

# 报文包讲解

---

报文包讲解

HTTP

HTTP请求

**BurpSuite** 破解版安装

1.4.1 下载 java 环境

1.4.2 破解并激活 BurpSuite

**BurpSuite**超详细使用教程！

**goby**的使用与**xray**联动

一、Goby下载

二、Goby安装

三、Goby使用

四xray安装

概述

特点

支持的漏洞类型

下载与安装

使用参数

与xray联动

## HTTP

HTTP(超文本传输协议)是今天所有web应用程序使用的通信协议。最初，HTTP只是一个获取基本文本的静态资源而开发的简单协议，后来人们以各种形式扩展和利用它。使其能够支持如今常见的复杂分布式应用长须。HTTP使用于一种用于消息的模型：客户端送出一条请求信息，而后由服务器返回一条响应信息。该协议基本上不需要连接，虽然HTTP使用有状态的TCP协议作为它的传输机制，但每次请求与响应交换都会自动完成，并且可能使用不同的TCP连接

## HTTP请求

所有HTTP消息（请求与响应）中都包含一个或几个单行显示的消息头（header），然后是一个强制空白行，最后是消息主体（可选）。以下是一个典型的HTTP请求头

```
GET / HTTP/1.1
```

```
Host: www.baidu.com
Cookie: BAIDUID_BFESS=1877D00FA2AAEB1E09D36D982FE78F7A:FG=1
Sec-Ch-Ua: "Chromium";v="95", ";Not A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

**get:** 一个说明HTTP方法的动词，最常用的方法为GET，他的主要作用是从Web服务器获取一个资源。post head options put

**accept:** Accept: 浏览器支持的MIME类型分别是: text/html、application/xhtml+xml、application/xml和/

**MIME:** 多功能internet邮件扩充服务。

**text:** 用于标准化的表示的文本信息，文本信息可以是多种字符集和或者多种格式的；

text/html表示html文档

**application:** 用于传输应用程序数据或者二进制数据

application/xhtml+xml表示xhtml文档

application/xml: 表示xml文档

**Referer:** 消息头用于表示请求的原始URL

**Accept-Language:** 浏览器支持的余元，zh-en表示简体中文；zh表示中文

**User-Agent:** 消息头提供与浏览器或其他生成请求客户端软件有关的信息

**Host:** 消息头用于指定出现在被访问的完整URL中的主机名称

**Cookie:** 消息头用于提交服务器向客户端发布的其他参数

**Httponly:** 如果设置这个属性,将无法通过客户端javascript直接访问cookie

**connection:** 表示持久的客户端与服务器连接。**connection:keep-alive**

**X\_Forwarded\_For:**是用来识别通过HTTP代理或负载均衡方式连接到web服务器客户端最原始的ip地址的http请求字段

**Location:**这个消息头用于在重定向响应(那些状态码以3开头的响应)中说明重定向的目标。

**状态码:200 :** 本状态码表示已成功提交请求,且响应主体中包含请求结果

**302:.**本状态码将浏览器暂时重定向到另外一个在Location消息头中指定的URL.客户端应在随后的请求中恢复使用原始URL.

**400 Bad Request:**本状态码表示客户端提交了一个无效的HTTP请求。当以某种无效的方式修改请求时(例如在URL中插入二个空格符),可能会遇到这个状态码。

**404 Not Found:**本状态码表示所请求的资源并不存在。

**500 Internal Server Error**本状态码表示服务器在执行请求时遇到错误。

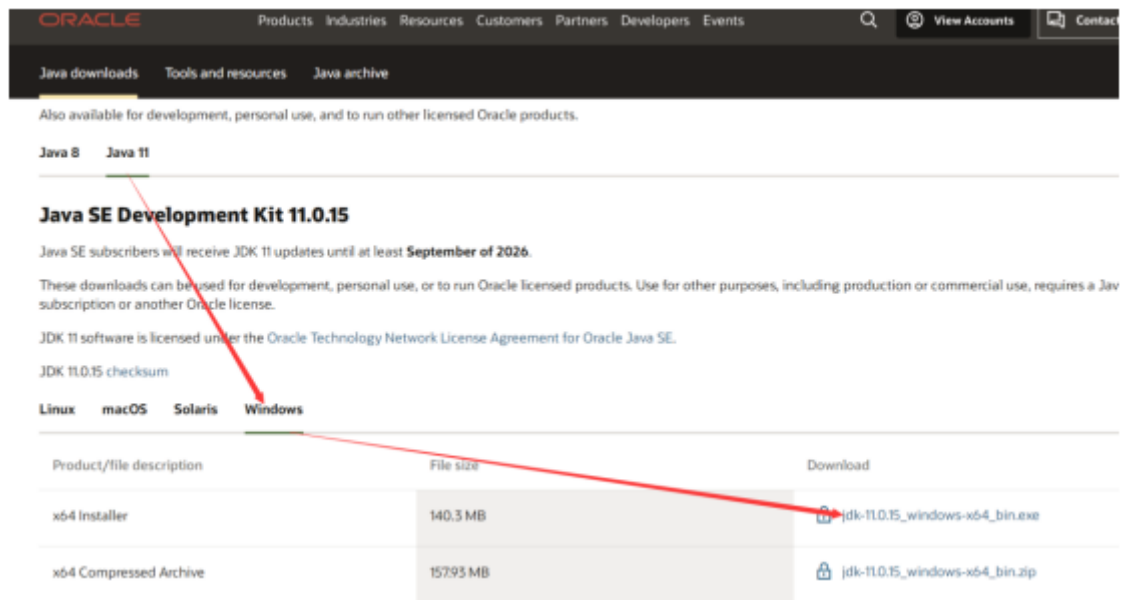
## BurpSuite 破解版安装

---

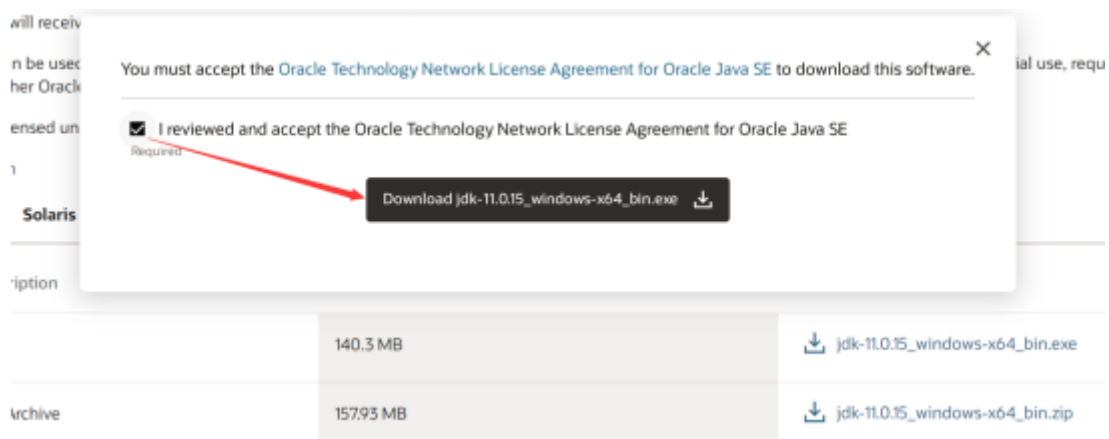
安装版本 BurpSuite\_Pro\_v2021.9.1 破解版本,需要在 windows10 系统上安装和使用

### 1.4.1 下载 java 环境

1、下载 jdk 环境: <https://www.oracle.com/java/technologies/downloads/#java11>



下载时需要登录 Oracle 账号，如果没有账号，可以先注册再登录。



2、下载完成后，双击打开安装，点击下一步。



安装目录保持默认即可。



安装完成后，点击关闭即可完成安装。

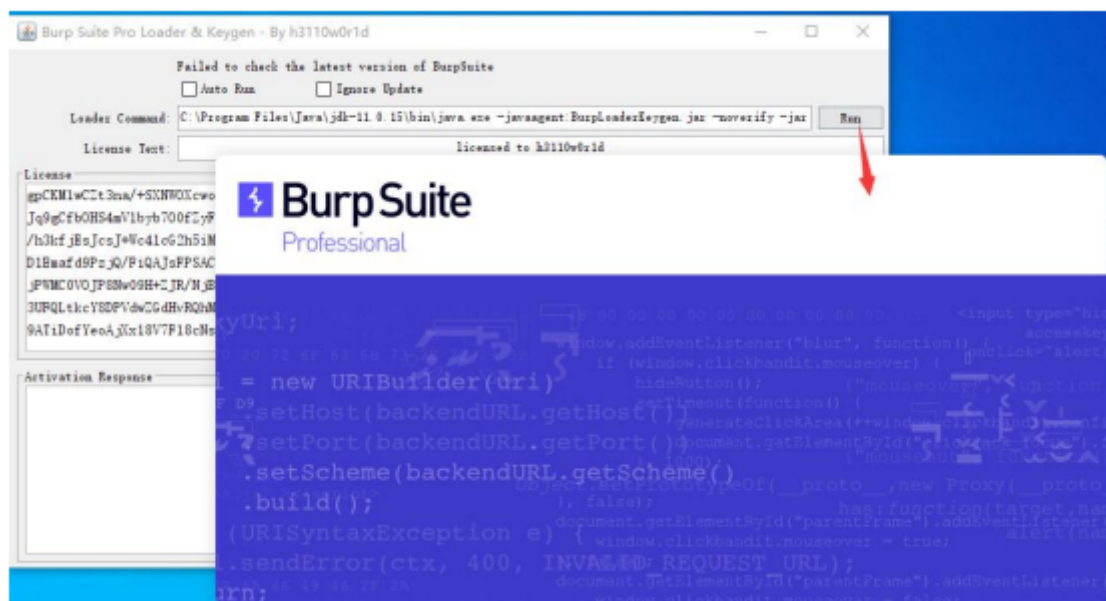


## 1.4.2 破解并激活 BurpSuite

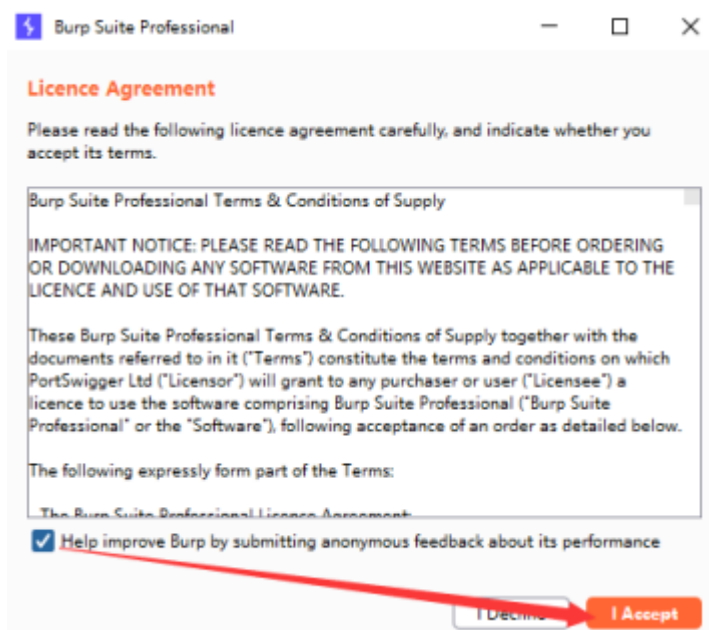
1、解压“BurpSuite\_Pro\_v2021.9.1 破解版本”安装包到虚拟机，“BurpLoaderKeygen”是破解注册机，需要先打开注册。

| BurpSuite_Pro_v2021.9.1破解版本 |                           |                 |                     |            |
|-----------------------------|---------------------------|-----------------|---------------------|------------|
|                             | 名称                        | 修改日期            | 类型                  | 大小         |
|                             | BurpLoaderKeygen          | 2022/3/24 17:25 | Executable Jar File | 19 KB      |
|                             | BurpSuite                 | 2021/4/4 2:42   | 图标                  | 5 KB       |
|                             | burpsuite_pro_v2021.9.1   | 2021/10/27 2:19 | Executable Jar File | 531,084 KB |
|                             | BurpSuiteLoader           | 2021/10/27 2:22 | Windows 批处理...      | 1 KB       |
|                             | BurpSuiteLoader.sh        | 2021/10/27 2:22 | SH 文件               | 1 KB       |
|                             | BurpSuiteLoader           | 2021/4/4 2:57   | VBScript Script ... | 1 KB       |
|                             | BurpSuiteLoader_v2021.9.1 | 2020/4/30 3:28  | Executable Jar File | 167 KB     |
|                             | config.cfg                | 2022/3/24 17:25 | CFG 文件              | 1 KB       |
|                             | 创建桌面快捷方式                  | 2021/10/27 4:08 | Windows 批处理...      | 2 KB       |

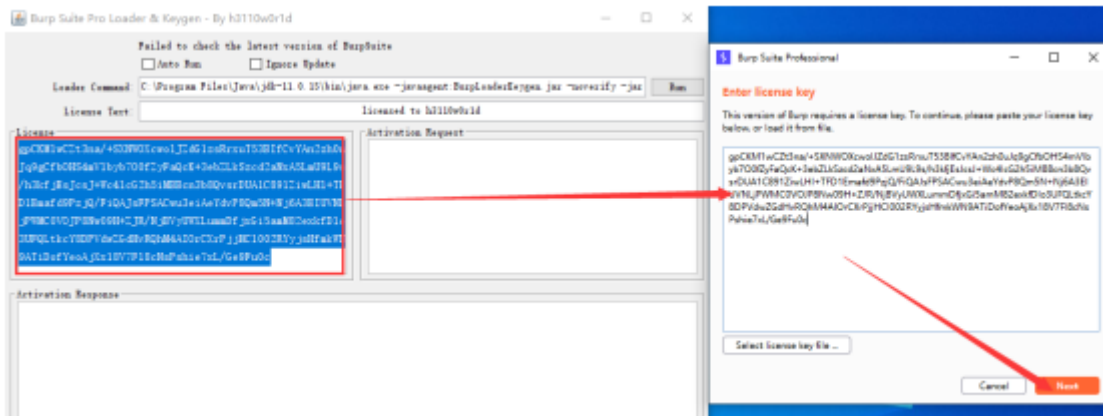
2、注册打开后，点击“Run”会自动调用左侧命令框中的命令打开 BurpSuite 程序。



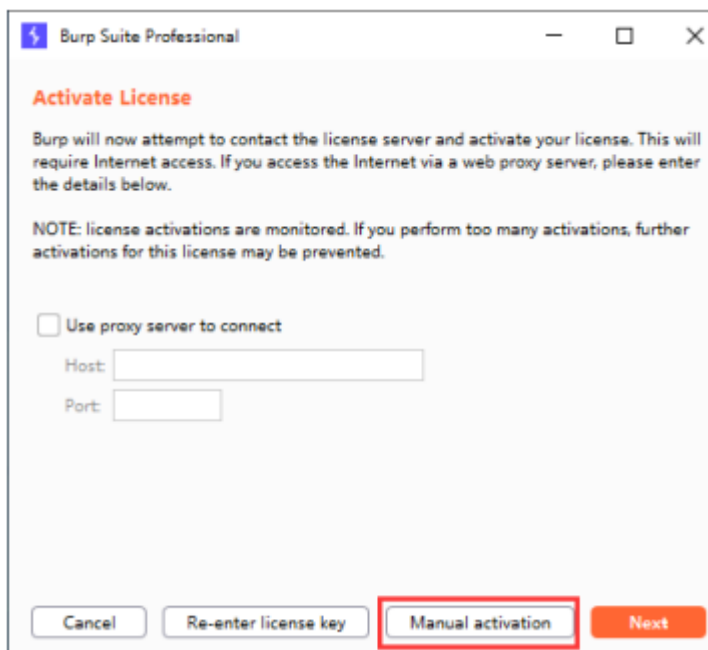
3、BuspSuite 打开后，点击“I Acceopt”我接发



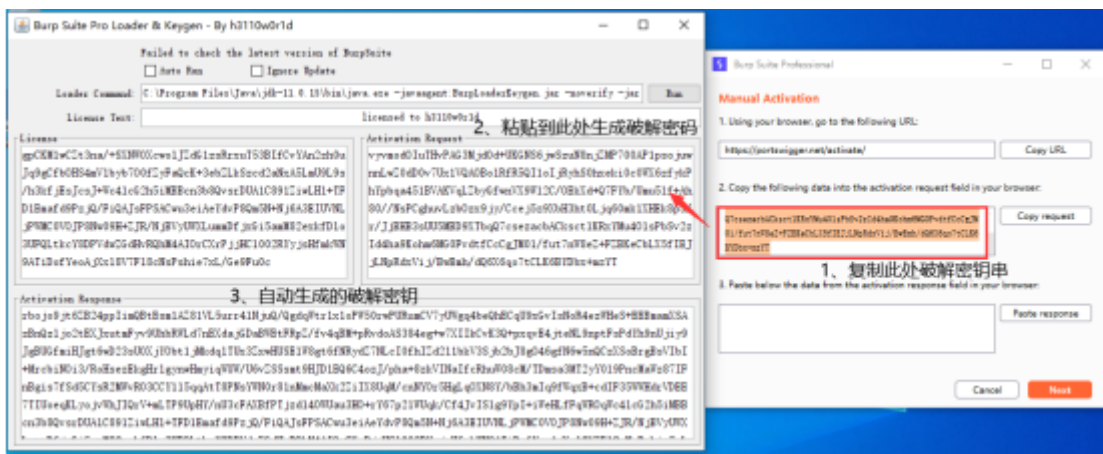
4、而后在注册机中全选 License 中的密钥，并复制到 BurpSuite 的密钥输入，并点击“Next”



5、此处代理设置不需要做任何操作，直接点击“Manual activation（人工激活）”



6、在 BurpSuite 中的第二项内容框中的把内容复制到注册机上的“Activation Request（激活请求）” 此时注册会自劢生成“Activation Response（激活反应）”中的破解密钥。

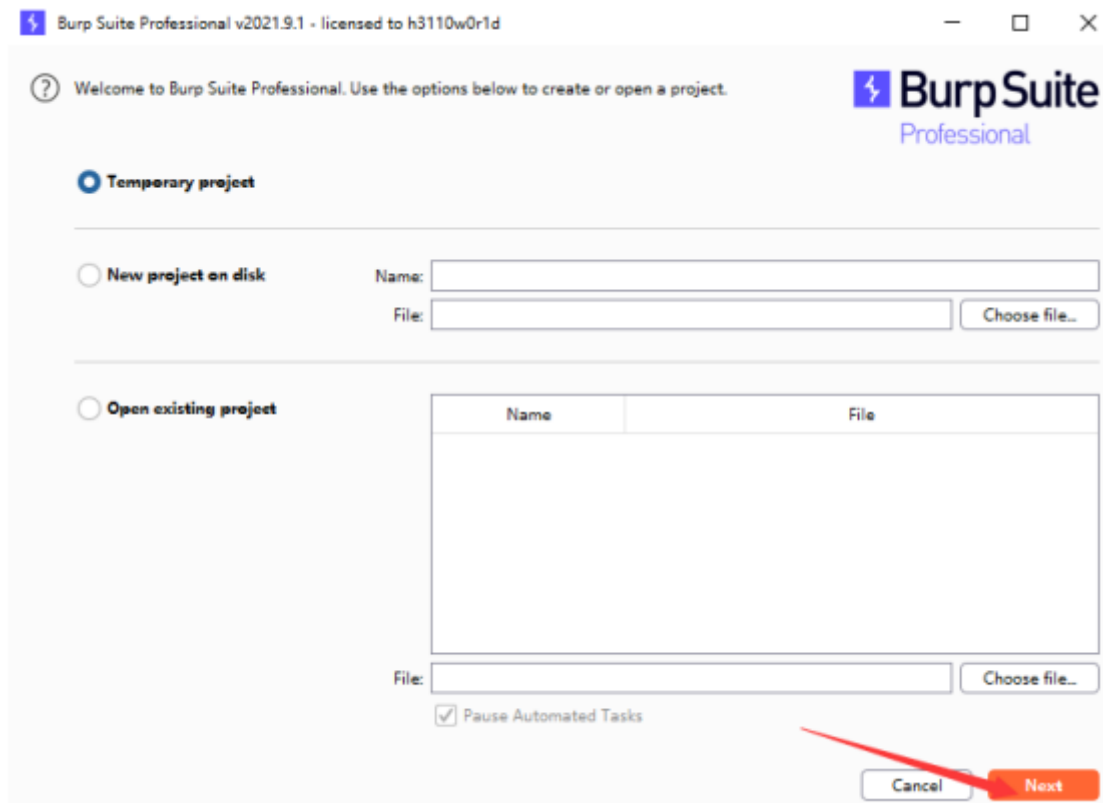


7、在注册机中的“Activation Response（激活反应）” 中的破解密钥，复制到 BurpSuite 中的激活密钥框中，并点击“Next”

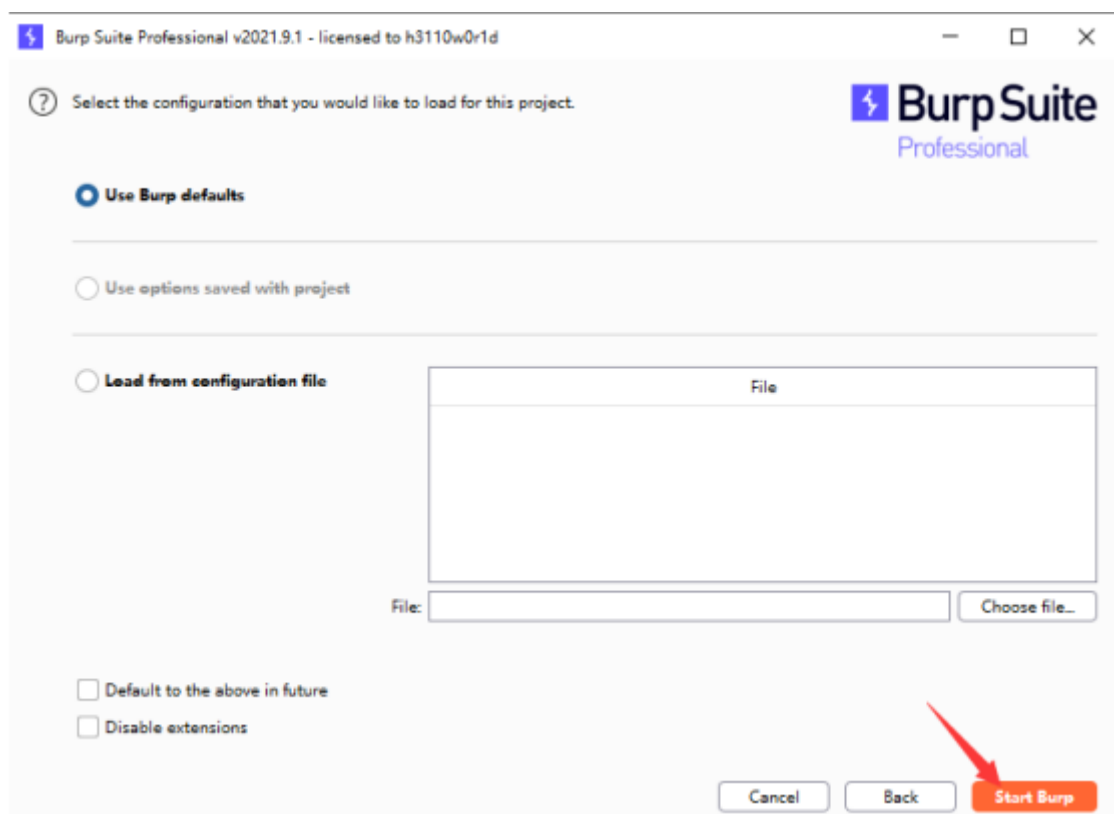








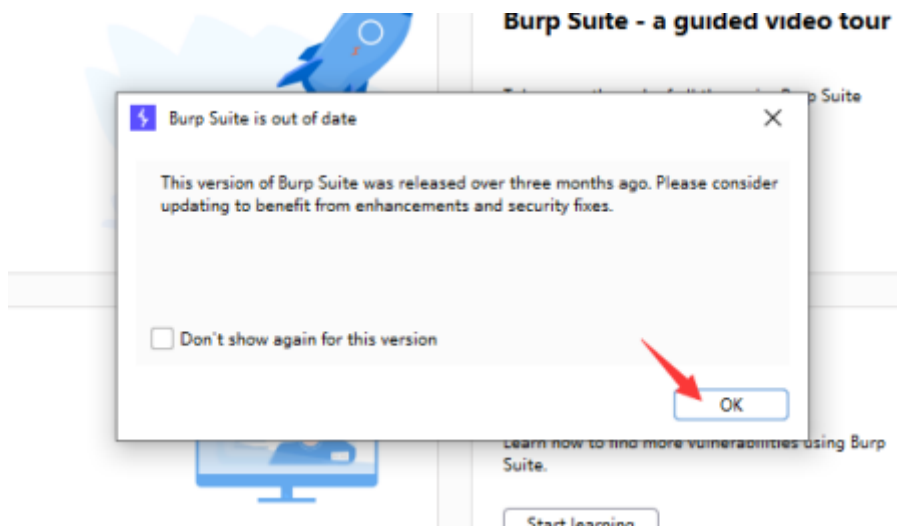
10、点击“Start Burp”按钮即可。



11、打开后有更新提示，可以直接点击“OK”。

内容提示：“This version of Burp Suite was released over three months ago. Please consider updating to benefit from enhancements and security fixes.”

这个版本的 BurpSuite 是三个多月前发布的，请考虑更新，以便从增强和安全修复中获益。”



注意：往后使用 BurpSuite 时，也是先打开注册机，并点击“Run”启动 BurpSuite。

## BurpSuite超详细使用教程！

---

看这个即可([https://blog.csdn.net/qq\\_53577336/article/details/122393296](https://blog.csdn.net/qq_53577336/article/details/122393296))

## goby的使用与xray联动

---

### 一、Goby下载

官网下载地址：(<https://cn.gobies.org/>)

Goby主要特性：

实战性：Goby并不关注漏洞库的数量有多少，而是关注真正用于实际攻击的漏洞数量，以及漏洞的利用深度（最小精准集合体，打造权威性）；

体系性：打通渗透前，渗透中，以及渗透后的完整流程完整DOM事件收集，自动化触发。






















高效性：利用积累的规则库，全自动的实现IT资产攻击面的梳理；效率提升数倍，发包更少速度更快、更精准；

平台性：发动广泛的安全人员的力量，完善上面提到的所有资源库；包括基于社区的数据共享，插件发布，漏洞共享等；

艺术性：安全工具原本就比较偏门，我们更多的关注功能而非美观度，所有大部分的安全工具都是其貌不扬；我们希望使用Goby能给大家带来感官上的享受。

## 二、Goby安装

下载到安装包并解压，打开Goby.exe即可。

|   |                                       |                 |         |           |
|---|---------------------------------------|-----------------|---------|-----------|
|    | api-ms-win-crt-runtime-l1-1-0.dll     | 2022/2/15 17:39 | 应用程序扩展  | 23 KB     |
|    | api-ms-win-crt-stdio-l1-1-0.dll       | 2022/2/15 17:39 | 应用程序扩展  | 25 KB     |
|    | api-ms-win-crt-string-l1-1-0.dll      | 2022/2/15 17:39 | 应用程序扩展  | 25 KB     |
|    | api-ms-win-crt-time-l1-1-0.dll        | 2022/2/15 17:39 | 应用程序扩展  | 21 KB     |
|    | api-ms-win-crt-utility-l1-1-0.dll     | 2022/2/15 17:39 | 应用程序扩展  | 19 KB     |
|    | blink_image_resources_200_percent.pak | 2022/2/15 17:39 | PAK 文件  | 5 KB      |
|    | content_resources_200_percent.pak     | 2022/2/15 17:39 | PAK 文件  | 1 KB      |
|    | content_shell.pak                     | 2022/2/15 17:39 | PAK 文件  | 7,307 KB  |
|    | d3dcompiler_47.dll                    | 2022/2/15 17:39 | 应用程序扩展  | 4,077 KB  |
|    | ffmpeg.dll                            | 2022/2/15 17:39 | 应用程序扩展  | 1,788 KB  |
|    | Goby.exe                              | 2022/2/15 17:39 | 应用程序    | 69,507 KB |
|    | icudtl.dat                            | 2022/2/15 17:39 | DAT 文件  | 9,933 KB  |
|    | libEGL.dll                            | 2022/2/15 17:39 | 应用程序扩展  | 17 KB     |
|    | libGLESv2.dll                         | 2022/2/15 17:39 | 应用程序扩展  | 3,763 KB  |
|    | LICENSE.electron.txt                  | 2022/2/15 17:39 | 文本文档    | 2 KB      |
|    | LICENSES.chromium.html                | 2022/2/15 17:39 | HTML 文档 | 1,862 KB  |
|    | msvcp140.dll                          | 2022/2/15 17:39 | 应用程序扩展  | 627 KB    |
|  | natives_blob.bin                      | 2022/2/15 17:39 | BIN 文件  | 171 KB    |
|  | node.dll                              | 2022/2/15 17:39 | 应用程序扩展  | 18,144 KB |
|  | ucrtbase.dll                          | 2022/2/15 17:39 | 应用程序扩展  | 993 KB    |
|  | ui_resources_200_percent.pak          | 2022/2/15 17:39 | PAK 文件  | 110 KB    |

CSDN @关键词

## 三、Goby使用

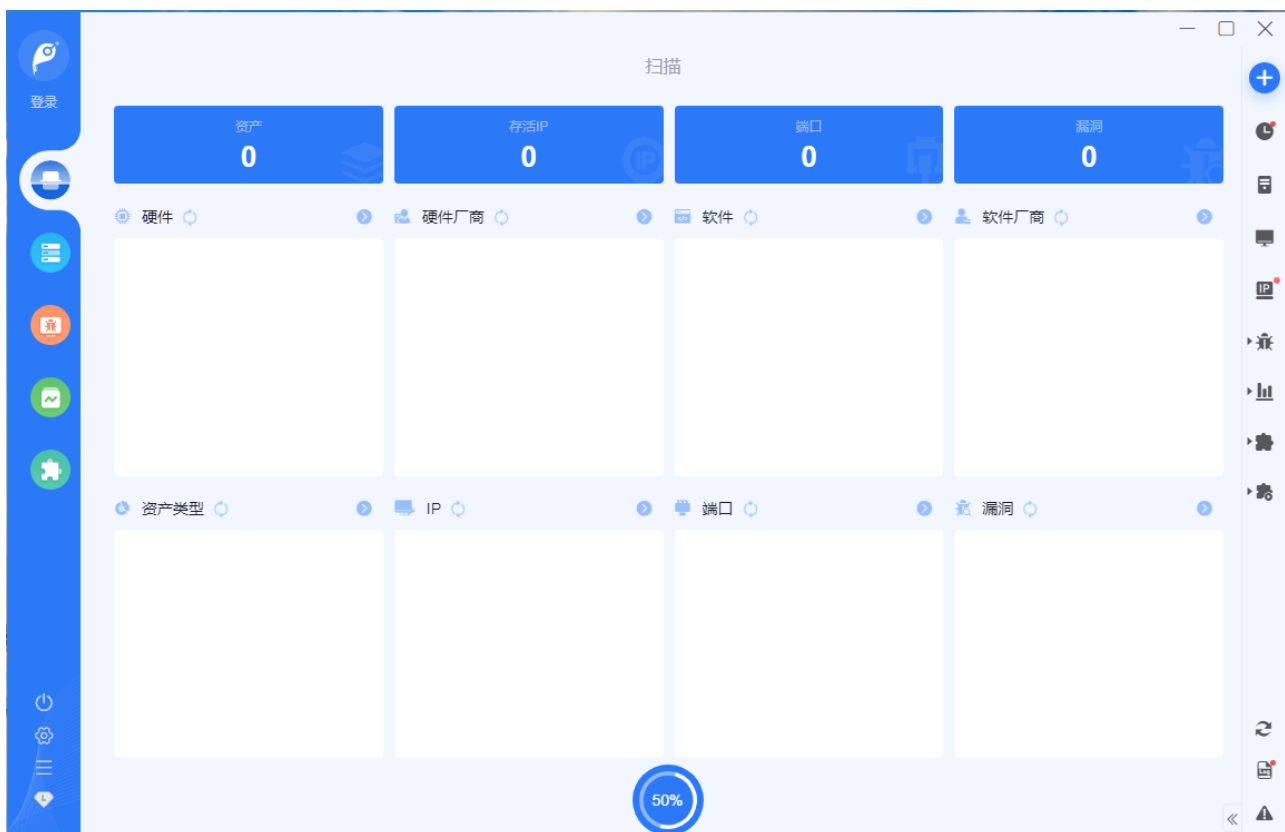
1.打开Goby到首页，左下角可以切换语言



2. 点击扫描，新建扫描任务。（不仅可以扫ip，还可以扫域名）

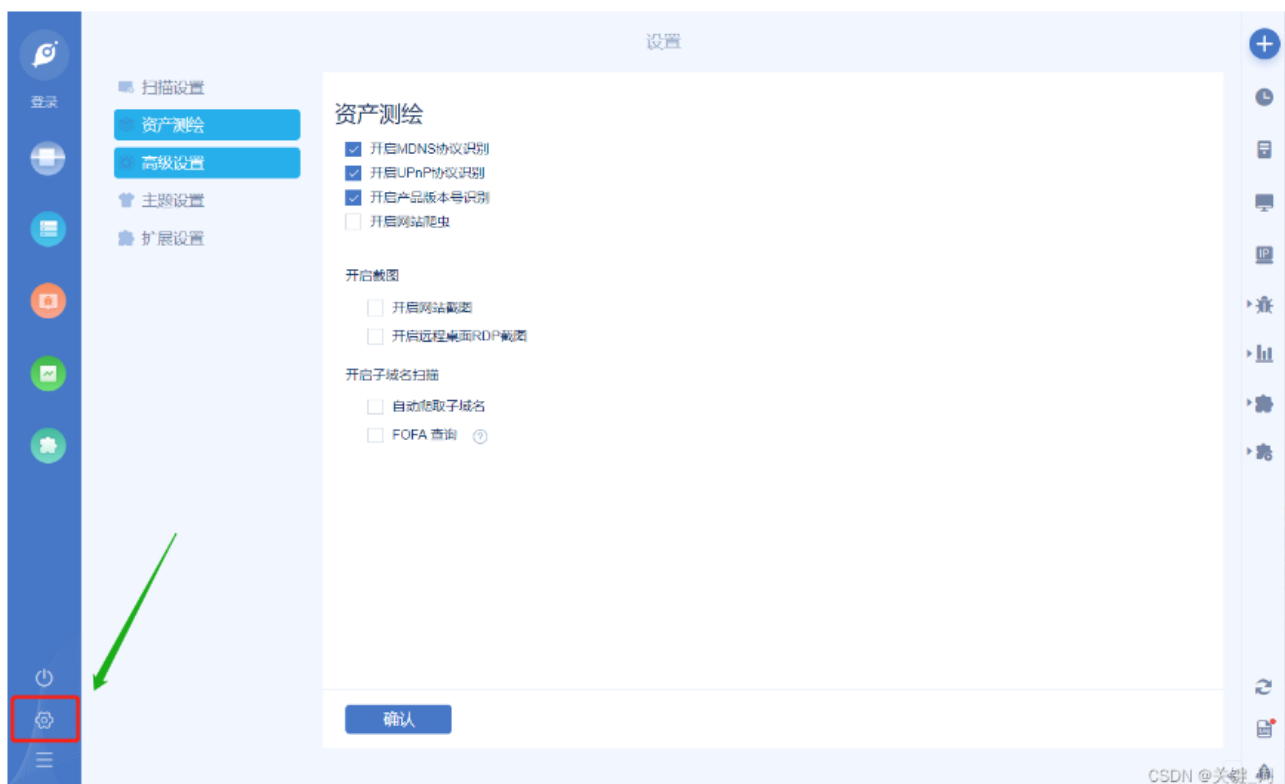


3. 点击开始，任务便开始扫描。

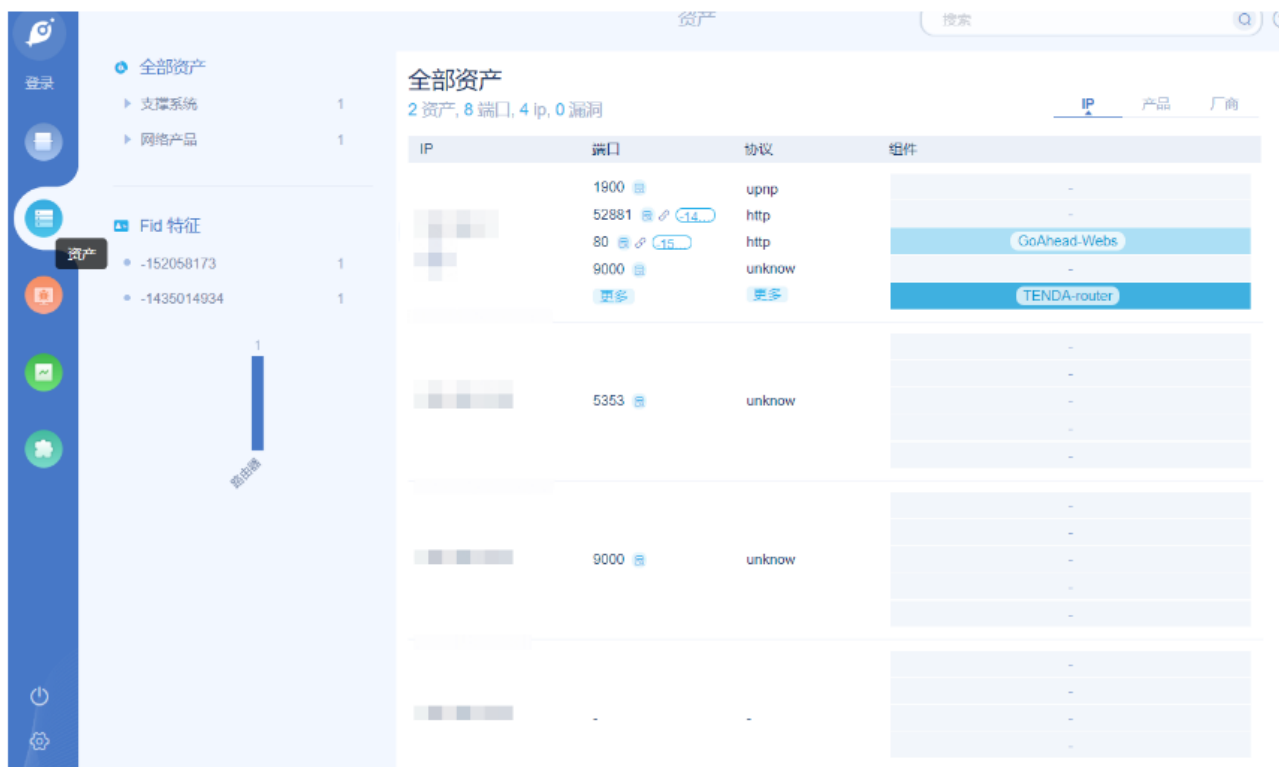


4.还可以点击左下角的设置，设置相应内容。

能开启很多功能，比如网站截图、结合fofa的apikey



5.扫描完毕后，可以查看资产。



6.查看报告，点击右上角可以下载报告。



## 四xray安装

网址: (<https://stack.chaitin.com/>)

## 概述

Xray是一款功能强大的安全评估工具，支持主动、被动多种扫描方式，支持常见web漏洞的自动化测试，可以灵活定义POC，功能丰富，调用简单，支持多种操作系统

## 特点

检测速度快

支持范围广

高级可定制

安全无威胁

更新速度快

## 支持的漏洞类型

XSS漏洞检测 (key: xss)

SQL 注入检测 (key: sqldet)

命令/代码注入检测 (key: cmd-injection)

目录枚举 (key: dirscan)

路径穿越检测 (key: path-traversal)

XML 实体注入检测 (key: xxe)

文件上传检测 (key: upload)

弱口令检测 (key: brute-force)

jsonp 检测 (key: jsonp)

ssrf 检测 (key: ssrf)

基线检查 (key: baseline)

任意跳转检测 (key: redirect)

CRLF 注入 (key: crlf-injection)

Struts2 系列漏洞检测 (高级版, key: struts)

Thinkphp系列漏洞检测 (高级版, key: thinkphp)






























POC 框架 (key: phantasm)

## 下载与安装

GitHub地址: <https://github.com/chaitin/xray/releases>





## 支持多种操作系统安装与下载

| Name   | Size    | ModTime             | Actions  |
|--|---------|---------------------|--|
|  xray_linux_386.zip         | 17.5 MB | 2021-10-25 19:18:04 | Download     |
|  xray_linux_arm64.zip       | 17.3 MB | 2021-10-25 19:18:01 | Download     |
|  xray_linux_amd64.zip       | 19.2 MB | 2021-10-25 19:17:57 | Download     |
|  xray_darwin_amd64.zip      | 19.3 MB | 2021-10-25 19:17:53 | Download     |
|  xray_windows_386.exe.zip   | 17.7 MB | 2021-10-25 19:17:50 | Download     |
|  sha256.txt                 | 1 KB    | 2021-10-25 19:17:46 | Download     |
|  xray_darwin_arm64.zip      | 18.5 MB | 2021-10-25 19:17:46 | Download     |
|  xray_windows_amd64.exe.zip | 19.1 MB | 2021-10-25 19:17:42 | Download     |
|  xray_linux_arm.zip         | 19.2 MB | 2021-10-25 19:17:39 | Download     |

CSDN @TEN\_杰尼龟

## 2、进行解压，发现就一个exe文件

|  |                  |              |           |
|--|------------------|--------------|-----------|
|  xray_windows_386.exe     | 2021-10-25 18:30 | 应用程序         | 39,979 KB |
|  xray_windows_386.exe.zip | 2021-10-26 17:26 | 360压缩 ZIP 文件 | 18,092 KB |

## 3、使用cmd命令行定位到当前xray.exe所在的路径

```
E:\T001s\scan\xary>dir
驱动器 E 中的卷是 本地磁盘
卷的序列号是 7E2D-F0C0

E:\T001s\scan\xary 的目录

2021-10-26  17:27    <DIR>          .
2021-10-26  17:27    <DIR>          ..
2021-10-25  18:30         40,938,496 xray_windows_386.exe
               1 个文件         40,938,496 字节
               2 个目录  431,102,029,824 可用字节
```

CSDN @TEN\_杰尼龟

## 运行该文件

```
E:\T00ls\scan\xray>xray_windows_386.exe

XRAY



Version: 1.8.1/93d778e6/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 yaml poc
  transform        transform other script to gamma
  reverse          Run a standalone reverse server
  convert          convert results from json to html or from html
  genca            GenerateToFile CA certificate and key
```

同时xray\_windows\_386.exe文件的同目录下生成了config.yaml配置文件

|  |                  |     |
|--|------------------|-----|
|  config.yaml          | 2021-10-26 17:28 | YAN |
|  xray_windows_386.exe | 2021-10-25 18:30 | 应用  |

```
C:\ruanjian\xray>.\xray_windows_amd64.exe webscan -h

XRAY

Version: 1.9.3/b3165028/COMMUNITY

NAME:
  webscan - Run a webscan task

USAGE:
  webscan [command options] [arguments...]

OPTIONS:
  --list, -l          list plugins
  --plugins value, --plugin value, --plug value  specify the plugins to run, separated by ','
  --poc value, -p value  specify the poc to run, separated by ','
  --level value       specify the level of poc to run, separated by ','
  --tags value        specify the level of poc to run, separated by ','
```

这样我们就安装成功了

# 使用参数

下载对应系统的版本后，解压缩zip文件，Linux / Mac用户在终端（终端）运行，Windows用户请在Powershell或其他高级Shell中运行，在CMD中运行可能体验不佳。

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 xxx.html
```

使用 HTTP 代理进行被动扫描：

设置浏览器 http 代理为<http://127.0.0.1:7777>，然后使用浏览器访问网页，就可以自动分析代理流量并扫描。

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

快速测试单个 url, 无爬虫：

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

例：简单爬虫

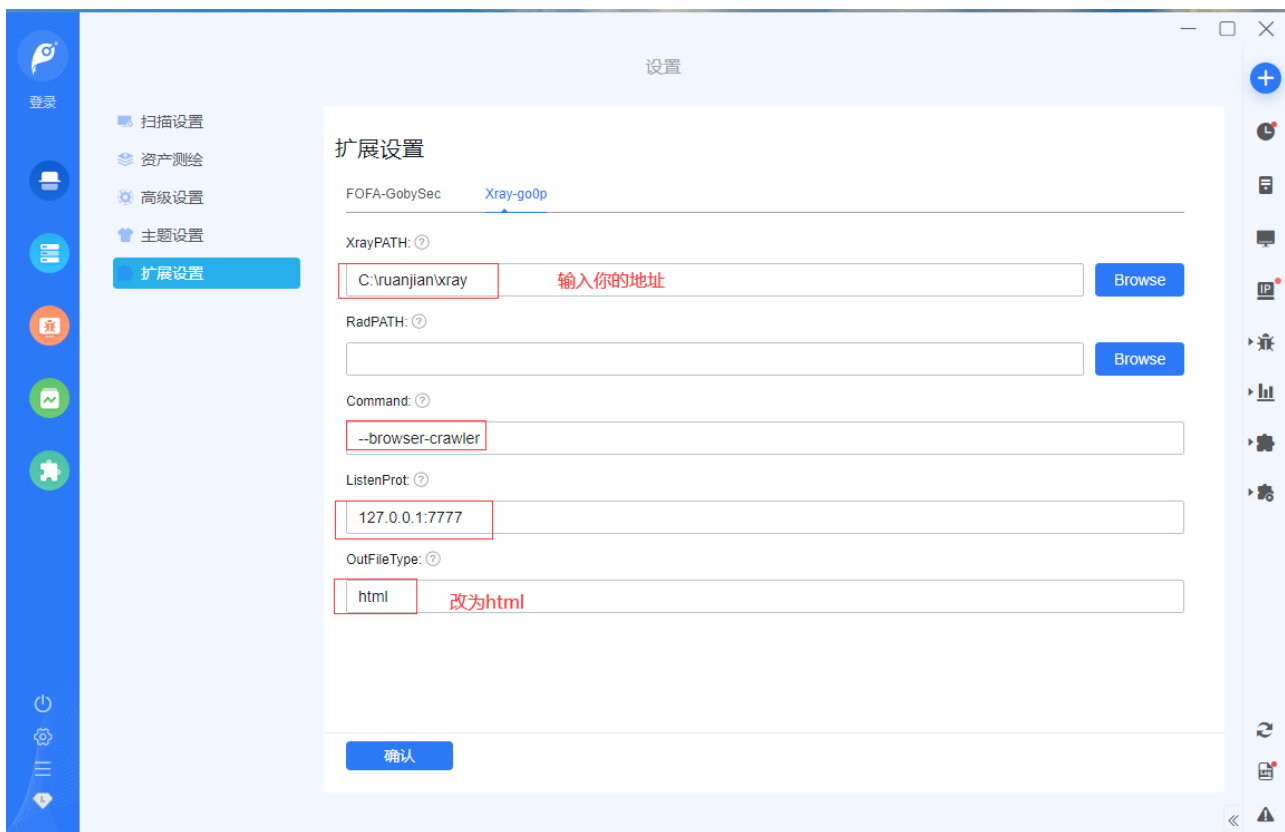
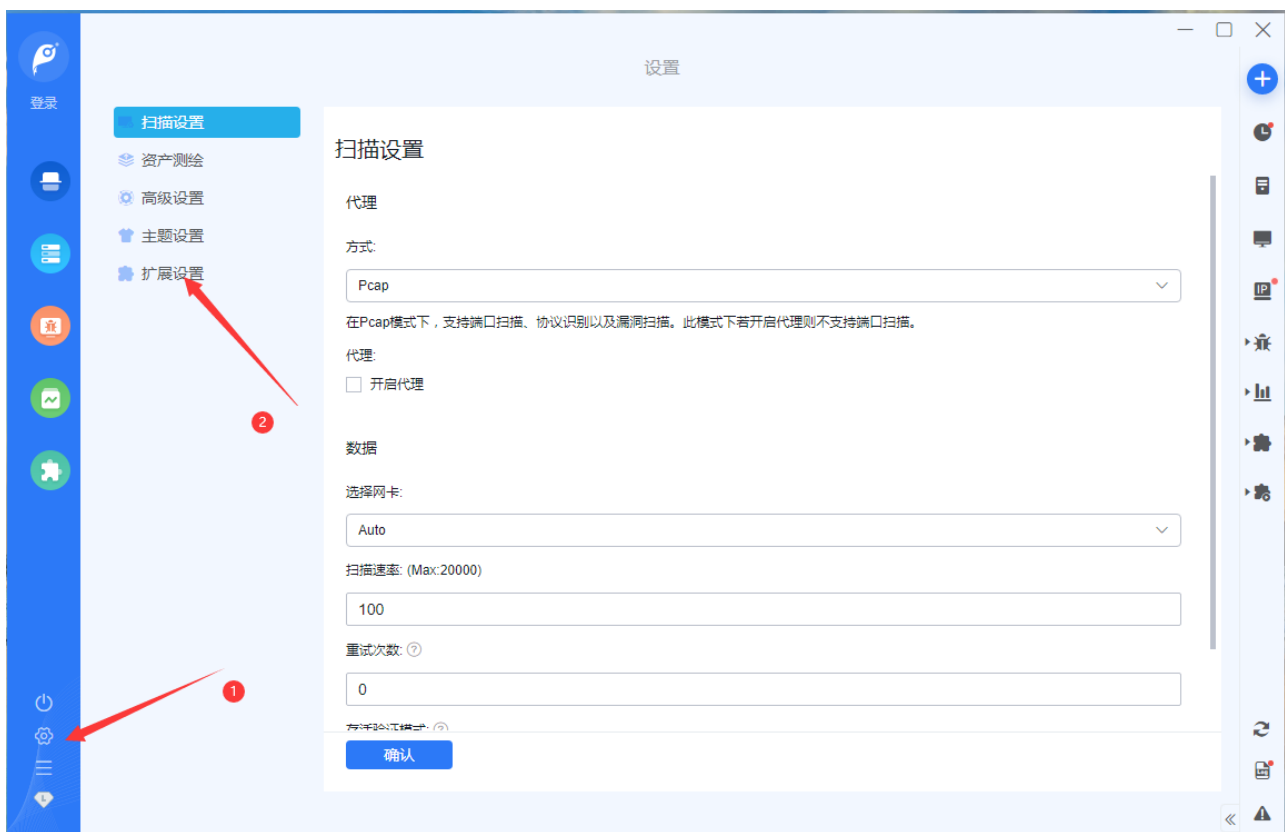
```
C:\ruanjian\xray>.\xray_windows_amd64.exe webscan --basic-crawler http://192.168.10.23/control/login.php --html-output result.html
```



| 此电脑 > 本地磁盘 (C:) > ruanjian > xray |                  |         |           |  |
|-----------------------------------|------------------|---------|-----------|--|
| 名称                                | 修改日期             | 类型      | 大小        |  |
| config.yaml                       | 2022/10/30 22:23 | YAML 文件 | 14 KB     |  |
| module.xray.yaml                  | 2022/10/30 22:23 | YAML 文件 | 4 KB      |  |
| plugin.xray.yaml                  | 2022/10/30 22:23 | YAML 文件 | 4 KB      |  |
| result                            | 2022/10/30 22:35 | HTML 文件 | 1,967 KB  |  |
| xray.yaml                         | 2022/10/30 22:23 | YAML 文件 | 1 KB      |  |
| xray_windows_amd64                | 2022/10/13 18:26 | 应用程序    | 66,315 KB |  |

最后输出到了这个html文件

## 与xray联动



## 扩展设置

FOFA-GobySec Xray-go0p

XrayPATH: ?

C:\ruanjian\xray

Browse

RadPATH: ?

Browse

Command: ?

--browser-crawler

ListenProt: ?

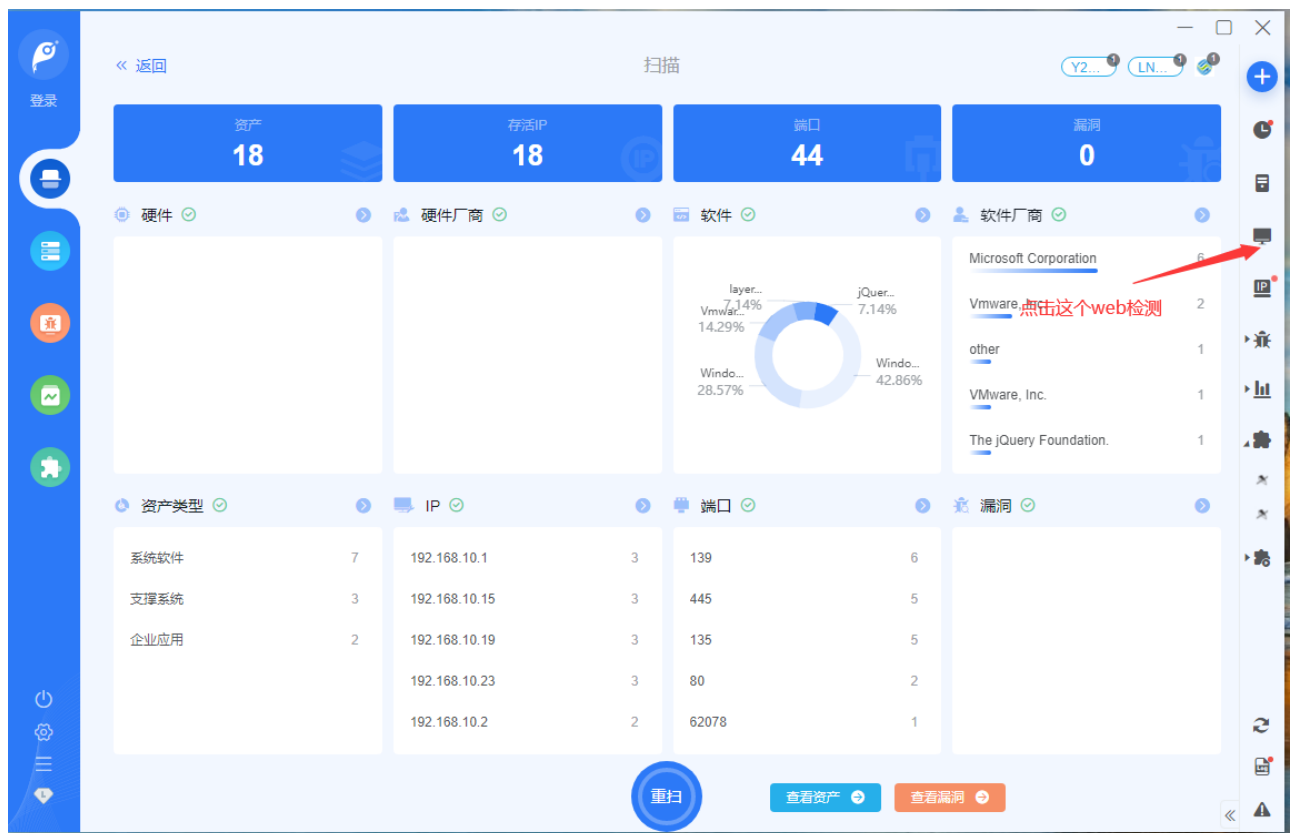
127.0.0.1:7777

OutFileType: ?

html

确认

放报告的地方



Web检测

全部资产

1 端口, 1 ip

导出

| IP            | FID   | 端口 | 服务器                              | 名称                            |
|---------------|-------|----|----------------------------------|-------------------------------|
| 192.168.10.23 | 6C... | 80 | Apache/2.4.23 (Win32) OpenSSL... | Amaze UI Admin index Examples |

Xray-cra...

共 1 条 1 页