Searchsploit

Exploit Database（https://github.com/offensive-security/exploit-database）这是Offensive Security（https://www.offensive-security.com/）赞助的一个项目。存储了大量的漏洞利用程序，可以帮助安全研究者和渗透测试工程师更好的进行安全测试工作，目前是世界上公开收集漏洞最全的数据库，该仓库每天都会更新，exploit-db提供searchsploit利用files.csv进行搜索离线漏洞库文件的位置。

一下是searchsploit官方网站
https://www.exploit-db.com/searchsploit

二，官方帮助文档翻译（中英文对照）
-c, --case [Term] Perform a case-sensitive search (Default is inSEnsITiVe).
-c、 --case[Term]执行区分大小写的搜索（默认为不区分大小写）。

-e, --exact [Term] Perform an EXACT match on exploit title (Default is AND) [Implies "-t"].
-e、 --exact[Term]对利用漏洞的标题执行完全匹配（默认为AND）[表示“-t”]。

-h, --help Show this help screen.
-h、 --帮助显示此帮助屏幕。

-j, --json [Term] Show result in JSON format.
-j、 --json[Term]以json格式显示结果。

-m, --mirror [EDB-ID] Mirror (aka copies) an exploit to the current working directory.
-m、 --mirror[EDB-ID]将攻击镜像（aka copies）到当前工作目录。

-o, --overflow [Term] Exploit titles are allowed to overflow their columns.
-o、 --溢出[Term]允许利用漏洞标题溢出其列。

-p, --path [EDB-ID] Show the full path to an exploit (and also copies the path to the clipboard if possible).
-p、 --path[EDB-ID]显示攻击的完整路径（如果可能，还将路径复制到剪贴板）。

-t, --title [Term] Search JUST the exploit title (Default is title AND the file's path).
-t、 --title[Term]仅搜索利用漏洞的标题（默认为标题和文件路径）。

-u, --update Check for and install any exploitdb package updates (deb or git).
-u、 --更新检查并安装任何漏洞数据库包更新（deb或git）。

-w, --www [Term] Show URLs to Exploit-DB.com rather than the local path.
-w、 --www[Term]显示要利用-DB.com而不是本地路径的URL。

-x, --examine [EDB-ID] Examine (aka opens) the exploit using $PAGER.
-x、 --examine[EDB-ID]使用$PAGER检查（aka打开）漏洞。

--colour Disable colour highlighting in search results.
--在搜索结果中禁用颜色突出显示。

--id Display the EDB-ID value rather than local path.
--id显示EDB-id值，而不是本地路径。

--nmap [file.xml] Checks all results in Nmap's XML output with service version (e.g.: nmap -sV -oX file.xml).
--nmap[file.xml]使用服务版本检查nmap的xml输出中的所有结果（例如：nmap-sV-oX file.xml）。

Use "-v" (verbose) to try even more combinations
使用“-v”（详细）尝试更多的组合

--exclude="term" Remove values from results. By using "|" to separated you can chain multiple values.
--exclude=“term”从结果中移除值。通过使用“|”来分隔，可以链接多个值。

e.g. --exclude="term1|term2|term3".
e.g.--exclude=“条款1 |条款2 |条款3”。

三，常用命令

searchsploit mysql
查找Mysql的相关漏洞

```
C:\root> searchsploit mysql
------------------------------------------------------------ ----------------------------------------
 Exploit Title                                              |  Path
                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------ ----------------------------------------
Active Calendar 1.2 - '/data/mysqlevents.php?css' Cross-Site S | exploits/php/webapps/29653.txt
Advanced Poll 2.0 - 'mysql_host' Cross-Site Scripting          | exploits/php/webapps/33972.txt
Agora 1.4 RC1 - 'MysqlfinderAdmin.php' Remote File Inclusion   | exploits/php/webapps/2726.txt
Asterisk 'asterisk-addons' 1.2.7/1.4.3 - CDR_ADDON_MYSQL Modul | exploits/linux/remote/30677.pl
Banex PHP MySQL Banner Exchange 2.21 - 'admin.php' Multiple SQ | exploits/php/webapps/28307.txt
Banex PHP MySQL Banner Exchange 2.21 - 'members.php?cfg_root'  | exploits/php/webapps/28308.txt
Banex PHP MySQL Banner Exchange 2.21 - 'signup.php?site_name'  | exploits/php/webapps/28306.txt
CMSQLite / CMySQLite 1.3 - Cross-Site Request Forgery          | exploits/php/webapps/14096.html
CMSQLite 1.2 / CMySQLite 1.3.1 - Remote Code Execution         | exploits/php/webapps/14654.php
CSP MySQL User Manager 2.3.1 - Authentication Bypass           | exploits/linux/webapps/44589.txt
Cholod MySQL Based Message Board - 'Mb.cgi' SQL Injection      | exploits/cgi/webapps/27464.txt
Cisco Firepower Threat Management Console 6.0.1 - Hard-Coded M | exploits/linux/local/40465.txt
Froxlor Server Management Panel 0.9.33.1 - MySQL Login Informa | exploits/php/webapps/37725.txt
GEDCOM_TO_MYSQL - '/PHP/index.php?nom_branche' Cross-Site Scri | exploits/php/webapps/31731.txt
GEDCOM_TO_MYSQL - '/PHP/info.php' Multiple Cross-Site Scriptin | exploits/php/webapps/31732.txt
GEDCOM_TO_MYSQL - '/PHP/prenom.php' Multiple Cross-Site Script | exploits/php/webapps/31730.txt
JSPMySQL Administrador - Multiple Vulnerabilities              | exploits/jsp/webapps/38098.txt
KBVault MySQL 0.16a - Arbitrary File Upload                    | exploits/aspx/webapps/42184.txt
```

searchsploit -u
更新searchsploit

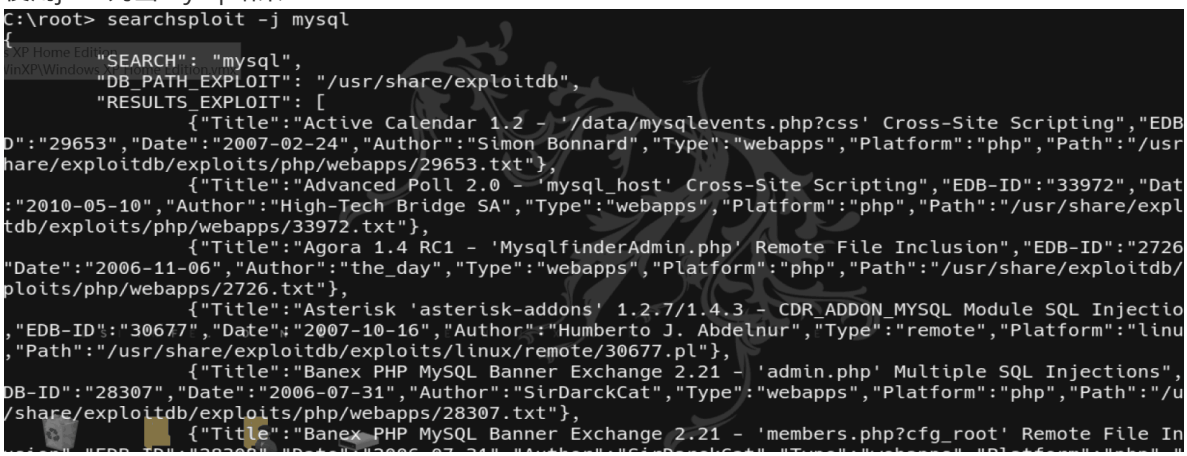
```
C:\root> searchsploit -u
[i] Updating via apt package management (Expect weekly-ish updates): exploitdb

Hit:1 https://mirrors.aliyun.com/deepin panda InRelease
Ign:2 http://mirrors.aliyun.com/kali sana InRelease
Ign:3 http://mirrors.aliyun.com/kali-security sana/updates InRelease
Err:4 http://mirrors.aliyun.com/kali sana Release
  404  Not Found [IP: 113.105.168.157 80]
Err:5 http://mirrors.aliyun.com/kali-security sana/updates Release
  404  Not Found [IP: 113.105.168.157 80]
Hit:6 http://ppa.launchpad.net/hzwhuang/ss-qt5/ubuntu xenial InRelease
Hit:7 http://mirrors.ustc.edu.cn/kali kali-rolling InRelease
Ign:8 http://mirrors.ustc.edu.cn/kali-security kali-current/updates InRelease
Err:9 http://mirrors.ustc.edu.cn/kali-security kali-current/updates Release
  404  Not Found [IP: 202.38.95.110 80]
Hit:10 http://mirrors.neusoft.edu.cn/kali kali-rolling InRelease
```

searchsploit -w mysql
让列出的结果通过uir的形式查看

```
C:\root> searchsploit mysql
------------------------------------------------------------ ----------------------------------------
 Exploit Title                                              |  Path
                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------ ----------------------------------------
Active Calendar 1.2 - '/data/mysqlevents.php?css' Cross-Site S | exploits/php/webapps/29653.txt
Advanced Poll 2.0 - 'mysql_host' Cross-Site Scripting          | exploits/php/webapps/33972.txt
Agora 1.4 RC1 - 'MysqlfinderAdmin.php' Remote File Inclusion   | exploits/php/webapps/2726.txt
Asterisk 'asterisk-addons' 1.2.7/1.4.3 - CDR_ADDON_MYSQL Modul | exploits/linux/remote/30677.pl
Banex PHP MySQL Banner Exchange 2.21 - 'admin.php' Multiple SQ | exploits/php/webapps/28307.txt
Banex PHP MySQL Banner Exchange 2.21 - 'members.php?cfg_root'  | exploits/php/webapps/28308.txt
Banex PHP MySQL Banner Exchange 2.21 - 'signup.php?site_name'  | exploits/php/webapps/28306.txt
CMSQLite / CMySQLite 1.3 - Cross-Site Request Forgery          | exploits/php/webapps/14096.html
CMSQLite 1.2 / CMySQLite 1.3.1 - Remote Code Execution         | exploits/php/webapps/14654.php
CSP MySQL User Manager 2.3.1 - Authentication Bypass           | exploits/linux/webapps/44589.txt
Cholod MySQL Based Message Board - 'Mb.cgi' SQL Injection      | exploits/cgi/webapps/27464.txt
Cisco Firepower Threat Management Console 6.0.1 - Hard-Coded M | exploits/linux/local/40465.txt
Froxlor Server Management Panel 0.9.33.1 - MySQL Login Informa | exploits/php/webapps/37725.txt
GEDCOM_TO_MYSQL - '/PHP/index.php?nom_branche' Cross-Site Scri | exploits/php/webapps/31731.txt
GEDCOM_TO_MYSQL - '/PHP/info.php' Multiple Cross-Site Scriptin | exploits/php/webapps/31732.txt
GEDCOM_TO_MYSQL - '/PHP/prenom.php' Multiple Cross-Site Script | exploits/php/webapps/31730.txt
JSPMySQL Administrador - Multiple Vulnerabilities              | exploits/jsp/webapps/38098.txt
KBVault MySQL 0.16a - Arbitrary File Upload                    | exploits/aspx/webapps/42184.txt
```

searchsploit -j mysql

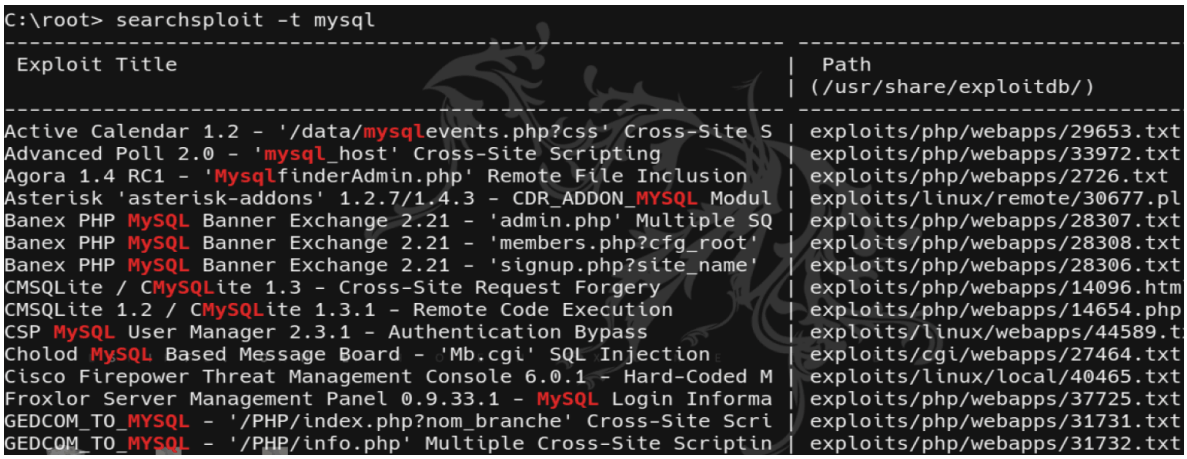
使用json列出mysql结果



```
C:\root> searchsploit -j mysql
{
        "SEARCH": "mysql",
        "DB_PATH_EXPLOIT": "/usr/share/exploitdb",
        "RESULTS_EXPLOIT": [
                {"Title":"Active Calendar 1.2 - '/data/mysqlevents.php?css' Cross-Site Scripting","EDB
D":"29653","Date":"2007-02-24","Author":"Simon Bonnard","Type":"webapps","Platform":"php","Path":"/usr
hare/exploitdb/exploits/php/webapps/29653.txt"},
                {"Title":"Advanced Poll 2.0 - 'mysql_host' Cross-Site Scripting","EDB-ID":"33972","Dat
:"2010-05-10","Author":"High-Tech Bridge SA","Type":"webapps","Platform":"php","Path":"/usr/share/expl
tdb/exploits/php/webapps/33972.txt"},
                {"Title":"Agora 1.4 RC1 - 'MysqlfinderAdmin.php' Remote File Inclusion","EDB-ID":"2726
"Date":"2006-11-06","Author":"the_day","Type":"webapps","Platform":"php","Path":"/usr/share/exploitdb/
ploits/php/webapps/2726.txt"},
                {"Title":"Asterisk 'asterisk-addons' 1.2.7/1.4.3 - CDR_ADDON_MYSQL Module SQL Injectio
,"EDB-ID":"30677","Date":"2007-10-16","Author":"Humberto J. Abdelnur","Type":"remote","Platform":"linu
,"Path":"/usr/share/exploitdb/exploits/linux/remote/30677.pl"},
                {"Title":"Banex PHP MySQL Banner Exchange 2.21 - 'admin.php' Multiple SQL Injections",
DB-ID":"28307","Date":"2006-07-31","Author":"SirDarckCat","Type":"webapps","Platform":"php","Path":"/u
/share/exploitdb/exploits/php/webapps/28307.txt"},
                {"Title":"Banex PHP MySQL Banner Exchange 2.21 - 'members.php?cfg_root' Remote File In
```

searchsploit -t mysql

仅搜索利用漏洞的标题



```
C:\root> searchsploit -t mysql
------------------------------------------------------------ ------------------------------
 Exploit Title                                              |  Path
                                                            | (/usr/share/exploitdb/)
------------------------------------------------------------ ------------------------------
Active Calendar 1.2 - '/data/mysqlevents.php?css' Cross-Site S | exploits/php/webapps/29653.txt
Advanced Poll 2.0 - 'mysql_host' Cross-Site Scripting          | exploits/php/webapps/33972.txt
Agora 1.4 RC1 - 'MysqlfinderAdmin.php' Remote File Inclusion   | exploits/php/webapps/2726.txt
Asterisk 'asterisk-addons' 1.2.7/1.4.3 - CDR_ADDON_MYSQL Modul | exploits/linux/remote/30677.pl
Banex PHP MySQL Banner Exchange 2.21 - 'admin.php' Multiple SQ | exploits/php/webapps/28307.txt
Banex PHP MySQL Banner Exchange 2.21 - 'members.php?cfg_root'  | exploits/php/webapps/28308.txt
Banex PHP MySQL Banner Exchange 2.21 - 'signup.php?site_name'  | exploits/php/webapps/28306.txt
CMSQLite / CMySQLite 1.3 - Cross-Site Request Forgery          | exploits/php/webapps/14096.htm
CMSQLite 1.2 / CMySQLite 1.3.1 - Remote Code Execution         | exploits/php/webapps/14654.php
CSP MySQL User Manager 2.3.1 - Authentication Bypass           | exploits/linux/webapps/44589.t
Cholod MySQL Based Message Board - 'Mb.cgi' SQL Injection      | exploits/cgi/webapps/27464.txt
Cisco Firepower Threat Management Console 6.0.1 - Hard-Coded M | exploits/linux/local/40465.txt
Froxlor Server Management Panel 0.9.33.1 - MySQL Login Informa | exploits/php/webapps/37725.txt
GEDCOM_TO_MYSQL - '/PHP/index.php?nom_branche' Cross-Site Scri | exploits/php/webapps/31731.txt
GEDCOM_TO_MYSQL - '/PHP/info.php' Multiple Cross-Site Scriptin | exploits/php/webapps/31732.txt
```