

# 一、分别使用 AWVS 和 Xray（被动扫描模式）去扫描任一 SRC 允许测试的目标，对比扫描结果的不同；

## 1. AWVS

### 1.1 AWVS 的安装与启动

搜索

```
docker search awvs
```

获取镜像

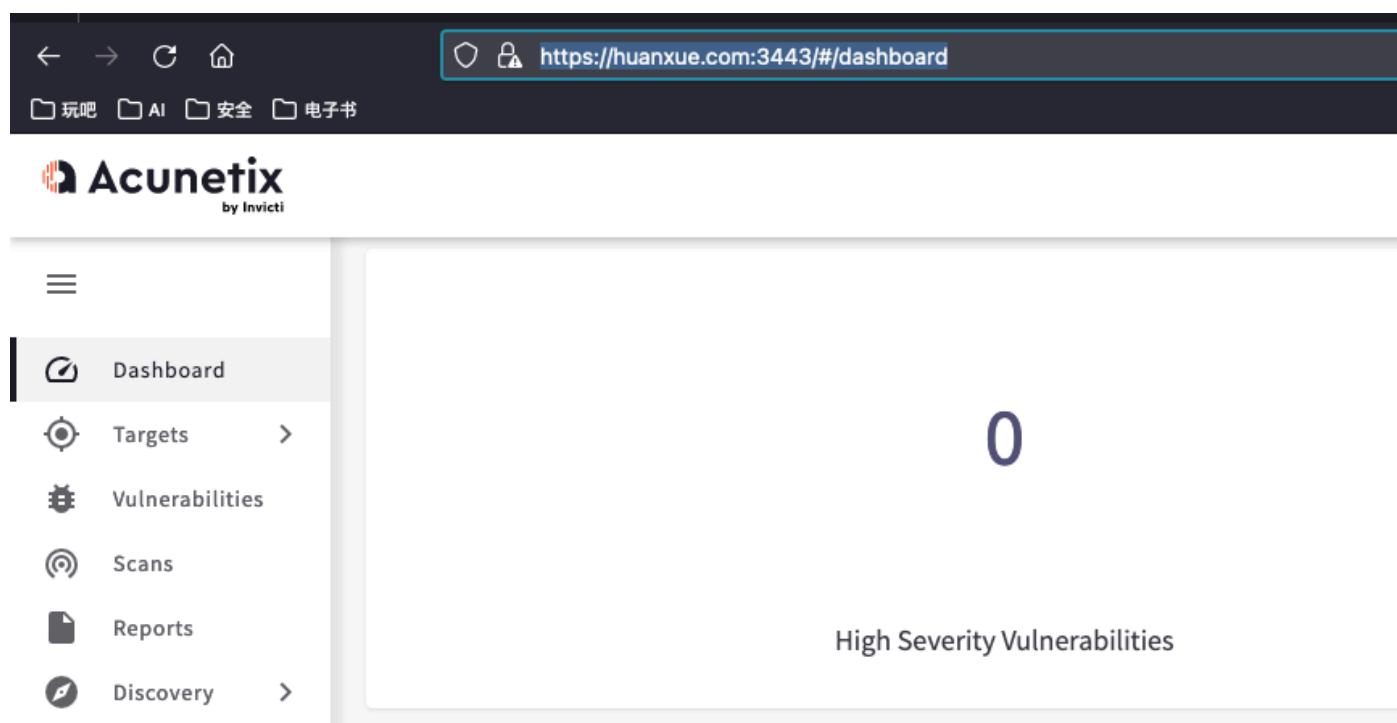
```
docker pull dockermi3aka/awvs
```

启动

```
docker run -dit -p 3443:3443 dockermi3aka/awvs
```

访问

```
https://huanxue.com:3443/#/dashboard
```



## 1.2 AWVS 扫描（应用类主动扫描）

1.2.1 添加目标站点，位置：“Targets--Add Targets”，输入后点击“save”进行保存。

Add Targets

Address: http://... Description: 后台管理 (内网测试)

Add another Target

Save

## 1.2.2 选择“scan”

Scans

New Scan Stop Scans Delete Scans

| Target | Target Description | Scan Profile | Schedule                            | Vulnerabilities |
|--------|--------------------|--------------|-------------------------------------|-----------------|
| ...    | ...                | Full Scan    | Last run on Sep 2, 2023, 9:37:26 AM | 0 1 1 2         |

点击新建扫描任务按钮“New Scan”

Scans

New Scan

| Target                 | Target Description | Scan Profile | Schedule                            |
|------------------------|--------------------|--------------|-------------------------------------|
| http://www.tonesun.com | tonesun            | Full Scan    | Last run on Sep 2, 2023, 9:37:26 AM |

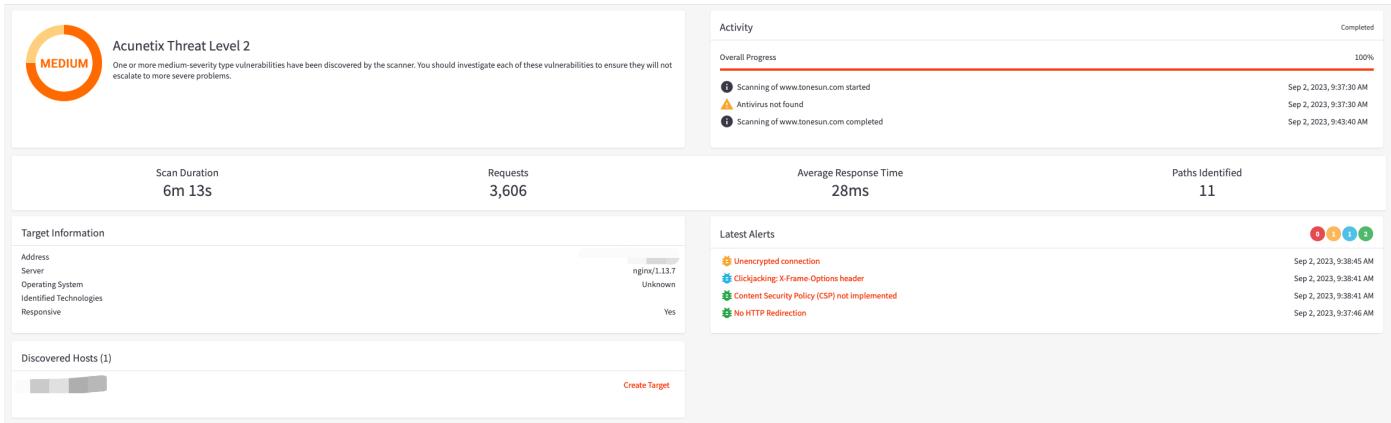
勾选目标站点，点击“scan”

Select targets to Scan

Scan

| Address  | Description   | Type        | Vulnerabilities | Last Scan Status                                     |
|--|---------------|-------------|-----------------|--|
| <input checked="" type="checkbox"/> http://... | ops(开发环境, 内网) | Web/Network | 0 1 1 2         | Not Scanned  |
| <input type="checkbox"/> http://...            | tonesun       | Web/Network | 0 1 1 2         | Completed<br>Last Scanned on Sep 2, 2023, 9:37:26 AM |
| <input type="checkbox"/> http://...            | 后台管理 (内网测试)   | Web/Network | 0 1 1 2         | Not Scanned  |

扫描结果



## 2. Xray

### 2.1 Xray 的安装

#### 2.1.1 访问 Xray 官网

<https://docs.xray.cool>

#### 2.1.2 查看文档页中的快速开始

<https://docs.xray.cool/#/tutorial/prepare>

#### 2.1.3 下载

##### 下载地址

<https://stack.chaitin.com/tool/detail/1>

##### 下载 mac 版本的

## 全部版本

|                |            |
|----------------|------------|
| 1.9.11         | 2023-05-18 |
| 1.9.10         | 2023-05-15 |
| 1.9.9          | 2023-05-11 |
| 1.9.8          | 2023-04-25 |
| 1.9.7          | 2023-04-20 |
| 1.9.6          | 2023-05-25 |
| 1.9.5          | 2023-04-11 |
| 1.9.4          | 2023-01-10 |
| 1.9.3          | 2022-10-13 |
| 1.9.1          | 2022-07-25 |
| 1.9.0(Preview) | 2022-06-21 |
| 1.8.5          | 2022-06-14 |
| 1.8.4          | 2022-06-01 |

该版本为 用友NC NCMessageServlet反序列化漏洞 注入漏洞 的应急版本，相较于上个版本，除了添加了一个POC外，未改动其他内容。

## 更新内容

想要检测该漏洞的师傅，可以使用

```
./xray ws --poc poc-yaml-yongyou-nc-ncmessageservlet-rce --url  
http://example.com
```

进行检测。

相关参考链接：[CT stack](#)

- 1. xray\_darwin\_amd64.zip
- 2. xray\_linux\_386.zip
- 3. xray\_linux\_amd64.zip
- 4. xray\_windows\_386.exe.zip
- 5. xray\_windows\_amd64.exe.zip
- 6. xray\_darwin\_arm64.zip
- 7. xray\_darwin\_amd64.zip
- 8. sha256.txt

## 2.1.4 压缩包解压到指定目录

```
~/apps/xray ➔ ls -l
total 136688
-r--r--r--  1 wan  staff      1513  9  2 10:49 ca.crt
-r-----  1 wan  staff      1675  9  2 10:49 ca.key
-rw-r--r--  1 wan  staff    14621  9  2 11:19 config.yaml
-rw-r--r--  1 wan  staff     3291  9  2 10:44 module.xray.yaml
-rw-r--r--  1 wan  staff     3867  9  2 10:44 plugin.xray.yaml
-rw-r--r--  1 wan  staff      382  9  2 10:44 xray.yaml
-rwxr-xr-x@ 1 wan  staff  69943336  5 18 14:28 xray_darwin_amd64
~/apps/xray ➔
```

## 2.1.5 启动前，修改配置

```
# 被动代理配置
# 更多解释见 https://docs.xray.cool/#/configuration/mitm
mitm:
  ca_cert: ./ca.crt          # CA 根证书路径
  ca_key: ./ca.key            # CA 私钥路径
  basic_auth:                 # 基础认证的用户名密码
    username: ""
    password: ""
  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: ['*.*.com', '*.*.com']      # 允许访问的 Hostname, 支持格式
    hostname_disallowed:      # 不允许访问的 Hostname, 支持格式如 t.com、*.t.com、1.1.1.1、1
    - '*google*'
```

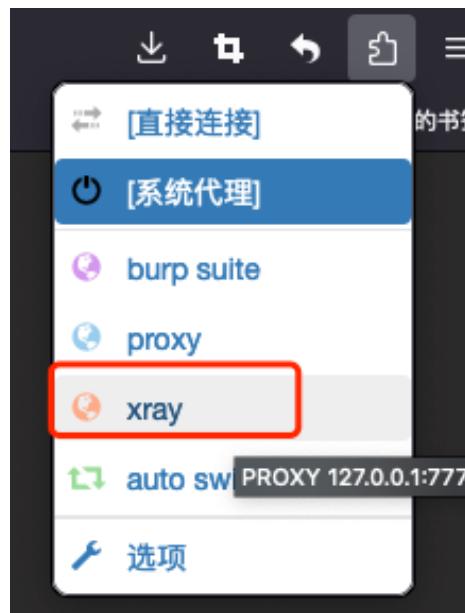
## 2.1.6 启用xray被动模式代理

```
./xray_darwin_amd64 webscan --listen 127.0.0.1:7777 --html-output test.html
```

```
xstream/RCE(LDAP)/CVE-2021-21344
xstream/RCE(LDAP)/CVE-2021-39141
xstream/RCE(LDAP)/CVE-2021-39146
xstream/RCE/CVE-2013-7285
xstream/RCE/CVE-2020-26217
xstream/RCE/CVE-2021-21345
xstream/RCE/CVE-2021-21346
xstream/RCE/CVE-2021-21347
xstream/RCE/CVE-2021-21350
xstream/RCE/CVE-2021-21351
xstream/RCE/CVE-2021-39139
xstream/RCE/CVE-2021-39144
xstream/RCE/CVE-2021-39145
xstream/RCE/CVE-2021-39147
xstream/RCE/CVE-2021-39148
xstream/RCE/CVE-2021-39149
xstream/RCE/CVE-2021-39151
xstream/RCE/CVE-2021-39153
xstream/RCE/CVE-2021-39154
xstream/SSRF/CVE-2020-26258
xstream/SSRF/CVE-2021-21342
xstream/SSRF/CVE-2021-21349
xstream/SSRF/CVE-2021-39150
xstream/SSRF/CVE-2021-39152
xxe/xxe/blind
```

```
[INFO] 2023-09-05 09:51:49 [collector:mitm.go:215] loading cert from ./ca.crt and ./ca.key
[INFO] 2023-09-05 09:51:50 [collector:mitm.go:271] starting mitm server at 127.0.0.1:7777
[]
```

## 2.1.7 启用浏览器代理



## 2.1.8 访问测试站点页面，进行简单的功能测试

```
[INFO] 2023-09-05 10:05:27 [default:dispatcher.go:444] processing GET [REDACTED]
[INFO] 2023-09-05 10:05:27 [default:dispatcher.go:444] processing GET [REDACTED]
[INFO] 2023-09-05 10:05:27 [default:dispatcher.go:444] processing POST [REDACTED]
[*] scanned: 7, pending: 2, requestSent: 2256, latency: 54.52ms, failedRatio: 0.00%
[INFO] 2023-09-05 10:05:34 [default:dispatcher.go:444] processing POST [REDACTED]
[*] scanned: 9, pending: 1, requestSent: 2389, latency: 53.12ms, failedRatio: 0.00%
[INFO] 2023-09-05 10:05:39 [default:dispatcher.go:444] processing PUT http://[REDACTED]
[*] scanned: 10, pending: 1, requestSent: 2407, latency: 52.97ms, failedRatio: 0.00%
[*] scanned: 10, pending: 1, requestSent: 2769, latency: 53.90ms, failedRatio: 0.00%
[INFO] 2023-09-05 10:05:46 [default:dispatcher.go:444] processing POST [REDACTED]
[*] scanned: 11, pending: 1, requestSent: 3105, latency: 44.27ms, failedRatio: 0.00%
[*] All pending requests have been scanned
[*] scanned: 12, pending: 0, requestSent: 3301, latency: 32.79ms, failedRatio: 0.00%
```

## 2.1.9 查看生成的报告

A screenshot of the XRay web application interface. The top navigation bar shows 'XRAY'. Below it is a search bar labeled 'Search Target' and a 'Reload' button. The main area is titled 'Web Vulnerabilities' and displays a table with one row. The table columns are 'ID', 'Target', 'PluginName / VulnType', and 'CreateTime'. The single entry is ID 1, Target [REDACTED], PluginName / VulnType: baseline/cors/reflected, and CreateTime: 2023-09-06 09:26:29. At the bottom of the page, it says 'Powered by XRay Team'.

## 3. 扫描结果对比

| 对比项      | 项目   | 描述   |
|----------|------|--|
| 扫描方式     | AWVS | 主动扫描   |
|          | Xray | 被动扫描   |
| 查看方式     | AWVS | 系统中，访问 Scans 页面，点击对应的条目，就可查看扫描结果                       |
|          | Xray | 通过命令行中的 --html-output 选项来指定结果的输出类型，名称与位置，结束后打开对应文件进行查看 |
| 站点安全现状描述 | AWVS | 扫描结果中可以看到目标站点当前的整体风险等级评价                               |
|          | Xray | 无  |
| 系统信息     | AWVS | 扫描结果中有目标站点的系统信息描述                                      |
|          | Xray | 无  |
| 漏洞描述     | AWVS | 漏洞信息描述详细，有具体的漏洞等级，发现漏洞时的请求和响应，修复建议以及漏洞编号信息             |
|          | Xray | 漏洞信息描述简明，仅有有发现漏洞的插件，以及漏洞类型，发现漏洞时的请求和响应                 |

**个人总结：** AWVS 的扫描结果比较详细，内容丰富，但其因主动扫描的方式，很可能被安全防护设备拦截，所以通常会用于内网项目的扫描，操作时最好和运维团队打招呼。Xray 的代理模式（被动扫描），其扫描结果言简意赅，没有漏洞等级以及漏洞编号等描述，适合有一定安全从业经验和了解常见漏洞及其原理的安全工作者使用。

## 二、使用 Nessus 扫描任一主机，要求使用全端口扫描，提供主机扫描报告；

### 1. Nessus 的下载与安装

#### 1.1 获取官方激活码

```
https://zh-cn.tenable.com/products/nessus/activation-code?tns_redirect=true
```

#### 1.2 点击立即注册

| Nessus Expert  | Nessus Professional   | Nessus Essentials  |
|--|---|--|
| <a href="#">免费试用</a>   | <a href="#">立即购买</a>  | <a href="#">立即注册</a>   |
| Nessus Expert 是专为需要更多评估功能的安全专业人士量身打造的，他们不局限于仅评估传统 IT 资产。安全专业人士可以保障 Web 应用程序的安全、云基础设施，并获取与互联网相连攻击面的可见性。 | Nessus Professional 可满足奋战在一线的安全专家之所需，能够快速轻松识别并修复漏洞，包括软件缺陷、未安装补丁、恶意软件和配置错误，涵盖多款操作系统、设备和应用。 | Nessus Essentials 是一款免费漏洞扫描程序，可作为漏洞评估的绝佳切入点。可获得无异于 Nessus Professional 订阅用户所享的强大扫描程序，支持扫描 16 个 IP。 |
| 适用于顾问、渗透测试人员、开发人员和安全从业人员   | 适用于顾问、渗透性测试人员和安全专业人士  | 适用于教育工作者、学生以及网络安全领域的入门从业人员   |
| <b>Nessus Expert 功能</b>  | <b>Nessus Professional 特性</b>   | <b>Nessus Essentials 特性</b>  |
| 扫描 IP 数量不受限制   | 扫描 IP 数量不受限制  | 扫描 16 个 IP   |
| Web 应用程序扫描   | 功能不受限制，包括实时结果与配置审查  | 漏洞与配置检查点多达数千，评估又快又准  |
| 外部攻击面扫描  | 准确、高速的资产发现，广泛的覆盖与分析范围   | 无代理式网络扫描   |
| 扫描云基础设施  | 全球最大的持续更新型漏洞与配置检查库  | 通过 Tenable Community 提供支持  |
| 全面的功能，包括实时检测结果和配置审计  | 电子邮件与社区支持   | 使用不限地点   |

## 1.3 填写注册信息后，点击“开始”，将会有激活码发送至邮箱

### Tenable Nessus® Essentials

Tenable Nessus Essentials 包含在 Tenable Nessus 系列中，可用来扫描您的环境（每个扫描程序最多 16 个 IP 地址），可获得无异于 Nessus 订阅用户所享的高速、深度评估，以及无代理式扫描便利性。

请注意，Nessus Essentials 不支持执行合规性检查或内容审查、实时结果或使用 Nessus 虚拟设备。如果您需要这些额外的功能，请购买 [Tenable Nessus Professional](#) 订阅。

想要在教育机构中使用 Nessus Essentials？请先通过 [Tenable for Education](#) 计划注册 Nessus Essentials。

对了解如何使用 Nessus 感兴趣？我们的[按需培训课程](#)通过提供一系列有针对性的视频，帮助学生开发构建块，以便有效使用 Nessus 漏洞评估解决方案。从资产发现到漏洞评估再到合规性，参与者将学习在各种业务用例中有效地利用 Nessus。[了解详情。](#)

#### 注册以获取激活码

名字  姓氏

商业电子邮件

勾选表示同意接收 Tenable 更新内容

Tenable 仅按其隐私政策所述处理您的个人数据。

[开始](#)

## 1.4 从邮箱中获取激活码和下载地址



## Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the [Nessus Professional datasheet](#).

### Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:

[REDACTED]

[Download Nessus](#)

This is a one-time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

### 1.5 跳转下载地址，进行下载

## Tenable Nessus

### 1 Download and Install Nessus

#### Choose Download

##### Version

Nessus - 10.6.0

##### Platform

macOS - x86\_64

[Download](#)
[Checksum](#)
[Download by curl >](#)
[Docker >](#)
[Virtual Machines >](#)

### 2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

### 3 Getting Started

Check out our [documentation](#) for Nessus

### Summary

**Release Date:** Aug 29, 2023

**Release Notes:**

[Tenable Nessus 10.6.0 Release Notes](#)

**Signing Keys:**

RPM-GPG-KEY-Tenable-4096 (10.4 & above)

RPM-GPG-KEY-Tenable-2048 (10.3 & below)

## 1.6 校验软件完整性

```
md5 Nessus-10.6.0.dmg
```

```
~/Downloads ➔ md5 Nessus-10.6.0.dmg
```

```
MD5 (Nessus-10.6.0.dmg) = 6becc7f8e89017bbdeaefbd4fef37769
```

**MD5:** 6becc7f8e89017bbdeaefbd4fef37769

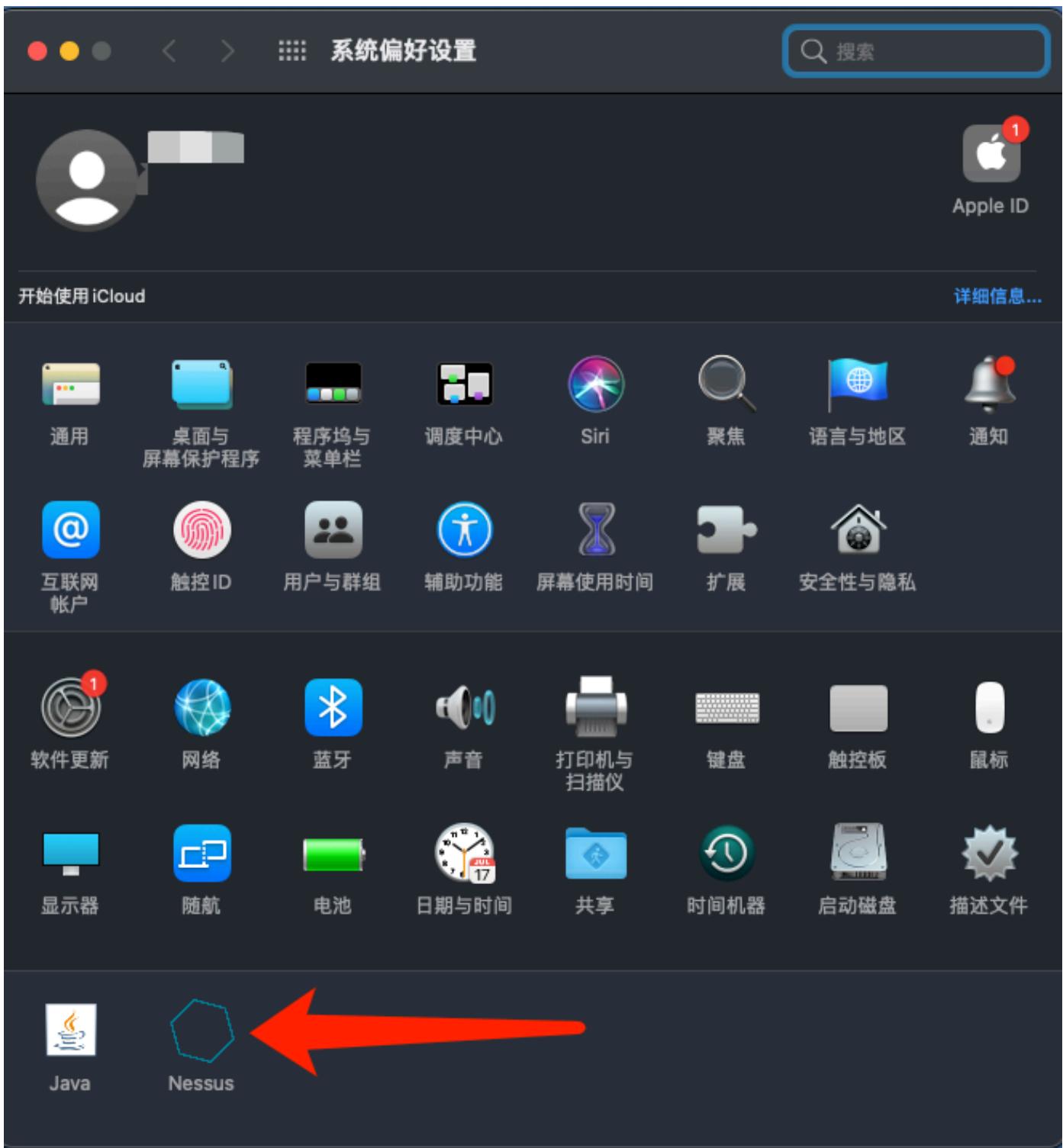
**SHA256:** cf26b3b3b76263fc2c4a7b13a510558972c5ee2eb6840025b9206097cfa1b09b

## 1.7 双击下载好的包，进行安装

已经安装过了，这里略过，以及后面的插件安装，都是自动的，等待就行了。

## 1.8 启动与停止

点击苹果右上角图标，选择“隐私偏好设置”



点击“Nessus”后，点击锁，输入密码解锁后，点击“Start Nessus”启动，“Stop Nessus”停止。



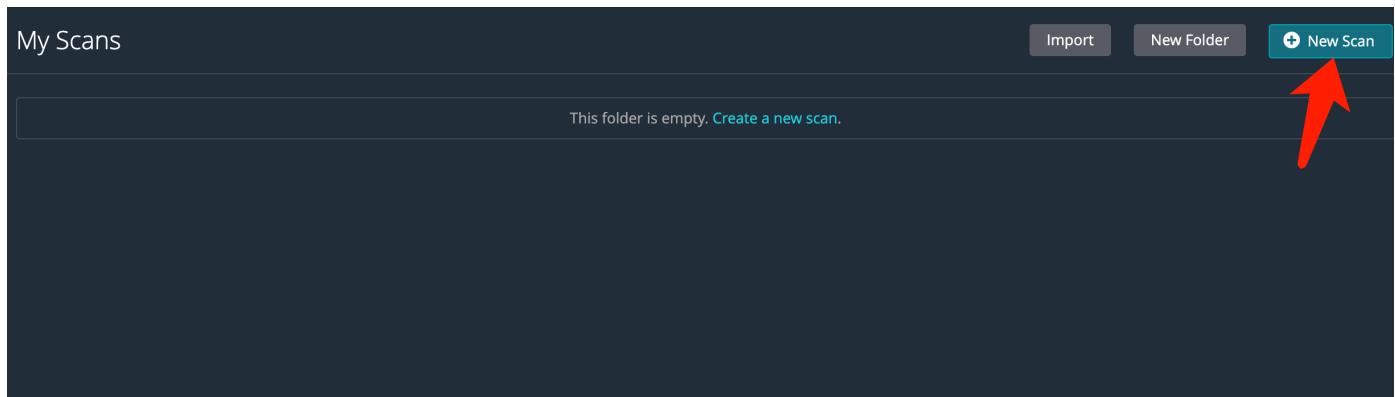
## 1.9 访问

The screenshot shows a web browser window with the URL `https://localhost:8834/#/` in the address bar. The address bar also includes a warning icon and the text '不安全 | <https://localhost:8834/#/>'. The main content is a login form for 'Nessus Essentials' by 'tenable'. It features fields for 'root' (username) and 'Password', both with placeholder text. There is a 'Remember Me' checkbox and a 'Sign In' button. At the bottom, a copyright notice reads '© 2023 Tenable™, Inc.'

## 2. 扫描

## 2.1 新建扫描任务

### 2.1.1 “My Scans” 点击 “New Scan”



### 2.1.2 选择高级扫描

Scan Templates [Back to Scans](#)

Scanner DISCOVERY VULNERABILITIES

**Host Discovery**  
A simple scan to discover live hosts and open ports.

**Basic Network Scan**  
A full system scan suitable for any host.

**Advanced Scan**  
Configure a scan without using any recommendations.

**Advanced Dynamic Scan**  
Configure a dynamic plugin scan without recommendations.

**Malware Scan**  
Scan for malware on Windows and Unix systems.

**Mobile Device Scan**  
Assess mobile devices via Microsoft Exchange or an MDM. UPGRADE

### 2.1.3 扫描设置

#### 基础配置

Settings    Credentials    Plugins

**BASIC**

- General
- Schedule
- Notifications

**DISCOVERY**

**ASSESSMENT**

**REPORT**

**ADVANCED**

Name: first scan task

Description: 第一个扫描任务

Folder: My Scans

Targets: 06

Upload Targets    Add File

Save    Cancel

## 端口设置

Settings    Credentials    Plugins

**BASIC**

**DISCOVERY**

- Host Discovery
- Port Scanning**
- Service Discovery
- Identity

**ASSESSMENT**

**REPORT**

**ADVANCED**

**Ports**

Consider unscanned ports as closed

Port scan range: 1-65535

**Local Port Enumerators**

SSH (netstat)

WMI (netstat)

SNMP

Only run network port scanners if local port enumeration failed

Verify open TCP ports found by local port enumerators

## 保存扫描任务

New Scan / Advanced Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Email Recipient(s) Example: me@example.com, you@example.com

Result Filters Add Filter

Save Cancel

## 2.2 开始扫描

My Scans

Import New Folder + New Scan

Search Scans 1 Scan

| Name            | Schedule  | Last Scanned | Actions |
|-----------------|-----------|--------------|---------|
| first scan task | On Demand | N/A          | ▶ X     |

## 2.3 等待扫描结果

| Name            | Schedule  | Last Scanned     | Actions |
|-----------------|-----------|------------------|---------|
| first scan task | On Demand | Today at 9:27 AM | X       |

## 2.4 扫描结果

| Vulnerabilities 20             |                        |       |   |
|--------------------------------|------------------------|-------|---|
| Filter                         | Search Vulnerabilities | Count |   |
| Ser.                           | CVSS                   | VPR   | Name  |
| <input type="checkbox"/> MIXED | ...                    | ...   | SSH (Multiple Issues)   |
| <input type="checkbox"/> INFO  | ...                    | ...   | HTTP (Multiple Issues)  |
| <input type="checkbox"/> INFO  | ...                    | ...   | SSH (Multiple Issues)   |
| <input type="checkbox"/> INFO  | ...                    | ...   | SSH (Multiple Issues)   |
| <input type="checkbox"/> INFO  | ...                    | ...   | Nessus SYN scanner  |
| <input type="checkbox"/> INFO  | ...                    | ...   | Service Detection   |
| <input type="checkbox"/> INFO  | ...                    | ...   | Web Server No 404 Error Code Check  |
| <input type="checkbox"/> INFO  | ...                    | ...   | Common Platform Enumeration (CPE)   |
| <input type="checkbox"/> INFO  | ...                    | ...   | Device Type   |
| <input type="checkbox"/> INFO  | ...                    | ...   | ICMP Timestamp Request Remote Disclosure                                      |
| <input type="checkbox"/> INFO  | ...                    | ...   | MySQL Server Detection  |
| <input type="checkbox"/> INFO  | ...                    | ...   | Nessus Scan Information   |
| <input type="checkbox"/> INFO  | ...                    | ...   | OS Identification   |
| <input type="checkbox"/> INFO  | ...                    | ...   | OS Security Patch Assessment Not Available                                    |
| <input type="checkbox"/> INFO  | ...                    | ...   | Patch Report  |
| <input type="checkbox"/> INFO  | ...                    | ...   | Service Detection (HELP Request)  |
| <input type="checkbox"/> INFO  | ...                    | ...   | Target Credential Status by Authentication Protocol - No Credentials Provided |
| <input type="checkbox"/> INFO  | ...                    | ...   | TCP/IP Timestamps Supported   |
| <input type="checkbox"/> INFO  | ...                    | ...   | Traceroute Information  |

## 2.5 导出扫描结果

Generate Report - 1 Host Selected ×

**Report Format:**  HTML  PDF  CSV **Select a Report Template:**

**SYSTEM**

Complete List of Vulnerabilities by Host

Detailed Vulnerabilities By Host (Selected)

Detailed Vulnerabilities By Plugin

Vulnerability Operations

**Template Description:**  
This report presents detailed vulnerabilities by host.

**Filters Applied:**  
None

Generate Report Cancel  Save as default

选择带漏洞详情的形式进行导出

## 2.6 查看报告



Report generated by Nessus™

first scan task

Thu, 07 Sep 2023 09:46:33 CST

### TABLE OF CONTENTS

#### Vulnerabilities by Host

- Host 1
- Host 2

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

[REDACTED]



### Scan Information

Start time: Thu Sep 7 09:27:24 2023

End time: Thu Sep 7 09:46:31 2023

### Host Information

IP:

OS: Linux Kernel 2.6

### Vulnerabilities

#### 134220 - nginx < 1.17.7 Information Disclosure

##### Synopsis

The remote web server is affected by an information disclosure vulnerability.

##### Description

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

##### See Also

<http://www.nessus.org/u?fd026623>

##### Solution

三、安装 Burp，分别在本机上实现全局代理和局部代理，提供设置过程的说明文档；

# 1. 概念

## 1.1 局部代理

局部代理IP，顾名思义，改变局部的IP，可以只让某个浏览器或应用使用此代理，不影响其他程序软件运行的使用IP，也不会影响其他软件使用本地网络。

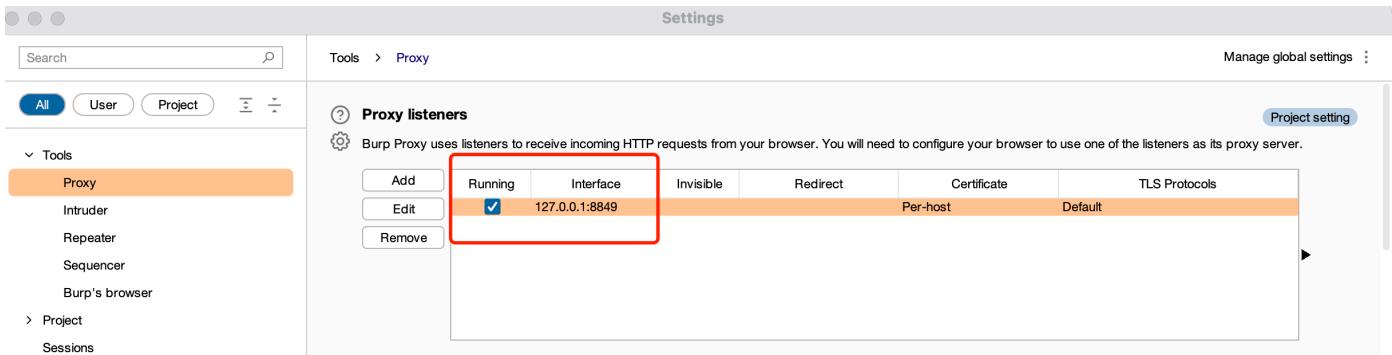
## 1.2 全局代理

所谓全局代理IP，就是改变整个客户端的上网IP，不管是什程序，它对支持代理协议的软件和大多数浏览器生效，都将使用代理IP上网。

# 2. 设置方法

## 2.1 局部代理

### 2.1.1 启动 Burp, 设置代理ip和端口



### 2.1.2 打开火狐浏览器，配置代理ip和端口

## 连接设置

×

### 配置访问互联网的代理服务器

不使用代理服务器

自动检测此网络的代理设置

使用系统代理设置

手动配置代理

HTTP 代理

端口

也将此代理用于 HTTPS

HTTPS Proxy

端口

SOCKS 主机

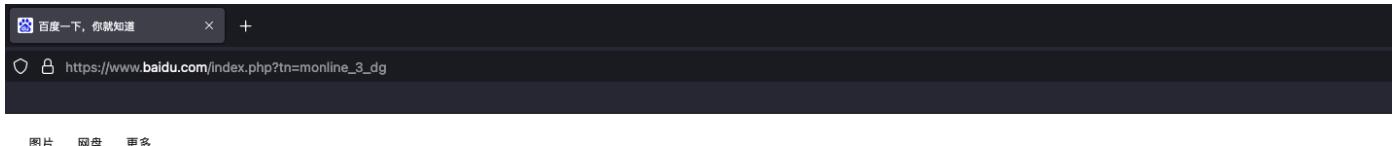
端口

SOCKS v4  SOCKS v5

自动代理配置的 URL (PAC)

不使用代理

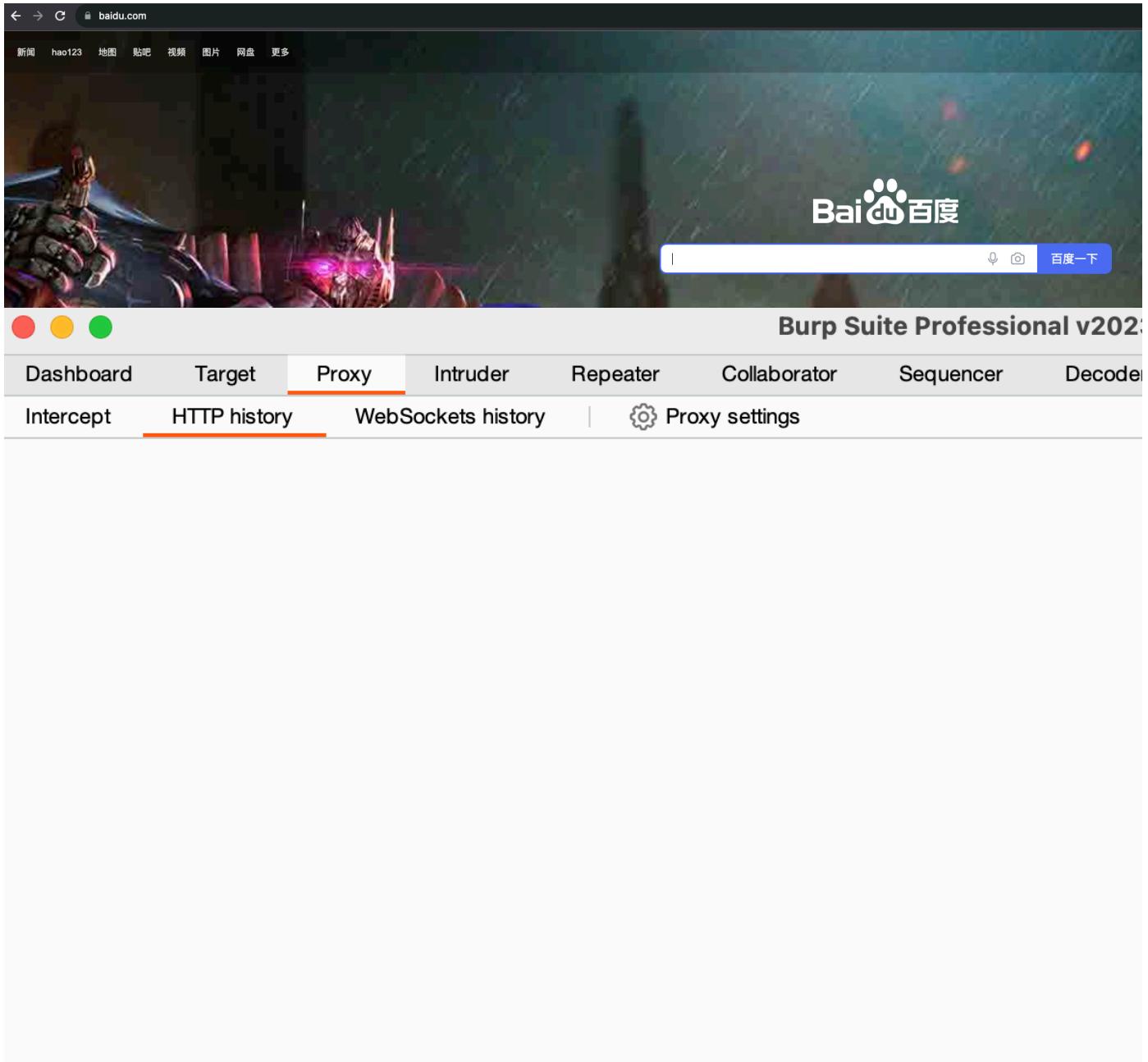
### 2.1.3 使用火狐浏览器访问任意网址，然后观察 Burp 抓包情况



百度一下

| #   | Host                                   | Method | URL  | Params | Edited | Status |
|-----|--|--------|--|--------|--------|--------|
| 178 | https://www.baidu.com                  | GET    | /index.php?tn=monline_3_dg                 | ✓      |        | 200    |
| 179 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/events/1/bb19...   |        |        | 200    |
| 180 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/impression-stat... |        |        | 200    |
| 181 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/impression-stat... |        |        | 200    |
| 182 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/sessions/1/9eb...  |        |        | 200    |
| 183 | https://incoming.telemetry.mozilla.net | POST   | /submit/firefox-desktop/newtab/1/1d6c...   |        |        | 200    |
| 188 | https://hectorstatic.baidu.com         | GET    | /cd37ed75a9387c5b.js                       |        |        | 200    |
| 191 | https://www.baidu.com                  | GET    | /sugrec?&prod=pc_his&from=pc_web...        | ✓      |        | 200    |
| 192 | https://www.baidu.com                  | GET    | /home/feed/feedwater?id=2&offset=1&...     | ✓      |        | 200    |
| 193 | https://hpd.baidu.com                  | GET    | /v.gif?ct=2&qid=0xe616f4b1000dcc3f...      | ✓      |        | 200    |
| 195 | https://www.baidu.com                  | GET    | /cache/fpid/chromelib_1_1.js?_=16940...    | ✓      |        | 200    |
| 202 | https://hpd.baidu.com                  | GET    | /v.gif?ct=2&qid=0xe616f4b1000dcc3f...      | ✓      |        | 200    |
| 203 | https://www.baidu.com                  | GET    | /-----A-----/-----B-----/-----C-----       | ✓      |        | 200    |

## 2.1.4 使用其他浏览器，访问任意网址，然后观察 Burp 抓包情况

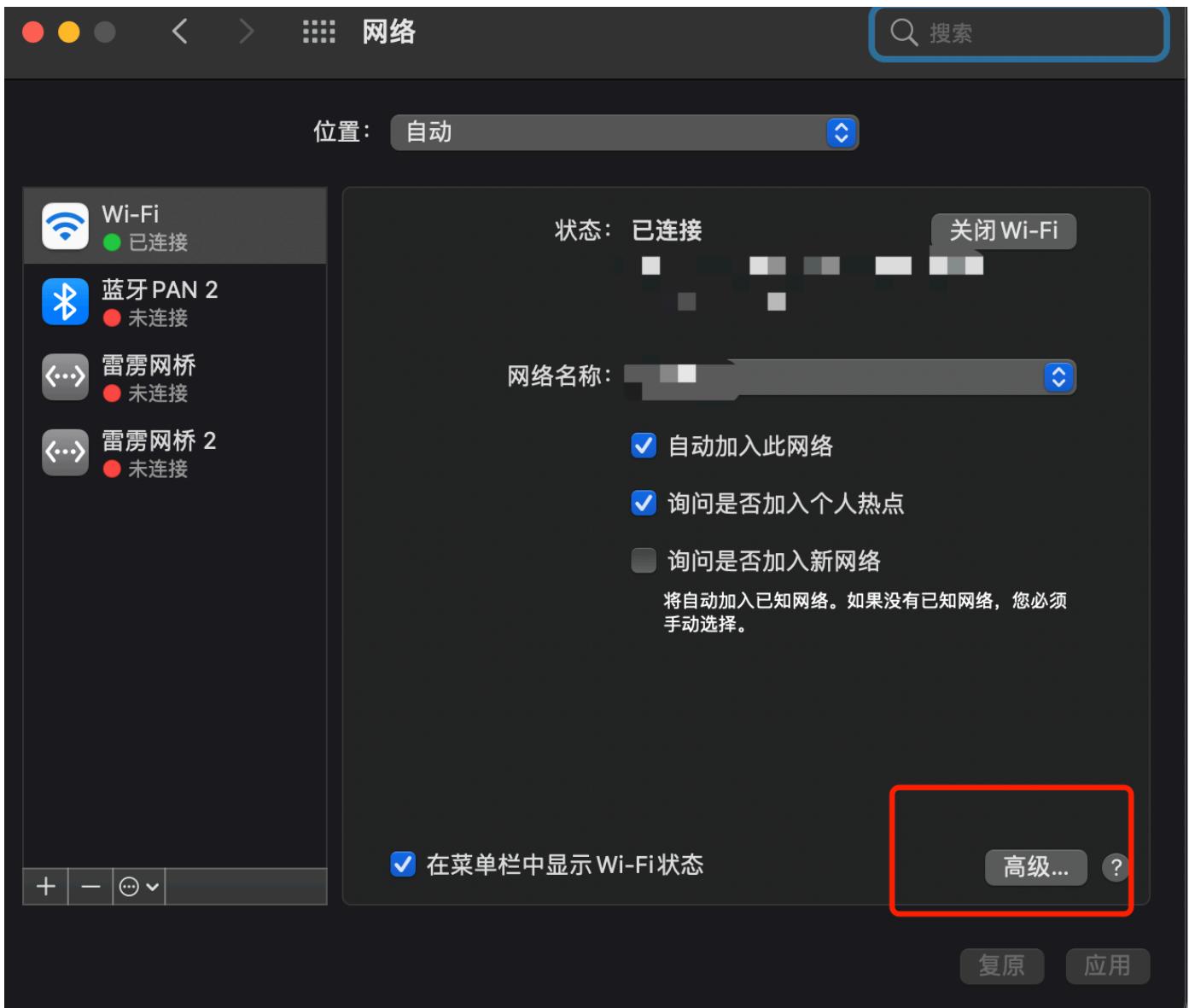


并没有流量进入 Burp

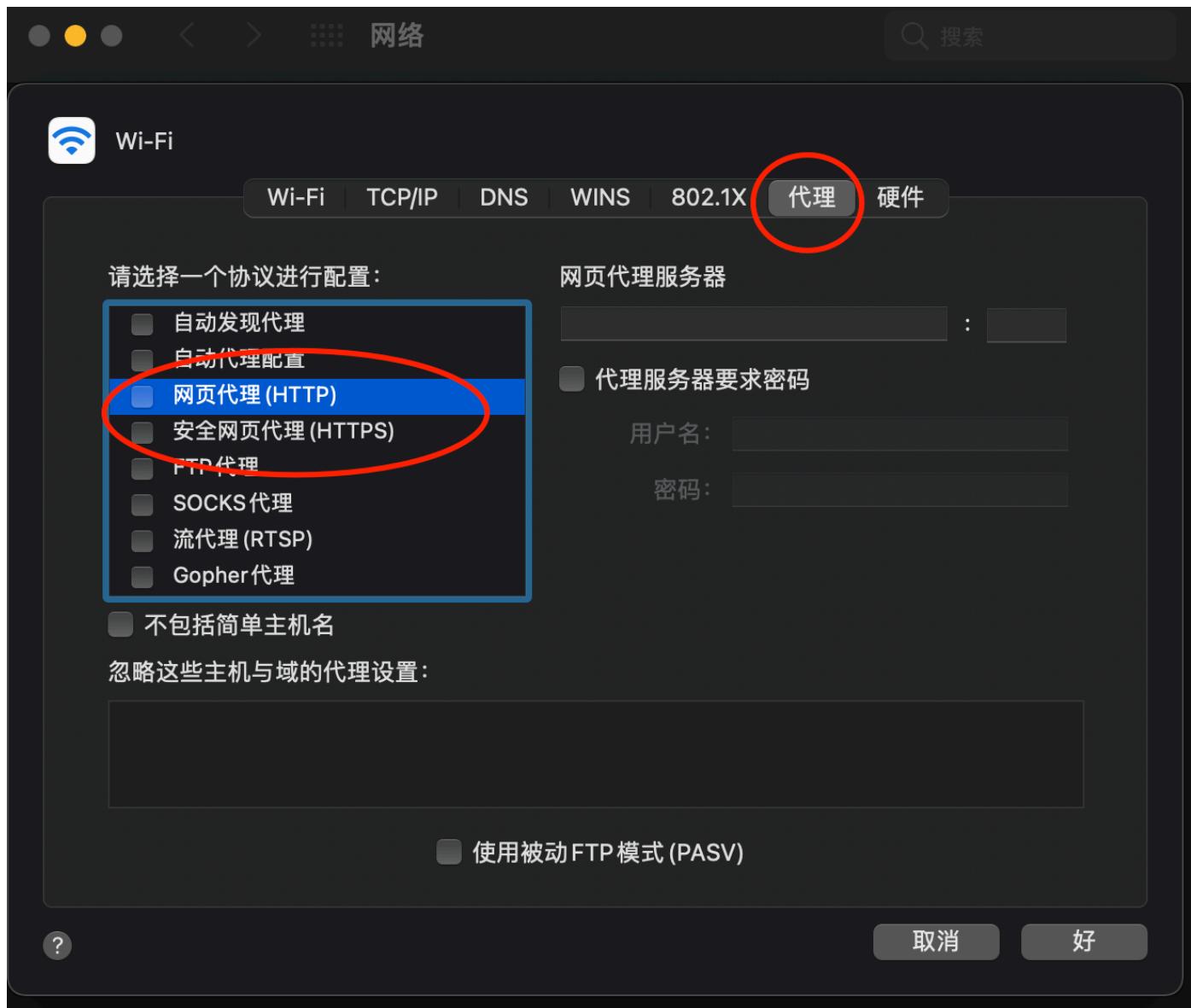
## 2.1.5 查看系统代理情况，点击“网络偏好与设置”



2.1.6 点击“高级”



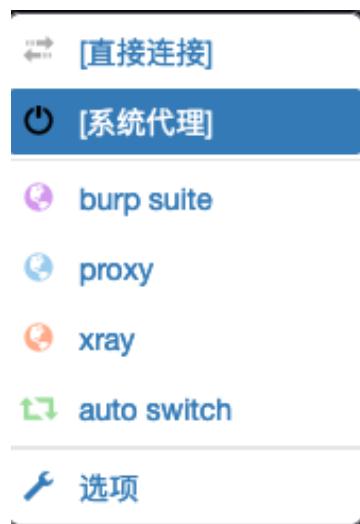
## 2.1.7 点击“代理”，查看系统代理情况



由此可以看出，通过火狐浏览器设置的代理，仅仅作用于火狐浏览器本身应用的代理，并不是系统级别的代理。

## 2.2 全局代理

### 2.2.1 关闭火狐浏览器的代理ip和端口



## 2.2.2 打开谷歌浏览器，配置代理ip和端口

The screenshot shows the 'System' section of the Chrome settings. A red box highlights the 'Open your computer's proxy settings' link.

**系统**

使用硬件加速模式 (如果可用)

打开您计算机的代理设置

**Wi-Fi**

Wi-Fi | TCP/IP | DNS | WINS | 802.1X | **代理** | 硬件

请选择一个协议进行配置：

- 自动发现代理
- 自动代理配置
- 网页代理 (HTTP)
- 安全网页代理 (HTTPS)
- FTP 代理
- SOCKS 代理
- 流代理 (RTSP)
- Gopher 代理

网页代理服务器

127.0.0.1 : 8849

代理服务器要求密码

用户名：

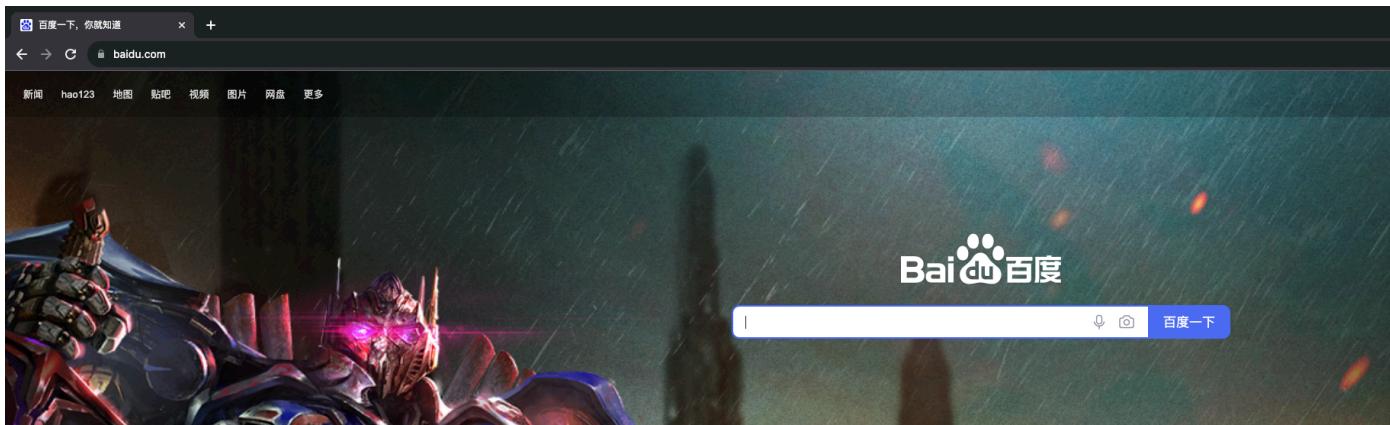
密码：

忽略这些主机与域的代理设置：

使用被动FTP模式 (PASV)

? 取消 好

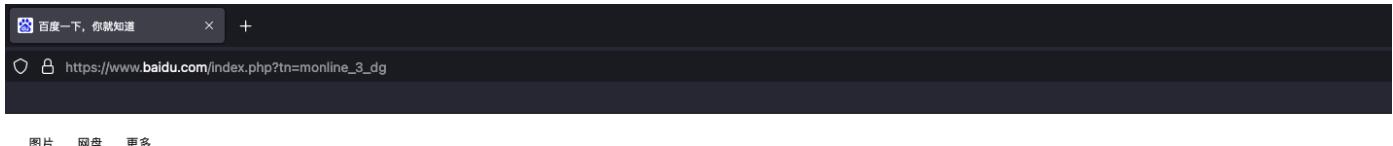
## 2.2.3 谷歌浏览器访问任意网址



## 2.2.4 观察 Burp 中的流量

| #  | Host                           | Method | URL                                      | Params |
|----|--------------------------------|--------|--|--------|
| 7  | https://www.baidu.com          | GET    | /  |        |
| 14 | https://hectorstatic.baidu.com | GET    | /cd37ed75a9387c5b.js                     |        |
| 18 | https://www.baidu.com          | GET    | /home/feed/feedwater?id=2&offset=1&...   | ✓      |
| 19 | https://www.baidu.com          | GET    | /sugrec?&prod=pc_his&from=pc_web...      | ✓      |
| 24 | https://mbd.baidu.com          | GET    | /newspage/api/getpcvoicelist?callback... | ✓      |
| 21 | https://hpd.baidu.com          | GET    | /v.gif?ct=2&logFrom=feed_index&logIn...  | ✓      |
| 39 | https://hpd.baidu.com          | GET    | /v.gif?ct=2&logFrom=feed_index&logIn...  | ✓      |
| 35 | https://hpd.baidu.com          | GET    | /v.gif?ct=2&logFrom=feed_index&logIn...  | ✓      |
| 25 | https://hpd.baidu.com          | GET    | /v.gif?logFrom=feed_index&ct=2&sid=3...  | ✓      |
| 51 | https://hpd.baidu.com          | GET    | /v.gif?ct=2&logFrom=feed_index&logIn...  | ✓      |
| 47 | https://hpd.baidu.com          | GET    | /v.gif?ct=2&logFrom=feed_index&logIn...  | ✓      |
| 43 | https://hpd.baidu.com          | GET    | /v.gif?ct=2&logFrom=feed_index&logIn...  | ✓      |
| 10 | https://hpd.baidu.com          | GET    | /v.gif?ct=2&logFrom=feed_index&logIn...  | /      |

## 2.2.5 火狐浏览器访问任意网站



Bai<sup>du</sup>百度

 百度一下

## 2.2.6 观察 Burp 中的流量

| #   | Host                                   | Method | URL  | Params | Edited | Status |
|-----|--|--------|--|--------|--------|--------|
| 178 | https://www.baidu.com                  | GET    | /index.php?tn=monline_3_dg                 | ✓      |        | 200    |
| 179 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/events/1/bb19...   |        |        | 200    |
| 180 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/impression-stat... |        |        | 200    |
| 181 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/impression-stat... |        |        | 200    |
| 182 | https://incoming.telemetry.mozilla.net | POST   | /submit/activity-stream/sessions/1/9eb...  |        |        | 200    |
| 183 | https://incoming.telemetry.mozilla.net | POST   | /submit/firefox-desktop/newtab/1/1d6c...   |        |        | 200    |
| 188 | https://hectorstatic.baidu.com         | GET    | /cd37ed75a9387c5b.js                       |        |        | 200    |
| 191 | https://www.baidu.com                  | GET    | /sugrec?&prod=pc_his&from=pc_web...        | ✓      |        | 200    |
| 192 | https://www.baidu.com                  | GET    | /home/feed/feedwater?id=2&offset=1&...     | ✓      |        | 200    |
| 193 | https://hpd.baidu.com                  | GET    | /v.gif?ct=2&qid=0xe616f4b1000dcc3f&...     | ✓      |        | 200    |
| 195 | https://www.baidu.com                  | GET    | /cache/fpid/chromelib_1_1.js?_=16940...    | ✓      |        | 200    |
| 202 | https://hpd.baidu.com                  | GET    | /v.gif?ct=2&qid=0xe616f4b1000dcc3f&...     | ✓      |        | 200    |
| ... | ...                                    | ...    | ...  | ...    | ...    | ...    |

## 2.2.7 查看系统代理情况

The screenshot shows the macOS Network preferences window. At the top, there's a large blue toggle switch for Wi-Fi. Below it, under "首选网络" (Preferred Network), there's a Wi-Fi icon and a lock icon. Under "其他网络" (Other Networks), there's a right-pointing arrow icon. A red arrow points to the "网络偏好设置..." (Network Preferences...) button. The main content area is titled "网络" (Network). It shows a Wi-Fi icon and the word "Wi-Fi". Below that is a tab bar with "Wi-Fi", "TCP/IP", "DNS", "WINS", "802.1X", "代理" (selected), and "硬件".  
  
The "代理" tab contains the following configuration:

- 请选择一个协议进行配置: (Select a protocol to configure)
  - 自动发现代理
  - 自动代理配置
  - 网页代理 (HTTP)
  - 安全网页代理 (HTTPS)
  - FTP代理
  - SOCKS代理
  - 流代理 (RTSP)
  - Gopher代理
- 网页代理服务器 (Web Proxy Server):
  - 127.0.0.1 : 8849
  - 代理服务器要求密码 (Proxy server requires password)
  - 用户名: (Username): [empty field]
  - 密码: (Password): [empty field]
- 忽略这些主机与域的代理设置: (Ignore proxy settings for these hosts and domains): [empty list box]
  - 使用被动FTP模式 (PASV) (Use Passive FTP mode (PASV))

At the bottom, there are "取消" (Cancel) and "好" (OK) buttons.

**总结：**其实从不同浏览中设置代理就可以看出，但我们使用火狐设置的时候，直接就在浏览器内部设置就可以了，但是如果使用谷歌浏览器设置，他打开的是计算机网络设置，这里设置的是计算机的代理，所以火狐中设置的是局部代理，仅火狐浏览器应用中的流量会走 Burp 代理，其他应用并不受影响。但是如果从谷歌中跳转设置的是计算机的代理，那么这台计算机上所有应用的网络请求都会走 Burp 代理，这就是全局代理了。

## 四、利用 Burp 实现对 HTTPS 站点的抓包。

### 1. 概念

#### 1.1 HTTPS 的实现原理

HTTPS 整体过程分为证书验证阶段和数据传输阶段：

##### 1. 证书验证阶段

- (1) 浏览器发起 HTTPS 请求。
- (2) 服务器返回 HTTPS 证书。
- (3) 客户端验证证书是否合法，如果不合法则告警。

##### 2. 数据传输阶段

- (1) 当证书合法后，在本地生成一个随机数。
- (2) 通过公钥对随机数进行加密，然后将随机数发送给服务端。
- (3) 服务端通过私钥对随机数进行解密。
- (4) 服务端通过随机数对返回的数据进行对称加密，将加密后的内容返回给客户端。

### 1.2 证书

HTTP 协议被认为不安全是因为传输过程容易被监听者监听、伪造服务器，而 HTTPS 协议主要解决的便是网络传输的安全性问题。

首先我们假设不存在认证机构，任何人都可以制作证书，这带来的安全风险便是经典的“中间人攻击”问题。

#### 1.2.1 证书中都包含哪些信息？

- 颁发机构信息
- 公钥
- 公司信息
- 域名
- 有效期
- 指纹
- 等等

## 1.2.2 证书的合法性

首先，权威机构是要有认证的，不是随便一个机构都有资格颁发证书，不然也不叫做权威机构。

另外，证书的可信性基于信任制，权威机构需要对其颁发的证书进行信用背书，只要是权威机构生成的证书，我们就认为是合法的。

所以权威机构会对申请者的信息进行审核，不同等级的权威机构对审核的要求也不一样，于是证书也分为免费的、便宜的和贵的。

## 1.2.3 浏览器如何校验证书的合法性？

浏览器发起 HTTPS 请求时，服务器会返回网站的 SSL 证书，浏览器需要对证书做以下验证：

- (1) 验证域名、有效期等信息是否正确。证书上都有包含这些信息，比较容易完成验证；
- (2) 判断证书来源是否合法。每份签发证书都可以根据验证链查找到对应的根证书，操作系统、浏览器会在本地存储权威机构的根证书，利用本地根证书可以对对应机构签发证书完成来源验证；
- (3) 判断证书是否被篡改。需要与 CA 服务器进行校验；
- (4) 判断证书是否已吊销。通过CRL（Certificate Revocation List 证书注销列表）和 OCSP（Online Certificate Status Protocol 在线证书状态协议）实现，其中 OCSP 可用于第3步中以减少与 CA 服务器的交互，提高验证效率。

## 1.3 使用代理对 HTTPS 进行抓包

HTTPS 的数据是加密的，常规下抓包工具代理请求后抓到的包内容是加密状态，无法直接查看。

但是，浏览器只会提示安全风险，如果用户授权仍然可以继续访问网站，完成请求。因此，只要客户端是我们自己的终端，我们授权的情况下，便可以组建中间人网络，而抓包工具便是作为中间人的代理。

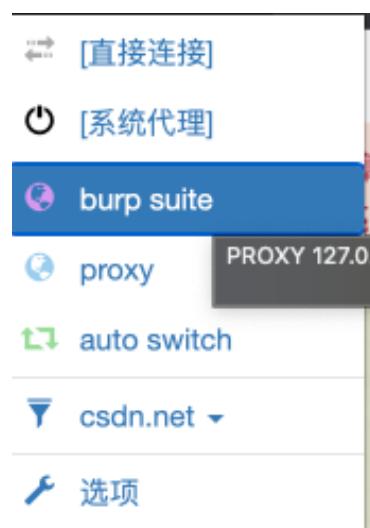
通常 HTTPS 抓包工具的使用方法是会生成一个证书，用户需要手动把证书安装到客户端中，然后终端发起的所有请求通过该证书完成与抓包工具的交互，然后抓包工具再转发请求到服务器，最后把服务器返回的结果在控制台输出后再返回给终端，从而完成整个请求的闭环。

## 2. Burp 证书安装

### 2.1 启动 Burp

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Below the tabs, there are several buttons: 'Forward', 'Drop', 'Intercept is off' (which is currently highlighted in red), 'Action', and 'Open browser'. The main area of the interface is currently empty.

## 2.2 设置浏览器代理



## 2.3 访问下面地址

The screenshot shows a web browser window with the address bar containing 'http://burp/'. In the background, the Burp Suite Professional interface is visible, showing its welcome screen.

## 2.4 点击“CA Certificate”，会下载一个证书

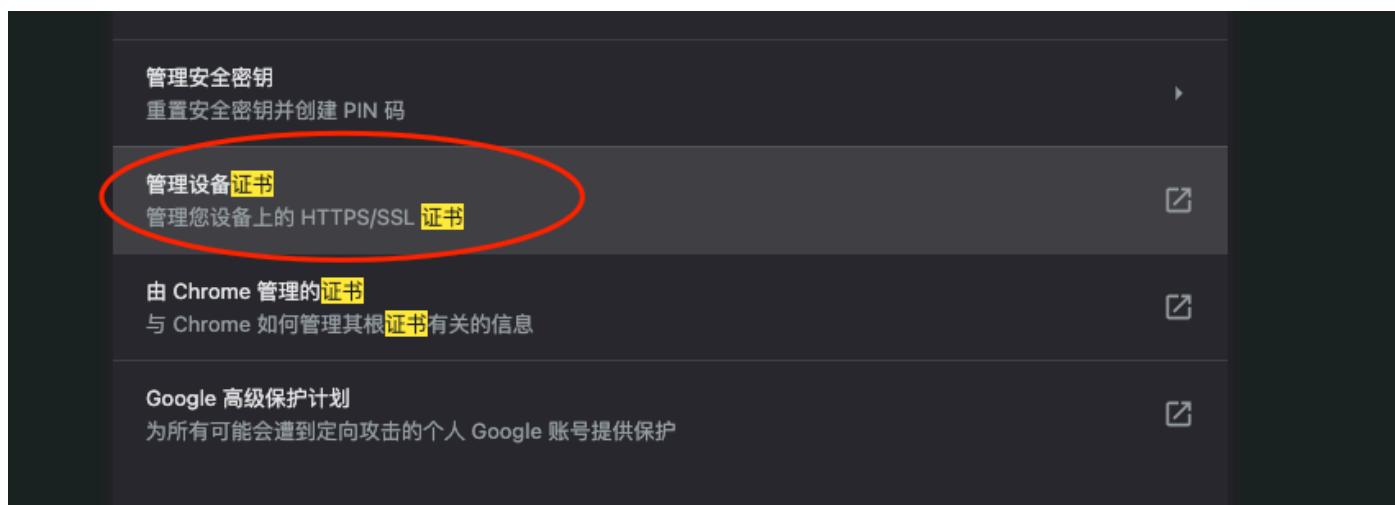
The screenshot shows the Burp Suite Professional interface. A red arrow points to the 'CA Certificate' button in the top right corner of the header bar.

## 2.5 将生成的证书导入浏览器中

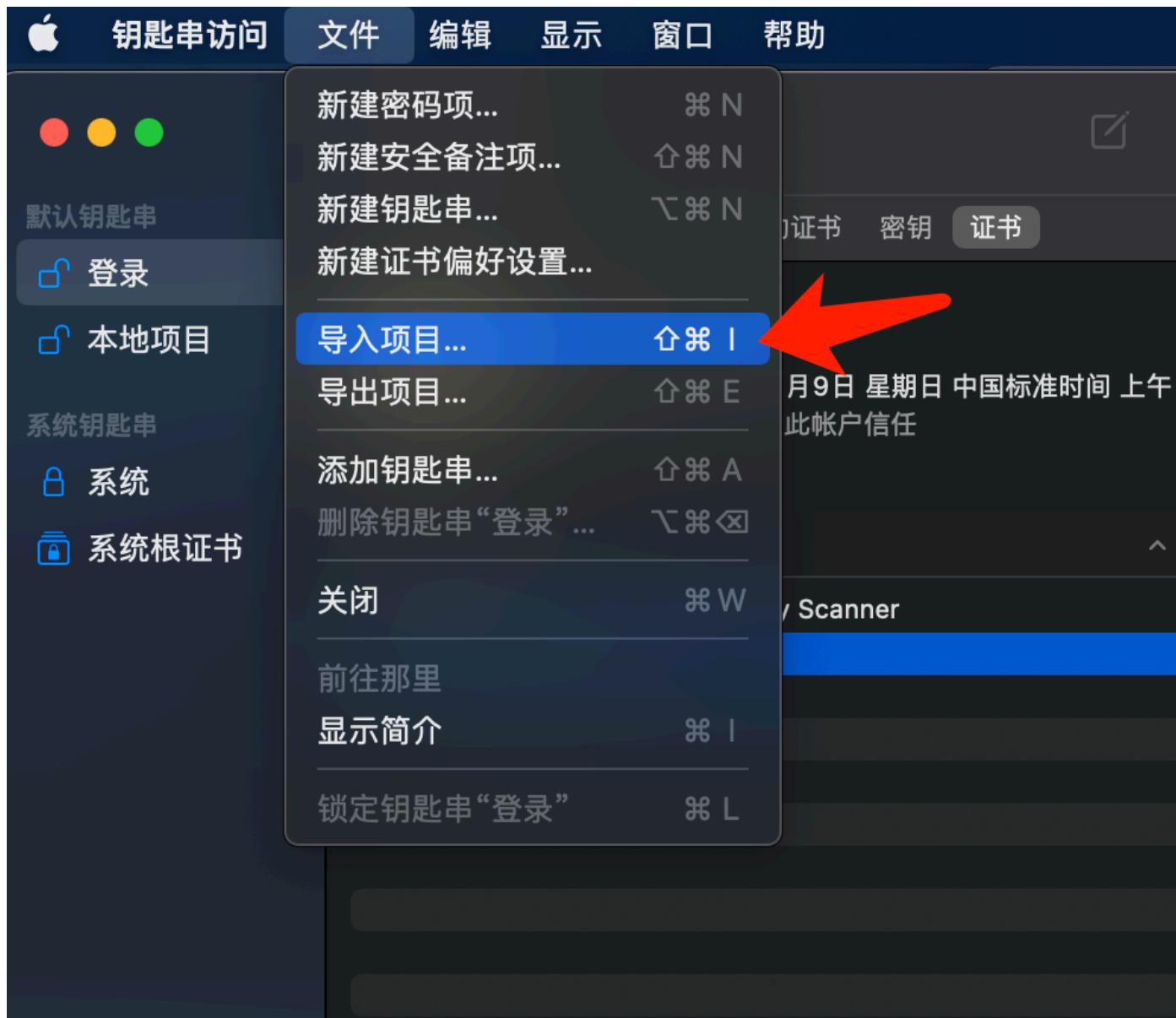
### 2.5.1 打开浏览器设置，搜索证书



### 2.5.2 点击“管理设备证书”



### 2.5.3 将下载的证书导入



### 2.5.4 搜索刚导入的证书，设置为“始终信任”

名称



Insecure Root CA For X-Ray Scanner



PortSwigge

新建证书偏好设置...

拷贝“PortSwigger CA”

删除“PortSwigger CA”

导出“PortSwigger CA”...

显示简介

评估“PortSwigger CA”...



PortSwigger CA



PortSwigger CA

根证书颁发机构

过期时间：2033年1月9日 星期日 中国标准时间 上午10:51:08

+ 此证书已标记为受此帐户信任

信任

使用此证书时： 始终信任



加密套接字协议层 (SSL) 始终信任



安全邮件 (S/MIME) 始终信任



可扩展认证协议 (EAP) 始终信任



IP 安全 (IPsec) 始终信任



代码签名 始终信任



时间戳 始终信任





## ▼ 细节

## 2.6 访问 HTTPS 站点，查看 Burp 流量抓取情况。

Intercept    **HTTP history**    WebSockets

Filter: Hiding CSS, image and general binary content

| #    | Host                                   | Method |
|------|--|--------|
| 2353 | https://internal-api-security.feish... | OPTION |
| 2354 | https://internal-api-security.feish... | GET    |
| 2355 | https://googleads.g.doubleclick....    | GET    |
| 2356 | https://ev.csdn.net                    | POST   |
| 2357 | https://www.baidu.com                  | GET    |
| 2366 | https://hectorstatic.baidu.com         | GET    |
| 2369 | https://www.baidu.com                  | GET    |
| 2370 | https://www.baidu.com                  | GET    |
| 2371 | https://hector.baidu.com               | GET    |
| 2379 | https://mbd.baidu.com                  | GET    |
| 2380 | https://internal-api-security.feish... | OPTION |
| 2381 | https://ev.csdn.net                    | POST   |
| 2382 | https://internal-api-security.feish... | GET    |