使用格式: sqlmap [参数]

参数:

-h, --help 显示基本的帮助文档

-hh 显示高级帮助

--version 显示当前版本号

-v VERBOSE Verbosity level: 0-6 (default 1)

目标:

至少要提供这些参数中的一个来定义

参数

-d DIRECT 用于连接数据库的连接字符串

-u URL, --url=URL 目标URL (e.g. "http://www.site.com/vuln.php?id=1")

-l LOGFILE 用Burp 或者 WebScarab解析目标代理文日志

-x SITEMAPURL 远程解析目标网站的路径

-m BULKFILE 扫描文件中的多个目标

-r REQUESTFILE 从文件中加载http地址

-g GOOGLEDORK 用谷歌解析目标

-c CONFIGFILE 从ini的配置文件加载

要求:

这些参数是用来如何连接到目标网站

--method=METHOD 对给定的HTTP方法（例如把武力使用）

--data=DATA 将要发送的数据字符串

--param-del=PARA.. 用于分裂参数值的字符

--cookie=COOKIE HTTP Cookie标头值 cooike注入

--cookie-del=COO.. 用于分割饼干值的字符

--load-cookies=L.. 含Netscape / wget cookies文件格式

--drop-set-cookie 忽略设置的头部信息

--user-agent=AGENT HTTP用户代理标头值

--random-agent 使用随机选择HTTP用户代理标头值

--host=HOST HTTP主机头值

--referer=REFERER HTTP Referer报头值

-H HEADER, --hea.. 额外的头部信息 (e.g. "X-Forwarded-For: 127.0.0.1")

--headers=HEADERS 额外的标题 (e.g. "Accept-Language: fr\nETag: 123")

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

--auth-cred=AUTH.. HTTP认证证书(name:password)

--auth-file=AUTH.. HTTP认证PEM证书/私钥文件

--ignore-401 忽略HTTP 401错误（未授权的）

--proxy=PROXY 使用代理连接到目标网址

--proxy-cred=PRO.. 代理身份验证凭据（名称：密码）

--proxy-file=PRO.. 从文件中加载代理列表

--ignore-proxy 忽略系统默认代理设置

--tor 使用洋葱路由网络

--tor-port=TORPORT 设置洋葱路由的代理端口

--tor-type=TORTYPE 设置Tor代理类型（HTTP、SOCKS4或SOCKS5（默认））

--check-tor 查看洋葱路由的正确使用

--delay=DELAY 每个HTTP请求之间的想应时间

--timeout=TIMEOUT 等待超时连接（默认30）默认为秒

--retries=RETRIES 重试时，连接超时（默认3）

--randomize=RPARAM 给定参数的随机变化值（s）

--safe-url=SAFEURL 在测试过程中经常访问的网址地址

--safe-post=SAFE.. post数据发送到一个安全的网址

--safe-req=SAFER.. 安全HTTP请求从文件加载

--safe-freq=SAFE.. 一个给定的安全地址的两次访问之间的测试请求

--skip-urlencode 跳过有效载荷数据的网址编码

--csrf-token=CSR.. 参数用来举行反CSRF令牌

--csrf-url=CSRFURL URL地址访问提取防CSRF令牌

--force-ssl 使用SSL / HTTPS力

--hpp 使用HTTP参数污染的方法

--eval=EVALCODE Evaluate provided Python code before the request (e.g.

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

优化参数:

这些选项可用于优化性能sqlmap

-o 打开所有的优化开关

--predict-output 普通查询输出预测

--keep-alive 使用持久HTTP（S）连接

--null-connection 检索页面长度没有实际的HTTP响应体

--threads=THREADS 最大并发HTTP请求数（S）（默认为1）

注入:

这些选项可以用来指定要测试的参数，提供自定义注入有效载荷和随意篡改剧本

-p TESTPARAMETER 可检验参数（s）

--skip=SKIP 对给定参数的跳过测试（s）

--skip-static 跳过不出现动态的测试参数

--dbms=DBMS 强制后端数据库管理系统到这个值

--dbms-cred=DBMS.. 数据库管理系统认证证书（用户：密码）

--os=OS 强制后端的数据库管理系统操作系统到这个值

--invalid-bignum 使用大数字无效值

--invalid-logical 使用逻辑操作的无效值

--invalid-string 使用随机字符串无效值

--no-cast 关闭有效载荷模块

--no-escape 关闭字符串逃逸机制

--prefix=PREFIX 注入有效载荷前缀字符串

--suffix=SUFFIX 注入有效载荷后缀字符串

--tamper=TAMPER 用于篡改注入数据的给定脚本

检测:

这些选项可用于自定义检测阶段

--level=LEVEL 要执行的测试水平（1-5，默认为1）

--risk=RISK 要执行的测试的风险（1-3，默认为1）

--string=STRING 当查询评估为真时的字符串匹配

--not-string=NOT.. 当查询评估为假时的字符串匹配

--regexp=REGEXP 正则表达式匹配查询时进行真正的

--code=CODE HTTP代码时匹配的查询表达式为真

--text-only 仅基于文本内容的页面比较

--titles 仅根据他们的标题进行比较

技术:

这些选项可以用来调整特定SQL注入测试技术

--technique=TECH SQL注入技术的使用（默认“beustq”）

--time-sec=TIMESEC 延迟数据库管理系统响应的秒数（默认为5）

--union-cols=UCOLS 为联合查询的SQL注入测试列范围

--union-char=UCHAR 字符使用bruteforcing列数

--union-from=UFROM 表使用从联合查询的SQL注入的一部分

--dns-domain=DNS.. 使用的域名DNS泄露攻击

--second-order=S.. 搜索的第二级响应结果页面的网址

指纹:

-f, --fingerprint 执行广泛的数据库管理系统版本指纹

枚举参数:

这些选项可以用来枚举后端数据库管理系统信息、结构和数据中包含的

平台.此外，你可以运行你自己的SQL语句

-a, --all Retrieve everything

-b, --banner 检索数据库标志

--current-user 检索数据库管理系统当前用户

--current-db 检索数据库

--hostname 检索数据库服务器的主机名

--is-dba 检测当前用户是不是数据库的管理员

--users 枚举数据库用户

--passwords 枚举数据库用户密码的哈希值

--privileges 枚举数据库管理系统用户权限

--roles 枚举数据库管理系统用户角色

--dbs 枚举数据库

--tables 枚举数据库管理系统中的数据库表

--columns 枚举数据库管理中的数据库表列

--schema 枚举数据库架构

--count 搜索表的条目数

--dump 扒裤衩子

--dump-all 扒数据库数毛毛

--search 搜索数据库列和数据库名称

--comments 检测数据库的信息

-D DB 枚举数据库

-T TBL 枚举数据库的表

-C COL 枚举数据库表的列

-X EXCLUDECOL 不枚举的数据库管理系统数据库表

-U USER 数据库用户枚举

--exclude-sysdbs Exclude DBMS system databases when enumerating tables

--pivot-column=P.. 主数据库表名称

--where=DUMPWHERE Use WHERE condition while table dumping

--start=LIMITSTART 查询输出第一个输出条目的检索

--stop=LIMITSTOP 查询最后输出项的检索

--first=FIRSTCHAR 查询第一个输出字字符检索

--last=LASTCHAR 查询最后输出字字符检索

--sql-query=QUERY 要执行的SQL语句

--sql-shell 提示一个SQL shell

--sql-file=SQLFILE 从给定的文件执行SQL语句（S）

暴力破解:

这些选项可以用来运行蛮力测试

--common-tables 检查常见表的存在性

--common-columns 检查公共列的存在

用户定义函数注入:

这些选项可用于创建自定义的用户定义函数

--udf-inject 注入用户自定义的函数

--shared-lib=SHLIB 共享库的本地路径

文件系统访问:

这些选项可用于访问后台数据库管理系统的底层文件系统

--file-read=RFILE 从后台的数据库管理系统文件系统中读取一个文件

--file-write=WFILE 在后台的数据库管理系统文件系统上写一个本地文件

--file-dest=DFILE 后台数据库的绝对路径写

操作系统访问:

这些选项可用于访问后台数据库管理系统底层操作系统

--os-cmd=OSCMD 执行操作系统命令

--os-shell 用于交互式操作系统shell的提示

--os-pwn 显示OOB shell, Meterpreter or或者VNC

--os-smbrelay One click prompt for an OOB shell, Meterpreter or VNC

--os-bof 存储过程缓冲区溢出开发

--priv-esc 数据库进程用户权限升级

--msf-path=MSFPATH 本地路径在metasploit框架安装

--tmp-path=TMPPATH 临时文件目录的远程绝对路径

Windows注册表访问:

这些选项可用于访问后台数据库管理系统的注册表

--reg-read 读取一个窗口注册表项

--reg-add 写一个窗口注册表项的数据

--reg-del 删除一个注册表项

--reg-key=REGKEY Windows注册表

--reg-value=REGVAL 注册表项的关键值

--reg-data=REGDATA 注册表键值数据

--reg-type=REGTYPE 注册表键值类型

常规:

这些选项可以用来设置一些常规的工作参数

-s SESSIONFILE 从存储加载会话（sqlite）文件

-t TRAFFICFILE Log all HTTP traffic into a textual file

--batch Never ask for user input, use the default behaviour

--binary-fields=.. Result fields having binary values (e.g. "digest")

--charset=CHARSET 用于数据检索的力字符编码

--crawl=CRAWLDEPTH 从目标网址开始抓取网站

--crawl-exclude=.. 正则表达式从爬行排除页 (e.g. "logout")

--csv-del=CSVDEL 限定使用CSV输出特性 (default ",")

--dump-format=DU.. 转储数据格式 (CSV (default), HTML or SQLITE)

--eta 显示为每个输出估计的到达时间

--flush-session 当前目标的刷新会话文件

--forms 目标网址的解析和测试形式

--fresh-queries 忽略存储在会话文件中的查询结果

--hex 使用数据库管理系统的十六进制函数（S）进行数据检索

--output-dir=OUT.. 自定义输出目录路径

--parse-errors 解析和显示响应中的数据库管理系统错误消息 --save=SAVECONFIG 保存选项来配置INI文件

--scope=SCOPE 正则表达式过滤提供代理日志目标

--test-filter=TE.. 选择测试的有效载荷和/或头文件(e.g. ROW)

--test-skip=TEST.. 跳过试验载荷和/或标题 (e.g. BENCHMARK)

--update 更新sqlmap

杂项:

-z MNEMONICS 短期记忆(e.g. "flu,bat,ban,tec=EU")

--alert=ALERT 运行主机操作系统命令（s）时，SQL注入是发现

--answers=ANSWERS 漏洞答案集(e.g. "quit=N,follow=N")

--beep 当有注入点被发现的时候报警

--cleanup 清理数据库从sqlmap具体UDF和表

--dependencies 检查没有的（非核心）sqlmap依赖包

--disable-coloring 禁用控制台输出着色

--gpage=GOOGLEPAGE 使用谷歌这一结果从指定的页码

--identify-waf 使一个WAF／IPS / IDS保护全面测试

--mobile 模仿智能手机通过HTTP用户代理标头

--offline 在脱机模式下工作（只使用会话数据）

--page-rank 显示网页排名（PR）为谷歌这一结果

--purge-output 安全地删除输出目录中的所有内容

--skip-waf 跳过WAF／IPS / IDS保护启发式检测

--smart 只有积极的启发式（S）进行彻底的测试

--sqlmap-shell 提示一个互动的sqlmap shell

--tmp-dir=TMPDIR 用于存储临时文件的本地目录

--wizard 为初学者用户提供简单的向导界面