

【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

```
1 ./xapp_darwin_amd64
```

```
(python3.8) {10:39}~/Desktop/tools ◀ ./xapp_darwin_amd64
┌───┴───┐
┌─XRAY─┴─┐
└─v0.0.2─┘
[INF] 24-08-31 10:40:06 更新配置文件于以下位置: /Users/xiaobai/.xray/xapp/xapp-config.example.yaml [app.go:385]
[INF] 24-08-31 10:40:06 使用以下位置的配置文件: /Users/xiaobai/.xray/xapp/xapp-config.yaml [app.go:447]
[INF] 24-08-31 10:40:06 未能正确加载配置文件或配置文件不存在, 使用默认配置 [app.go:449]
[ERR] 24-08-31 10:40:06 detect-url:util-reminder: 未接收到任何探测目标 [reminder.go:39]
XAPP:

示例:
  Scan single target:    xapp -t http://192.168.1.1:8000
  L> multiple targets:  xapp -t http://192.168.1.1:8000 -t http://192.168.1.1:8001
  L> target file:       xapp -i a.txt
  Show plugin:          xapp -v
  L> run one plugin:    xapp -t http://192.168.1.1:8000 -r "./finger/finger.yml"
  L> run plugins:       xapp -t http://192.168.1.1:8000 -r "./finger/*.yml"

描述:
  web application scanner

命令:
  lint  对 yaml 脚本进行静态格式校验
  score 对 yaml 指纹脚本进行评分
  help, h Shows a list of commands or help for one command
```

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

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

```
(python3.8) {10:56}~/Desktop/tools ◉ ./xapp_darwin_amd64 -t http://x.x.x
[INF] 24-08-31 10:56:24 使用以下位置的配置文件: /Users/xiaobai/.xray/xapp/xapp-config.yaml [app.go:447]
[INF] 24-08-31 10:56:26 [1] website: [302 Moved Temporarily] http://180.167.36.202:91/
└─ Apache[!:-]
  └─ fofa: header="Server: Apache" || body="<title>Test Page for Apache Installation</title>" || body="<TITLE>Test Page for the SSL/TLS-aware
tallation on Web Site</TITLE>" || body="<html><body><h1>It works!</h1></body></html>" || body="<html>Apache is functioning normally</html>" || body="<body><center>This
g shared among many domains.<br>To view the domain you are looking for, simply enter the domain name in the location bar of your web browser.<br>"
  └─ 登陆页面[!:-]
    └─ fofa: body="type=\"password\"" || body="登录"
  └─ 宏景HCM管理系统[!:-]
    └─ fofa: body="人力与人才信息管理系统"
(python3.8) {10:56}~/Desktop/tools ◉
```

扫描多个url

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

```
(python3.8) {10:58}~/Desktop/tools ◉ ./xapp_darwin_amd64 -i urls.txt
[INF] 24-08-31 10:59:52 使用以下位置的配置文件: /Users/xiaobai/.xray/xapp/xapp-config.yaml [app.go:447]
[INF] 24-08-31 10:59:54 [1] website: [200 OK] http://x.x.x
└─ Apache[!:-]
  └─ fofa: header="Server: Apache" || body="<title>Test Page for Apache Inst
tallation on Web Site</TITLE>" || body="<html><body><h1>It works!</h1></body></html>" || body="<html>A
g shared among many domains.<br>To view the domain you are looking for, simply enter the domain name i
[INF] 24-08-31 10:59:54 [2] website: [200 OK] http://x.x.x
└─ Apache[!:-]
  └─ fofa: header="Server: Apache" || body="<title>Test Page for Apache Inst
tallation on Web Site</TITLE>" || body="<html><body><h1>It works!</h1></body></html>" || body="<html>A
g shared among many domains.<br>To view the domain you are looking for, simply enter the domain name i
[INF] 24-08-31 10:59:54 [3] website: [200 OK] http://x.x.x
└─ OpenResty[!:-]
  └─ fofa: body="<center>openresty/" || header="ngx_openresty" || body="Than
e this page, the OpenResty web platform is successfully installed and working" || header="server: open
海康威视综合安防管理平台[!:-]
  └─ fofa: title="综合安防管理平台" || icon_hash="808437027"
[INF] 24-08-31 10:59:54 [4] website: [302 Moved Temporarily] http://x.x.x
└─ 登陆页面[!:-]
  └─ fofa: body="type=\"password\"" || body="登录"
└─ Apache[!:-]
  └─ fofa: header="Server: Apache" || body="<title>Test Page for Apache Inst
tallation on Web Site</TITLE>" || body="<html><body><h1>It works!</h1></body></html>" || body="<html>A
g shared among many domains.<br>To view the domain you are looking for, simply enter the domain name i
  └─ 宏景HCM管理系统[!:-]
    └─ fofa: body="人力与人才信息管理系统"
[INF] 24-08-31 10:59:54 [5] website: [200 ] https://x.x.x
└─ PHP[!:-]
  └─ fofa: header="x-powered-by: php" || body=".php?" || header="php_errors"
  └─ Advantech-WebAccess[!:-]
    └─ fofa: body="/bw_template1.dwt" && body="/broadweb/webaccessclientsetup.
/broadweb/WebAccessClientSetup.exe" || body="/broadWeb/bwuconfig.asp" || header="advantech webaccess"
e" || body="<html><!-- #BeginTemplate \"/Templates/bw_template1.dwt\" -->" || body="<a href=\" /broadwe
ntech webaccess 首页"
  └─ Phusion[!:-]
    └─ fofa: header="Phusion"
[INF] 24-08-31 10:59:56 [6] website: [302 Redirect] http://x.x.x
└─ 海康威视 (Hikvision) [!:-]
  └─ fofa: header="Hikvision" || header="_goaheadwebSessionId" || header="DV
Hikvision-Cameras-and-Surveillance[!:-]
```

更多用法

```
1 # 扫描单个url
2 xapp -t http://www.test.com
3 # 扫描多个url
4 xapp -i urls.txt
5 # 指定指纹扫描单个目标:
6 xapp -r xxx.yml -t https://www.example.com
7 echo https://www.example.com | xapp -r xxx.yml
8 # 指定指纹扫描多个目标:
9 xapp -r xxx.yml -t https://www.example.com -t https://www.example2.com
10 xapp -r xxx.yml -i targets.txt
11 cat targets.txt | xapp -r xxx.yml
12 # 指定多个指纹进行扫描:
13 xapp -r xxx.yml -r yyy.yml -t https://www.example.com
14 xapp -r "./finger/web/*.yml" -t https://www.example.com
15 xapp -r "./finger/**/*.yml" -t https://www.example.com
16 # 指定group进行扫描:
17 xapp -g web.list -t https://www.example.com
```

下载地址

```
1 Github:
2 https://github.com/chaitin/xray/releases?q=xapp
3 (国外速度快)CT stack:
4 https://stack.chaitin.com/tool/detail/1311 (国内速度快)
5 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"

```
1 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

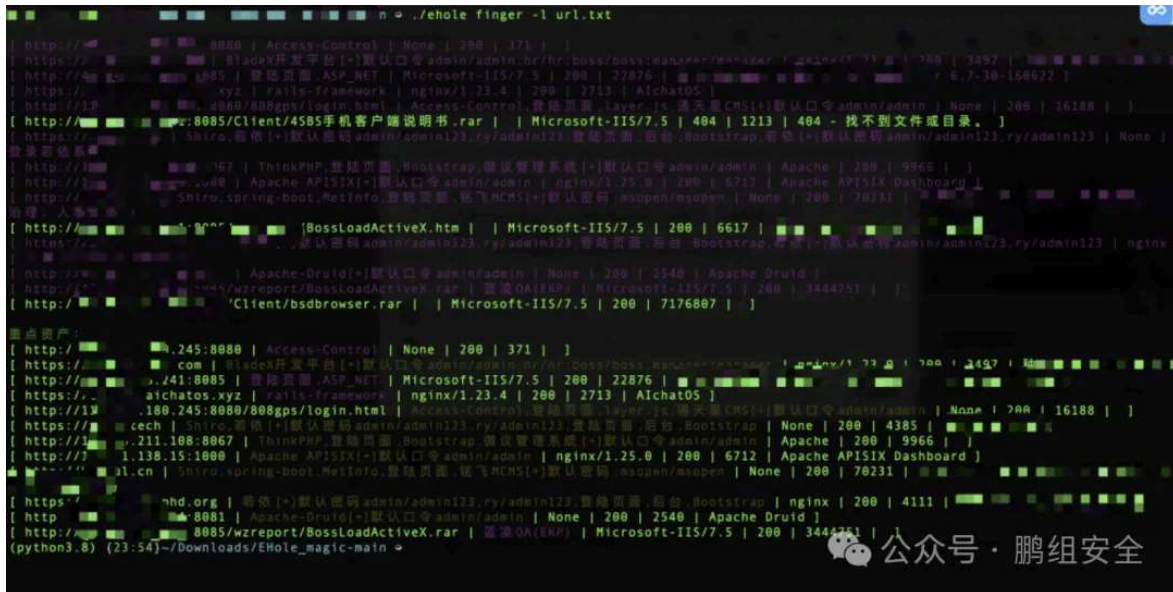
```
1 ehole finger -b ip="180.140.20.182" // 支持所有hunter语法
```

多个url识别

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

单个目标识别

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



下载地址

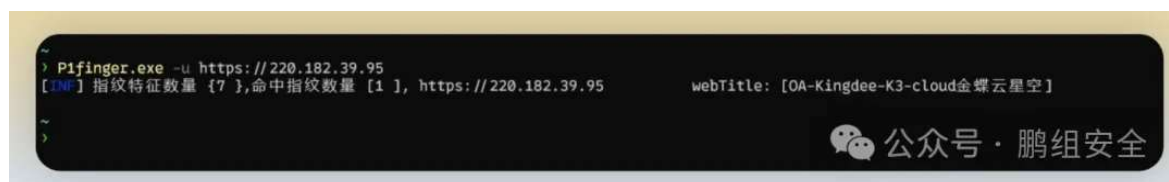
- 1 github:
- 2 https://github.com/LemonLove7/EHole_magic
- 3 鹏组安全社区:
- 4 <https://comm.pgpsec.cn/54.html>

P1finger

P1finger 红队行动下的重点资产指纹识别工具

单个目标探测

- 1 `P1finger -u [target]`



多目标探测

- 1 `P1finger -uf [target file]`



下载地址

- 1 github:
- 2 <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

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

```
(python3.8) {11:34}~/Downloads/hfinger_darwin_amd64 @ ./hfinger -u http://x.x.x
hfinger
v1.0.5 By:Hack All Sec
[*] Total number of fingerprints: 1451
[*] Total number of products, web frameworks, and CMS: 1213
[08-31 11:34:31] [+] [http://x.x.x/dex.asp] [Hikvision IP Camera] [200] [Hikvision-Webs] [index]
```

多目标探测

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

```
(python3.8) {11:34}~/Downloads/hfinger_darwin_amd64 @ ./hfinger -f /Use...urls.txt
hfinger
v1.0.5 By:Hack All Sec
[*] Total number of fingerprints: 1451
[*] Total number of products, web frameworks, and CMS: 1213
[08-31 11:35:46] [+] [http://x.x.x/3080/] [PHP] [200] [Apache/2.2.3 (Unix) PHP/4.4.4] [None]
[08-31 11:35:46] [+] [http://x.x.x/3071/] [PHP] [200] [Apache/2.2.19 (Win32) PHP/5.2.17] [None]
[08-31 11:35:46] [*] [http://x.x.x/91/1084025ab54c0d51/] [Not Matched] [404] [Apache-Coyote/1.1] [ERROR: PAGE INFO]
[08-31 11:35:46] [+] [http://x.x.x/8001/] [海康威视综合安防管理平台] [404] [Apache/2.2.19 (Ubuntu)] [ERROR: PAGE INFO]
[08-31 11:35:46] [*] [https://x.x.x/ng.com.cn/137e6af34a7c4438/] [Not Matched] [200] [Apache/2.4.18 (Debian)] [None]
[08-31 11:35:47] [+] [http://x.x.x/8080/index.asp] [Hikvision IP Camera] [200] [Hikvision-Webs] [index]
```

下载地址

- 1 github:
- 2 <https://github.com/HackAllSec/hfinger>

★ 付费圈子

欢迎加入社区！

代码审计+免杀+渗透学习资源+各种资料文档+各种工具+付费会员

进成员内部群



👉 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>

“ 大家好! 在等待已久之后, 我们非常激动地宣布, 全新的APP终于正式上线了! 无论你是工作狂还是学业繁忙, 还是想要更多时间去追逐自己的兴趣爱好, 我们的APP将成为你生活中的得力助手, 让你事半功倍, 从容面对各种挑战。

请使用手机默认浏览器打开进行安装

👤 公众号 · 鹏组安全

免责声明

由于传播、利用本公众号渗透安全团队所提供的信息而造成的任何直接或者间接的后果及损失, 均由使用者本人负责, 公众号渗透安全团队及作者不为此承担任何责任, 一旦造成后果请自行承担! 如有侵权烦请告知, 我们会立即删除并致歉。谢谢!

好文分享 收藏 赞一下最美 点在看哦

