链滴

SQLMAP 注入参数详解

作者：General

原文链接：https://ld246.com/article/1604623909529

来源网站：链滴

-technique

拓展：sql注入工具sqlmap使用参数说明

Options（选项）

--version 显示程序的版本号并退出
-h, --help 显示此帮助消息并退出
-v VERBOSE 详细级别：0-6（默认为1）
Target（目标）：以下至少需要设置其中一个选项，设置目标URL。
-d DIRECT 直接连接到数据库。
-u URL, --url=URL 目标URL。
-l LIST 从Burp或WebScarab代理的日志中解析目标。
-r REQUESTFILE 从一个文件中载入HTTP请求。
-g GOOGLEDORK 处理Google dork的结果作为目标URL。
-c CONFIGFILE 从INI配置文件中加载选项。

Request（请求）

这些选项可以用来指定如何连接到目标URL。
--data=DATA 通过POST发送的数据字符串
--cookie=COOKIE HTTP Cookie头
--cookie-urlencode URL 编码生成的cookie注入
--drop-set-cookie 忽略响应的Set - Cookie头信息
--user-agent=AGENT 指定 HTTP User - Agent头
--random-agent 使用随机选定的HTTP User - Agent头
--referer=REFERER 指定 HTTP Referer头
--headers=HEADERS 换行分开，加入其他的HTTP头
--auth-type=ATYPE HTTP身份验证类型（基本，摘要或NTLM）(Basic, Digest or NTLM)
--auth-cred=ACRED HTTP身份验证凭据（用户名:密码）
--auth-cert=ACERT HTTP认证证书（key_file，cert_file）
--proxy=PROXY 使用HTTP代理连接到目标URL
--proxy-cred=PCRED HTTP代理身份验证凭据（用户名：密码）
--ignore-proxy 忽略系统默认的HTTP代理
--delay=DELAY 在每个HTTP请求之间的延迟时间，单位为秒
--timeout=TIMEOUT 等待连接超时的时间（默认为30秒）
--retries=RETRIES 连接超时后重新连接的时间（默认3）
--scope=SCOPE 从所提供的代理日志中过滤器目标的正则表达式
--safe-url=SAFURL 在测试过程中经常访问的url地址

--safe-freq=SAFREQ 两次访问之间测试请求，给出安全的URL

Optimization（优化）

这些选项可用于优化SqlMap的性能。

-o 开启所有优化开关

--predict-output 预测常见的查询输出

--keep-alive 使用持久的HTTP（S）连接

--null-connection 从没有实际的HTTP响应体中检索页面长度

--threads=THREADS 最大的HTTP（S）请求并发量（默认为1）

Injection（注入）

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 可测试的参数（S）

--dbms=DBMS 强制后端的DBMS为此值

--os=OS 强制后端的DBMS操作系统为这个值

--prefix=PREFIX 注入payload字符串前缀

--suffix=SUFFIX 注入payload字符串后缀

--tamper=TAMPER 使用给定的脚本（S）篡改注入数据

Detection（检测）

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 执行测试的等级（1-5，默认为1）

--risk=RISK 执行测试的风险（0-3，默认为1）

--string=STRING 查询时有效时在页面匹配字符串

--regexp=REGEXP 查询时有效时在页面匹配正则表达式

--text-only 仅基于在文本内容比较网页

Techniques（技巧）

这些选项可用于调整具体的SQL注入测试。

--technique=TECH SQL注入技术测试（默认BEUST）

--time-sec=TIMESEC DBMS响应的延迟时间（默认为5秒）

--union-cols=UCOLS 定列范围用于测试UNION查询注入

--union-char=UCHAR 用于暴力猜解列数的字符

Fingerprint（指纹）

-f, --fingerprint 执行检查广泛的DBMS版本指纹

Enumeration（枚举）

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SQL语句。

-b, --banner 检索数据库管理系统的标识

--current-user 检索数据库管理系统当前用户

--current-db 检索数据库管理系统当前数据库

--is-dba 检测DBMS当前用户是否DBA

--users 枚举数据库管理系统用户

--passwords 枚举数据库管理系统用户密码哈希

--privileges 枚举数据库管理系统用户的权限

--roles 枚举数据库管理系统用户的角色

--dbs 枚举数据库管理系统数据库

--tables 枚举的DBMS数据库中的表

--columns 枚举DBMS数据库表列

--dump 转储数据库管理系统的数据库中的表项

--dump-all 转储所有的DBMS数据库表中的条目

--search 搜索列（S），表（S）和/或数据库名称（S）

-D DB 要进行枚举的数据库名

-T TBL 要进行枚举的数据库表

-C COL 要进行枚举的数据库列

-U USER 用来进行枚举的数据库用户

--exclude-sysdbs 枚举表时排除系统数据库

--start=LIMITSTART 第一个查询输出进入检索

--stop=LIMITSTOP 最后查询的输出进入检索

--first=FIRSTCHAR 第一个查询输出字的字符检索

--last=LASTCHAR 最后查询的输出字字符检索

--sql-query=QUERY 要执行的SQL语句

--sql-shell 提示交互式SQL的shell

Brute force（蛮力）

这些选项可以被用来运行蛮力检查。

--common-tables 检查存在共同表

--common-columns 检查存在共同列

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

这些选项可以用来创建用户自定义函数。

--udf-inject 注入用户自定义函数
--shared-lib=SHLIB 共享库的本地路径

File system access（访问文件系统）

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 从后端的数据库管理系统文件系统读取文件
--file-write=WFILE 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 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）

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 执行操作系统命令
--os-shell 交互式的操作系统的shell
--os-pwn 获取一个OOB shell，meterpreter或VNC
--os-smbrelay 一键获取一个OOB shell，meterpreter或VNC
--os-bof 存储过程缓冲区溢出利用
--priv-esc 数据库进程用户权限提升
--msf-path=MSFPATH Metasploit Framework本地的安装路径
--tmp-path=TMPPATH 远程临时文件目录的绝对路径

Windows注册表访问

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

General（一般）

这些选项可以用来设置一些一般的工作参数。
-t TRAFFICFILE 记录所有HTTP流量到一个文本文件中
-s SESSIONFILE 保存和恢复检索会话文件的所有数据
--flush-session 刷新当前目标的会话文件
--fresh-queries 忽略在会话文件中存储的查询结果

--eta 显示每个输出的预计到达时间
--update 更新SqlMap
--save file保存选项到INI配置文件
--batch 从不询问用户输入，使用所有默认配置。

Miscellaneous（杂项）

--beep 发现SQL注入时提醒
--check-payload IDS对注入payloads的检测测试
--cleanup SqlMap具体的UDF和表清理DBMS
--forms 对目标URL的解析和测试形式
--gpage=GOOGLEPAGE 从指定的页码使用谷歌dork结果
--page-rank Google dork结果显示网页排名（PR）
--parse-errors 从响应页面解析数据库管理系统的错误消息
--replicate 复制转储的数据到一个sqlite3数据库
--tor 使用默认的Tor（Vidalia/ Privoxy