【工具篇】大佬都在用的几款web指纹识别工具

原创 lemonlove7 鹏组安全 2024年08月31日 11:42 江西

由于微信公众号推送机制改变了，快来星标不再迷路，谢谢大家！

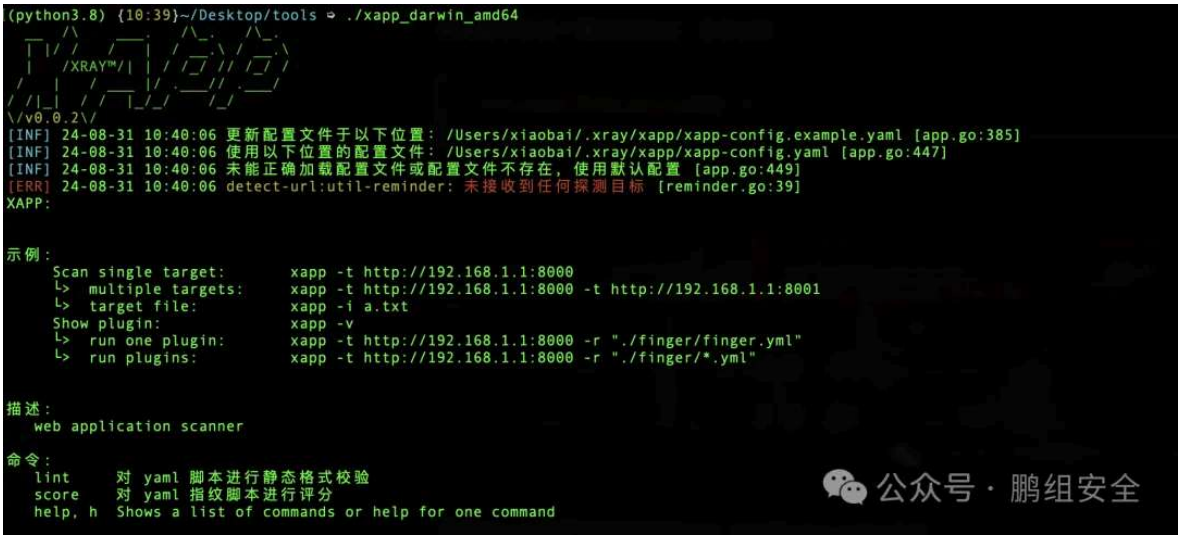
xapp

xapp是一款专注于web指纹识别的工具。你可以使用xapp对web目标所使用的技术进行识别，为安全测试做好准备。

xapp继承了x系列工具的一贯优点，通过简单易用的命令行参数和一致的规则语法，帮助用户快速、高效地进行web指纹识别，并为安全测试做好充分准备。我们期待与社区共同构建一个丰富的指纹规则库，为所有用户提供免费和高效的指纹识别服务。

根据自己系统下载对应版本，之后运行

```
./xapp_darwin_amd64
```



会在Users路径下生成文件xapp-config.example.yaml

到 https://github.com/chaitin/xray-plugins 下载指纹文件，放入和xapp-config.example.yaml相同路径下

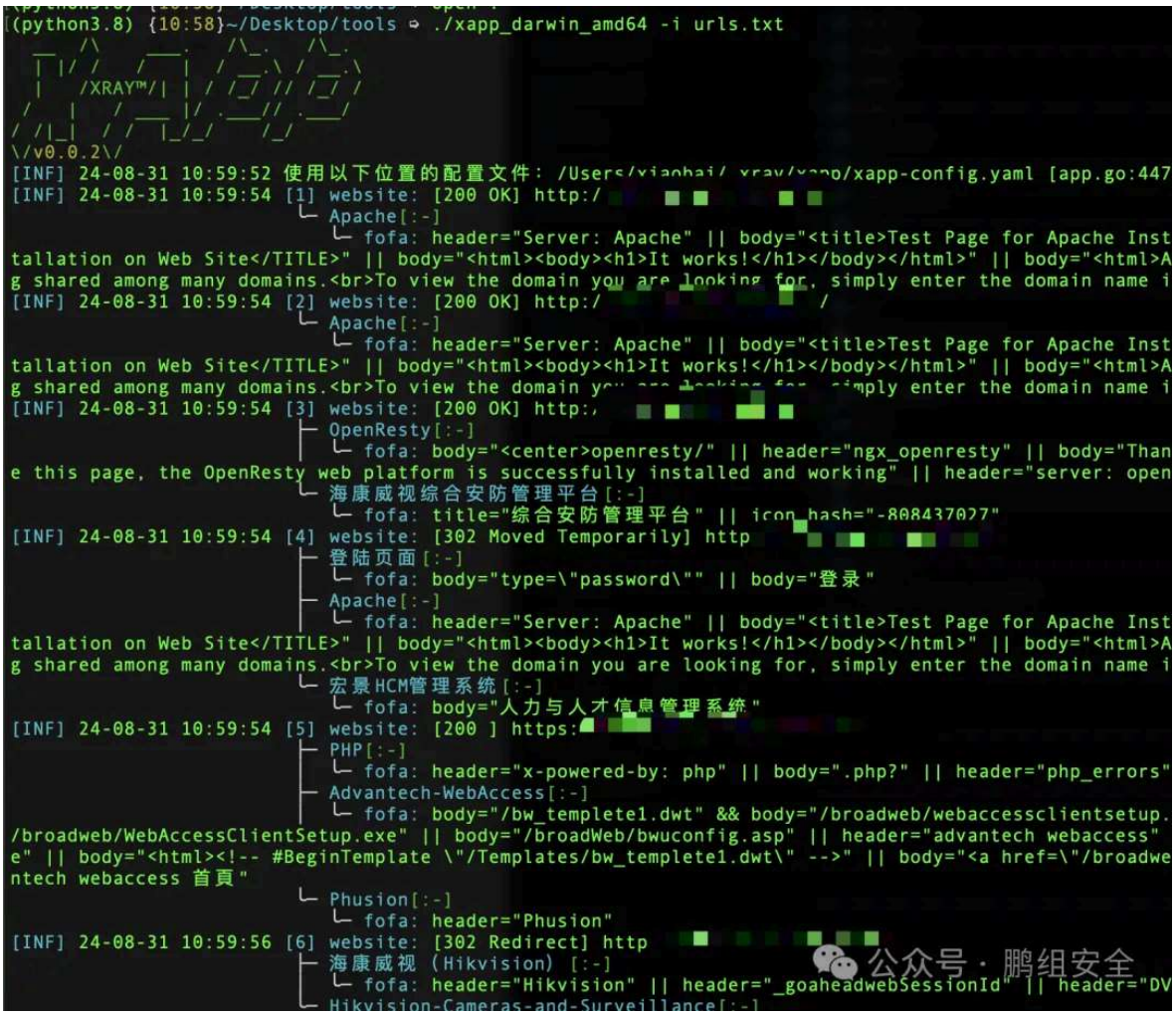
简单使用

单个url

```
./xapp_darwin_amd64 -t http://x.x.x
```

扫描多个url

```
./xapp_darwin_amd64 -i urls.txt
```



更多用法

```
# 扫描单个url
xapp -t http://www.test.com
# 扫描多个url
xapp -i urls.txt
# 指定指纹扫描单个目标：
xapp -r xxx.yml -t https://www.example.com
echo https://www.example.com | xapp -r xxx.yml
# 指定指纹扫描多个目标：
xapp -r xxx.yml -t https://www.example.com -t https://www.example2.com
xapp -r xxx.yml -i targets.txt
cat targets.txt | xapp -r xxx.yml
# 指定多个指纹进行扫描：
xapp -r xxx.yml -r yyy.yml -t https://www.example.com
xapp -r "./finger/web/*.yml" -t https://www.example.com
xapp -r "./finger/**/*.yml" -t https://www.example.com
# 指定group进行扫描：
xapp -g web.list -t https://www.example.com
```

下载地址

```
Github:
https://github.com/chaitin/xray/releases?q=xapp
(国外速度快)CT stack:
https://stack.chaitin.com/tool/detail/1311 (国内速度快)
xapp 跨平台支持，下载时选择需要的版本下载。
```

EHole_magic

EHole(棱洞)魔改。可对路径进行指纹识别；支持识别出来的重点资产进行漏洞检测(支持从hunter和fofa中提取资产)、默认口令提示、waf识别等功能

使用

poc检测默认不开启，在poc.ini中将poc=no改为poc=yes开启

ftp爆破默认不开启，在poc.ini中将brute=no改为brute=yes开启

路径进行指纹识别默认不开启，在poc.ini中将route=no改为route=yes开启

waf识别：发送正常 `HTTP` 请求，并判断是否存在 `WAF` 若存在根据指纹判断其类型-->若正常 `HTTP` 检测不出 `WAF` ，则附加恶意的请求尝试出发 WAF 并分析其类型

无害检测：poc.ini中设置waf_harmless=yes启用

有害检测：poc.ini中设置waf_harmful=yes启用

fofa识别

注意：从FOFA识别需要配置FOFA 密钥以及邮箱，在config.ini内配置好密钥以及邮箱即可使用。

搜索无结果 解决方案：如：将domain="baidu.com"改为domain='"baidu.com"'

```
ehole finger -s domain="baidu.com"  // 支持所有fofa语法
```

hunter识别

注意：从hunter识别需要配置hunter 密钥，在config.ini内配置好密钥即可使用。

搜索无结果 与fofa解决方案相同

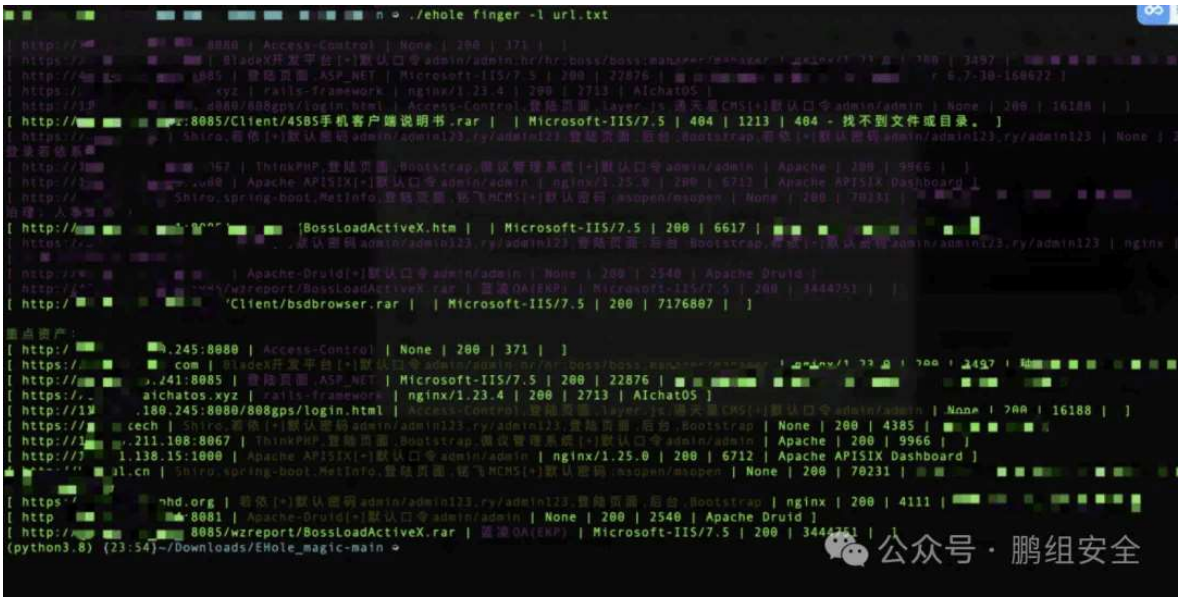
```
ehole finger -b ip="180.140.20.182"  // 支持所有hunter语法
```

多个url识别

```
ehole finger -l 1.txt  // 从文件中加载url扫描
```

单个目标识别

```
ehole finger -u http://www.baidu.com // 单个url检测
```



下载地址

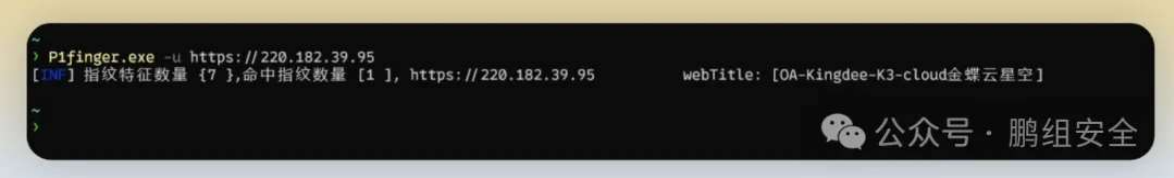
```
github:
https://github.com/lemonlove7/EHole_magic
鹏组安全社区:
https://comm.pgpsec.cn/54.html
```

P1finger

P1finger 红队行动下的重点资产指纹识别工具

单个目标探测

```
P1finger -u [target]
```



多目标探测

```
P1finger -uf [target file]
```

下载地址

```
github:
https://github.com/P001water/P1finger?tab=readme-ov-file
```

hfinger

一个用于web框架、CDN和CMS指纹识别的高性能命令行工具

单个目标探测

```
./hfinger -u http://x.x.x
```

多目标探测

```
./hfinger -f urls.txt
```

下载地址

```
github:
https://github.com/HackAllSec/hfinger
```

👇点击下方链接查看详细介绍👇

鹏组安全社区VIP福利介绍V1.2版本-社区介绍

社区地址：https://comm.pgpsec.cn/user

好文分享　　收藏　　赞一下最美　点在看哦