

Xray安装及使用

一款半开源的功能强大的安全评估工具，支持主动扫描和被动扫描。

🌟 Demo

```
→ release git:(master) x./xray_darwin_amd64
```

[🏠 使用文档](#) [↓ 下载地址](#)

注意：Xray 不开源，直接下载构建的二进制文件即可，仓库内主要为社区贡献的 poc，每次 Xray 发布将自动打包。

基础爬虫模式进行扫描（主动扫描）

```
xray webscan --basic-crawler http://testphp.vulnweb.com --html-output vuln.html
```

```
^@[INFO] 2021-12-21 22:08:07 [basic-crawler:crawler.go:351] workingTask:9 reaminTask:0 WorkerCount:11
[*] scanned: 0, pending: 20, requestSent: 46, latency: 452.86ms, failedRatio: 0.00%
[Vuln: dirscan]-output result.json+-html-output report.html
Target      "http://testphp.vulnweb.com/crossdomain.xml"
VulnType    "sensitive/crossdomain"
Payload     "/crossdomain.xml"

[Vuln: dirscan]po
Target      "http://testphp.vulnweb.com/.idea/workspace.xml"
VulnType    "config/ide"
Payload     "/.idea/workspace.xml"

[INFO] 2021-12-21 22:08:12 [basic-crawler:crawler.go:351] workingTask:8 reaminTask:0 WorkerCount:11
[*] scanned: 0, pending: 29, requestSent: 81, latency: 517.93ms, failedRatio: 0.00%
^@[INFO] 2021-12-21 22:08:17 [basic-crawler:crawler.go:351] workingTask:2 reaminTask:0 WorkerCount:11
[*] scanned: 0, pending: 38, requestSent: 117, latency: 533.34ms, failedRatio: 0.00%
[INFO] 2021-12-21 22:08:18 [basic-crawler:basic_crawler.go:78] crawler stopped
[INFO] 2021-12-21 22:08:19 [default:dispatcher.go:433] processing GET http://testphp.vulnweb.com/index.php
[*] scanned: 0, pending: 38, requestSent: 187, latency: 505.86ms, failedRatio: 0.00%
^@[Vuln: dirscan]
Target      "http://testphp.vulnweb.com/.idea/modules.xml"
VulnType    "config/ide"
Payload     "/.idea/modules.xml"
```

打开 vuln.html 查看扫描报告

Web Vulnerabilities				HTML	Search Target	Reload
ID	Target	PluginName / VulnType	CreateTime			
+	1	http://testphp.vulnweb.com/crossdomain.xml	dirscan/sensitive/crossdomain	2021-12-21 22:08:09		
+	2	http://testphp.vulnweb.com/idea/workspace.xml	dirscan/config/ide	2021-12-21 22:08:10		
+	3	http://testphp.vulnweb.com/idea/modules.xml	dirscan/config/ide	2021-12-21 22:08:27		
+	4	http://testphp.vulnweb.com/index.bak	dirscan/backup/default	2021-12-21 22:08:50		
+	5	http://testphp.vulnweb.com/images/	dirscan/directory/default	2021-12-21 22:08:52		
+	6	http://testphp.vulnweb.com/guestbook.php	xss/reflected/default	2021-12-21 22:09:12		
+	7	http://testphp.vulnweb.com/guestbook.php	xss/reflected/default	2021-12-21 22:09:13		
+	8	http://testphp.vulnweb.com/search.php	xss/reflected/default	2021-12-21 22:09:15		
+	9	http://testphp.vulnweb.com/search.php	baseline/sensitive/server-error	2021-12-21 22:09:16		
+	10	http://testphp.vulnweb.com/index.zip	dirscan/backup/default	2021-12-21 22:09:30		
+	11	http://testphp.vulnweb.com/artists.php	baseline/sensitive/server-error	2021-12-21 22:09:38		
+	12	http://testphp.vulnweb.com/artists.php	sqldef/blind-based/default	2021-12-21 22:09:54		
+	13	http://testphp.vulnweb.com/listproducts.php	baseline/sensitive/server-error	2021-12-21 22:09:56		

代理模式进行扫描（被动扫描）

1.使用命令生成证书

```
xray genca
```

```
~/tools/xray xray genca

Version: 1.8.2/79e7dd56/COMMUNITY

CA certificate ca.crt and key ca.key generated

~/tools/xray ls
ca.crt      ca.key      config.yaml xray
```

2.需要在本机和浏览器中分别安装证书。本机安装直接点击证书进行安装即可，浏览器选择右上角 - 设置选项



同步并保存数据

登录

新建标签页

⌘T

新建窗口

⌘N

新建隐私窗口

⇧⌘P

书签



历史



下载

⌘J

密码

扩展和主题

⇧⌘A

打印...

⌘P

另存页面为...

⌘S

在页面中查找...

⌘F

缩放



100%



设置

⌘,

更多工具



帮助



3.选择 隐私与安全-查看证书-导入 对应的证书 ca.crt



4.设置代理

vim config.yaml 配置监听地址

```
allow_ip_range: [] # 允许的 ip, 可以是 ip 或者 cidr 字符串
restriction: # 代理能够访问的资源限制, 以下各项为空表示不限制
  hostname_allowed: [ 127.0.0.1 ] # 允许访问的 Hostname, 支持格式如 t.com, *.t.com, 1.1.1.1, 1.1.1.1/24, 1.1-4.1.1-8
  hostname_disallowed: # 不允许访问的 Hostname, 支持格式如 t.com, *.t.com, 1.1.1.1, 1.1.1.1/24, 1.1-4.1.1-8
    - '*google*'
    - '*github*'
    - '*.gov.cn'
```

浏览器安装 FoxyProxy Standard 插件 [安装地址](#)

浏览器中选择扩展->寻找更多附加组件-> 搜索 FoxyProxy

推荐

扩展

主题

插件

管理您的扩展



以下的部分推荐是基于您的已安装附加组件、选项设置和使用统计得出的个性化结果。[详细了解](#)



Video DownloadHelper
作者: mig

添加至 Firefox

轻松下载视频。适用于 YouTube、Facebook、Vimeo、Twitch、Dailymotion、Periscope 等数百个视频网站。

★★★★★ 用户量: 2,084,553



New Tab Override
作者: Sören Hentzschel

添加至 Firefox

设置每次打开新标签页时您看到的页面。

★★★★★ 用户量: 72,778



Dark Reader
作者: Alexander Shutau

添加至 Firefox

启用夜间模式以获得更好的视觉体验。

★★★★★ 用户量: 740,680



Tree Style Tab
作者: Piro (piro_or)

添加至 Firefox

您是否有一大堆打开的标签页? 试试在整齐的侧栏中进行管理。

★★★★★ 用户量: 141,325

Firefox 设置

附加组件帮助

寻找更多附加组件

隐私政策

扩展 主题 更多...

查找附加组件

FoxyProxy Standard
作者: Eric H. Jung

FoxyProxy是一个高级的代理管理工具,它完全替代了Firefox有限的代理功能。它提供比SwitchProxy、ProxyButton、QuickProxy、xyzproxy、ProxyTex、TorButton等等更多的功能。

移除

推荐

172,591 用户 573 评价 4.2 星

5	★	377
4	★	76
3	★	41
2	★	15
1	★	64

为您的体验打分

您使用 FoxyProxy Standard 的体验如何?

登录以评价此扩展

举报此附加组件的滥用行为

阅读全部 573 条评价

屏幕截图

FoxyProxy 配置

1. 点击添加按钮



FoxyProxy 选项



添加



导入



Import Proxy List



导出



全部删除



删除浏览器数据



查询我的 IP



日志



关于

2.设置转发地址为 127.0.0.1，端口为 7777

标题或描述 (可选)	代理类型
<input type="text" value="xray"/>	HTTP
颜色	代理 IP 地址或 DNS 名称
<div>#66cc66</div>	127.0.0.1
	端口
	7777
	用户名 (可选)
	username
	密码 (可选)

<div>取消 保存并添加另一个 保存并编辑模式 保存</div>	

3.开启代理

选择刚才配置好的 xray



开启 xray 被动扫描

```
xray webscan --listen 127.0.0.1:7777 --html-output dvwa-vul.html
```

运行 DVWA

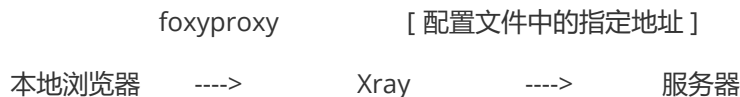
```
docker run -d --name dvwa -p 8080:80 -p 33060:3306 sagikazarmark/dvwa
```

在DVWA中进行操作和访问，之后打开 dvwa-vul.html 查看漏洞

ID	Target	PluginName / VulnType	CreateTime
1	http://127.0.0.1:8080/README.md	dirscan/debug/readme	2021-12-21 23:40:09
2	http://127.0.0.1:8080/phpinfo.php	dirscan/debug/php	2021-12-21 23:40:10
3	http://127.0.0.1:8080/CHANGELOG.md	dirscan/debug/readme	2021-12-21 23:40:10
4	http://127.0.0.1:8080/vulnerabilities/sql/help/	dirscan/directory/help	2021-12-21 23:40:19
5	http://127.0.0.1:8080/vulnerabilities/sql/source/	dirscan/directory/source	2021-12-21 23:40:19
6	http://127.0.0.1:8080/vulnerabilities/sql/	xss/reflected/default	2021-12-21 23:40:19
7	http://127.0.0.1:8080/vulnerabilities/upload/help/	dirscan/directory/help	2021-12-21 23:40:29
8	http://127.0.0.1:8080/vulnerabilities/upload/source/	dirscan/directory/source	2021-12-21 23:40:29
9	http://127.0.0.1:8080/vulnerabilities/upload/	xss/reflected/default	2021-12-21 23:40:29
10	http://127.0.0.1:8080/vulnerabilities/csrf/help/	dirscan/directory/help	2021-12-21 23:40:31
11	http://127.0.0.1:8080/vulnerabilities/csrf/source/	dirscan/directory/source	2021-12-21 23:40:31
12	http://127.0.0.1:8080/vulnerabilities/csrf/	xss/reflected/default	2021-12-21 23:40:31
13	http://127.0.0.1:8080/vulnerabilities/captcha/help/	dirscan/directory/help	2021-12-21 23:40:32
14	http://127.0.0.1:8080/vulnerabilities/captcha/source/	dirscan/directory/source	2021-12-21 23:40:32
15	http://127.0.0.1:8080/vulnerabilities/captcha/	xss/reflected/default	2021-12-21 23:40:33
16	http://127.0.0.1:8080/vulnerabilities/sql/	baseline/sensitive/server-error	2021-12-21 23:40:36

流量走向

代理模式下的基本架构为，扫描器作为中间人，首先原样转发流量，并返回服务器响应给浏览器等客户端，通讯两端都认为自己直接与对方对话，同时记录该流量，然后修改参数并重新发送请求进行扫描。



快速使用

在使用之前，请务必阅读并同意 [License](#) 文件中的条款，否则请勿安装使用本工具。

1. 使用基础爬虫爬取并对爬虫爬取的链接进行漏洞扫描

```
xray webscan --basic-crawler http://example.com --html-output vuln.html
```

2. 使用 HTTP 代理进行被动扫描

```
xray webscan --listen 127.0.0.1:7777 --html-output proxy.html
```

设置浏览器 http 代理为 `http://127.0.0.1:7777`，就可以自动分析代理流量并扫描。

3. 只扫描单个url，不使用爬虫

```
xray webscan --url http://example.com/?a=b --html-output single-url.html
```

4. 手动指定本次运行的插件

默认情况下，将会启用所有内置插件，可以使用下列命令指定本次扫描启用的插件。

```
xray webscan --plugins cmd-injection,sqldet --url http://example.com
xray webscan --plugins cmd-injection,sqldet --listen 127.0.0.1:7777
```


5. 指定输出文件的格式

可以指定将本次扫描的漏洞信息输出到某个文件中:

```
xray webscan --url http://example.com/?a=b \  
--text-output result.txt --json-output result.json --html-output report.html
```

[报告样例](#)

其他用法请阅读文档: <https://docs.xray.cool>