超級註入工具Sqlmap命令詳解

原創 暗夜銘少 黑客滲透測試技術 前天

收錄於話題
#sql注入攻擊 1 #黑客攻擊 1

Sqlmap 是一款開源軟件，用於檢測和利用數據庫漏洞，
並提供注入惡意代碼的選項。
它是一種滲透測試工具，可以自動檢測和利用SQL 注入缺
陷，並在終端中提供其用戶界面。
該軟件在命令行運行，可供下載用於不同的操作系統：
Linux，Windows 和Mac OS 操作系統。

Sqlmap 支持檢測MySQL，Oracle，PostgreSQL，
Microsoft SQL Server，Microsoft Access，IBM DB2，SQLite，
Firebird 和SAP MaxDB 等數據庫的各種安全漏洞
採用五種獨特的SQL 注入技術，分別是：
1：基於布爾的盲注，即可以根據返回頁面判斷條件真假的注入。
2：基於時間的盲注，即不能根據頁面返回內容判斷任何信息，用條件語句查看時間延遲語句是否執行（即頁面返回時間是否增加）來判斷。
3：基於報錯注入，即頁面會返回錯誤信息，或者把注入的語句的結果直接返回在頁面中。
4：聯合查詢注入，可以使用union 的情況下的注入。
5：堆查詢注入，可以同時執行多條語句的執行時的注入。

sqlmap使用幫助

1.1 Options
-h, --help 顯示基本幫助信息。該幫助信息相對比較少。
-hh 顯示高級幫助信息。該幫助信息相對比較多。
--version 顯示程序版本信息。
-v VERBOSE 詳細級別（取值0-6，默認是1）。
1.2 Target:目標選項
至少需要使用下面的其中一個選項來設置目標。
-d DIRECT 指定直接數據庫連接的連接字符串。直接連接到數據庫。
-u URL, --url=URL 指定URL 目標(如："http://www.xxxx.com/vuln.php?id=1")
-l LOGFILE 從Burp 或WebScarab 代理的日誌中解析目標

-x SITEMAPURL 從遠程站點地圖(.xml)文件解析目標
-m BULKFILE 掃描文本文件中給出的多個目標。批量掃描。
-r REQUESTFILE 從文件中加載HTTP 請求
-g GOOGLEDORK 將Google dork 的結果作為目標URL
-c CONFIGFILE 從INI 配置文件中加載選項
1.3 Request:請求選項
這些選項可以用來指定如何連接到目標URL。
--method=METHOD 強制使用給定的HTTP 方法(如：PUT)
--data=DATA 通過POST 方法發送數據字符串
--param-del=PARA.. 指定用於分割參數值的字符
--cookie=COOKIE HTTP Cookie 頭
--cookie-del=COO.. 指定用於分割Cookie 值的字符
--load-cookies=L.. 指定包含Netscape/wget 格式的Cookie 的文件
--drop-set-cookie 忽略響應中的Set-Cookie 頭
--user-agent=AGENT 指定HTTP User-Agent 頭
--random-agent 使用隨機選定的HTTP User-Agent 頭
--host=HOST 指定HTTP Host header
--referer=REFERER 指定HTTP Referer header
-H HEADER, --hea.. 指定額外的header (如："X-Forwarded-For: 12
7.0.0.1")
--headers=HEADERS 指定額外的headers (如："Accept-Language:
fr\nETag: 123")
--auth-type=AUTH.. 指定HTTP 身份驗證類型(Basic, Digest, NTLM
or PKI)
--auth-cred=AUTH.. 指定HTTP 身份驗證憑據(name:password)
--auth-file=AUTH.. 指定HTTP 身份驗PEM 證書。當Web 服務器需要
客戶端證書進行身份驗證時，需要提供兩個文件:key_file、cert_file。key_file

是格式為PEM 文件，包含著你的私鑰，cert_file 是格式為PEM 的連接文件。
--ignore-code=IG.. 忽略HTTP error 碼(如：401)
--ignore-proxy 忽略系統默認代理配置
--ignore-redirects 忽略重定向的嘗試
--ignore-timeouts 忽略連接超時
--proxy=PROXY 使用代理連接目標URL
--proxy-cred=PRO.. 代理認證憑證(name:password)
--proxy-file=PRO.. 從文件中加載代理列表
--tor 使用Tor 匿名網絡
--tor-port=TORPORT 設置Tor 代理端口
--tor-type=TORTYPE 設置Tor代理類型(HTTP, SOCKS4 or SOCKS5 (default))
--check-tor 檢查Tor 的是否正確使用
--delay=DELAY 可以設定兩個HTTP(S)請求間的延遲
--timeout=TIMEOUT 可以設定一個HTTP(S)請求超過多久判定為超時 (default 30)
--retries=RETRIES 設置連接超時後的重試次數(default 3)
--randomize=RPARAM 設定某一個參數值在每一次請求中隨機的變化
--safe-url=SAFEURL URL address to visit frequently during testing
--safe-post=SAFE.. POST 數據發送到安全的URL
--safe-req=SAFER.. 從文件加載安全的HTTP 請求
--safe-freq=SAFE.. Test requests between two visits to a given safe URL
--skip-urlencode 跳過URL 的有效載荷數據編碼
--csrf-token=CSR.. 保存反CSRF 令牌
--csrf-url=CSRFURL 訪問提取anti-CSRF 令牌

--force-ssl 強制使用SSL/HTTPS
--hpp 使用HTTP 參數污染的方法
--eval=EVALCODE 在請求之前評估提供的Python 代碼(如:
"import hashlib;id2=hashlib.md5(id).hexdigest
()")
1.3 Optimization:優化選項
這些參數用於優化sqlmap 的性能。
-o 打開所有的優化開關
--predict-output 預測常見的查詢輸出
--keep-alive 使用HTTP(s)長連接（persistent 是不是翻譯成持久
更恰當？）
--null-connection 沒有實際的HTTP 響應時的檢索頁面長度
--threads=THREADS HTTP(s)最大並發請求數(默認是1)
1.4 Injection:注入選項
這些選項可以用來指定對哪些參數測試，提供一般的注入方式和可選可修
改的腳本注入。
-p TESTPARAMETER 可測試的參數
--skip=SKIP 跳過指定的參數
--skip-static 跳過靜態測試參數
--param-exclude=.. 使用正則表達式從測試中排除參數
--dbms=DBMS 強制指定後端的DBMS
--dbms-cred=DBMS.. DBMS 身份認證憑證(user:password)
--os=OS 強制指定後端的DBMS 操作系統
--invalid-bignum Use big numbers for invalidating values
--invalid-logical Use logical operations for invalidating values
--invalid-string Use random strings for invalidating values
--no-cast 關閉payload 構造機制

--no-escape 關閉字符逃避機制
--prefix=PREFIX 注入有效載荷前綴字符
--suffix=SUFFIX 注入有效負載後綴字符串
--tamper=TAMPER 使用給定的腳本修改注入的數據
1.5 Detection:探測選項
這些選項可用於自定義檢測階段
--level=LEVEL 測試等級(1-5, default 1)
--risk=RISK 測試的風險等級(1-3, default 1)
--string=STRING 字符串匹配查詢時被評估為True
--not-string=NOT.. 字符串匹配查詢時被評估為False
--regexp=REGEXP 正則表達式匹配查詢時被評估為True
--code=CODE HTTP code to match when query is evalu
ated to True
--text-only 僅根據文本內容比較頁面
--titles 僅根據其標題比較頁面
1.6 Techniques
這些選項可用於調整具體的SQL 注入測試.
--technique=TECH SQL 注入技術測試(default "BEUSTQ")
--time-sec=TIMESEC DBMS 響應的延遲時間(default 5)
--union-cols=UCOLS 指定用於測試UNION 查詢注入的列範圍
--union-char=UCHAR 暴力猜測列的字符數
--union-from=UFROM SQL 注入UNION 查詢使用的格式
--dns-domain=DNS.. DNS 洩露攻擊使用的域名
--second-order=S.. URL 搜索產生的結果頁面
Fingerprint:指紋
-f, --fingerprint 執行廣泛的DBMS 版本指紋檢查
Enumeration:枚舉

這些選項可以用來列舉後端數據庫管理系統的信息、表中的結構和數據。
此外，您還可以運行自定義的SQL 語句。
-a, --all 獲取所有信息
-b, --banner 獲取DBMS 標識
--current-user 獲取DBMS 當前用戶
--current-db 獲取DBMS 當前數據庫
--hostname 獲取DBMS 當前主機名
--is-dba 檢測當前用戶是否是DBA
--users 枚舉DBMS 用戶
--passwords 枚舉DBMS 用戶密碼hash
--privileges 枚舉DBMS 用戶權限
--roles 枚舉DBMS 用戶角色
--dbs 枚舉DBMS 數據庫
--tables 枚舉DBMS 數據庫中的表
--columns 枚舉DBMS 數據庫表的列
--schema 枚舉DBMS 架構
--count 檢索表的項目數。如果只想獲取表中的數據個數而
不是具體的內容可以使用這個參數，
--dump 轉儲DBMS 數據庫表
--dump-all 轉儲DBMS 所有數據庫表
--search 搜索列、表和（或）數據庫名
--comments 獲取DBMS 註釋
-D DB 指定要枚舉的DBMS 數據庫名
-T TBL 指定要枚舉的DBMS 表
-C COL 指定要枚舉的DBMS 列
-X EXCLUDE 指定不要枚舉的DBMS 數據庫
-U USER 指定要枚舉的DBMS 用戶

--exclude-sysdbs 枚舉表時排除DBMS 系統數據庫
--pivot-column=P.. 關鍵列的名稱
--where=DUMPWHERE Use WHERE condition while table dum
ping
--start=LIMITSTART First dump table entry to retrieve
--stop=LIMITSTOP Last dump table entry to retrieve
--first=FIRSTCHAR 獲取第一個查詢輸出字的字符
--last=LASTCHAR 獲取最後查詢的輸出字字符
--sql-query=QUERY 要執行的SQL 語句
--sql-shell 交互式SQL shell
--sql-file=SQLFILE 從給定的文件執行sql 語句
1.7 Brute force
這些選項可以被用來運行暴力檢查
--common-tables 檢查是否存在共同的表（與給定的表相對比）
--common-columns 檢查是否存在共同的列（與給定的列相對比）
1.8 User-defined function injection:用戶自定義函數注入
這些選項可以用來創建用戶自定義函數。
--udf-inject 注入用戶自定的函數
--shared-lib=SHLIB 共享庫的本地路徑
1.9 File system access:訪問文件系統
這些選項可以被用來訪問後端數據庫管理系統的底層文件系統
--file-read=RFILE 從後端的DBMS 文件系統讀取文件
--file-write=WFILE 編輯後端DBMS 文件系統中的文件
--file-dest=DFILE 後端DBMS 寫入文件的絕對路徑
2.0 Operating system access:操作系統訪問
這些選項可以用於訪問後端數據庫管理系統的底層操作系統
--os-cmd=OSCMD 執行操作系統命令

--os-shell 提示使用交互式操作系統shell
--os-pwn 獲取一個OOB shell，meterpreter 或VNC
--os-smbrelay 一鍵獲取一個OOBshell，meterpreter 或VNC
--os-bof 存儲過程緩衝區溢出利用
--priv-esc 數據庫進程用戶權限提升
--msf-path=MSFPATH MetasploitFramework 本地的安裝路徑
--tmp-path=TMPPATH 遠程臨時文件目錄的絕對路徑
2.1 Windows registry access:Windows 註冊表訪
問
這些選項可以被用來訪問後端數據庫管理系統Windows 註冊表。
--reg-read 讀取一個Windows 註冊表項值
--reg-add 寫入一個Windows 註冊表項值數據
--reg-del 刪除Windows 註冊表鍵值
--reg-key=REGKEY Windows 註冊表鍵
--reg-value=REGVAL Windows 註冊表鍵值
--reg-data=REGDATA Windows 註冊表鍵值數據
--reg-type=REGTYPE Windows 註冊表項值類型
2.2 General:一般選項
這些選項可以用來設置一些一般的工作參數
-s SESSIONFILE 從保存的.sqlite 文件中恢復會話
-t TRAFFICFILE 記錄所有HTTP 流量到一個文本文件中
--batch 使用所有默認配置，從不詢問用戶輸入
--binary-fields=.. Result fields having binary values (eg "digest"
)
--check-internet Check Internet connection before assessing t
he target
--crawl=CRAWLDEPTH 從目標URL 爬取網站

--crawl-exclude=.. 從爬取頁中排除正則表達式(eg "logout")
--csv-del=CSVDEL CSV 輸出中使用的分割字符(default ",")
--charset=CHARSET 強製字符編碼(eg "0123456789abcdef")
--dump-format=DU.. 轉儲的數據格式(CSV (default), HTML or SQL
ITE)
--encoding=ENCOD.. 指定用於數據檢索的字符編碼(如：GBK)
--eta 顯示每個輸出的預計到達時間
--flush-session 刷新當前目標的會話文件
--forms 解析和測試目標URL 表單
--fresh-queries 忽略存儲在會話文件中的查詢結果
--har=HARFILE 將所有HTTP 流量記錄到HAR 文件中
--hex 使用DBMS 十六進制功能進行數據檢索
--output-dir=OUT.. 自定義輸出目錄路徑
--parse-errors 解析並顯示響應DBMS 錯誤消息
--save=SAVECONFIG 將選項保存到INI 配置文件
--scope=SCOPE 使用正則表達式從提供的代理日誌中篩選目標
--test-filter=TE.. 選擇測試的有效載荷和/或標題(eg ROW)
--test-skip=TEST.. 跳過試驗載荷和/或標題(eg BENCHMARK)
--update 更新（升級）sqlmap
2.3 Miscellaneous:其他
-z MNEMONICS 使用短記憶法(eg "flu,bat,ban,tec=EU")
--alert=ALERT 發現SQL 注入時，運行主機操作系統命令
--answers=ANSWERS 設置問題答案（用於sqlmap 提示輸入的情形)
(eg "quit=N,follow=N")
--beep 發現sql 注入時，發出蜂鳴聲
--cleanup 清除sqlmap 注入時在DBMS 中產生的udf 與表
--dependencies Check for missing (non-core) sqlmap depen

dencies
--disable-coloring 禁掉彩色輸出。
--gpage=GOOGLEPAGE 使用Google dork 結果進行注入測試
--identify-waf 進行WAF/IPS/IDS 保護測試。
--mobile 設定一個手機的User-Agent 來模仿手機登陸
--offline 使用離線模式(僅使用session 數據)
--purge-output 從輸出目錄安全刪除所有內容
--skip-waf 跳過WAF/IPS/IDS 啟發式檢測保護
--smart 進行積極的啟發式測試，快速判斷為註入的報錯點
進行注入
--sqlmap-shell 提示一個交互式的sqlmap shell
--tmp-dir=TMPDIR 用於存儲臨時文件的本地目錄
--web-root=WEBROOT Web 服務器文檔根目錄(eg "/var/www")
--wizard 簡單的嚮導界面。適用於新手。

sqlmap靈活多變

1、基於布爾的盲注，即可以根據返回頁面判斷條件真假的注入
2、基於時間的盲注，即不能根據頁面返回內容判斷任何信息，用條件語句查看時間延遲語句是否執行（即頁面返回時間是否增加）來判斷。
3、基於報錯注入，即頁面會返回錯誤信息，或者把注入的語句的結果直接返回在頁面中。
4、聯合查詢注入，可以使用union 的情況下的注入。
5、堆查詢注入，可以同時執行多條語句的執行時的注入。
此外，sqlmap 也支持多種數據庫：
MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access,

IBM DB2, SQLite, Firebird, Sybase 和SAP MaxDB.

sqlmap命令詳細講解

- –is-dba 當前用戶權限（是否為root 權限）
- –dbs 所有數據庫
- –current-db 網站當前數據庫
- –users 所有數據庫用戶
- –current-user 當前數據庫用戶
- –random-agent 構造隨機user-agent
- –passwords 數據庫密碼
- –proxy http://local:8080 –threads 10 (可以自定義線程加速) 代理
- –time-sec=TIMESEC DBMS 響應的延遲時間（默認為5 秒）

Options（選項）：

- –version 顯示程序的版本號並退出
- -h, –help 顯示此幫助消息並退出
- -v VERBOSE 詳細級別：0-6（默認為1）
- 保存進度繼續跑：

sqlmap -u “http://url/news?id=1“ –dbs-o “sqlmap.log” 保存進度

sqlmap -u “http://url/news?id=1“ –dbs-o “sqlmap.log” –resume 恢復已保存進度

Target（目標）：

以下至少需要設置其中一個選項，設置目標URL。

- -d DIRECT 直接連接到數據庫。
- -u URL, –url=URL 目標URL。

- -l LIST 從Burp 或WebScarab 代理的日誌中解析目標。
- -r REQUESTFILE 從一個文件中載入HTTP 請求。
- -g GOOGLEDORK 處理Google dork 的結果作為目標URL。
- -c CONFIGFILE 從INI 配置文件中加載選項。

Request（請求）：

這些選項可以用來指定如何連接到目標URL。

- –data=DATA 通過POST 發送的數據字符串
- –cookie=COOKIE HTTP Cookie 頭
- –cookie-urlencode URL 編碼生成的cookie 注入
- –drop-set-cookie 忽略響應的Set – Cookie 頭信息
- –user-agent=AGENT 指定HTTP User – Agent 頭
- –random-agent 使用隨機選定的HTTP User – Agent 頭
- –referer=REFERER 指定HTTP Referer 頭
- –headers=HEADERS 換行分開，加入其他的HTTP 頭
- –auth-type=ATYPE HTTP 身份驗證類型（基本，摘要或NTLM）(Basic, Digest or NTLM)
- –auth-cred=ACRED HTTP 身份驗證憑據（用戶名:密碼）
- –auth-cert=ACERT HTTP 認證證書（key_file，cert_file）
- –proxy=PROXY 使用HTTP 代理連接到目標URL
- –proxy-cred=PCRED HTTP 代理身份驗證憑據（用戶名：密碼）
- –ignore-proxy 忽略系統默認的HTTP 代理
- –delay=DELAY 在每個HTTP 請求之間的延遲時間，單位為秒
- –timeout=TIMEOUT 等待連接超時的時間（默認為30 秒）
- –retries=RETRIES 連接超時後重新連接的時間（默認3）
- –scope=SCOPE 從所提供的代理日誌中過濾器目標的正則表達式
- –safe-url=SAFURL 在測試過程中經常訪問的url 地址
- –safe-freq=SAFREQ 兩次訪問之間測試請求，給出安全的URL

Enumeration（枚舉）：

這些選項可以用來列舉後端數據庫管理系統的信息、表中的結構和數據。此外，您還可以運行您自己的SQL 語句。

- -b, –banner 檢索數據庫管理系統的標識
- –current-user 檢索數據庫管理系統當前用戶
- –current-db 檢索數據庫管理系統當前數據庫
- –is-dba 檢測DBMS 當前用戶是否DBA
- –users 枚舉數據庫管理系統用戶
- –passwords 枚舉數據庫管理系統用戶密碼哈希
- –privileges 枚舉數據庫管理系統用戶的權限
- –roles 枚舉數據庫管理系統用戶的角色
- –dbs 枚舉數據庫管理系統數據庫
- -D DBname 要進行枚舉的指定數據庫名
- -T TBLname 要進行枚舉的指定數據庫表（如：-T tablename –columns）
- –tables 枚舉的DBMS 數據庫中的表
- –columns 枚舉DBMS 數據庫表列
- –dump 轉儲數據庫管理系統的數據庫中的表項
- –dump-all 轉儲所有的DBMS 數據庫表中的條目
- –search 搜索列（S），表（S）和/或數據庫名稱（S）
- -C COL 要進行枚舉的數據庫列
- -U USER 用來進行枚舉的數據庫用戶
- –exclude-sysdbs 枚舉表時排除系統數據庫
- –start=LIMITSTART 第一個查詢輸出進入檢索
- –stop=LIMITSTOP 最後查詢的輸出進入檢索

- –first=FIRSTCHAR 第一個查詢輸出字的字符檢索
- –last=LASTCHAR 最後查詢的輸出字字符檢索
- –sql-query=QUERY 要執行的SQL 語句
- –sql-shell 提示交互式SQL 的shell

Optimization（優化）：

這些選項可用於優化SqlMap 的性能。
- -o 開啟所有優化開關
- –predict-output 預測常見的查詢輸出
- –keep-alive 使用持久的HTTP（S）連接
- –null-connection 從沒有實際的HTTP 響應體中檢索頁面長度
- –threads=THREADS 最大的HTTP（S）請求並發量（默認為1）

Injection（注入）：

這些選項可以用來指定測試哪些參數， 提供自定義的注入
payloads 和可選篡改腳本。
- -p TESTPARAMETER 可測試的參數（S）
- –dbms=DBMS 強制後端的DBMS 為此值
- –os=OS 強制後端的DBMS 操作系統為這個值
- –prefix=PREFIX 注入payload 字符串前綴
- –suffix=SUFFIX 注入payload 字符串後綴
- –tamper=TAMPER 使用給定的腳本（S）篡改注入數據

Detection（檢測）：

這些選項可以用來指定在SQL盲注時如何解析和比較HTTP響應頁面的內容。

- –level=LEVEL 執行測試的等級（1-5，默認為1）
- –risk=RISK 執行測試的風險（0-3，默認為1）
- –string=STRING 查詢時有效時在頁面匹配字符串
- –regexp=REGEXP 查詢時有效時在頁面匹配正則表達式
- –text-only 僅基於在文本內容比較網頁

Techniques（技巧）：

這些選項可用於調整具體的SQL 注入測試。

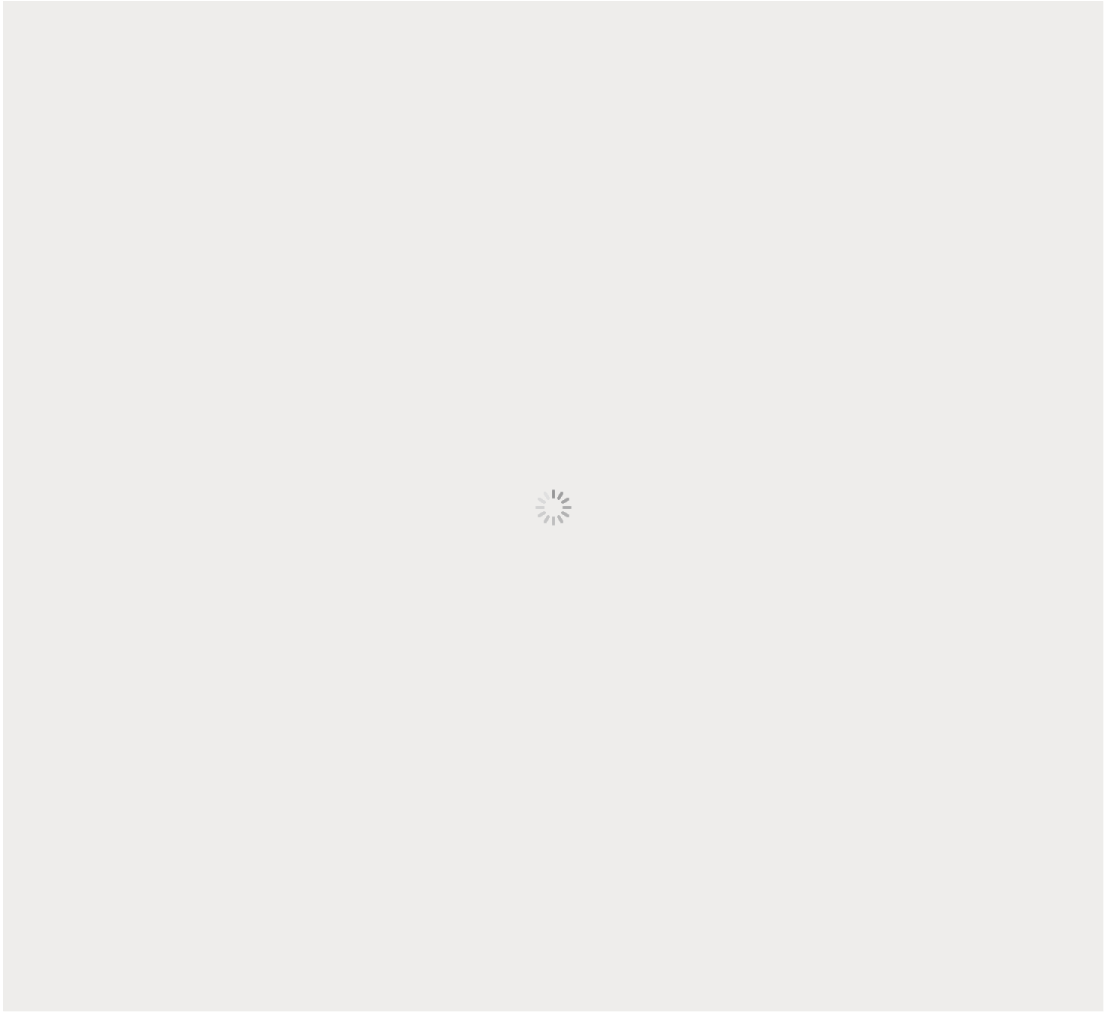
- –technique=TECH SQL 注入技術測試（默認BEUST）
- –time-sec=TIMESEC DBMS 響應的延遲時間（默認為5 秒）
- –union-cols=UCOLS 定列範圍用於測試UNION 查詢注入
- –union-char=UCHAR 用於暴力猜解列數的字符

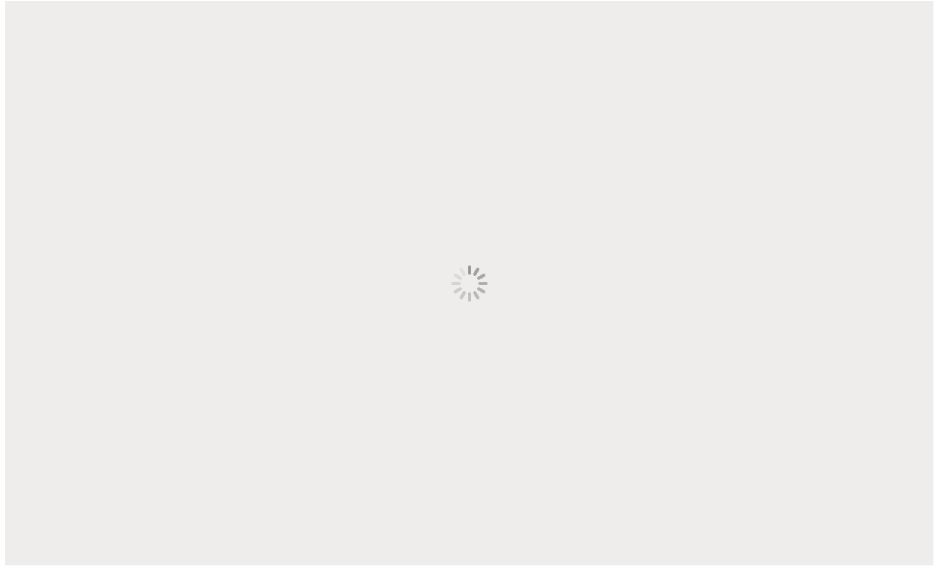
Fingerprint（指紋）：

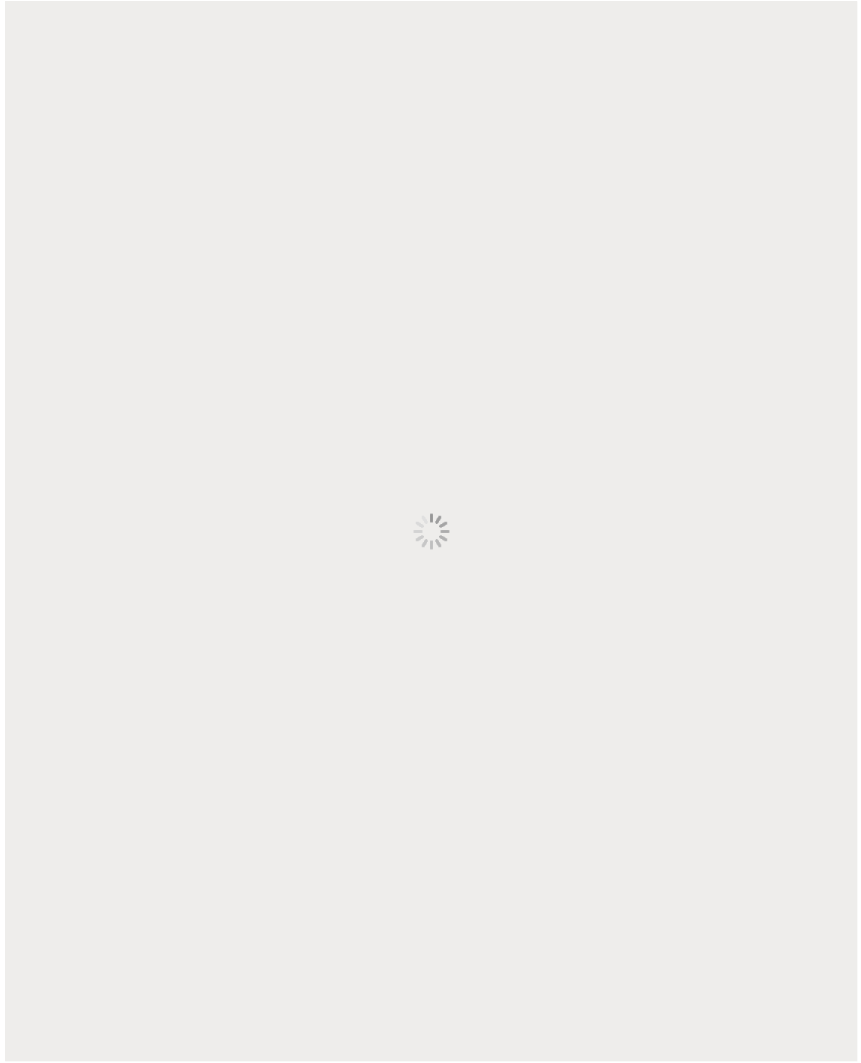
- -f, –fingerprint 執行檢查廣泛的DBMS 版本指紋

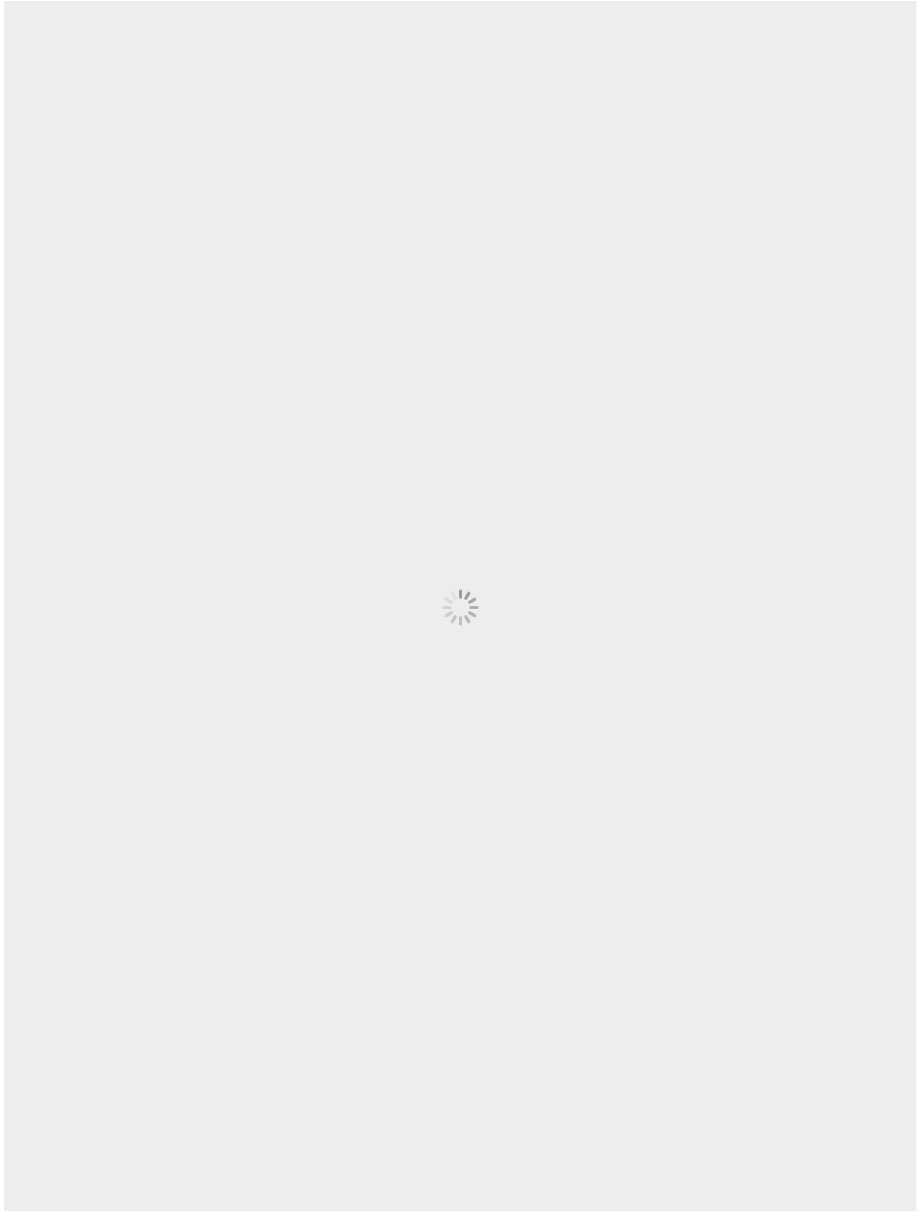
使用命令比較多，這裡就不一一講解了，想深度了解請看 **【sqlmap黑魔法】** 這本書，該書講比較透徹詳細，還有各種命令做實戰，包括每個系統安裝sqlmap都將比較全面。

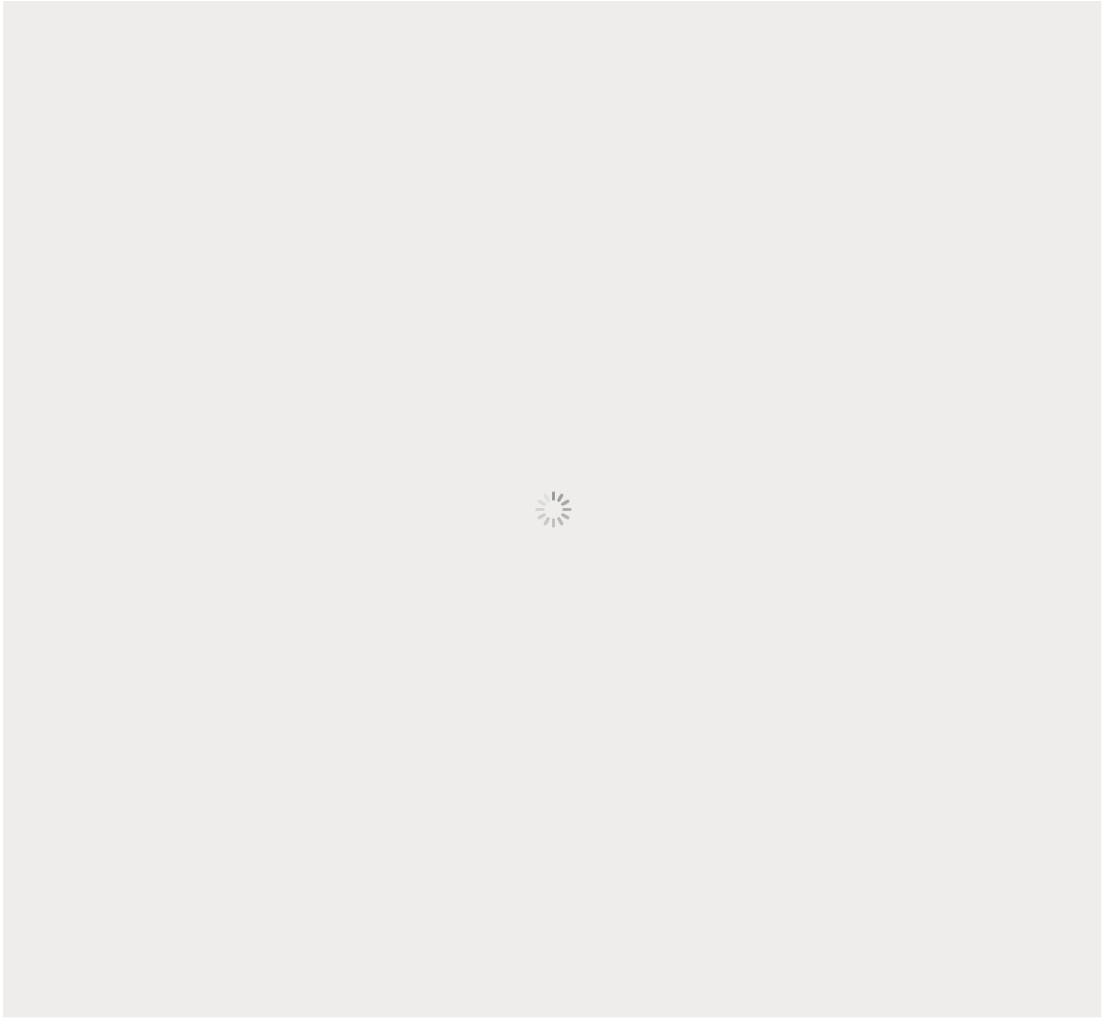

目录
第一章：安装 SQLmap.....
1.1 Windows 下 Sqlmap 的安装.....
1.2 Linux 下 Sqlmap 的安装.....
1.3 Mac 安装 Sqlmap.....
第二章：sqlmap 帮助信息详解.....
第三章：SQLMAP 命令详解.....
1. 1 SQLmap 简介.....
1.2 为什么要选用 SQLmap 这款工具？.....
微信号: sinxs9955

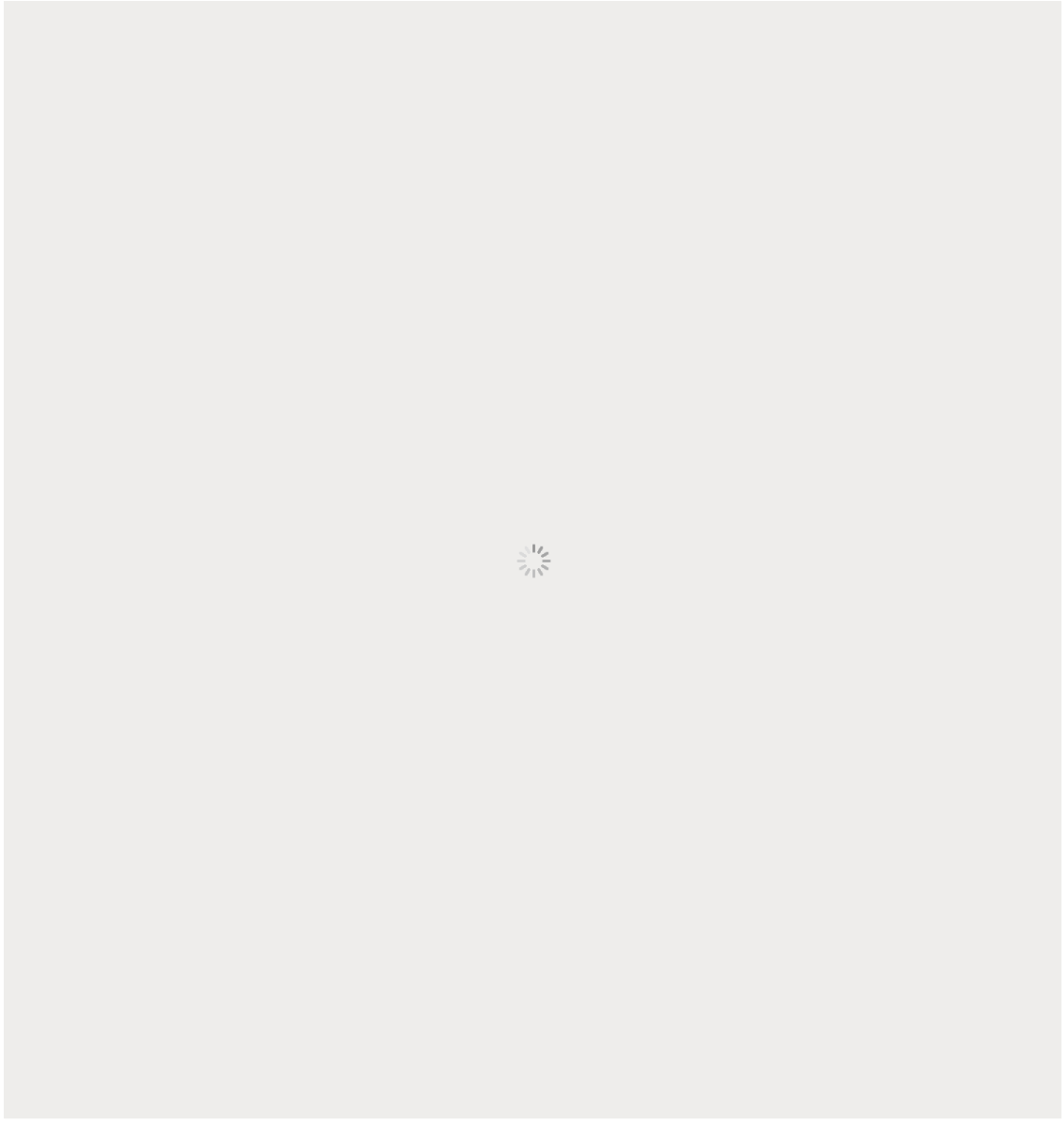


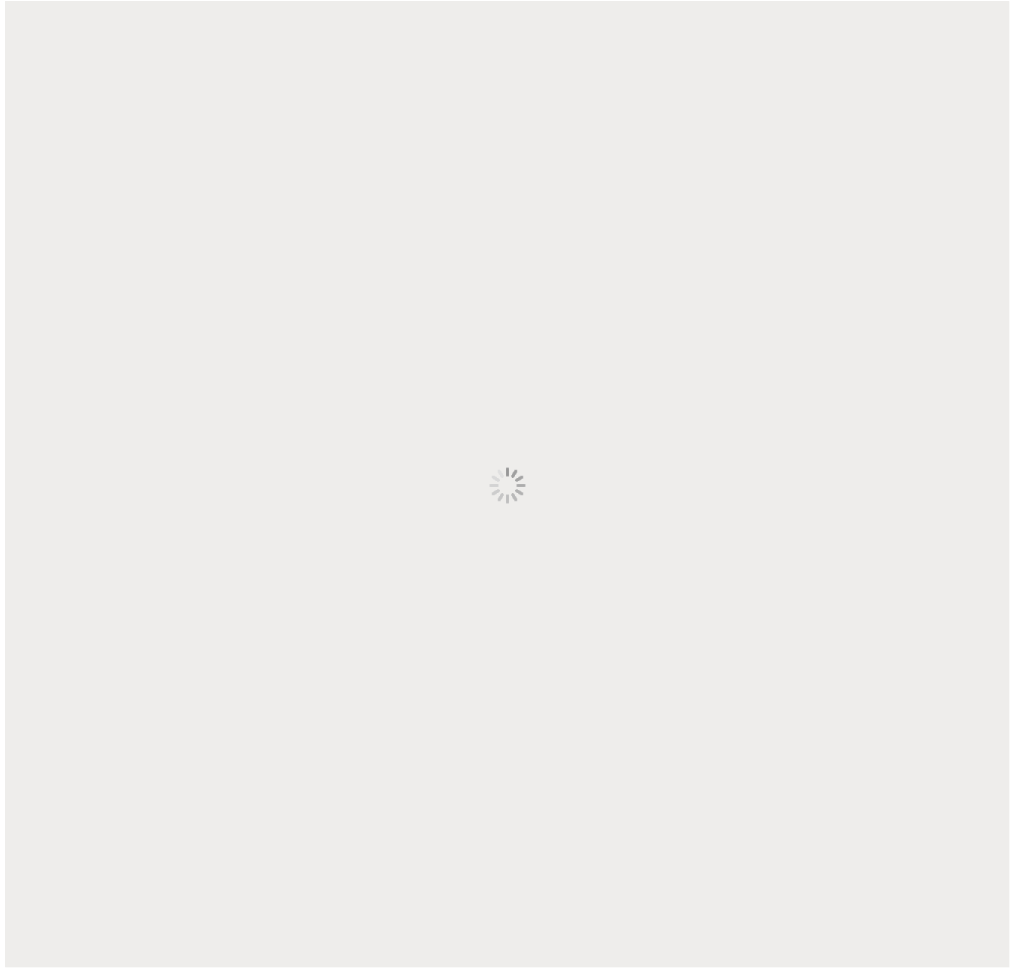












點擊左下方：閱讀原文獲取這本書

閱讀原文

喜歡此內容的人還喜歡

20億條記錄的MySQL大表，我們這樣遷移的

頂級架構師

為什麼別人總說你的SQL代碼寫得臭?

有關SQL