

Burpsuite 插件-SQLiPy 使用方法

by:裁决

一 . SQLiPy 介绍

SQLiPy 是 Burp Suite 的 Python 插件，它使用 SQLMap API 集成 SQLMap

二 . SQLiPy 安装要求:

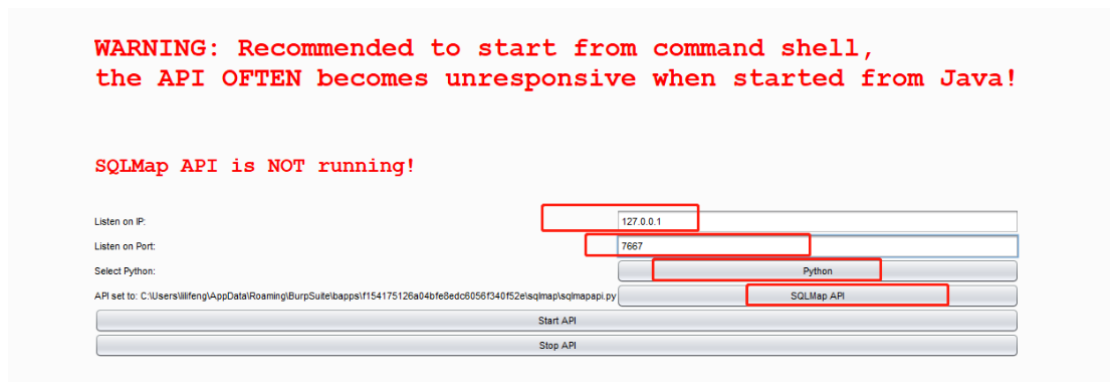
Jython 2.7 beta [参考 Jython 安装说明]

Java 1.7 或 1.8

三 . SQLiPy 用法:

SQLiPy 依赖于 SQLMap API 服务器的运行实例

可以在 sqlmap api 模块设置好 ip,端口,python 和 sqlmap api 位置之后,点击 start api 即可



或者可以使用一下命令启动 sqlmap api

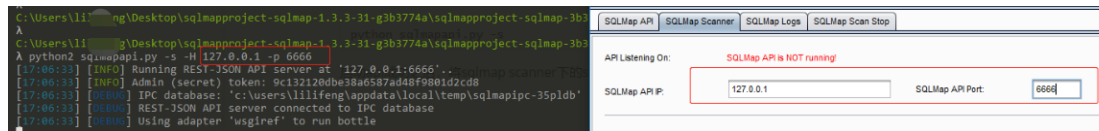
python sqlmapapi.py -s -H <ip> -p <port>

```
C:\Users\lilifeng\Desktop\sqlmapproject-sqlmap-1.3.3-31-g3b3774a\sqlmapproject-sqlmap-3b3774a>
λ python2 sqlmapapi.py -s -H 127.0.0.1 -p 6666
[17:06:33] [INFO] Running REST-JSON API server at '127.0.0.1:6666'..
[17:06:33] [INFO] Admin (secret) token: 9c132120dbe38a6587ad48f9801d2cd8
[17:06:33] [DEBUG] IPC database: 'c:\users\lilifeng\appdata\local\temp\sqlmapipc-35pldb'
[17:06:33] [DEBUG] REST-JSON API server connected to IPC database
[17:06:33] [DEBUG] Using adapter 'wsgiref' to run bottle
```

也可以执行，用 sqlmap 默认的

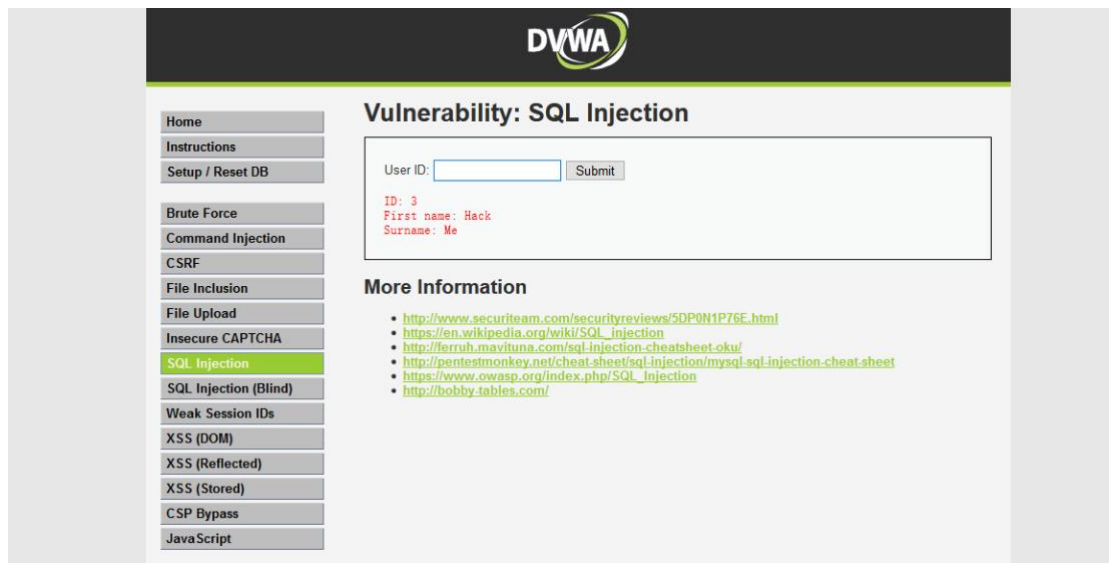
python sqlmapapi.py -s

启动 api 成功之后，将 sqlmap scanner 下的 sqlmap api ip 和 sqlmap api port 设置一下就好

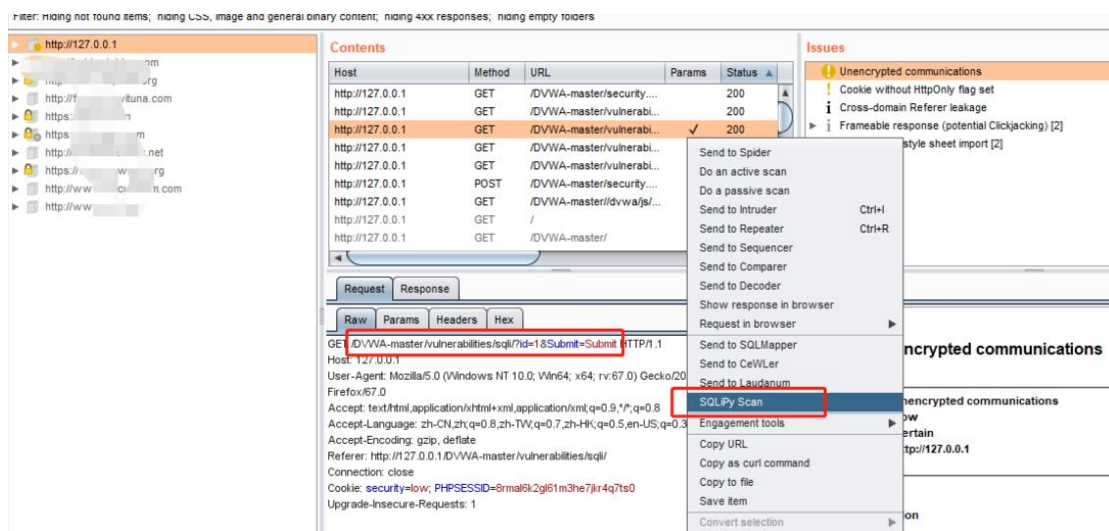


四 . SQLiPy 演示

1. 启动 DVWA,访问 sql 注入环境



2.将拦截的数据包发送到 SQLiPy Scan



可以看到 cookie 等参数已经填好了

API Listening On: SQLMap API is NOT running!


SQLMap API IP: SQLMap API Port:

HTTP Method: Default ▾

URL:

Post Data:

Cookies

Referer: 

User-Agent:

Custom Headers:

Test Parameter(s): ☐ Text Only

点击下方的 start

Auth Type: None ▾

Auth User:

Auth Pass:

Start Scan

如果存在漏洞就会显示

Site map
Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- ▼ http://127.0.0.1
- ▼ DVWA-master
 - ▼ /
 - ▼ /
 - ▼ about.php
 - ▼ dvwa
 - ▼ ids_log.php
 - ▼ instructions.php
 - ▼ logout.php
 - ▼ phpinfo.php
 - ▼ security.php
 - ▼ setup.php

Host	Method	URL	Params	Status	Le
http://127.0.0.1	GET	/DVWA-master/vulnerabi...		200	46
http://127.0.0.1	GET	/DVWA-master/vulnerabi...	✓	200	46
http://127.0.0.1	GET	/DVWA-master/vulnerabi...	✓	200	46
http://127.0.0.1	GET	/DVWA-master/vulnerabi...	✓	200	46

Issues

SQLMap Scan Finding [4]

- /DVWA-master/vulnerabilities/sql/
- /DVWA-master/vulnerabilities/sql/
- /DVWA-master/vulnerabilities/sql/
- /DVWA-master/vulnerabilities/sql/

- Cross-domain Referer leakage
- Frameable response (potential Clickjacking)
- Path-relative style sheet import