参考：
http://www.youknowi.xin/2018/05/%e4%ba%94%e6%9c%88%e6%8f%90%e5%89%8d%e6%80%bb%e7%bb%93%e7%af%87windowssqlmap-tamper-%e4%ba%86%e8%a7%a3/

sqlmap-tamper
apostrophemask.py 用 UTF-8 全角字符替换单引号字符 all
%EF%BC%871%EF%BC%87
apostrophenullencode.py 用非法双字节 unicode 字符替换单引号字符 MySQL 4, 5.0 and 5.5 oracle 10g postgresql 8.3 8.4 9.0
1 AND '1'='1″ 1 AND %00%271%00%27=%00%271
appendnullbyte.py 在 payload 末尾添加空字符编码 Microsoft Access
Example: ('1 AND 1=1') '1 AND 1=1%00'
base64encode.py 对给定的 payload 全部字符使用 Base64 编码 all
between.py 分别用“NOT BETWEEN 0 AND #”替换大于号“>”，“BETWEEN # AND #”替换等于号“=”
bluecoat.py 在 SQL 语句之后用有效的随机空白符替换空格符，随后用“LIKE”替换等于号“=”
SELECT id FROM users where id = 1
SELECT%09id FROM users where id LIKE 1
chardoubleencode.py 对给定的 payload 全部字符使用双重 URL 编码（不处理已经编码的字符）
charencode.py 对给定的 payload 全部字符使用 URL 编码（不处理已经编码的字符）
charunicodeencode.py 对给定的 payload 的非编码字符使用 Unicode URL 编码（不处理已经编码的字符）
concat2concatws.py 用“CONCAT_WS(MID(CHAR(0), 0, 0), A, B)”替换像“CONCAT(A, B)”的实例
equaltolike.py 用“LIKE”运算符替换全部等于 Microsoft SQL Server 2005 MySQL 4, 5.0 and 5.5
id=1 id like 1
greatest.py 用“GREATEST”函数替换大于号“>” MySQL 4, 5.0 and 5.5 oracle 10g postgresql 8.3 8.4 9.0
1 AND A > B 1 AND GREATEST(A,B+1)=A
halfversionedmorekeywords.py 在每个关键字之前添加 MySQL 注释 MySQL < 5.1 MySQL 4.0.18, 5.0.22
ifnull2ifisnull.py 用“IF(ISNULL(A), B, A)”替换像“IFNULL(A, B)”的实例 MySQL SQLite (possibly) SAP MaxDB (possibly)
绕过对 ifnull 的过滤
lowercase.py 用小写值替换每个关键字字符
modsecurityversioned.py 用注释包围完整的查询 mysql
modsecurityzeroversioned.py 用当中带有数字零的注释包围完整的查询
1 AND 2>1-- 1 /*!00000AND 2>1*/--
multiplespaces.py 在 SQL 关键字周围添加多个空格

nonrecursivereplacement.py 用 representations 替换预定义 SQL 关键字，适用于过滤器
双重查询语句。取代 predefined SQL 关键字 with 表示 suitable for 替代(例如 .replace(“SELECT”、”“)) filters
('1 UNION SELECT 2--')
1 UNIOUNIONN SELESELECTCT 2-
overlongutf8.py 转换给定的 payload 当中的所有字符
percentage.py 在每个字符之前添加一个百分号
asp 允许每个字符前面添加一个%号
randomcase.py 随机转换每个关键字字符的大小写
randomcomments.py 向 SQL 关键字中插入随机注释
用/**/分割 sql 关键字 INSERT IN//S//ERT
securesphere.py 添加经过特殊构造的字符串
sp_password.py 向 payload 末尾添加“sp_password” for automatic obfuscation from DBMS logs
space2comment.py 用“/**/”替换空格符
space2dash.py 用破折号注释符“--”其次是一个随机字符串和一个换行符替换空格符 mssql sqlite
绕过过滤‘=’ 替换空格字符(”)，(’ - ‘)后跟一个破折号注释，一个随机字符串和一个新行(’ n’)
1 AND 9227=9227 1--nVNaVoPYeva%0AAND--ngNvzqu%0A9227=9227
space2hash.py 用磅注释符“#”其次是一个随机字符串和一个换行符替换空格符 mysql mysql4.0 mysql5.0
space2morehash.py 用磅注释符“#”其次是一个随机字符串和一个换行符替换空格符 MySQL >= 5.1.13
space2mssqlblank.py 用一组有效的备选字符集当中的随机空白符替换空格符 sql service
space2mssqlhash.py 用磅注释符“#”其次是一个换行符替换空格符 mssql mysql
space2mysqlblank.py 用一组有效的备选字符集当中的随机空白符替换空格符 mysql
space2mysqldash.py 用破折号注释符“--”其次是一个换行符替换空格符 这是 mysql 的
space2plus.py 用加号“+”替换空格符 all
space2randomblank.py 用一组有效的备选字符集当中的随机空白符替换空格符 all
unionalltounion.py 用“UNION SELECT”替换“UNION ALL SELECT” all
unmagicquotes.py 用一个多字节组合%bf%27 和末尾通用注释一起替换空格符 宽字节绕过 GPC addslashes
varnish.py 添加一个 HTTP 头“X-originating-IP”来绕过 WAF
versionedkeywords.py 用 MySQL 注释包围每个非函数关键字
好像很有用的样子 versionedmorekeywords.py 用 MySQL 注释包围每个关键字
xforwardedfor.py 添加一个伪造的 HTTP 头“X-Forwarded-For”来绕过 WAF