SQLMAP 使用文档(中文)

> 笔者依据官方文档和自身理解翻译而来，如有错误之处欢迎联系ctfshow大菜鸡(笔者)反馈。
> 英文文档地址：https://github.com/sqlmapproject/sqlmap/wiki/Usage
> ctfshow靶场：https://ctf.show
> 技术交流QQ群：372619038
> 译者：CTFshow 大菜鸡

使用选项

```
用法: python sqlmap.py [选项]
基础选项:
  -h, --help            显示基础的帮助信息，然后退出
  -hh                   显示高级的帮助信息，然后退出
  --version             显示脚本的版本，然后退出
  -v VERBOSE            显示测试细节 默认数字1-6
  目标:
    至少选择下列一种模式
    -d 转发模式           给定连接字符串，连接目标数据库
    -u 直连模式, --url=   直接连接目标地址，例如:
                          http://www.site.com/vuln.php?id=1
    -l 日志模式           从Burp或者WebScarab载入代理日志文件
    -m 批量模式           从给定的文本文件扫描多个目标地址
    -r 请求模式           从文件中载入http请求
    -g 谷歌傻瓜模式        从谷歌搜索地址做为目标地址
    -c 配置模式           从ini配置文件载入目标地址
  请求:
    下面的选项是用来详细说明如何连接目标地址
    --method=方法        强制使用指定的方式进行连接，例如 PUT
    --data=数据          通过POST发送数据字符串，例如: --data="id=1"
    --param-del=参数分割 参数分割字符，例如: &
    --cookie=COOKIE      HTTP Cookie 头的值 例如: PHPSESSID=a8d127e..
    --cookie-del=COO..   cookie分割字符，例如: ;
    --load-cookies=L..   从文件载入cookie值
    --drop-set-cookie    忽略响应数据中的 Set-Cookie，即使用响应cookie
    --user-agent=AGENT   设置HTTP User-Agent 的值
    --random-agent       使用随机  User-Agent 的值
    --host=HOST          设置 HTTP Host 的值
```

```
    --referer=REFERER   设置 HTTP Referer 的值
    -H HEADER, --hea..  设置拓展头 例如：X-Forwarded-For: 127.0.0.1
    --headers=HEADERS   设置多个HTTP头 例如：Accept-Language: fr\nETag: 123
    --auth-type=AUTH..  设置HTTP认证类型 (Basic, Digest, NTLM 或 PKI)
    --auth-cred=AUTH..  设置HTTP认证账密 例如：name:password
    --auth-file=AUTH..  设置PEM私钥证书文件
    --ignore-code=IG..  忽略HTTP错误码 例如：401
    --ignore-proxy      忽略系统的代理设置
    --ignore-redirects  忽略重定向尝试
    --ignore-timeouts   忽略连接超时
    --proxy=PROXY       使用代理连接目标地址
    --proxy-cred=PRO..  使用代理进行HTTP认证 例如：name:password
    --proxy-file=PRO..  从文件中载入代理列表
    --tor               使用洋葱匿名网络
    --tor-port=TORPORT  设置洋葱匿名代理的非默认端口
    --tor-type=TORTYPE  设置洋葱匿名代理的类型 例如：HTTP, SOCKS4 或 SOCKS5
(默认))
    --check-tor         检查洋葱匿名代理网络是否可用
    --delay=DELAY       设置两次请求之间的延时，单位：秒
    --timeout=TIMEOUT   设置连接目标地址超时时间 (默认30秒)
    --retries=RETRIES   设置连接超时重试次数 (默认3次)
    --randomize=RPARAM  对给定的请求参数值进行随机化
    --safe-url=SAFEURL  设置在测试目标地址前访问的安全链接
    --safe-post=SAFE..  设置安全链接POST发送的数据
    --safe-req=SAFER..  从文件中载入安全链接列表
    --safe-freq=SAFE..  设置两次注入测试前访问安全链接的次数
    --skip-urlencode    跳过对攻击载荷的URL编码
    --csrf-token=CSR..  保存反CSRF令牌
    --csrf-url=CSRFURL  提取CSRF令牌的地址
    --force-ssl         强制使用 SSL/HTTPS
    --hpp               使用HTTP参数污染
    --eval=EVALCODE     请求前使用自定义python脚本 例如：
                        import hashlib;
                        id2=hashlib.md5(id).hexdigest()
  优化选项：
    下面的选项是用来优化sqlmap的性能
    -o                  打开所有优化选项开关
    --predict-output    预测常见查询输出
    --keep-alive        使用 HTTP(s) 持久化连接
    --null-connection   只检测响应数据长度，不检测响应内容
    --threads=THREADS   设置最大运行线程 (默认1线程)
  注入选项：
    下面的选项用来指定注入测试的定制参数和篡改脚本
    -p TESTPARAMETER    设置要注入的参数
    --skip=SKIP         设置要跳过注入的参数
    --skip-static       设置跳过静态参数
    --param-exclude=..  对要注入参数进行正则匹配 例如：ses
    --dbms=DBMS         指定注入地址的后台数据库名称
    --dbms-cred=DBMS..  指定数据库认证账密 例如：user:password
```

```
  --os=OS               指定注入地址的操作系统
  --invalid-bignum      对注入参数使用超大数字使其失效
  --invalid-logical     对注入参数使用逻辑运算使其失效
  --invalid-string      对注入参数使用随机字符串使其失效
  --no-cast             关闭攻击载荷的生成器
  --no-escape           关闭字符逃逸的生成器
  --prefix=PREFIX       攻击载荷的前缀
  --suffix=SUFFIX       攻击载荷的后缀
  --tamper=TAMPER       指定攻击载荷的篡改脚本
检测选项:
  下面的选项用来定制检测
  --level=LEVEL         指定注入测试级别 例如：1-5，默认 1
  --risk=RISK           指定注入测试风险等级，防止破坏数据 例如：1-3，默认 1
  --string=STRING       指定攻击载荷执行成功返回的字符串
  --not-string=NOT..    指定攻击载荷执行失败返回的字符串
  --regexp=REGEXP       指定攻击载荷执行成功匹配的正则表达式
  --code=CODE           指定攻击载荷执行成功返回的HTTP状态码
  --text-only           设置只检测返回文本来确定攻击载荷执行情况
  --titles              设置检测返回页面标题确定攻击载荷执行情况
技术选项:
  下面选项用来指定参数来调整指定的注入测试选项
  --technique=TECH      开启定制 (default "BEUSTQ")
  --time-sec=TIMESEC    指定目标数据库响应时间 (默认5秒)
  --union-cols=UCOLS    指定联合查询注入的列范围
  --union-char=UCHAR    指定联合查询猜测列数量最大长度
  --union-from=UFROM    指定联合查询使用的表
  --dns-domain=DNS..    指定DNS外带的解析地址
  --second-url=SEC..    指定二次注入的结果页面
  --second-req=SEC..    指定二次注入的结果页面列表文件
指纹选项:
  -f, --fingerprint     使用常见数据库指纹识别
枚举选项:
  下面的选项用来枚举后端数据库管理系统的信息、结构以及表内的包含数据。此外，你可以
  运行自己的SQL语句
  -a, --all             检索所有内容
  -b, --banner          检索数据库欢迎信息
  --current-user        检索数据库的当前用户
  --current-db          检索当前使用的数据库名称
  --hostname            检索数据库计算机名称
  --is-dba              检测当前用户是否为数据库管理员
  --users               枚举数据库的所有用户
  --passwords           枚举数据库的所有用户密码哈希值
  --privileges          枚举数据库的所有用户权限
  --roles               枚举数据库的所有用户角色
  --dbs                 枚举数据库的所有数据库
  --tables              枚举数据库的所有表
  --columns             枚举数据库的所有列
  --schema              枚举数据库汇总数据
  --count               检索数据库的记录总数
```

```
  --dump                转储数据库表的记录
  --dump-all            转储数据库的所有表记录，俗称脱裤
  --search              搜索指定列、表、数据库
  --comments            枚举时检测数据库的注释
  -D DB                 指定要枚举的数据库名称
  -T TBL                指定要枚举的表名称
  -C COL                指定要枚举的列名称
  -X EXCLUDE            指定排除枚举的数据库名称
  -U USER               指定枚举时的数据库用户
  --exclude-sysdbs      设置枚举时包含数据库系统自带表
  --pivot-column=P..    指定主键名称
  --where=DUMPWHERE     转储数据表时，使用where条件语句
  --start=LIMITSTART    转储表时，使用limit语句进行显示，设置limit的第一个参数
  --stop=LIMITSTOP      转储表时，使用limit语句进行显示，设置limit的第二个参数
  --first=FIRSTCHAR     查询时使用的第一个字符
  --last=LASTCHAR       查询时使用的最后一个字符
  --sql-query=QUERY     执行sql语句
  --sql-shell           使用可交互sql-shell
  --sql-file=SQLFILE    指定执行sql语句的文件
暴力破解选项:
  下面的选项用来设置暴力破解参数
  --common-tables       使用本地表名字典
  --common-columns      使用本地列明字典
自定义函数选项:
  下面的选项用来生成和运行自定义函数
  --udf-inject          注入自定义函数
  --shared-lib=SHLIB    指定本地函数共享库
文件系统访问选项:
  下面的选项用来设置目标系统的文件系统访问参数
  --file-read=FILE..    从目标系统的文件系统读入文件
  --file-write=FIL..    向目标系统的文件系统写入文件
  --file-dest=FILE..    要写入文件的绝对路径
操作系统访问选项:
  下面的选项用来设置对目标操作系统的访问参数
  --os-cmd=OSCMD        执行操作系统命令
  --os-shell            反弹操作系统的shell
  --os-pwn              反弹OOBshell, Meterpreter 或 VNC
  --os-smbrelay         一键反弹 OOB shell, Meterpreter or VNC
  --os-bof              保存缓冲器溢出攻击载荷
  --priv-esc            数据库账户提权
  --msf-path=MSFPATH    Metasploit Framework本地安装路径
  --tmp-path=TMPPATH    远程临时文件存放的绝对路径
Windows注册表访问选项:
  下面的选项用来设置Windows系统的注册表访问参数
  --reg-read            读取注册表的指定键值
  --reg-add             向注册表写入指定键值
  --reg-del             删除之策表指定键值
  --reg-key=REGKEY      设置注册表的键名
  --reg-value=REGVAL    设置注册表的键值
```

```
  --reg-data=REGDATA  设置注册表的键数据
  --reg-type=REGTYPE  设置注册表的键类型
公共选项:
  下面的选项用来设置公共参数
  -s SESSIONFILE      载入测试会话文件
  -t TRAFFICFILE      记录所有的HTTP测试结果至文本文件
  --answers=ANSWERS   设置默认回应 例如 quit=N,follow=N
  --base64=BASE64P..  设置参数包含base64数据
  --batch             静默执行，使用默认选项进行
  --binary-fields=..  返回结果包含二进制数据
  --check-internet    进行注入测试前，检查网络联通情况
  --crawl=CRAWLDEPTH  对指定地址爬虫测试
  --crawl-exclude=..  对匹配正则表达式的页面地址进行爬虫测试
  --csv-del=CSVDEL    设置csv格式的分割符
  --charset=CHARSET   设置盲注测试字符集  例如：0123456789abcdef
  --dump-format=DU..  对转储文件进行转换  例如：CSV(默认), HTML 或SQLITE
  --encoding=ENCOD..  设置检索时的字符集  例如：GBK
  --eta               显示输出耗时
  --flush-session     刷新当前目标地址的会话
  --forms             对目标地址提交表单测试
  --fresh-queries     忽略已缓存的查询结果
  --har=HARFILE       保存所有HTTP响应至HAR文件
  --hex               检索返回数据时使用16进制
  --output-dir=OUT..  自定义输出文件路径
  --parse-errors      显示页面上的数据库错误
  --preprocess=PRE..  使用指定脚本提交请求
  --postprocess=PO..  使用指定脚本处理请求响应
  --repair            转储未知字符时，使用的替换字符
  --save=SAVECONFIG   将当前的配置保存至配置文件
  --scope=SCOPE       使用正则表达式匹配代理地址列表
  --test-filter=TE..  选择标题且(或)为指定字符串的攻击载荷
  --test-skip=TEST..  忽略标题且(或)为指定字符串的攻击载荷
  --update            更新 sqlmap
其他选项:
  -z MNEMONICS        使用助记符 例如：flu,bat,ban,tec=EU
  --alert=ALERT       注测测试成功执行的本地系统命令
  --beep              注入点测试成功主板蜂鸣
  --cleanup           使用自定义函数情况数据库
  --dependencies      检查sqlmap的组件完整性
  --disable-coloring  关闭彩色输出
  --gpage=GOOGLEPAGE  谷歌傻瓜式注入扫描的页数
  --identify-waf      Make a thorough testing for a WAF/IPS protection
  --list-tampers      显示篡改脚本列表
  --mobile            使用手机UA
  --offline           离线模式
  --purge             安全卸载所有sqlmap内容
  --skip-waf          放弃测试具有启发式WAF保护的地址
  --smart             检测是否时启发式WAF保护
  --sqlmap-shell      反弹sqlmap的shell
```

```
    --tmp-dir=TMPDIR     设置sqlmap本地临时文件路径
    --web-root=WEBROOT   设置http服务的网页根目录 例如：/var/www
    --wizard             使用sqlmao时开启简单向导
```

CTFshow-大菜鸡 于 2020-11-14 夜完成