

# 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](https://t.me/ctfshow)

译者：CTFshow 大菜鸡

## 使用选项

```
1  用法：python sqlmap.py [选项]
2  基础选项：
3
4  -h, --help          显示基础的帮助信息，然后退出
5  -hh                显示高级的帮助信息，然后退出
6  --version          显示脚本的版本，然后退出
7  -v VERBOSE        显示测试细节 默认数字1-6
8  目标：
9
10  至少选择下列一种模式
11
12  -d 转发模式        给定连接字符串，连接目标数据库
13  -u 直连模式, --url=  直接连接目标地址，例如：
14                      http://www.site.com/vuln.php?id=1
15  -l 日志模式        从Burp或者WebScarab载入代理日志文件
16  -m 批量模式        从给定的文本文件扫描多个目标地址
17  -r 请求模式        从文件中载入http请求
18  -g 谷歌傻瓜模式    从谷歌搜索地址做为目标地址
19  -c 配置模式        从ini配置文件载入目标地址
20  请求：
21
22  下面的选项是用来详细说明如何连接目标地址
23  --method=方法      强制使用指定的方式进行连接，例如 PUT
24  --data=数据        通过POST发送数据字符串，例如：--data="id=1"
25  --param-del=参数分割 参数分割字符，例如：&
26  --cookie=COOKIE    HTTP Cookie 头的值 例如：PHPSESSID=a8d127e..
27  --cookie-del=COO..  cookie分割字符，例如：;
28  --load-cookies=L..  从文件载入cookie值
29  --drop-set-cookie   忽略响应数据中的 Set-Cookie，即使用响应cookie
30  --user-agent=AGENT  设置HTTP User-Agent 的值
31  --random-agent      使用随机 User-Agent 的值
32  --host=HOST        设置 HTTP Host 的值
33
```

```

34 --referer=REFERER 设置 HTTP Referer 的值
35 -H HEADER, --hea.. 设置拓展头 例如: X-Forwarded-For: 127.0.0.1
36 --headers=HEADERS 设置多个HTTP头 例如: Accept-Language: fr\nETag: 123
37 --auth-type=AUTH.. 设置HTTP认证类型 (Basic, Digest, NTLM 或 PKI)
38 --auth-cred=AUTH.. 设置HTTP认证账密 例如: name:password
39 --auth-file=AUTH.. 设置PEM私钥证书文件
40 --ignore-code=IG.. 忽略HTTP错误码 例如: 401
41 --ignore-proxy 忽略系统的代理设置
42 --ignore-redirects 忽略重定向尝试
43 --ignore-timeouts 忽略连接超时
44 --proxy=PROXY 使用代理连接目标地址
45 --proxy-cred=PRO.. 使用代理进行HTTP认证 例如: name:password
46 --proxy-file=PRO.. 从文件中载入代理列表
47 --tor 使用洋葱匿名网络
48 --tor-port=TORPORT 设置洋葱匿名代理的非默认端口
49 --tor-type=TORTYPE 设置洋葱匿名代理的类型 例如: HTTP, SOCKS4 或 SOCKS5
(默认)
50 --check-tor 检查洋葱匿名代理网络是否可用
51 --delay=DELAY 设置两次请求之间的延时, 单位: 秒
52 --timeout=TIMEOUT 设置连接目标地址超时时间 (默认30秒)
53 --retries=RETRIES 设置连接超时重试次数 (默认3次)
54 --randomize=RPARAM 对给定的请求参数值进行随机化
55 --safe-url=SAFEURL 设置在测试目标地址前访问的安全链接
56 --safe-post=SAFE.. 设置安全链接POST发送的数据
57 --safe-req=SAFER.. 从文件中载入安全链接列表
58 --safe-freq=SAFE.. 设置两次注入测试前访问安全链接的次数
59 --skip-urlencode 跳过对攻击载荷的URL编码
60 --csrf-token=CSR.. 保存反CSRF令牌
61 --csrf-url=CSRFURL 提取CSRF令牌的地址
62 --force-ssl 强制使用 SSL/HTTPS
63 --hpp 使用HTTP参数污染
64 --eval=EVALCODE 请求前使用自定义python脚本 例如:
65 import hashlib;
66 id2=hashlib.md5(id).hexdigest()
68 优化选项:
69 下面的选项是用来优化sqlmap的性能
70 -o 打开所有优化选项开关
72 --predict-output 预测常见查询输出
73 --keep-alive 使用 HTTP(s) 持久化连接
74 --null-connection 只检测响应数据长度, 不检测响应内容
75 --threads=THREADS 设置最大运行线程 (默认1线程)
76 注入选项:
77 下面的选项用来指定注入测试的定制参数和篡改脚本
78
79 -p TESTPARAMETER 设置要注入的参数
82 --skip=SKIP 设置要跳过注入的参数
83 --skip-static 设置跳过静态参数
84 --param-exclude=.. 对要注入参数进行正则匹配 例如: ses
85 --dbms=DBMS 指定注入地址的后台数据库名称
86 --dbms-cred=DBMS.. 指定数据库认证账密 例如: user:password

```

```

87  --os=OS          指定注入地址的操作系统
88  --invalid-bignum 对注入参数使用超大数字使其失效
89  --invalid-logical 对注入参数使用逻辑运算使其失效
90  --invalid-string 对注入参数使用随机字符串使其失效
91  --no-cast        关闭攻击载荷的生成器
92  --no-escape      关闭字符逃逸的生成器
93  --prefix=PREFIX 攻击载荷的前缀
94  --suffix=SUFFIX 攻击载荷的后缀
95  --tamper=TAMPER 指定攻击载荷的篡改脚本
96  检测选项:
97
98  下面的选项用来定制检测
99
100 --level=LEVEL    指定注入测试级别 例如: 1-5, 默认 1
101 --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
102 --string=STRING  指定攻击载荷执行成功返回的字符串
103 --not-string=NOT.. 指定攻击载荷执行失败返回的字符串
104 --regexp=REGEXP  指定攻击载荷执行成功匹配的正则表达式
105 --code=CODE      指定攻击载荷执行成功返回的HTTP状态码
106 --text-only      设置只检测返回文本来确定攻击载荷执行情况
107 --titles         设置检测返回页面标题确定攻击载荷执行情况
108 技术选项:
109
110 下面选项用来指定参数来调整指定的注入测试选项
111
112 --technique=TECH  开启定制 (default "BEUSTQ")
113 --time-sec=TIMESEC 指定目标数据库响应时间 (默认5秒)
114 --union-cols=UCOLS 指定联合查询注入的列范围
115 --union-char=UCHAR 指定联合查询猜测列数量最大长度
116 --union-from=UFROM 指定联合查询使用的表
117 --dns-domain=DNS.. 指定DNS外带的解析地址
118 --second-url=SEC.. 指定二次注入的结果页面
119 --second-req=SEC.. 指定二次注入的结果页面列表文件
120 指纹选项:
121
122 -f, --fingerprint 使用常见数据库指纹识别
123 枚举选项:
124
125 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
126 运行自己的SQL语句
127
128 -a, --all          检索所有内容
129 -b, --banner       检索数据库欢迎信息
130 --current-user     检索数据库的当前用户
131 --current-db       检索当前使用的数据库名称
132 --hostname         检索数据库计算机名称
133 --is-dba           检测当前用户是否为数据库管理员
134 --users            枚举数据库的所有用户
135 --passwords        枚举数据库的所有用户密码哈希值
136 --privileges        枚举数据库的所有用户权限
137 --roles            枚举数据库的所有用户角色
138 --dbs              枚举数据库的所有数据库
139 --tables           枚举数据库的所有表
140 --columns          枚举数据库的所有列
141 --schema           枚举数据库汇总数据
142 --count            检索数据库的记录总数

```

```

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

```

```

202 --reg-data=REGDATA 设置注册表的键数据
203 --reg-type=REGTYPE 设置注册表的键类型
205 公共选项：
206 下面的选项用来设置公共参数
207 -s SESSIONFILE 载入测试会话文件
208 -t TRAFFICFILE 记录所有的HTTP测试结果至文本文件
209 --answers=ANSWERS 设置默认回应 例如 quit=N, follow=N
210 --base64=BASE64P.. 设置参数包含base64数据
211 --batch 静默执行，使用默认选项进行
212 --binary-fields=.. 返回结果包含二进制数据
213 --check-internet 进行注入测试前，检查网络联通情况
214 --crawl=CRAWLDEPTH 对指定地址爬虫测试
215 --crawl-exclude=.. 对匹配正则表达式的页面地址进行爬虫测试
216 --csv-del=CSVDEL 设置csv格式的分割符
217 --charset=CHARSET 设置盲注测试字符集 例如：0123456789abcdef
218 --dump-format=DU.. 对转储文件进行转换 例如：CSV(默认)，HTML 或SQLITE
219 --encoding=ENCOD.. 设置检索时的字符集 例如：GBK
220 --eta 显示输出耗时
221 --flush-session 刷新当前目标地址的会话
222 --forms 对目标地址提交表单测试
223 --fresh-queries 忽略已缓存的查询结果
224 --har=HARFILE 保存所有HTTP响应至HAR文件
225 --hex 检索返回数据时使用16进制
226 --output-dir=OUT.. 自定义输出文件路径
227 --parse-errors 显示页面上的数据库错误
228 --preprocess=PRE.. 使用指定脚本提交请求
229 --postprocess=PO.. 使用指定脚本处理请求响应
230 --repair 转储未知字符时，使用的替换字符
231 --save=SAVECONFIG 将当前的配置保存至配置文件
232 --scope=SCOPE 使用正则表达式匹配代理地址列表
233 --test-filter=TE.. 选择标题且(或)为指定字符串的攻击载荷
234 --test-skip=TEST.. 忽略标题且(或)为指定字符串的攻击载荷
235 --update 更新 sqlmap
236
237 其他选项：
238
239 -z MNEMONICS 使用助记符 例如：flu,bat,ban,tec=EU
240 --alert=ALERT 注测测试成功执行的本地系统命令
241 --beep 注入点测试成功主板蜂鸣
242 --cleanup 使用自定义函数情况数据库
243 --dependencies 检查sqlmap的组件完整性
244 --disable-coloring 关闭彩色输出
245 --gpage=GOOGLEPAGE 谷歌傻瓜式注入扫描的页数
246 --identify-waf Make a thorough testing for a WAF/IPS protection
247 --list-tampers 显示篡改脚本列表
248 --mobile 使用手机UA
249 --offline 离线模式
250 --purge 安全卸载所有sqlmap内容
251 --skip-waf 放弃测试具有启发式WAF保护的地址
252 --smart 检测是否时启发式WAF保护
253 --sqlmap-shell 反弹sqlmap的shell

```

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

---

CTFshow-大菜鸡 于 2020-11-14 夜完成

