

burpsuite 插件之 Passive Scan Client 使用方法

by:裁决

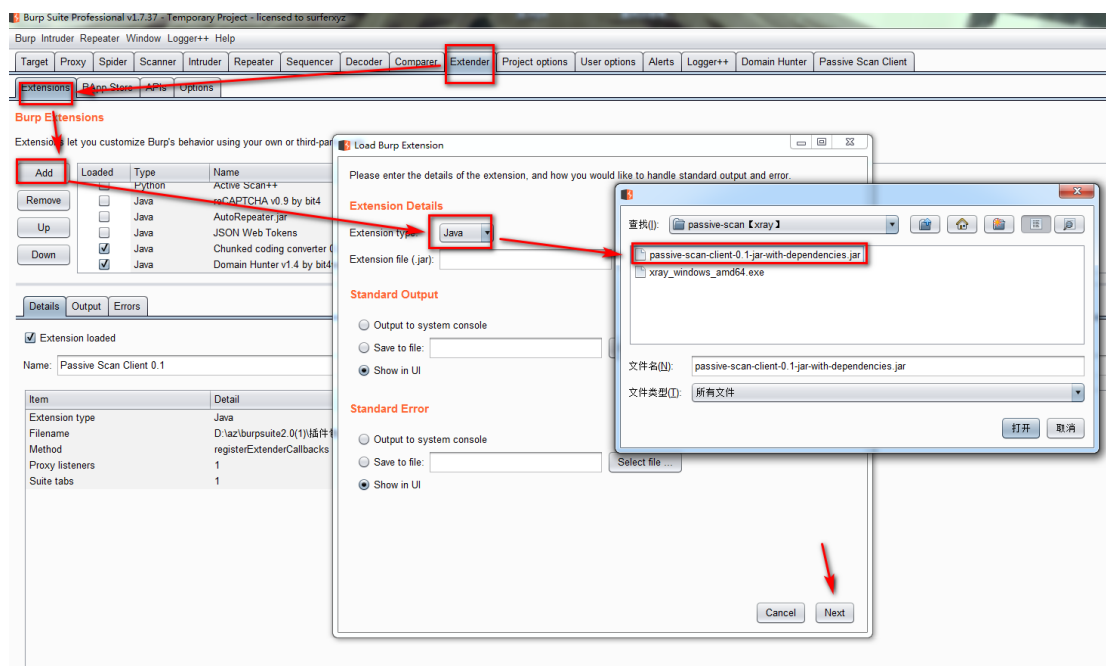
Passive Scan Client 介绍

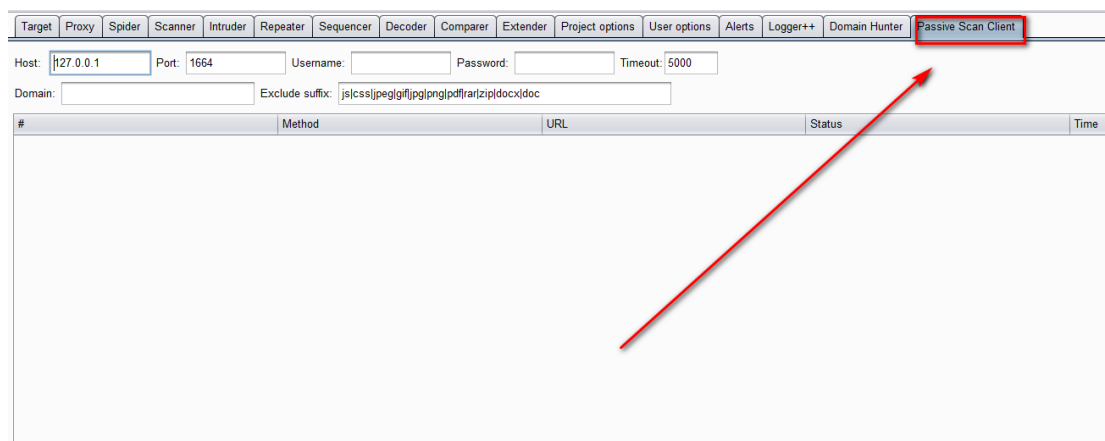
被动扫描流量转发插件

Passive Scan Client 项目主页

<https://github.com/c0ny1/passive-scan-client>

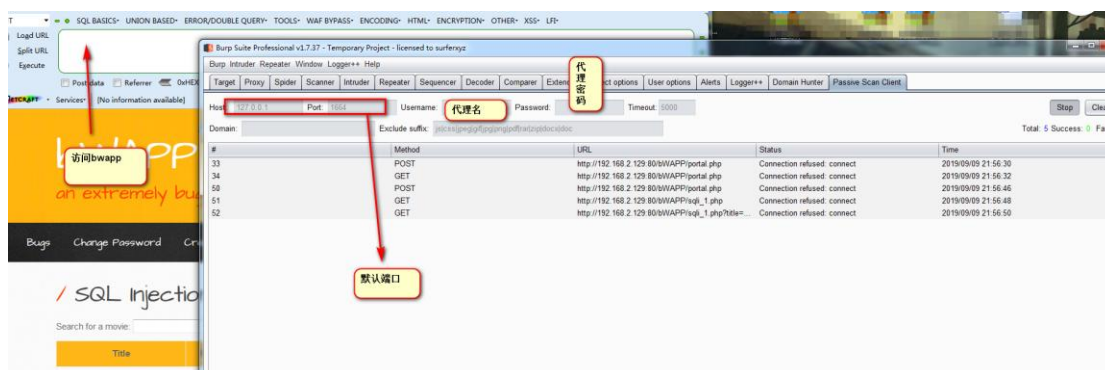
Passive Scan Client 安装方法





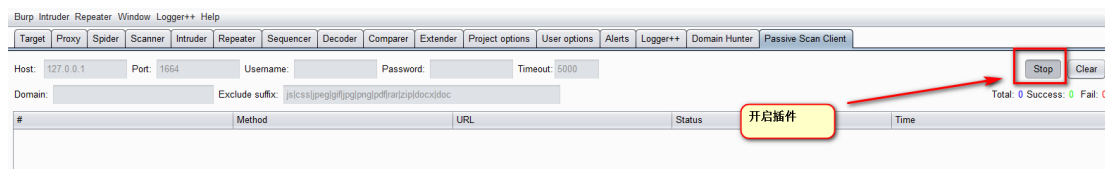
Passive Scan Client 使用方法

1.访问靶机，点击插件的 run 就可以了

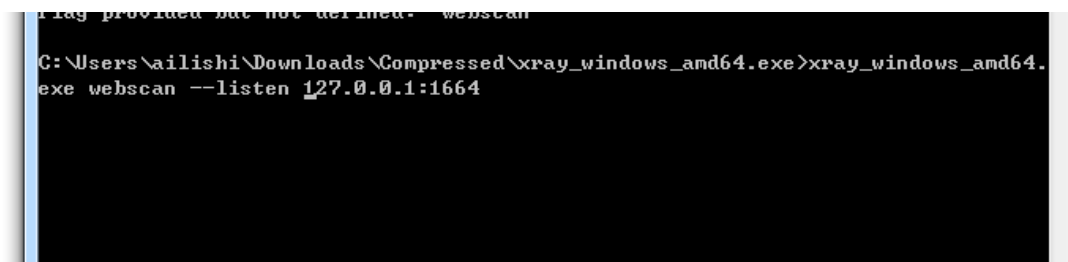


2.结合被动扫描插件使用

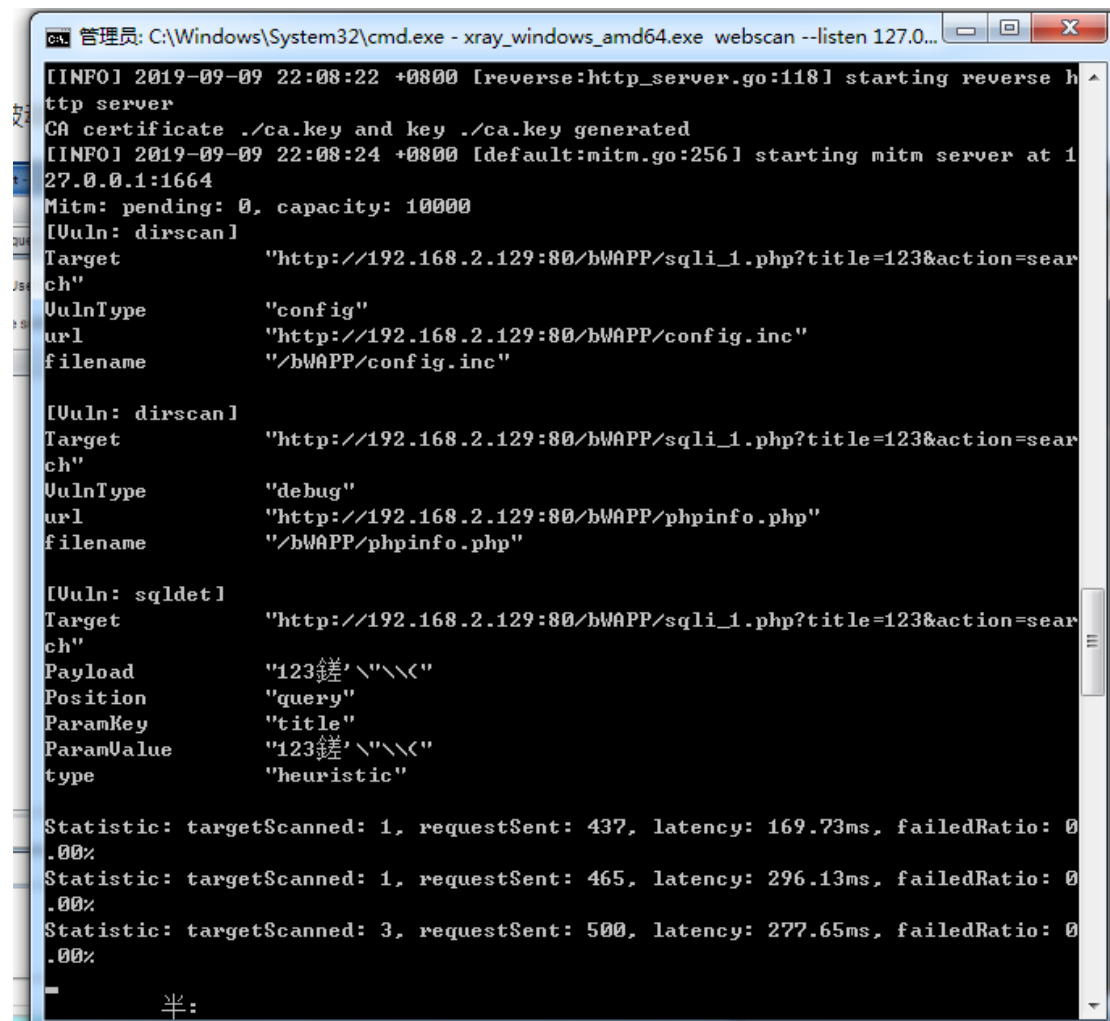
①开启插件



②选择一个扫描器，我这里用的长亭的，将代理设置为插件的地址和端口



③访问网站
扫到东西了



```
管理员: C:\Windows\System32\cmd.exe - xray_windows_amd64.exe webscan --listen 127.0.0.1
[INFO] 2019-09-09 22:08:22 +0800 [reverse:http_server.go:118] starting reverse http server
CA certificate ./ca.key and key ./ca.key generated
[INFO] 2019-09-09 22:08:24 +0800 [default:mitm.go:256] starting mitm server at 127.0.0.1:1664
Mitm: pending: 0, capacity: 10000
[Uvln: dirscan]
Target      "http://192.168.2.129:80/bWAPP/sqli_1.php?title=123&action=search"
UvlnType    "config"
url         "http://192.168.2.129:80/bWAPP/config.inc"
filename    "/bWAPP/config.inc"

[Uvln: dirscan]
Target      "http://192.168.2.129:80/bWAPP/sqli_1.php?title=123&action=search"
UvlnType    "debug"
url         "http://192.168.2.129:80/bWAPP/phpinfo.php"
filename    "/bWAPP/phpinfo.php"

[Uvln: sqldet]
Target      "http://192.168.2.129:80/bWAPP/sqli_1.php?title=123&action=search"
Payload     "123鎂'\\"<"
Position    "query"
ParamKey    "title"
ParamValue  "123鎂'\\"<"
type        "heuristic"

Statistic: targetScanned: 1, requestSent: 437, latency: 169.73ms, failedRatio: 0.00%
Statistic: targetScanned: 1, requestSent: 465, latency: 296.13ms, failedRatio: 0.00%
Statistic: targetScanned: 3, requestSent: 500, latency: 277.65ms, failedRatio: 0.00%

半:
```

注：扫描器不一定用这个啊