

# xff\_referer

使用插件SwitchyOmega，更方便切换代理，设置代理如下所示：

SwitchyOmega测试版

情景模式： abc

设定

🔧 界面

⚙️ 通用

📂 导入/导出

情景模式

🌐 abc

🌐 proxy

↕️ auto switch

+ 新建情景模式...

ACTIONS

代理服务器

| 网址协议 | 代理协议 | 代理服务器     |
|------|------|-----------|
| (默认) | HTTP | 127.0.0.1 |

显示高级设置

不代理的地址列表

不经过代理连接的主机列表: (每行一个主机)

(可使用通配符等匹配规则...)

127.0.0.1

:::1

localhost

在burp suite中设置代理：

TargetProxySpiderScannerIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser optionsAlerts

InterceptHTTP historyWebSockets historyOptions

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

| Add                               | Running                             | Interface      | Invisible | Redirect | Certificate |
|-----------------------------------|-------------------------------------|----------------|-----------|----------|-------------|
| <div>Edit</div> <div>Remove</div> | <input checked="" type="checkbox"/> | 127.0.0.1:8080 |           |          | Per-host    |

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for another installation of Burp.

Import / export CA certificate

Regenerate CA certificate

Intercept Client Requests

在请求包中添加一下信息：

X-Forwarded-For: 123.123.123.123  
Referer: https://www.google.com

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

TargetProxySpiderScannerIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options

InterceptHTTP historyWebSockets historyOptions

Request to http://111.198.29.45:57667

ForwardDropIntercept is onAction

RawHeadersHex

GET / HTTP/1.1  
Host: 111.198.29.45:57667  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:70.0) Gecko/20100101 Firefox/70.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Connection: close  
Upgrade-Insecure-Requests: 1  
Cache-Control: max-age=0  
X-Forwarded-For: 123.123.123.123  
Referer: https://www.google.com

释放数据包得到flag：

index × +

.198.29.45:57667

双11红包 最常访问 火狐官方网站 Mac 键盘快捷键 - Ap... Google 新手上路 Web2016讲课计划... XssNow Linux入门: Linux历... mac OS X下配置jdk...

cyberpeace{f569c0843581f077272c981976923df1}