# HTTP请求-XFF

### 访问环境

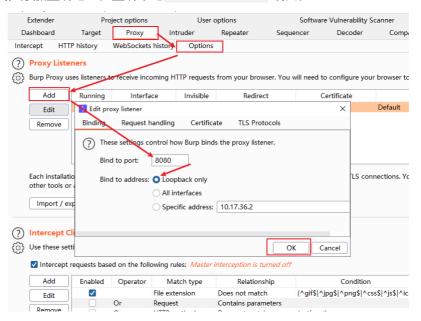
- 1. URL为: http://192.168.10.41 , 端口为默认 80 端口,请勿访问图片中端口。
- 2. 提示:必须从小红自己的计算机访问。



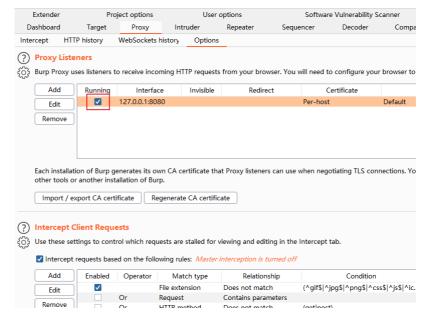
## 工具使用

Burp监听代理设置

1. 打开Burp工具,添加监听地址。监听本地 127.0.0.1 8080 端口。

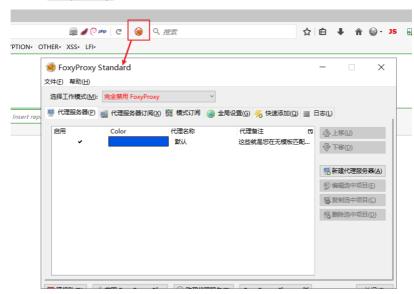


2. 勾选刚刚添加的代理地址

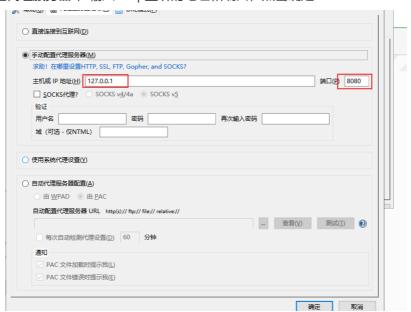


#### 浏览器代理设置 (如果存在Burp请忽略)

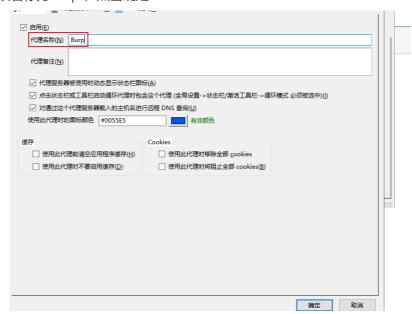
1. 这里介绍浏览器插件 FoxyProxy



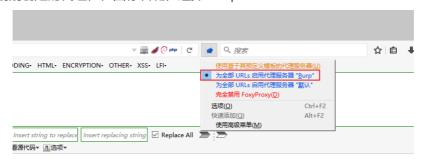
2. 点击右侧"新建代理服务器",输入Burp监听的地址和端口,点击确定



3. 再次"常规修改名称为Burp",点击确定



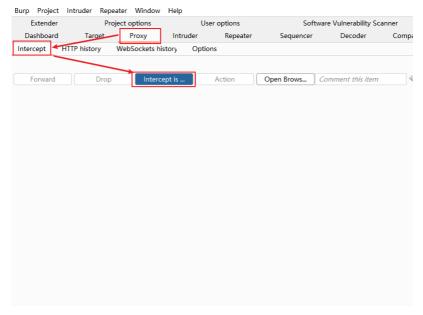
4. 浏览器使用刚刚创建的代理,在图标右键,选择"Burp"



## 拦截请求-修改字段

Burp拦截并修改请求

1. 设置Burp拦截模式



2. 浏览器刷新页面,Burp收到请求



# 获取Flag

1. 修改 X-Forwarded-For: 8.8.8.8 为 X-Forwarded-For: 127.0.0.1, 然后点击Forward放包。

```
Extender Project options User options Software Vulnerability Scanner

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Compaintercept HTTP history WebSockets history Options

Request to http://192.168.10.41:32769

Forward Drop Intercept is... Action Open Brows... Comment this item

Pretty Rav In Actions V

1 GET / H. TTP/1.1

2 Host: 192.168.10.41:32769

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; W0W64; rv:49.0) Gecko/20100101 Firefox/49.0

4 Accept-Language: zh-CN, zh; q=0.8, en-US; q=0.5, en; q=0.3

6 Accept-Ekcoding: gzip, deflate

7 DNT: 1

X-Forwarded-For: 127.0.0.1

9 Compection: close

10 Upgrade-Insecure-Requests: 1
```

