专注APT攻击与防御
https://micropoor.blogspot.com/

由于Sqlmap 是常用工具之一，所以本篇的篇幅较长，详解一次所有参数。

sqlmap参数详解：

Usage: python sqlmap.py [options]

Options（选项）:

-h, --help Show basic help message and exit **展示帮助文档 参数**
-hh Show advanced help message and exit **展示详细帮助文档 参数**
--version Show program's version number and exit **显示程序的版本号**
-v VERBOSE Verbosity level: 0-6 (default 1) **详细级别：0-6（默认为1）**

Target（目标）:

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

-d DIRECT Connection string for direct database connection **指定具体数据库**
-u URL, --url=URL Target URL (e.g. "http://www.site.com/vuln.php?id=1") **目标URL**
-l LOGFILE Parse target(s) from Burp or WebScarab proxy log file 解析目标(s)从Burp或WebScarab代理日志文件
-x SITEMAPURL Parse target(s) from remote sitemap(.xml) file 解析目标(s)从远程站点地图文件(.xml)
-m BULKFILE Scan multiple targets given in a textual file 扫描文本文件中给出的多个目标
-r REQUESTFILE Load HTTP request from a file **从本地文件加载HTTP请求 ，多用于post注入。**
-g GOOGLEDORK Process Google dork results as target URLs **处理Google的结果作为目标URL。**

-c CONFIGFILE Load options from a configuration INI file 从INI配置文件中加载选项。

Request（请求）：

These options can be used to specify how to connect to the target URL 这些选项可以用来指定如何连接到目标URL。

--method=METHOD Force usage of given HTTP method (e.g. PUT) 强制使用给定的HTTP方法（e.g. PUT）

--data=DATA Data string to be sent through POST **通过POST发送的数据字符串**

--param-del=PARA.. Character used for splitting parameter values 用于拆分参数值的字符

--cookie=COOKIE HTTP Cookie header value HTTP Cookie头的值

--cookie-del=COO.. Character used for splitting cookie values 用于分割Cookie值的字符

--load-cookies=L.. File containing cookies in Netscape/wget format 包含Netscape / wget格式的cookie的文件

--drop-set-cookie Ignore Set-Cookie header from response 从响应中忽略Set-Cookie头

--user-agent=AGENT HTTP User-Agent header value 指定 HTTP User - Agent头

--random-agent Use randomly selected HTTP User-Agent header value 使用随机选定的HTTP User - Agent头

--host=HOST HTTP Host header value HTTP主机头值

--referer=REFERER HTTP Referer header value 指定 HTTP Referer头

-H HEADER, --hea.. Extra header (e.g. "X-Forwarded-For: 127.0.0.1") 额外header

--headers=HEADERS Extra headers (e.g. "Accept-Language: fr\nETag: 123") 额外header

--auth-type=AUTH.. HTTP authentication type (Basic, Digest, NTLM or PKI) HTTP认证类型(Basic, Digest, NTLM or PKI)

--auth-cred=AUTH.. HTTP authentication credentials (name:password) HTTP认证凭证(name:password)

--auth-file=AUTH.. HTTP authentication PEM cert/private key file HTTP认证PEM认证/私钥文件

--ignore-401 Ignore HTTP Error 401 (Unauthorized) **忽略HTTP错误401**

--proxy=PROXY Use a proxy to connect to the target URL 使用代理连接到目标网址

--proxy-cred=PRO.. Proxy authentication credentials (name:password) 代理认证证书(name:password)

--proxy-file=PRO.. Load proxy list from a file 从文件中加载代理列表

--ignore-proxy Ignore system default proxy settings 忽略系统默认代理设置

--tor Use Tor anonymity network 使用Tor匿名网络

--tor-port=TORPORT Set Tor proxy port other than default 设置Tor代理端口而不是默认值

--tor-type=TORTYPE Set Tor proxy type (HTTP (default), SOCKS4 or SOCKS5) 设置Tor代理类型

--check-tor Check to see if Tor is used properly 检查Tor是否正确使用

--delay=DELAY Delay in seconds between each HTTP request 每个HTTP请求之间的延迟（秒）

--timeout=TIMEOUT Seconds to wait before timeout connection (default 30) 秒超时连接前等待（默认30）

--retries=RETRIES Retries when the connection timeouts (default 3) 连接超时时重试（默认值3）

--randomize=RPARAM Randomly change value for given parameter(s) 随机更改给定参数的值(s)

--safe-url=SAFEURL URL address to visit frequently during testing 在测试期间频繁访问的URL地址

--safe-post=SAFE.. POST data to send to a safe URL POST数据发送到安全URL

--safe-req=SAFER.. Load safe HTTP request from a file 从文件加载安全HTTP请求

--safe-freq=SAFE.. Test requests between two visits to a given safe URL 在两次访问给定安全网址之间测试请求

--skip-urlencode Skip URL encoding of payload data 跳过有效载荷数据的URL编码

--csrf-token=CSR.. Parameter used to hold anti-CSRF token 参数用于保存anti-CSRF令牌

--csrf-url=CSRFURL URL address to visit to extract anti-CSRF token 提取anti-CSRF URL地址访问令牌

--force-ssl Force usage of SSL/HTTPS 强制使用SSL / HTTPS

--hpp Use HTTP parameter pollution method 使用HTTP参数pollution的方法

--eval=EVALCODE Evaluate provided Python code before the request (e.g. 评估请求之前提供Python代码

"import hashlib;id2=hashlib.md5(id).hexdigest()")

Optimization（优化）:

These options can be used to optimize the performance of sqlmap 这些选项可用于优化sqlmap的性能

-o Turn on all optimization switches 开启所有优化开关

--predict-output Predict common queries output 预测常见的查询输出

--keep-alive Use persistent HTTP(s) connections 使用持久的HTTP（S）连接

--null-connection Retrieve page length without actual HTTP response body 从没有实际的HTTP响应体中检索页面长度

--threads=THREADS Max number of concurrent HTTP(s) requests (default 1) 最大的HTTP（S）请求并发量（默认为1）

Injection（注入）:

These options can be used to specify which parameters to test for,

provide custom injection payloads and optional tampering scripts

这些选项可以用来指定测试哪些参数， 提供自定义的注入payloads和可选篡改脚本。

-p TESTPARAMETER Testable parameter(s) 可测试的参数（S）

--skip=SKIP Skip testing for given parameter(s) 跳过对给定参数的测试

--skip-static Skip testing parameters that not appear to be dynamic 跳过测试不显示为动态的参数

--param-exclude=.. Regexp to exclude parameters from testing (e.g. "ses") 使用正则表达式排除参数进行测试（e.g. "ses"）

--dbms=DBMS Force back-end DBMS to this value 强制后端的DBMS为此值

--dbms-cred=DBMS.. DBMS authentication credentials (user:password) DBMS认证凭证(user:password)

--os=OS Force back-end DBMS operating system to this value 强制后端的DBMS操作系统为这个值

--invalid-bignum Use big numbers for invalidating values 使用大数字使值无效

--invalid-logical Use logical operations for invalidating values 使用逻辑操作使值无效

--invalid-string Use random strings for invalidating values 使用随机字符串使值无效

--no-cast Turn off payload casting mechanism 关闭有效载荷铸造机制

--no-escape Turn off string escaping mechanism 关闭字符串转义机制

--prefix=PREFIX Injection payload prefix string 注入payload字符串前缀

--suffix=SUFFIX Injection payload suffix string 注入payload字符串后缀

--tamper=TAMPER Use given script(s) for tampering injection data 使用给定的脚本（S）篡改注入数据

Detection（检测）:

These options can be used to customize the detection phase 这些选项可以用来指定在SQL盲注时如何解析和比较HTTP响应页面的内容。

--level=LEVEL Level of tests to perform (1-5, default 1) 执行测试的等级（1-5，默认为1）
--risk=RISK Risk of tests to perform (1-3, default 1) 执行测试的风险（0-3，默认为1）
--string=STRING String to match when query is evaluated to True 查询时有效时在页面匹配字符串
--not-string=NOT.. String to match when query is evaluated to False 当查询求值为无效时匹配的字符串
--regexp=REGEXP Regexp to match when query is evaluated to True 查询时有效时在页面匹配正则表达式
--code=CODE HTTP code to match when query is evaluated to True 当查询求值为True时匹配的HTTP代码
--text-only Compare pages based only on the textual content 仅基于在文本内容比较网页
--titles Compare pages based only on their titles 仅根据他们的标题进行比较

Techniques（技巧）:

These options can be used to tweak testing of specific SQL injection techniques
这些选项可用于调整具体的SQL注入测试。

--technique=TECH SQL injection techniques to use (default "BEUSTQ") SQL注入技术测试（默认BEUST）
--time-sec=TIMESEC Seconds to delay the DBMS response (default 5) DBMS响应的延迟时间（默认为5秒）
--union-cols=UCOLS Range of columns to test for UNION query SQL injection 定列范围用于测试UNION查询注入
--union-char=UCHAR Character to use for bruteforcing number of columns 用于暴力猜解列数的字符

--union-from=UFROM Table to use in FROM part of UNION query SQL injection 要在UNION查询SQL注入的FROM部分使用的表

--dns-domain=DNS.. Domain name used for DNS exfiltration attack 域名用于DNS漏出攻击

--second-order=S.. Resulting page URL searched for second-order response 生成页面的URL搜索为second-order响应

Fingerprint（指纹）:

-f, --fingerprint Perform an extensive DBMS version fingerprint 执行检查广泛的DBMS版本指纹

Enumeration（枚举）:

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

这些选项可以用来列举后端数据库管理系统的信息、表中的结构和数据。此外，您还可以运行您自己的SQL语句。

-a, --all Retrieve everything 检索一切

-b, --banner Retrieve DBMS banner 检索数据库管理系统的标识

--current-user Retrieve DBMS current user 检索数据库管理系统的标识

--current-db Retrieve DBMS current database 检索数据库管理系统当前数据库

--hostname Retrieve DBMS server hostname 检索数据库服务器的主机名

--is-dba Detect if the DBMS current user is DBA 检测DBMS当前用户是否DBA

--users Enumerate DBMS users 枚举数据库管理系统用户

--passwords Enumerate DBMS users password hashes 枚举数据库管理系统用户密码哈希

--privileges Enumerate DBMS users privileges 枚举数据库管理系统用户的权限

--roles Enumerate DBMS users roles 枚举数据库管理系统用户的角色

--dbs Enumerate DBMS databases 枚举数据库管理系统数据库

--tables Enumerate DBMS database tables 枚举的DBMS数据库中的表

--columns Enumerate DBMS database table columns 枚举DBMS数据库表列

--schema Enumerate DBMS schema 枚举数据库架构

--count Retrieve number of entries for table(s) 检索表的条目数

--dump Dump DBMS database table entries 转储数据库管理系统的数据库中的表项

--dump-all Dump all DBMS databases tables entries 转储数据库管理系统的数据库中的表项

--search Search column(s), table(s) and/or database name(s) 搜索列（S），表（S）和/或数据库名称（S）

--comments Retrieve DBMS comments 检索数据库的comments(注释、评论)

-D DB DBMS database to enumerate 要进行枚举的数据库名

-T TBL DBMS database table(s) to enumerate 要进行枚举的数据库表

-C COL DBMS database table column(s) to enumerate 要进行枚举的数据库列

-X EXCLUDECOL DBMS database table column(s) to not enumerate 要不进行枚举的数据库列

-U USER DBMS user to enumerate 用来进行枚举的数据库用户

--exclude-sysdbs Exclude DBMS system databases when enumerating tables 枚举表时排除系统数据库

--pivot-column=P.. Pivot column name 主列名称

--where=DUMPWHERE Use WHERE condition while table dumping 使用WHERE条件进行表转储

--start=LIMITSTART First query output entry to retrieve 第一个查询输出进入检索

--stop=LIMITSTOP Last query output entry to retrieve 最后查询的输出进入检索

--first=FIRSTCHAR First query output word character to retrieve 第一个查询输出字的字符检索

--last=LASTCHAR Last query output word character to retrieve 最后查询的输出字字符检索

--sql-query=QUERY SQL statement to be executed 要执行的SQL语句

--sql-shell Prompt for an interactive SQL shell 提示交互式SQL的shell

--sql-file=SQLFILE Execute SQL statements from given file(s) 从给定文件执行SQL语句

Brute force（蛮力）:

These options can be used to run brute force checks 这些选项可以被用来运行蛮力检查。

--common-tables Check existence of common tables 检查存在共同表

--common-columns Check existence of common columns 检查存在共同列

User-defined function injection（用户自定义函数注入）:

These options can be used to create custom user-defined functions 这些选项可以用来创建用户自定义函数。

--udf-inject Inject custom user-defined functions 注入用户自定义函数

--shared-lib=SHLIB Local path of the shared library 共享库的本地路径

File system access（访问文件系统）:

These options can be used to access the back-end database management system underlying file system

这些选项可以被用来访问后端数据库管理系统的底层文件系统。

--file-read=RFILE Read a file from the back-end DBMS file system 从后端的数据库管理系统文件系统读取文件

--file-write=WFILE Write a local file on the back-end DBMS file system 编辑后端的数据库管理系统文件系统上的本地文件

--file-dest=DFILE Back-end DBMS absolute filepath to write to 后端的数据库管理系统写入文件的绝对路径

Operating system access（操作系统访问）:

These options can be used to access the back-end database management system underlying operating system
这些选项可以用于访问后端数据库管理系统的底层操作系统。

--os-cmd=OSCMD Execute an operating system command 执行操作系统命令

--os-shell Prompt for an interactive operating system shell 交互式的操作系统的shell

--os-pwn Prompt for an OOB shell, Meterpreter or VNC 获取一个OOB shell，meterpreter或VNC

--os-smbrelay One click prompt for an OOB shell, Meterpreter or VNC 一键获取一个OOB shell，meterpreter或VNC

--os-bof Stored procedure buffer overflow exploitation 存储过程缓冲区溢出利用

--priv-esc Database process user privilege escalation 数据库进程用户权限提升

--msf-path=MSFPATH Local path where Metasploit Framework is installed Metasploit Framework本地的安装路径

--tmp-path=TMPPATH Remote absolute path of temporary files directory 远程临时文件目录的绝对路径

Windows registry access（Windows注册表访问）:

These options can be used to access the back-end database management system Windows registry

这些选项可以被用来访问后端数据库管理系统Windows注册表。

--reg-read Read a Windows registry key value 读一个Windows注册表项值
--reg-add Write a Windows registry key value data 写一个Windows注册表项值数据
--reg-del Delete a Windows registry key value 删除Windows注册表键值
--reg-key=REGKEY Windows registry key Windows注册表键
--reg-value=REGVAL Windows registry key value Windows注册表项值
--reg-data=REGDATA Windows registry key value data Windows注册表键值数据
--reg-type=REGTYPE Windows registry key value type Windows注册表项值类型

General（一般）:

These options can be used to set some general working parameters 这些选项可以用来设置一些一般的工作参数。

-s SESSIONFILE Load session from a stored (.sqlite) file 保存和恢复检索会话文件的所有数据
-t TRAFFICFILE Log all HTTP traffic into a textual file 记录所有HTTP流量到一个文本文件中
--batch Never ask for user input, use the default behaviour 从不询问用户输入，使用所有默认配置。
--binary-fields=.. Result fields having binary values (e.g. "digest") 具有二进制值的结果字段
--charset=CHARSET Force character encoding used for data retrieval 强制用于数据检索的字符编码
--crawl=CRAWLDEPTH Crawl the website starting from the target URL 从目标网址开始抓取网站
--crawl-exclude=.. Regexp to exclude pages from crawling (e.g. "logout") 正则表达式排除网页抓取

--csv-del=CSVDEL Delimiting character used in CSV output (default ",") 分隔CSV输出中使用的字符

--dump-format=DU.. Format of dumped data (CSV (default), HTML or SQLITE) 转储数据的格式

--eta Display for each output the estimated time of arrival 显示每个输出的预计到达时间

--flush-session Flush session files for current target 刷新当前目标的会话文件

--forms Parse and test forms on target URL 在目标网址上解析和测试表单

--fresh-queries Ignore query results stored in session file 忽略在会话文件中存储的查询结果

--hex Use DBMS hex function(s) for data retrieval 使用DBMS hex函数进行数据检索

--output-dir=OUT.. Custom output directory path 自定义输出目录路径

--parse-errors Parse and display DBMS error messages from responses 解析和显示响应中的DBMS错误消息

--save=SAVECONFIG Save options to a configuration INI file 保存选项到INI配置文件

--scope=SCOPE Regexp to filter targets from provided proxy log 使用正则表达式从提供的代理日志中过滤目标

--test-filter=TE.. Select tests by payloads and/or titles (e.g. ROW) 根据有效负载和/或标题(e.g. ROW)选择测试

--test-skip=TEST.. Skip tests by payloads and/or titles (e.g. BENCHMARK) 根据有效负载和/或标题跳过测试（e.g. BENCHMARK）

--update Update sqlmap 更新SqlMap

Miscellaneous（杂项）:

-z MNEMONICS Use short mnemonics (e.g. "flu,bat,ban,tec=EU") 使用简短的助记符

--alert=ALERT Run host OS command(s) when SQL injection is found 在找到SQL注入时运行主机操作系统命令

--answers=ANSWERS Set question answers (e.g. "quit=N,follow=N") 设置问题答案

--beep Beep on question and/or when SQL injection is found 发现SQL注入时提醒

--cleanup Clean up the DBMS from sqlmap specific UDF and tables SqlMap具体的UDF和表清理DBMS

--dependencies Check for missing (non-core) sqlmap dependencies 检查是否缺少（非内核）sqlmap依赖关系

--disable-coloring Disable console output coloring 禁用控制台输出颜色

--gpage=GOOGLEPAGE Use Google dork results from specified page number 使用Google dork结果指定页码

--identify-waf Make a thorough testing for a WAF/IPS/IDS protection 对WAF / IPS / IDS保护进行全面测试

--skip-waf Skip heuristic detection of WAF/IPS/IDS protection 跳过启发式检测WAF / IPS / IDS保护

--mobile Imitate smartphone through HTTP User-Agent header 通过HTTP User-Agent标头模仿智能手机

--offline Work in offline mode (only use session data) 在离线模式下工作（仅使用会话数据）

--page-rank Display page rank (PR) for Google dork results Google dork结果显示网页排名（PR）

--purge-output Safely remove all content from output directory 安全地从输出目录中删除所有内容

--smart Conduct thorough tests only if positive heuristic(s) 只有在正启发式时才进行彻底测试

--sqlmap-shell Prompt for an interactive sqlmap shell 提示交互式sqlmap shell

--wizard Simple wizard interface for beginner users 给初级用户的简单向导界面

- Micropoor