqlmap 发送的测试 payload 最好的等级就是 3。

–technique（延时太费时可以不选择它，默认测试所有）

B: Boolean-based blind SQL injection（布尔型注入）
E: Error-based SQL injection（报错型注入）
U: UNION query SQL injection（可联合查询注入）
S: Stacked queries SQL injection（可多语句查询注入）
T: Time-based blind SQL injection（基于时间延迟注入）

–risk 胆子肥一点，把它的等级调高点(自己搜下有影响)

-g 谷歌搜索注入点