



链滴

# burp + xray 联合

作者: [ying-hack](#)

原文链接: <https://ld246.com/article/1639054313094>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

今天我想给大家分享的是 burp + xray 打联合拳

首先我们了解一下这两款软件是干什么的。

## burp

burp是一款抓包软件，它有很多作用。

1. 抓包
2. 攻击模式(爆破，多线程发包等)
3. 对抓到的包进行重放
4. 爬虫
5. 加密，解密
6. 比较
7. 等

在此我就不再一一介绍burp的作用了。如果大家感兴趣我可以出一个关于burp的使用的文章

## xray

xray是一款自动化挖掘漏洞的软件，是长亭科技推出的一款供白帽子免费使用的漏洞挖掘软件。

```

XRAY
Version: 1.8.2/79e7dd56/COMMUNITY
NAME:
  xray - A powerful scanner engine [https://docs.xray.cool]
USAGE:
  [global options] command [command options] [arguments...]
COMMANDS:
  webscan, ws      Run a webscan task
  servicescan, ss Run a service scan task
  subdomain, sd   Run a subdomain task
  poclint, pl     lint yml poc
  transform       transform other script to gamma
  reverse         Run a standalone reverse server
  convert         convert results from json to html or from html to json
  genca          GenerateToFile CA certificate and key
  upgrade        check new version and upgrade self if any updates found
  version        Show version info
  help, h        Shows a list of commands or help for one command
GLOBAL OPTIONS:
  --config FILE      Load configuration from FILE (default: "config.yaml")
  --log-level value  Log level, choices are debug, info, warn, error, fatal
  --help, -h        show help
```

xray一款强大的扫描引擎

- genca 生成ca证书
- upgrade 更新xray
- version xray版本
- help 帮助
- convert 从html格式转化为json格式 或者 从json转化为html格式
- reverse 启动单独的盲打平台服务
- webscan 对web进行漏洞扫描
- serverscan 用来探测服务漏洞
- poclint 用来查看写的poc是否符合要求

## 接下来让我们看看它们两个如何打组合拳吧

首先让xray开启被动扫描模式，设置一个代理端口

```
xray ws -listen 127.0.0.1:7777 --html-output out.html
```

```
C:\rj\web目录扫描>xray ws -listen 127.0.0.1:7777 --html-output out.html

XRAY

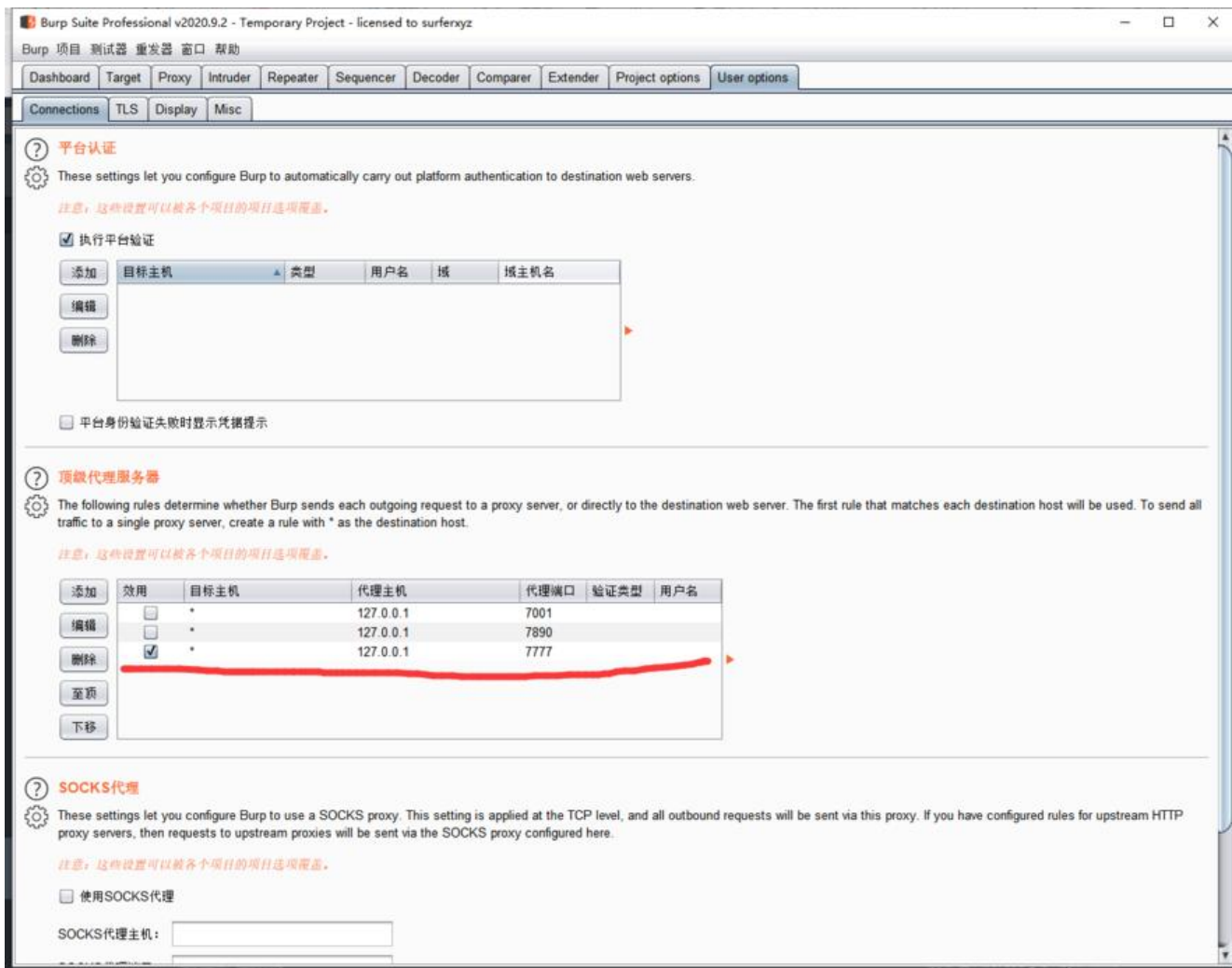
Version: 1.8.2/79e7dd56/COMMUNITY

[INFO] 2021-12-09 20:32:30 [default:entry.go:213] Loading config file from config.yaml
[WARN] 2021-12-09 20:32:32 [default:webscan.go:222] disable these plugins as that's not an advanced version, [struts thin
Enabled plugins: [sqldet jsonp redirect crlf-injection phantasm baseline cmd-injection xss xxe brute-force ssrf upload di
[INFO] 2021-12-09 20:32:32 [phantasm:phantasm.go:180] 343 pocs have been loaded (debug level will show more details)
These plugins will be disabled as reverse server is not configured, check out the reference to fix this error.
Ref: https://docs.xray.cool/#/configuration/reverse
Plugins:
poc-yaml-dlink-cve-2019-16920-rce
poc-yaml-jenkins-cve-2018-1000600
poc-yaml-jira-cve-2019-11581
poc-yaml-jira-ssrf-cve-2019-8451
poc-yaml-mongo-express-cve-2019-10758
poc-yaml-pandorafms-cve-2019-20224-rce
poc-yaml-saltstack-cve-2020-16846
poc-yaml-solr-cve-2017-12629-xxe
poc-yaml-supervisord-cve-2017-11610
poc-yaml-weblogic-cve-2017-10271
ssrf/ssrf/default
xxe/xxe/blind

[INFO] 2021-12-09 20:32:32 [collector:mitm.go:215] loading cert from ./ca.crt and ./ca.key
[INFO] 2021-12-09 20:32:33 [collector:mitm.go:270] starting mitm server at 127.0.0.1:7777
```

这样xray就开始监听本地7777端口

然后我们再去配置burp



在burp上设置代理为本地7777端口

然后我们就可以用burp访问页面，xray就会自动的扫描漏洞了。

我们是noobteam团队。如果想要了解关于计算机的知识可以关注我们的公众号。定期会分享一些知识哦！

