

Burp Suite 使用 | Pa55w0rd 's Blog

0x00 前言

Burp Suite 是 Web 应用程序测试的最佳工具之一，其多种功能可以帮我们执行各种任务. 请求的拦截和修改, 扫描 web 应用程序漏洞, 以暴力破解登陆表单, 执行会话令牌等多种的随机性检查。

大家都很熟悉工具的使用了，这里介绍几个技巧，欢迎大家补充

详细教程参考：

Burp Suite 说明书（开车版） 链接：<https://pan.baidu.com/s/1tNTzSO1eKDtRg7-T0cdjVQ> 提取码: 8un3 复制这段内容后打开百度网盘手机 App，操作更方便哦

<https://t0data.gitbooks.io/burpsuite/content/>

0x01 专业版激活问题

使用 burp-loader-keygen.jar 注册机激活

支持 1.6 - 目前最新的都能使用该注册机激活

注意有人利用这个破解补丁添加后门传播病毒，[后门分析帖子》》](#)

原始注册机文件的 MD5

burp-loader-keygen.jar MD5: A4A02E374695234412E2C66B0649B757

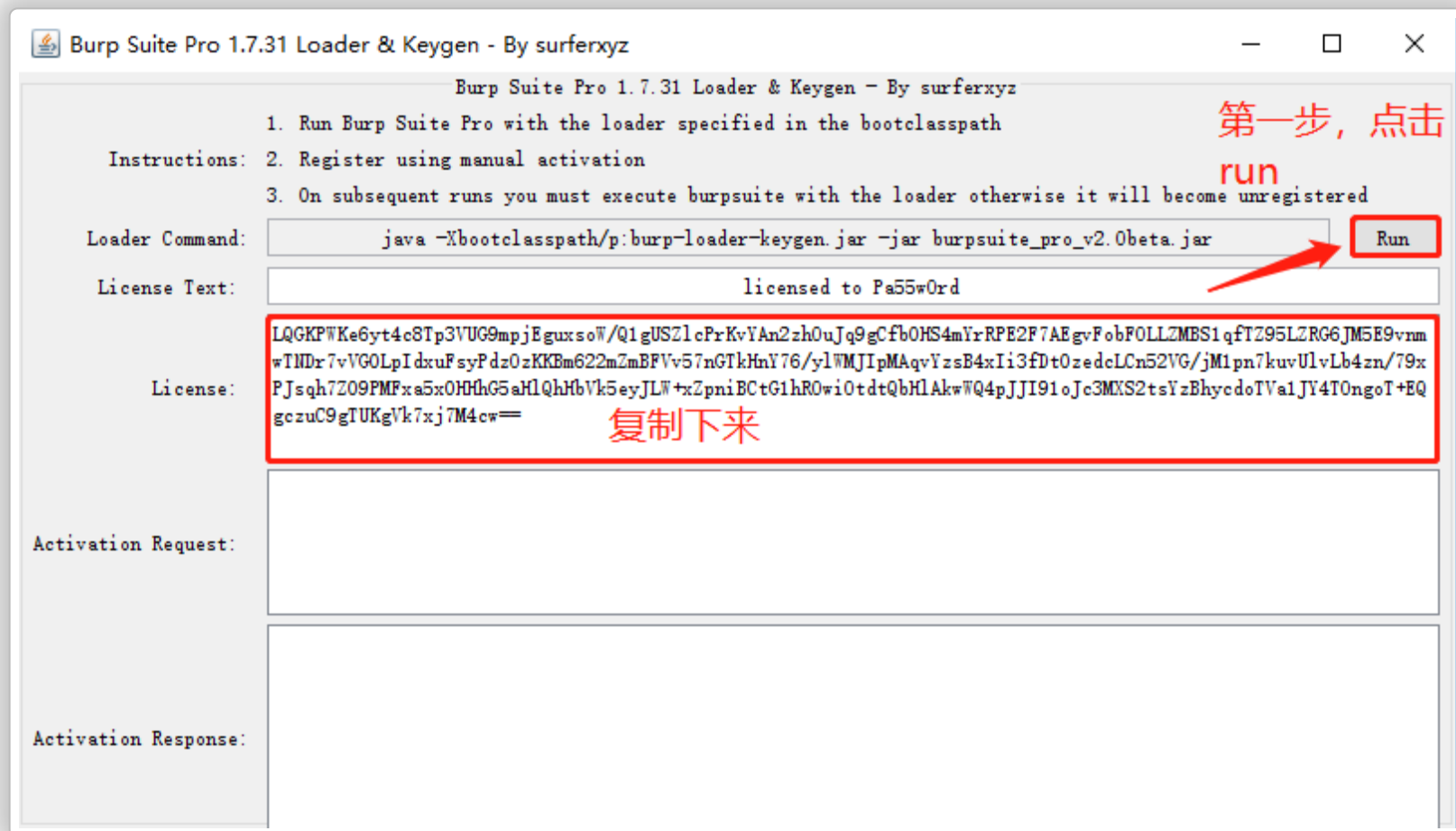
源文件 MD5 官网查看：

<http://releases.portswigger.net>

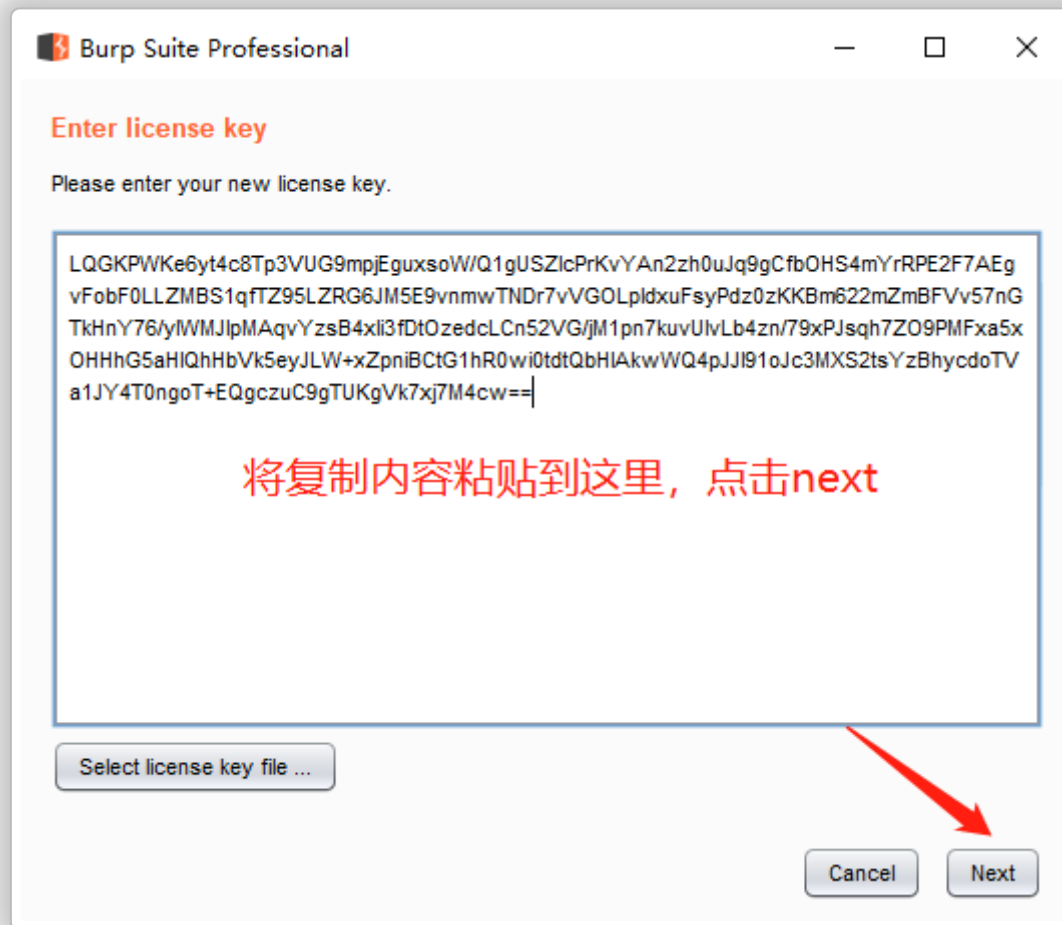
使用 burp-loader-keygen.jar 破解的，每次都需要在该工具上启动，或使用命令行启动 `java -Xbootclasspath/p:burp-loader-keygen.jar -jar burpsuite_pro.jar`

激活步骤

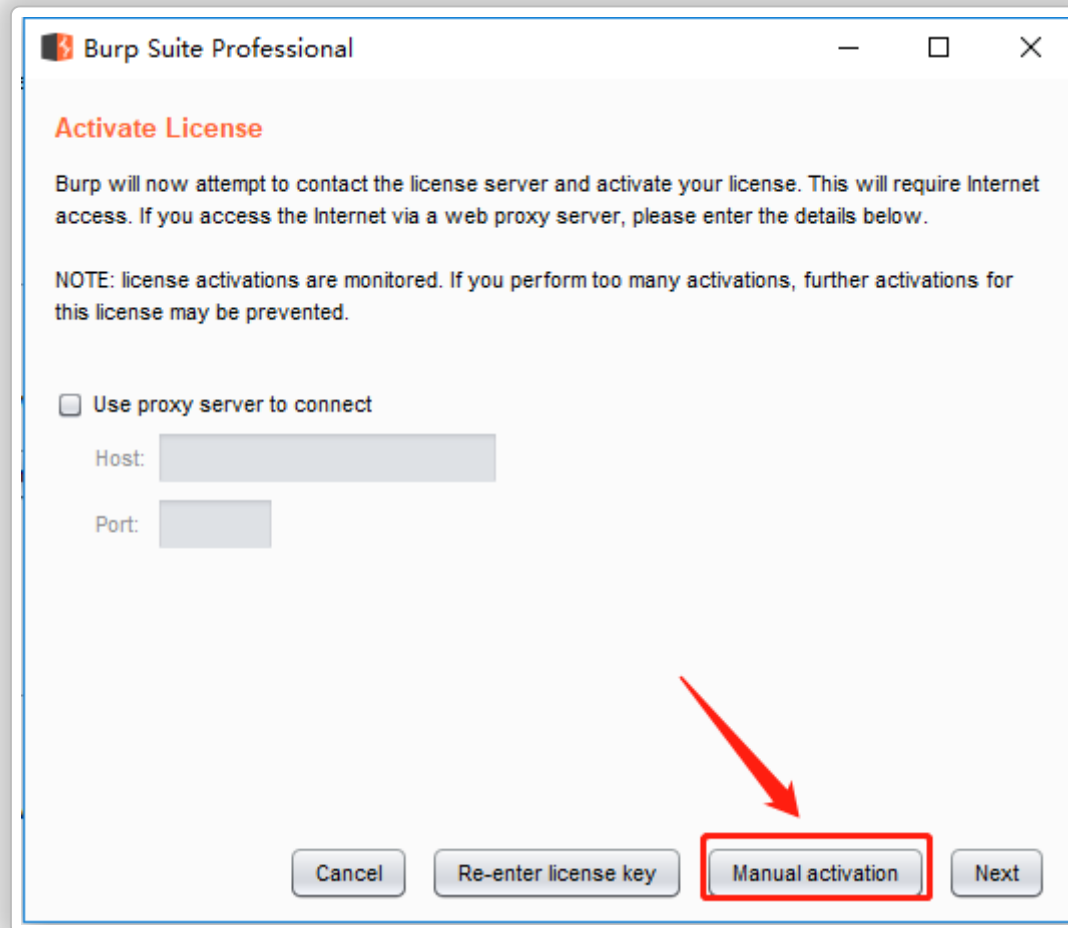
- 首先打开 burp-loader-keygen.jar



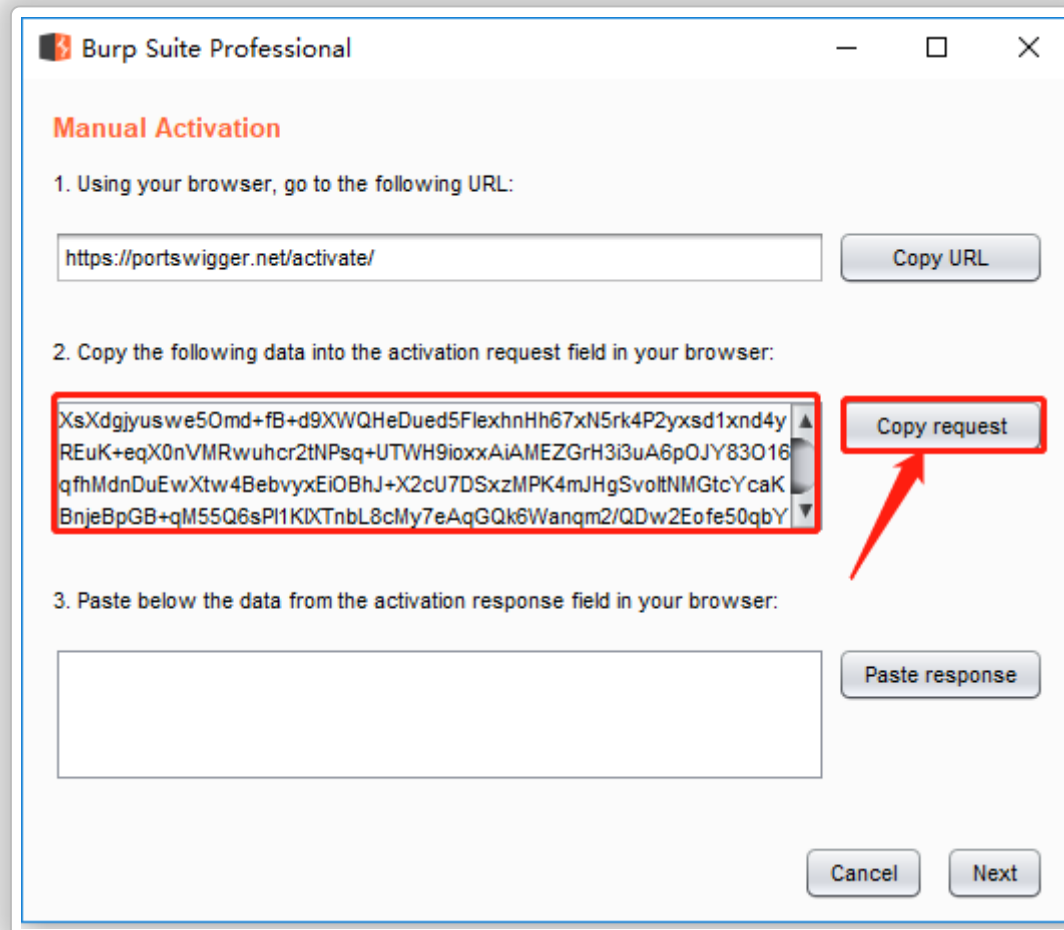
- 点击 burp, 将复制内容粘贴到 Enter license key, 点击 next



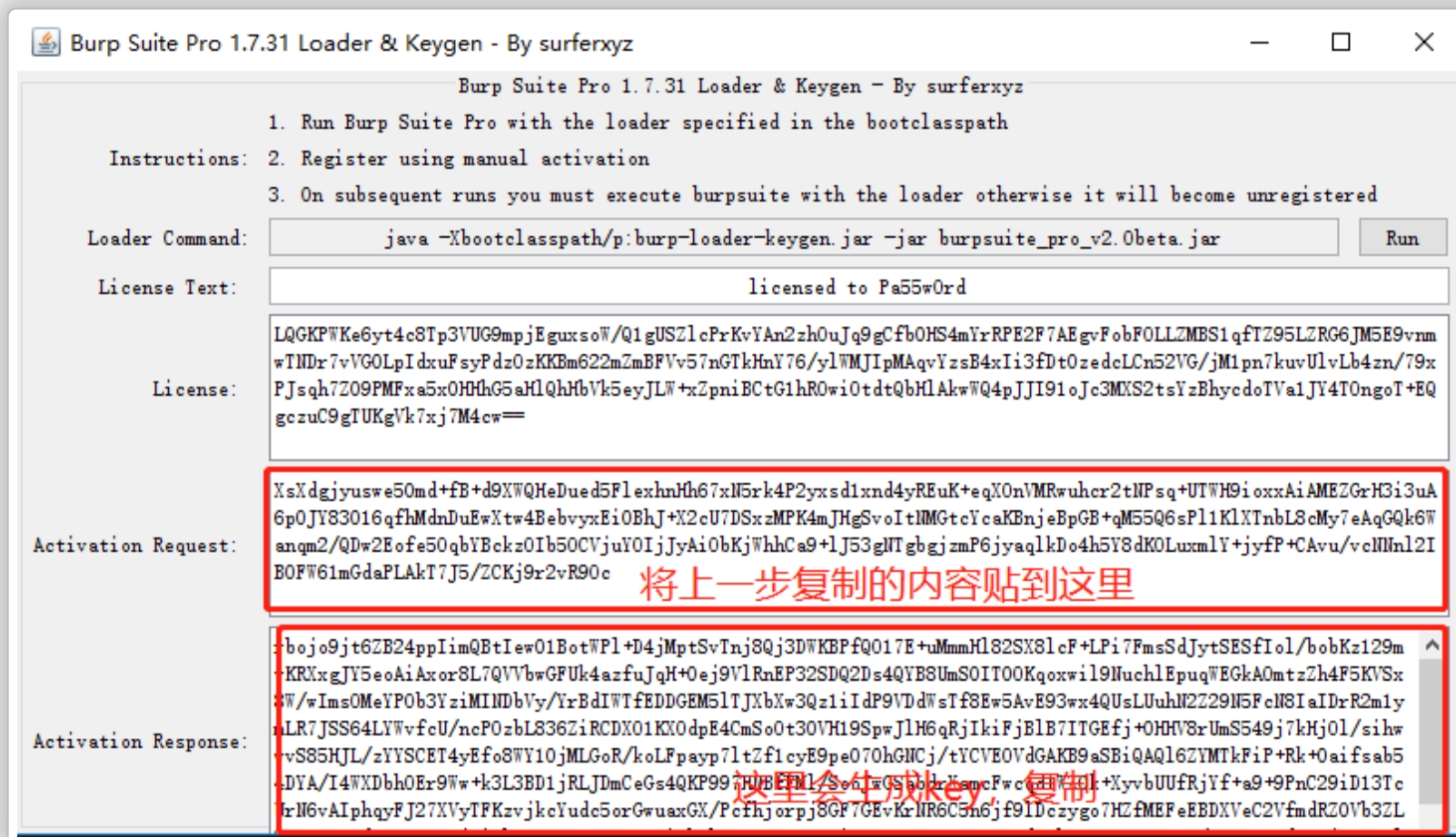
- 点击 Manual activation



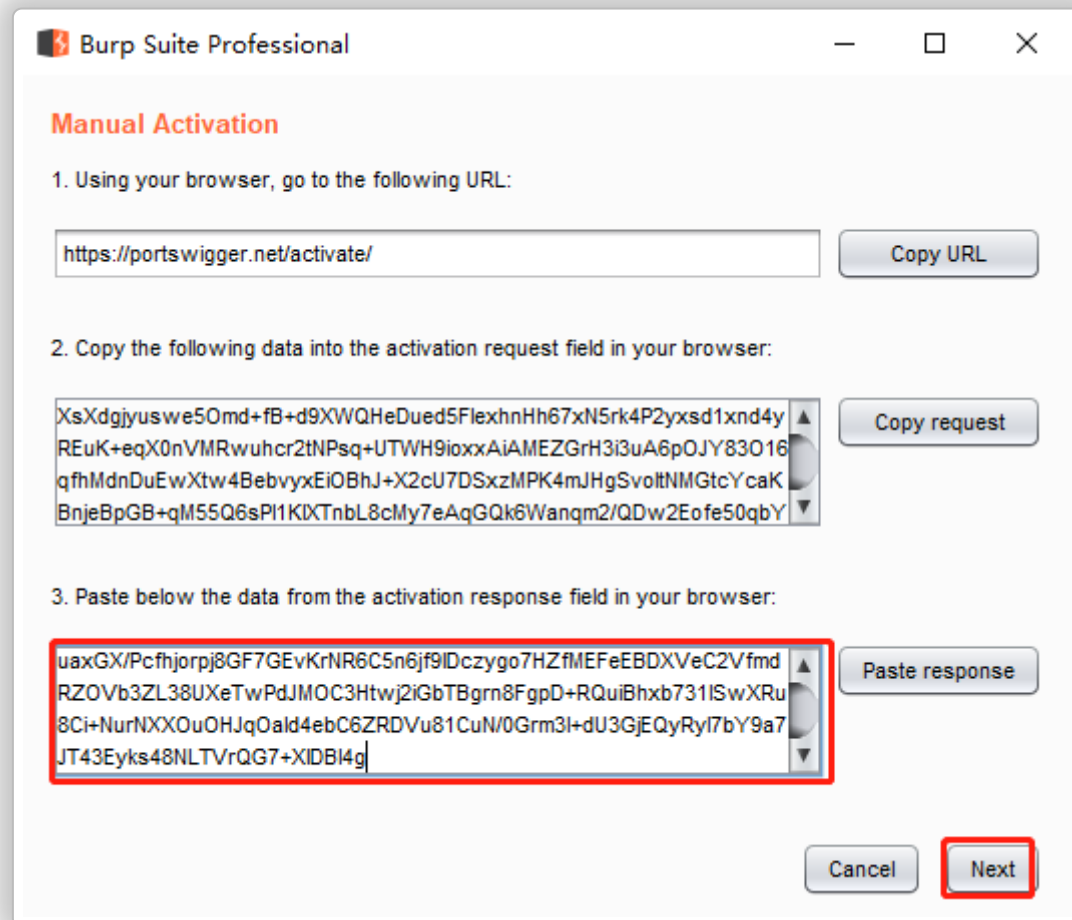
- 复制 2 中的内容

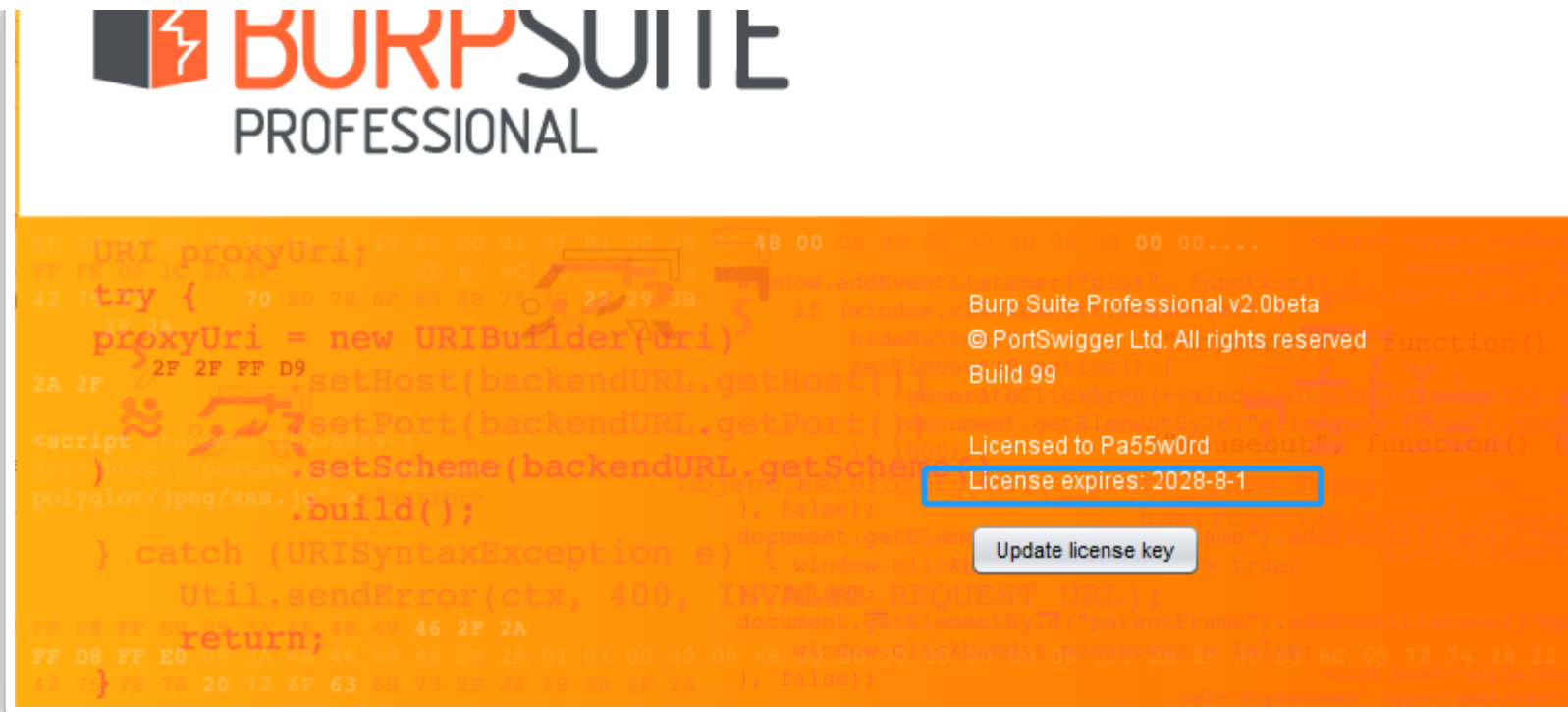


- 将复制内容粘贴到 burp-loader-keygen.jar 中的 Activation Request, 下方 Activation Response 会生成 key, 复制



- 回到 burp, 将复制内容粘贴到 3 中, 点击 next, 激活成功

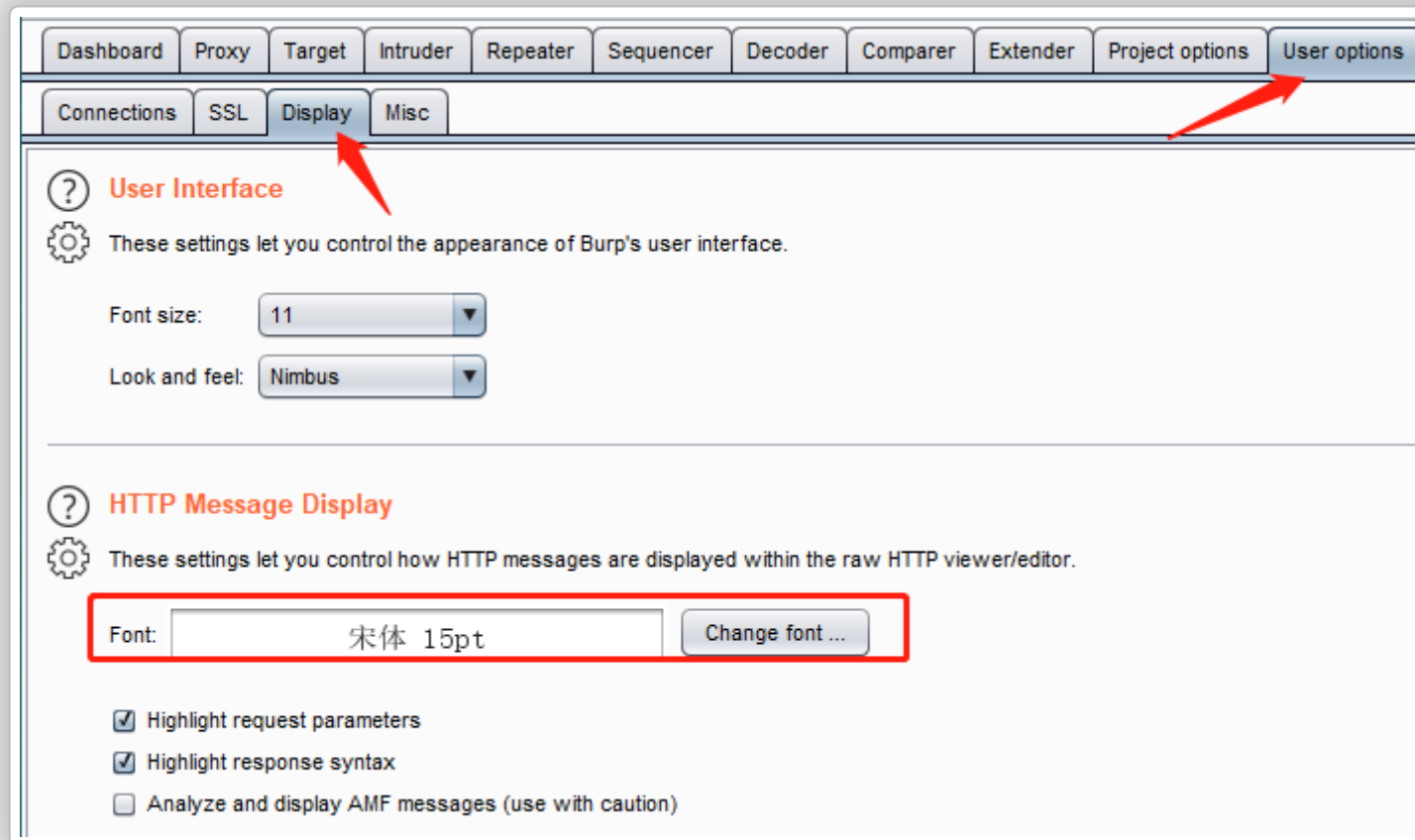




0x02 中文显示乱码问题

User options – Display – HTTP Message Display – Change font...

选择一个中文的字体格式，调整显示字体大小

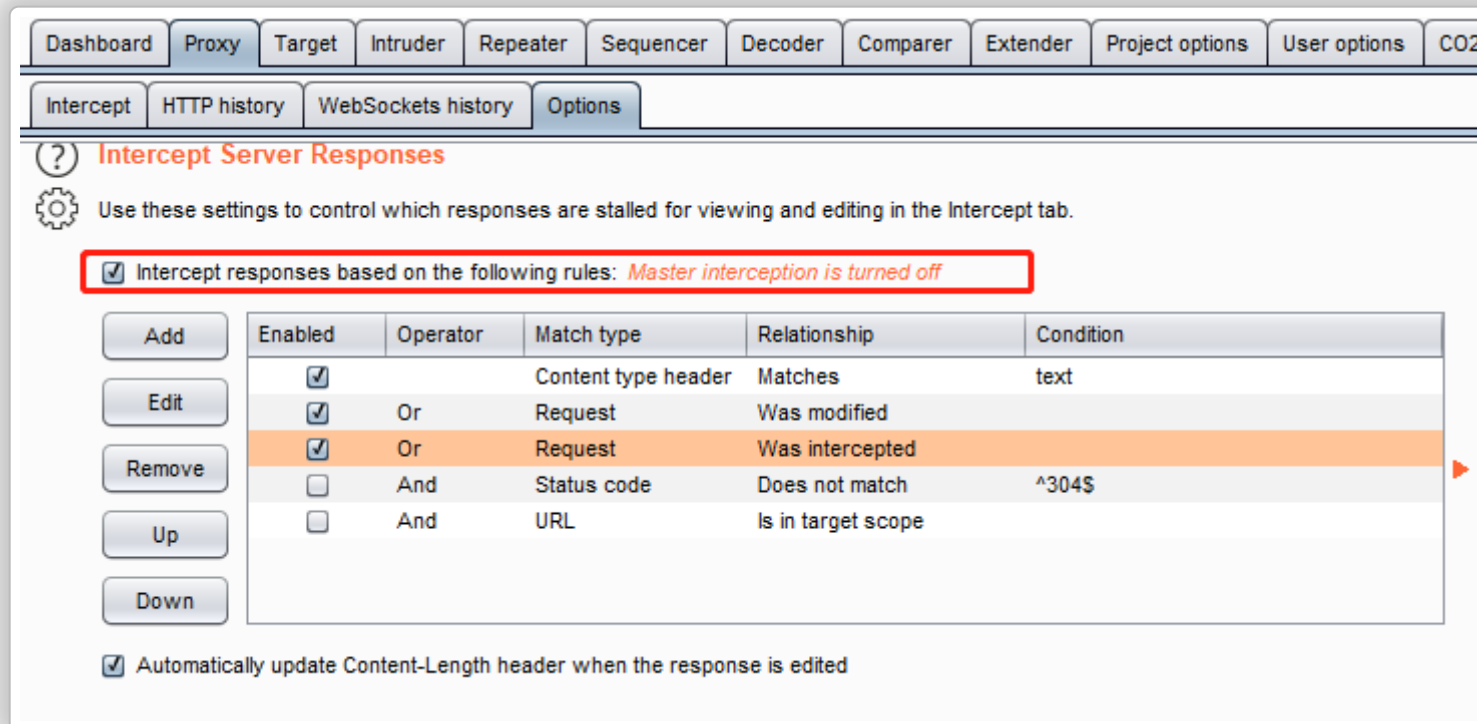


0x03 拦截响应包

很多时候，在测试验证码等认证漏洞的时候，只在前端验证，可以通过修改响应

包中的值绕过验证

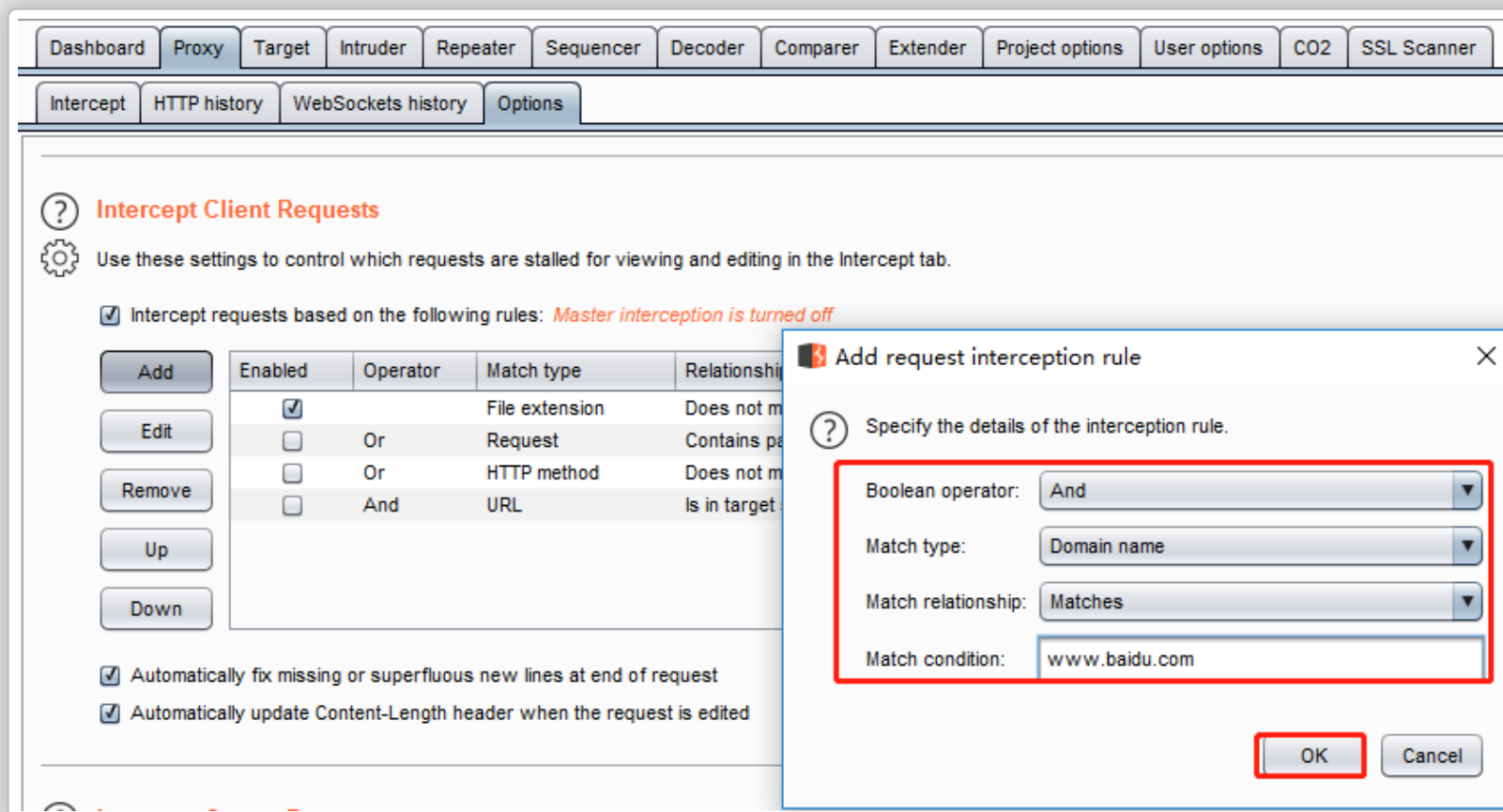
Proxy – Options – Intercept Server Responses 勾选启用



0x04 拦截指定 url 的请求响应包

请求包设置

Proxy – Options – Intercept Client Requests – Add



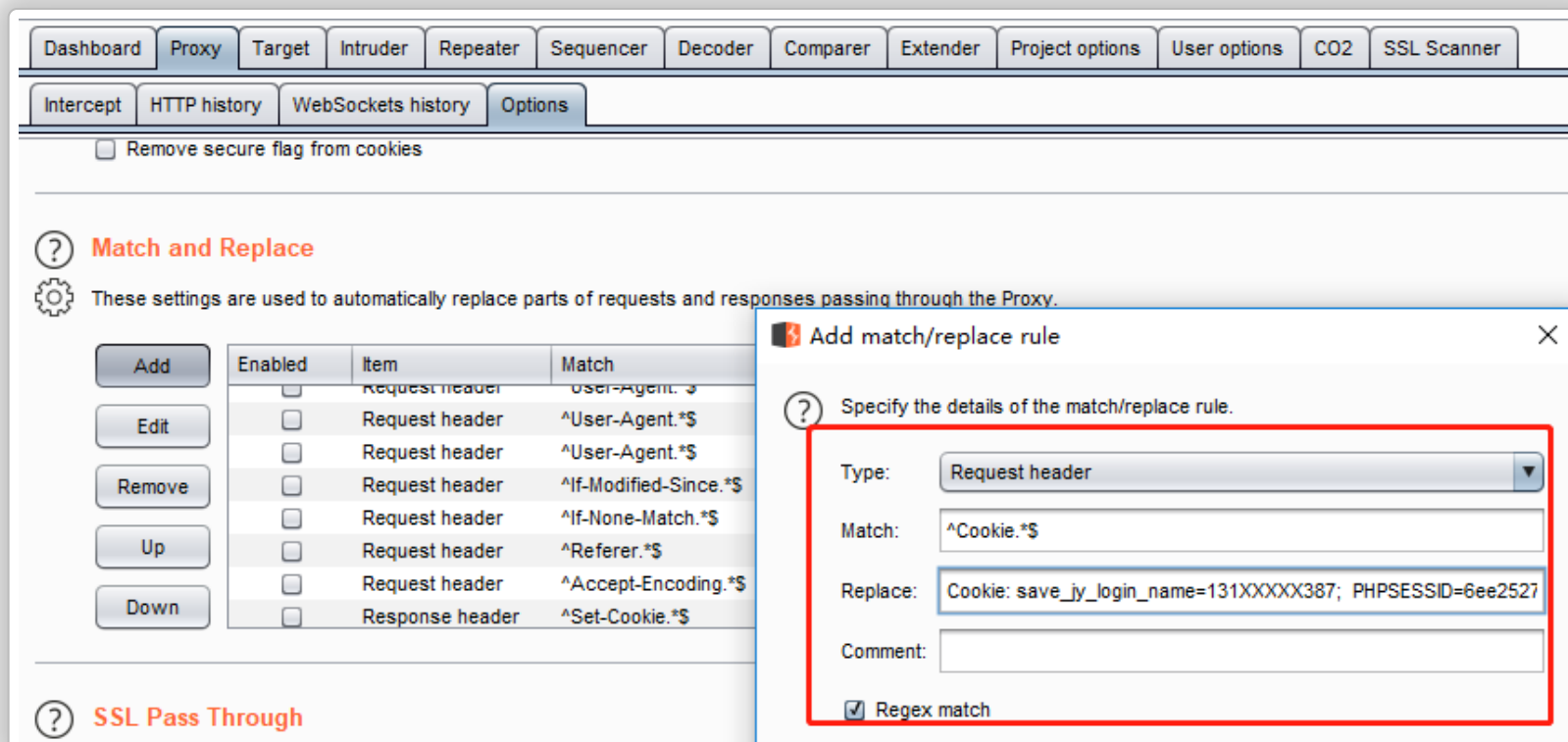
响应包设置

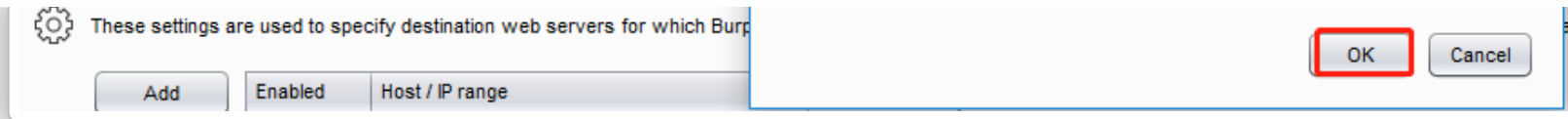
Proxy – Options – Intercept Server Responses – Add, 同上图设置

0x05 自动替换 cookie 等

如盲打 xss, 接收到 cookie 后, 需要在每个请求包中都替换 cookie

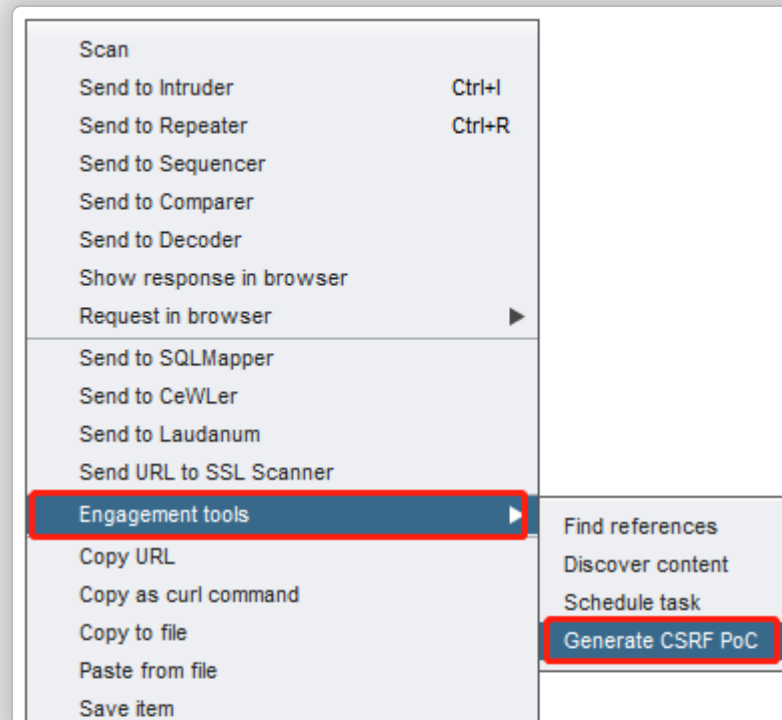
Proxy – Options – Match and Replace – Add(增加其他自动替换同理, 可以自动替换请求 / 响应内容, 这里以 cookie 为例)

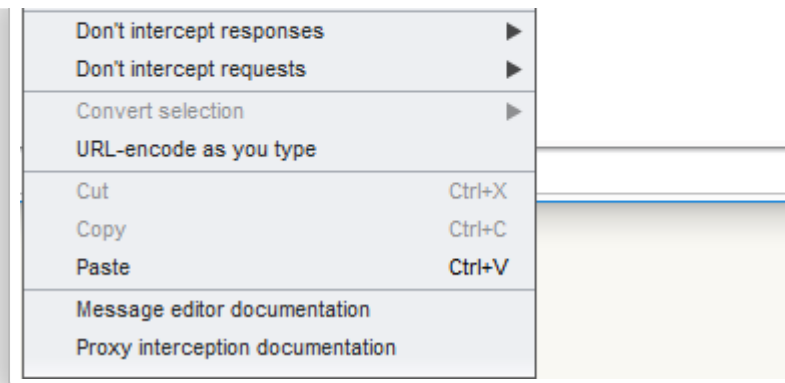




oxo6 生成 csrf poc

对拦截的请求，右键





0x07 条件竞争漏洞测试

“竞争条件” 发生在多个线程同时访问同一个共享代码、变量、文件等没有进行锁操作或者同步操作的场景中。

开发者在进行代码开发时常常倾向于认为代码会以线性的方式执行，而且他们忽视了并行服务器会并发执行多个线程，这就会导致意想不到的结果。

简单的说：本来你有 100 块钱，买一个商品要花 100，你可以多开启多个线程去跑，有可能不止一个用户买成功

“竞争条件” 漏洞有时很难通过黑盒 / 灰盒的方法来进行挖掘 因为这个漏洞很

受环境因素的影响，比如网络延迟、服务器的处理能力等。一般都会通过对代码进行审计来发现此类问题

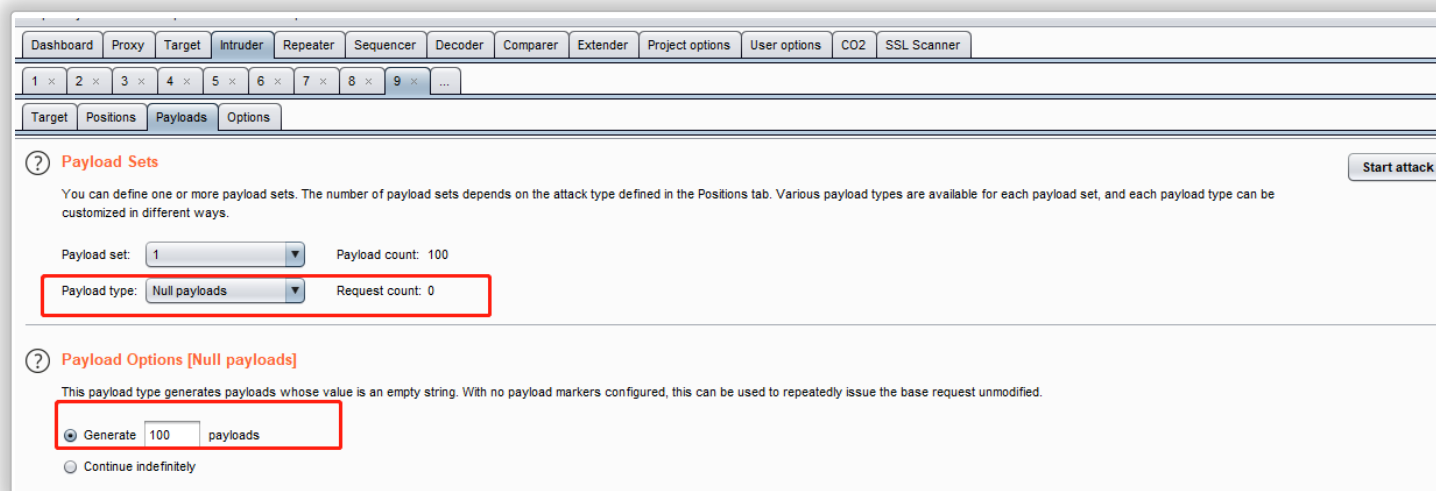
可以使用 Burp 的 intruder 功能来实现发送多个并发请求

将请求包发送至 Intruder

Intruder – Payloads – Payload Stes

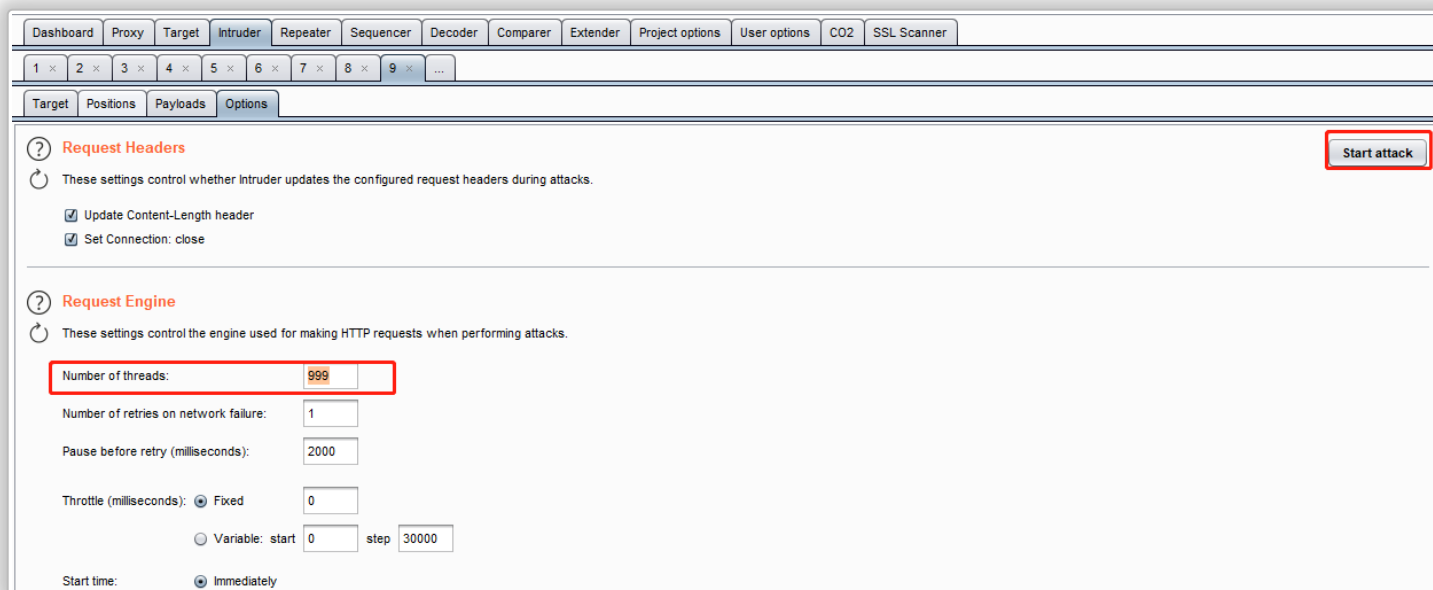
Payload type 设置为 Null payloads

Payload Options 次数设置 100 次



Intruder – Options – Request Engine

线程数设置最大 999 ， 点击 Start attack



oxo8 DNSlog 功能

Burp Collaborator 是从 Burp suite v1.6.15 版本添加的新功能，也就是

DNSlog, 监控 DNS 解析记录和 HTTP 访问记录, 在检测盲注类漏洞很好用, 也可以借助第三方服务

这里引出两个概念, **In-band attack** 与 **out-band attack** (带内与带外攻击), 带内与带外的区别核心在于是否使用不同的通信通道。

- 带内攻击

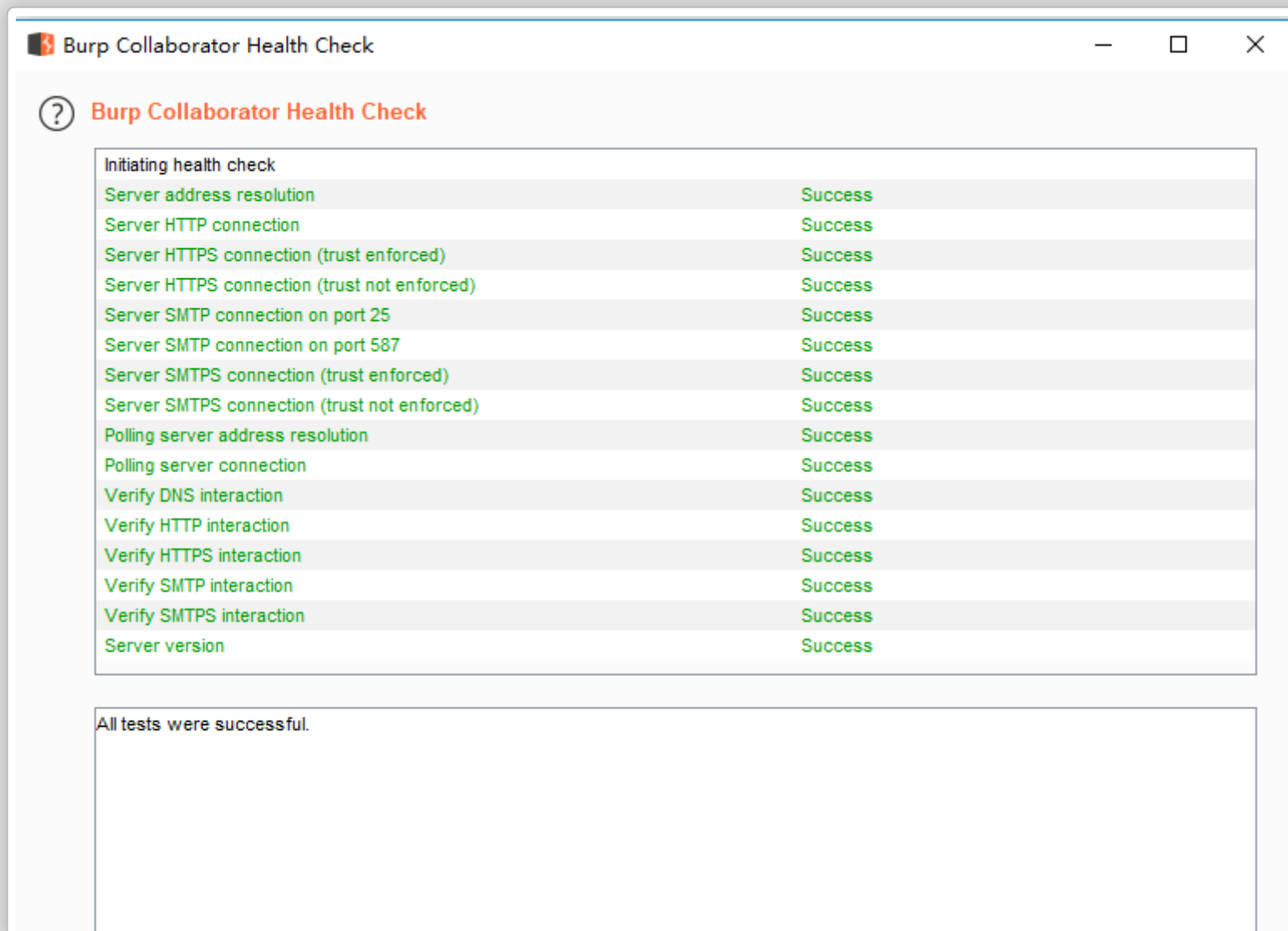
在一次攻击当中, 只有一条通道, 属于 in-band (带内) 攻击。常规的 web 测试模型就是我们向目标发送 payloads, 然后分析目标返回的数据。

- 带外攻击

现在同一次攻击下, 不止一条信道, 则属于 out-band (带外) 攻击。与外部服务交互行为发生在一个 payload 提交到目标应用上, 导致目标

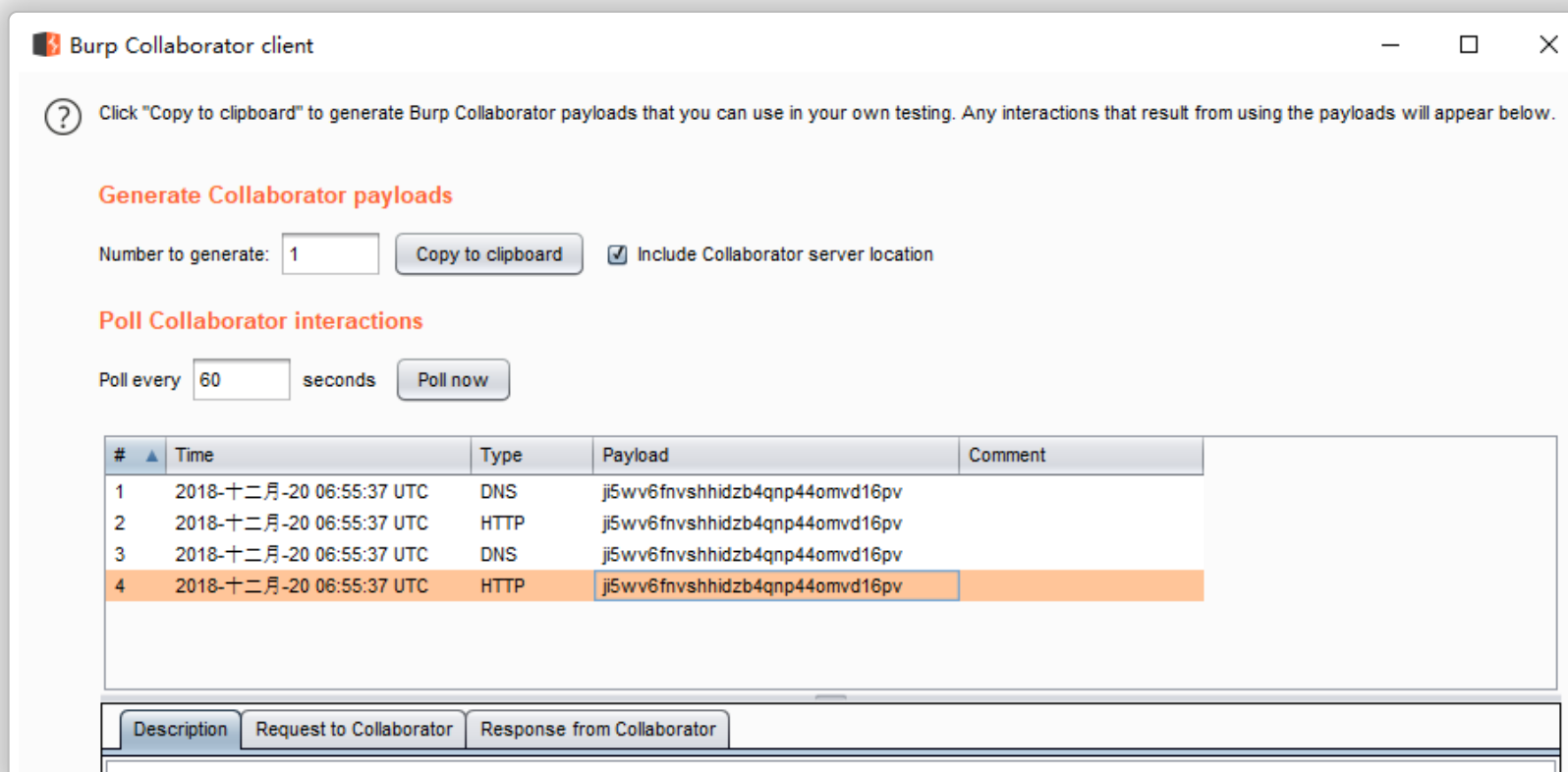
通过某个网络协议和一个外部的域名进行信息交互。和 ssrf 攻击类似, 让目标与 Collaborator 交互

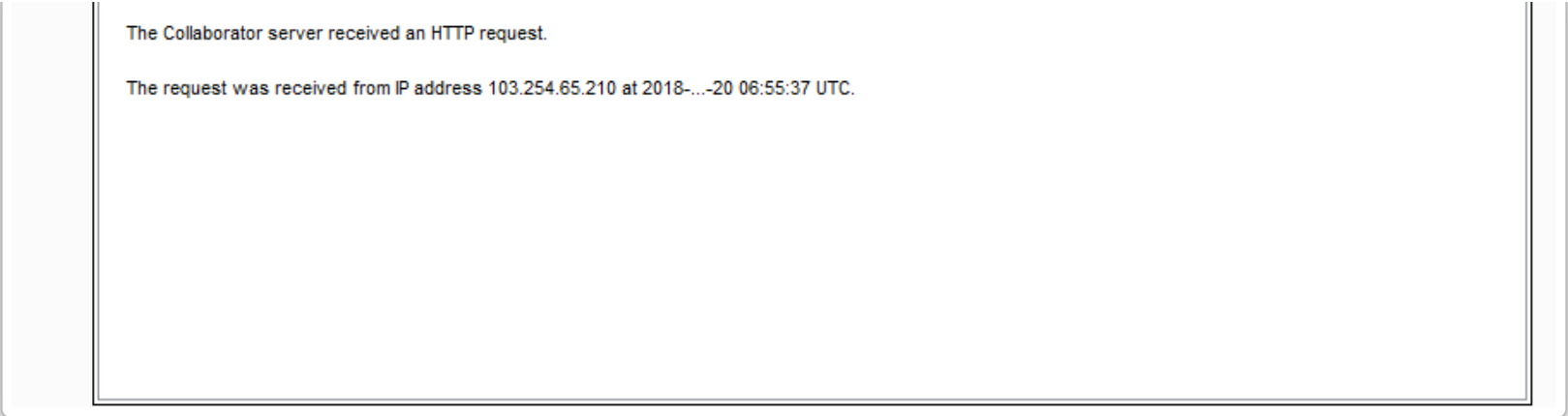
首先通过 project options - misc - burp collaborator server - run health check 检查信道是否通畅





启用 主界面菜单项 burp - burp collaborator client 即可启用
点击 Copy 头 clipboard , 添加到 payload 中





The Collaborator server received an HTTP request.

The request was received from IP address 103.254.65.210 at 2018-04-20 06:55:37 UTC.

带外信道根据不同场景一般用如下几类：

- burp 自带的 collaborator。主界面菜单项 burp - burp collaborator client 即可启用，可以在 project options - misc - burp collaborator server - run health check 检查信道是否通畅。无需第三方服务、不用注册，即开即用。由于我 burp 不离手，所以，这种带外信道方便、集成度高是它的最大优点，另外，burp 进行各类盲注（XXE、SQLi、CMDi 等等）的主动扫描时，也会用到 collaborator；

- 用脚本语言快速启用 web server。运行 `python3 -m http.server 8653` 或 `php -S 0.0.0.0:8088` 后，所有对它的 GET、HEAD 请求几类都能在日志中查看到。这种方式非常适用于攻击端与目标同在内网的场景，比如，无公网环境的 CTF 竞赛。不支持 POST 是它最大的短板；
- 借助第三方服务（<http://ceye.io/>、<http://requestbin.net/>）。效果上，类似第二种方式，但支持 DNS 查询、HTTP POST 方法，此外，由于这是长期有效的服务，所以，很适用于那些非实时触发的带外访问请求（如，二次 SQLi）。你可以隔两三天再去看有无访问记录。

全文完

本文由 简悦 SimpRead 优化，用以提升阅读体验。