简单Burp爆破使用方法

原创

Zeker62 于 2021-08-03 16:21:54 发布 378 收藏

分类专栏： 网络安全学习 文章标签： 安全 爆破

本文链接：https://blog.csdn.net/ZripenYe/article/details/119352315

网络安全学习 专栏收录该内容

134 篇文章 3 订阅

订阅专栏

burp的爆破就是强行暴力枚举对应的信息

这里用的是封神台的第二个靶场，本来适用于爆破的靶场在我做的时候不知道被哪个**删库了。

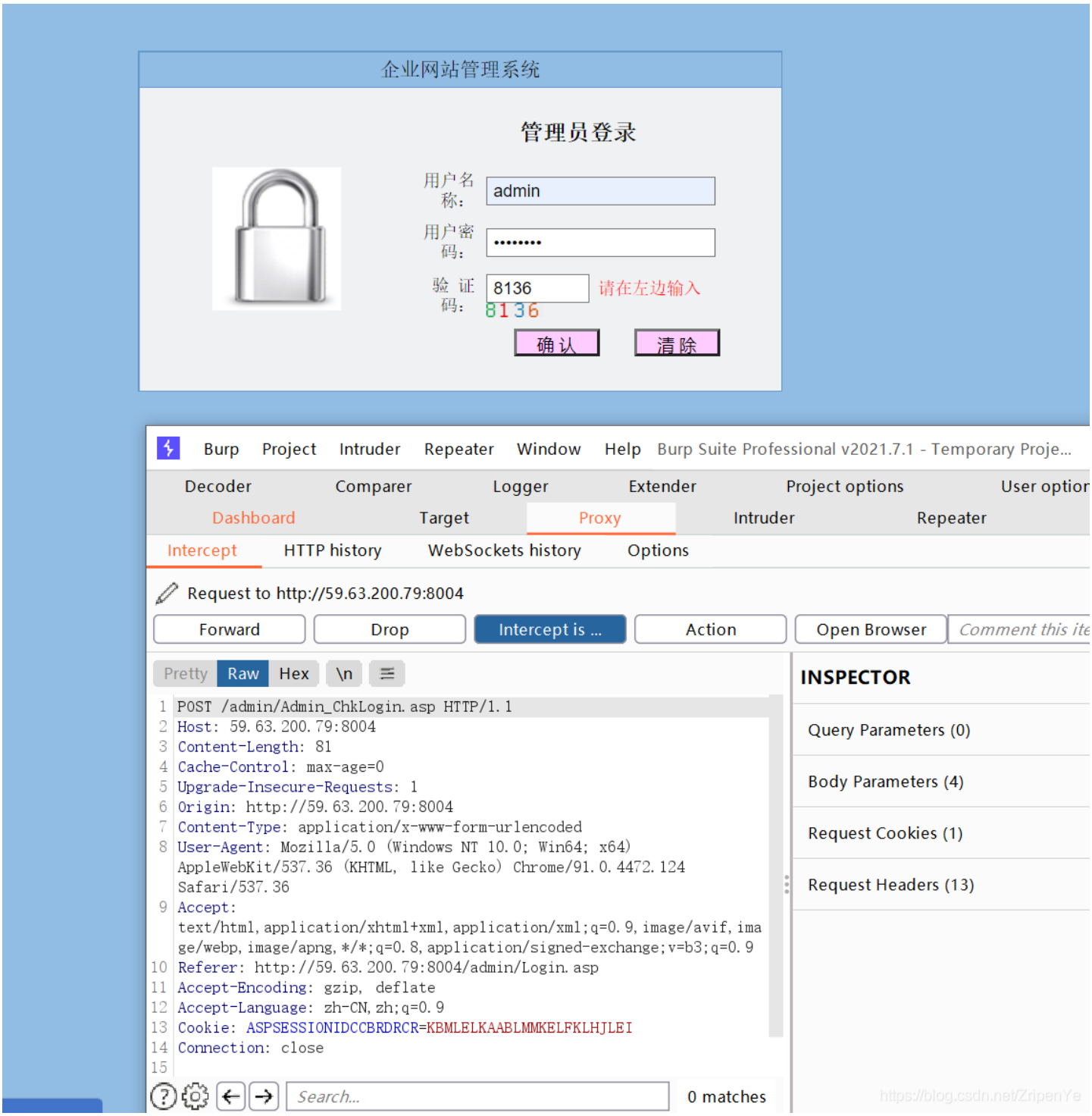
公共资源，合理利用

绕道了后台之后，出现管理员的账号密码

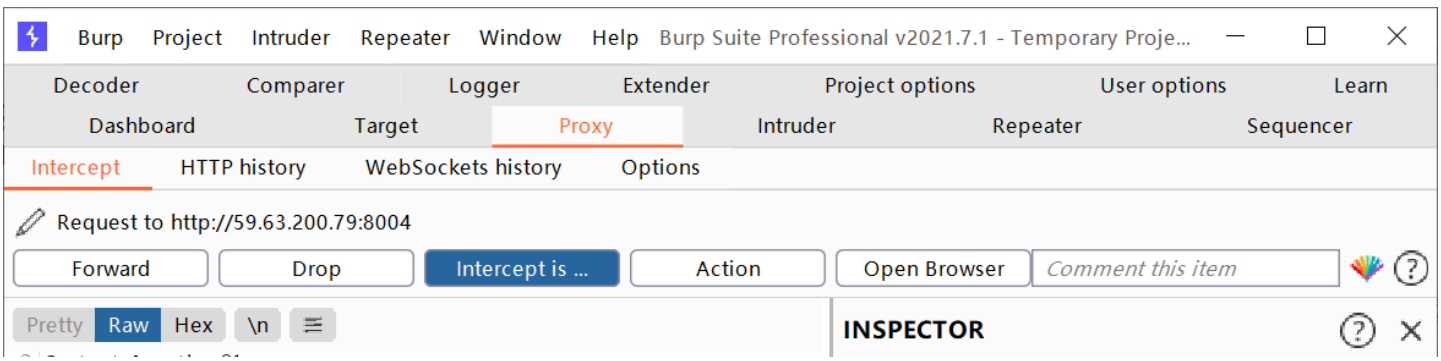
这个时候我们假装并不知道账号密码，所以进行暴力破解。

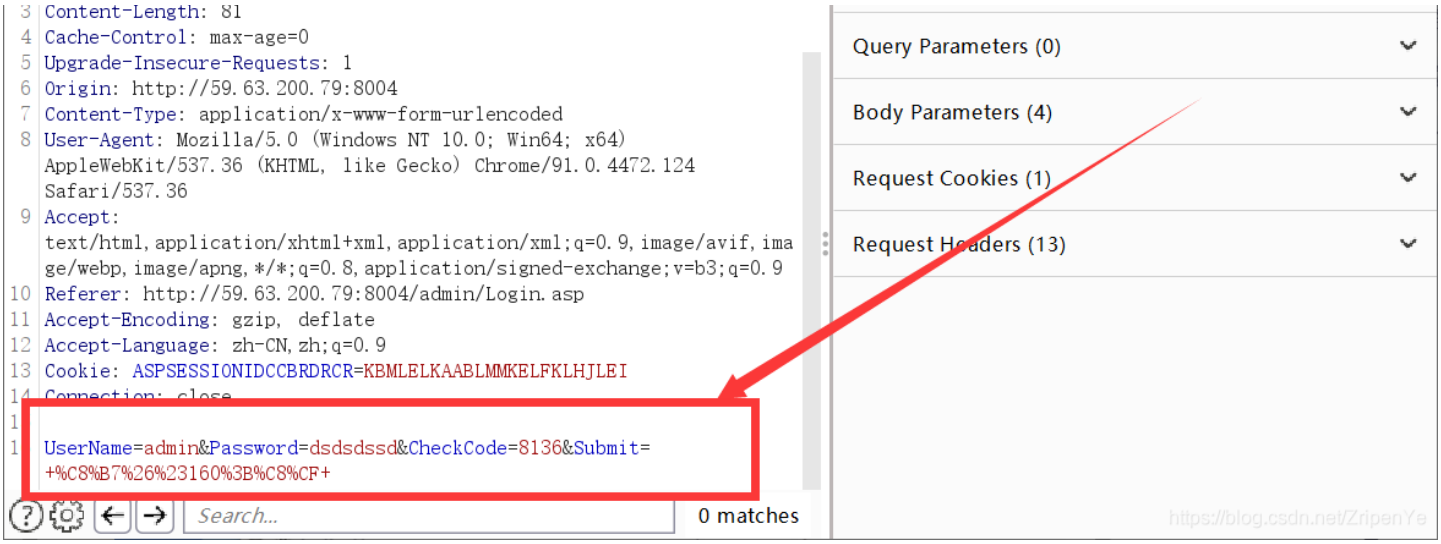
破解步骤

先随便输入账号密码，进行抓包



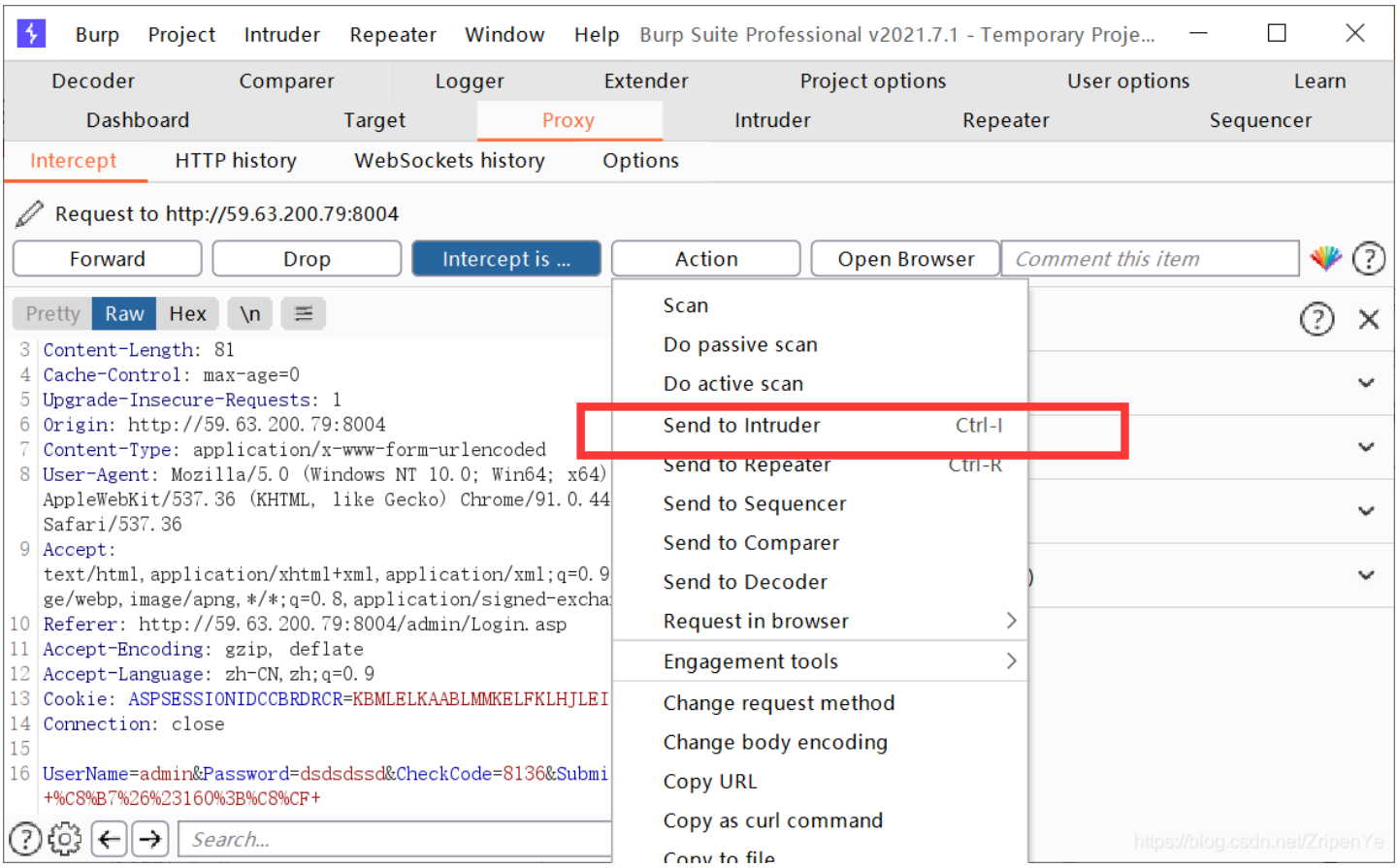
在包的下方有我们刚刚提交的信息



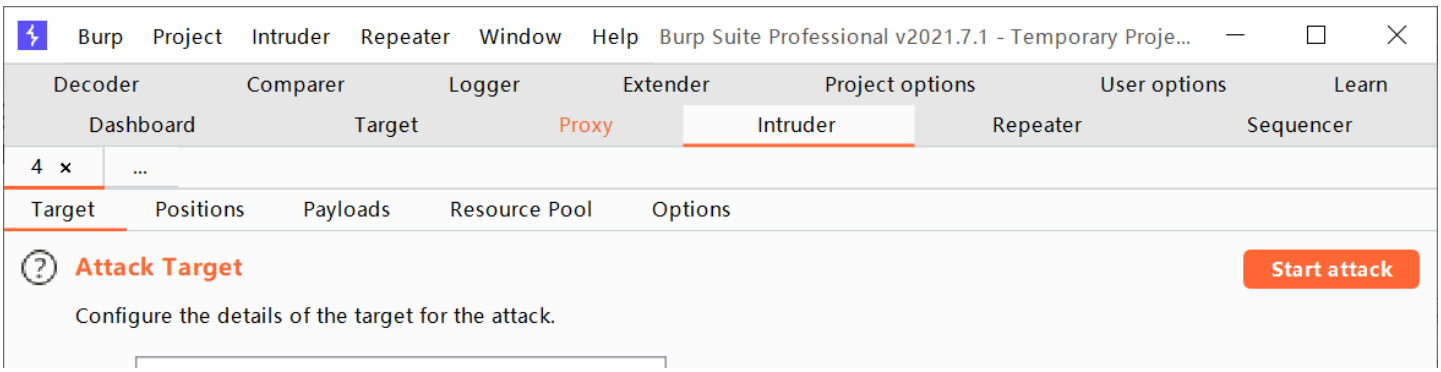


显而易见，账号密码的名称

启动攻击模式，进入这个模式，就可以进行暴力破解的尝试



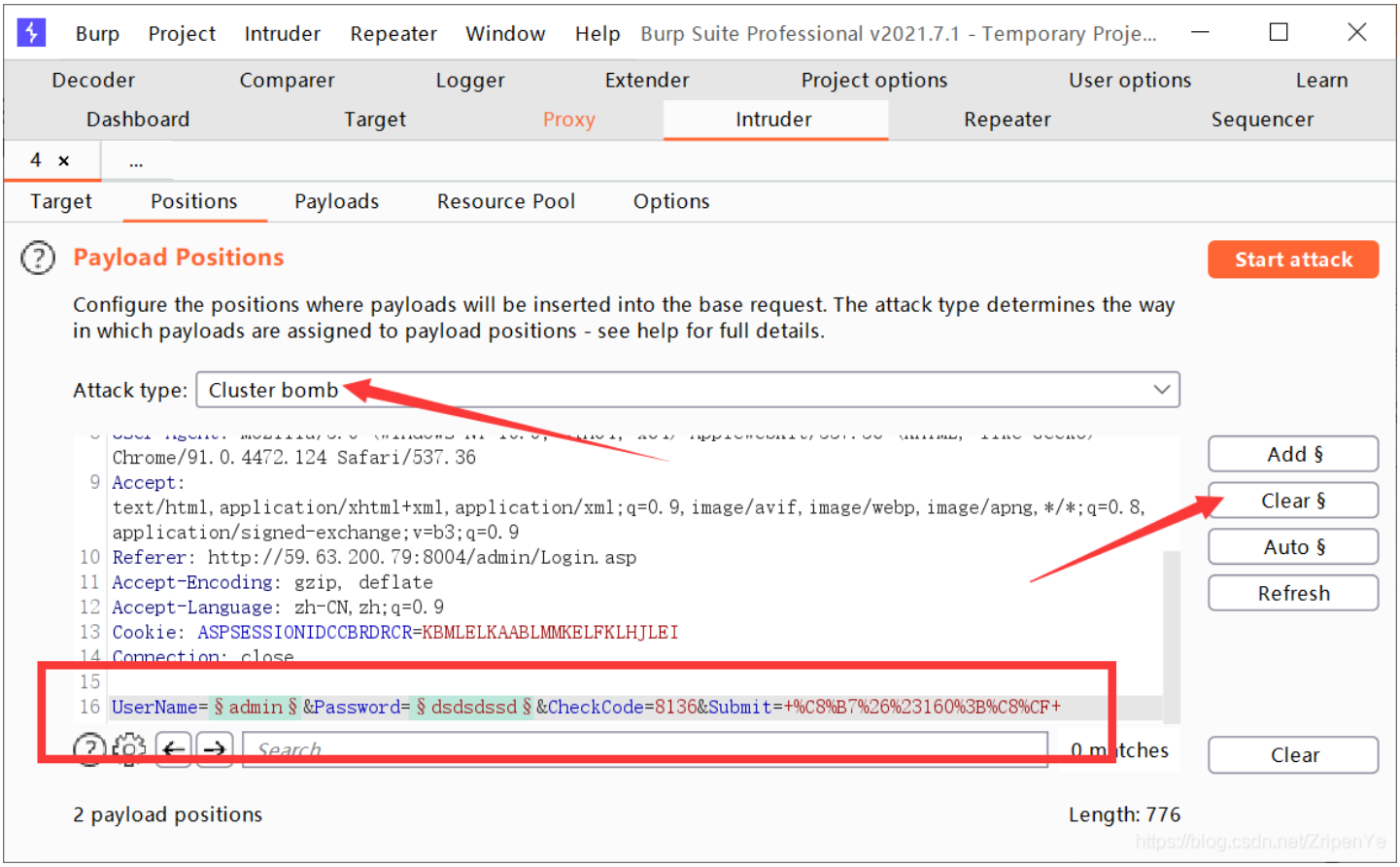
确定端口



使用分而治之的爆破模式

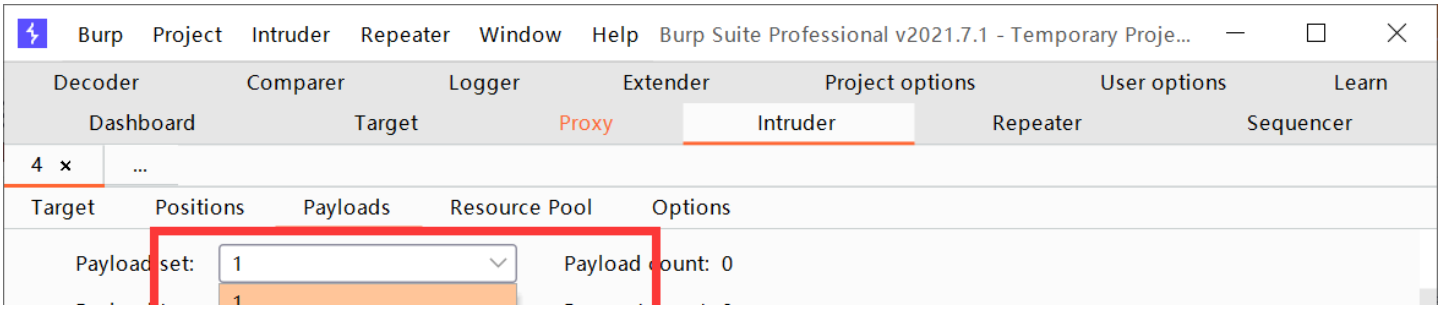
清除不必要的选项或者添加必要的选项

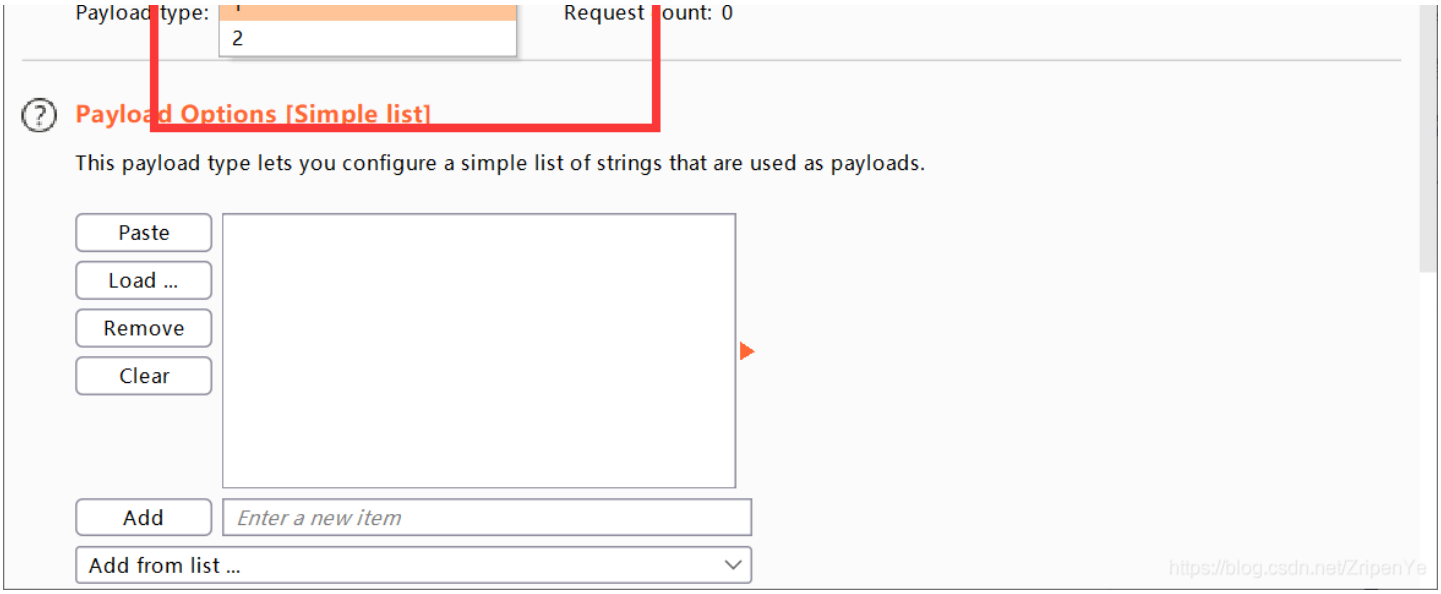
使用两个$中间元素都是我们要爆破的目标。



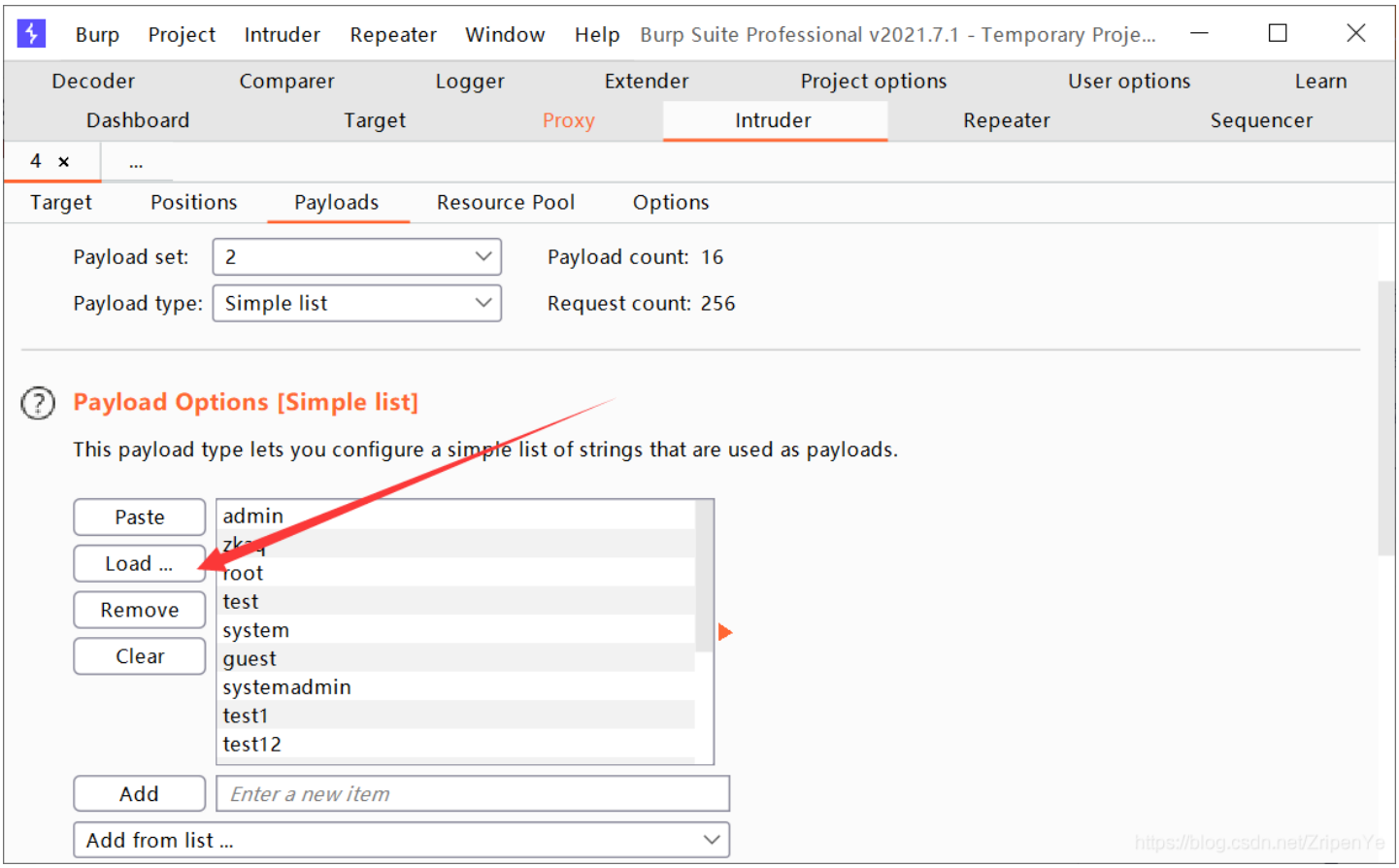
设置payload，添加字典

注意：1和2都要记得添加

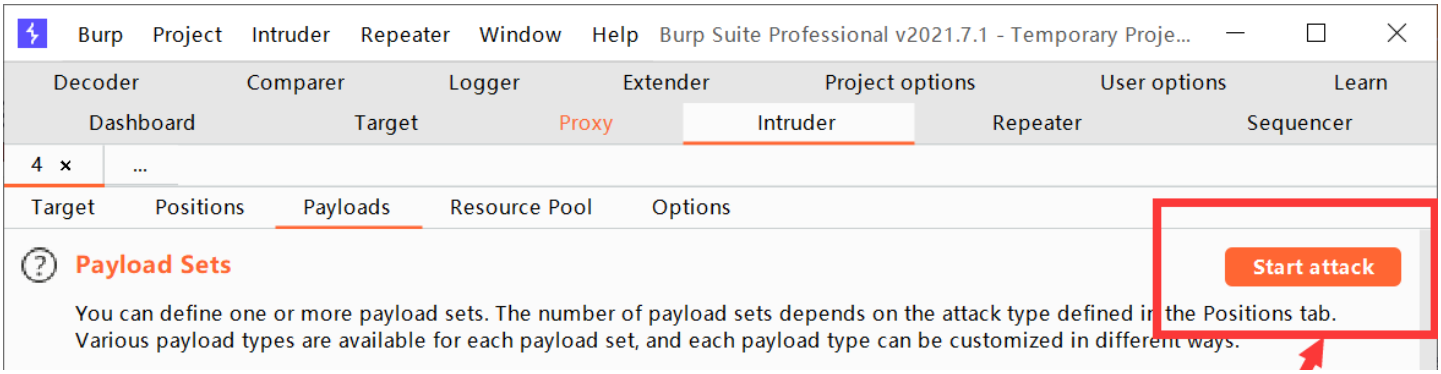


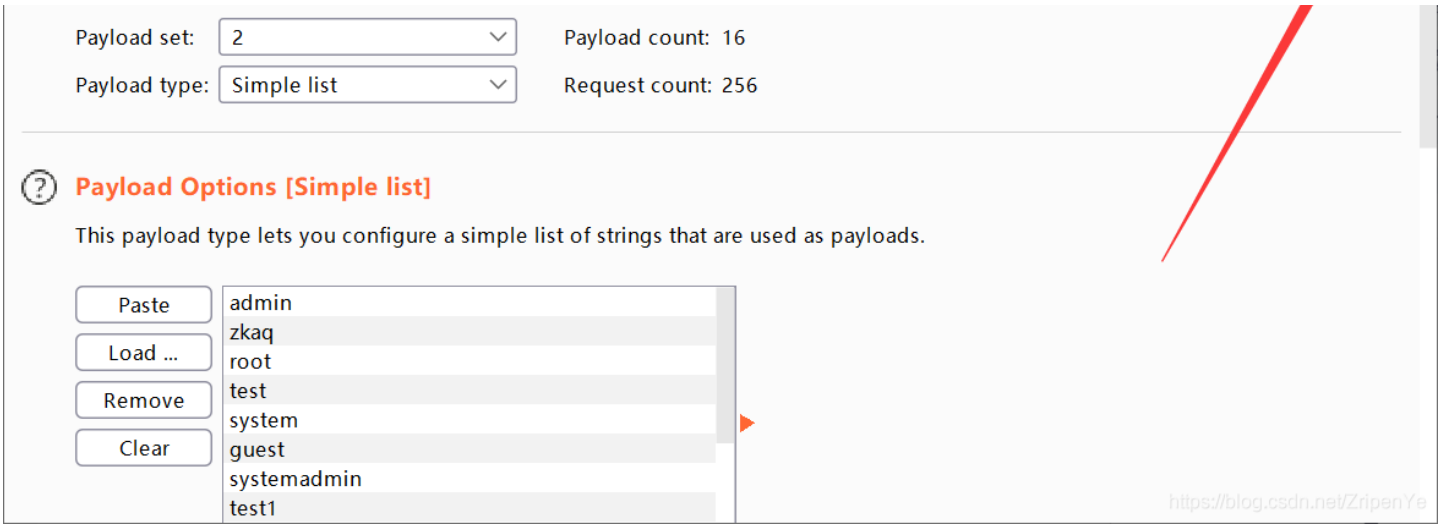


添加字典（txt格式）

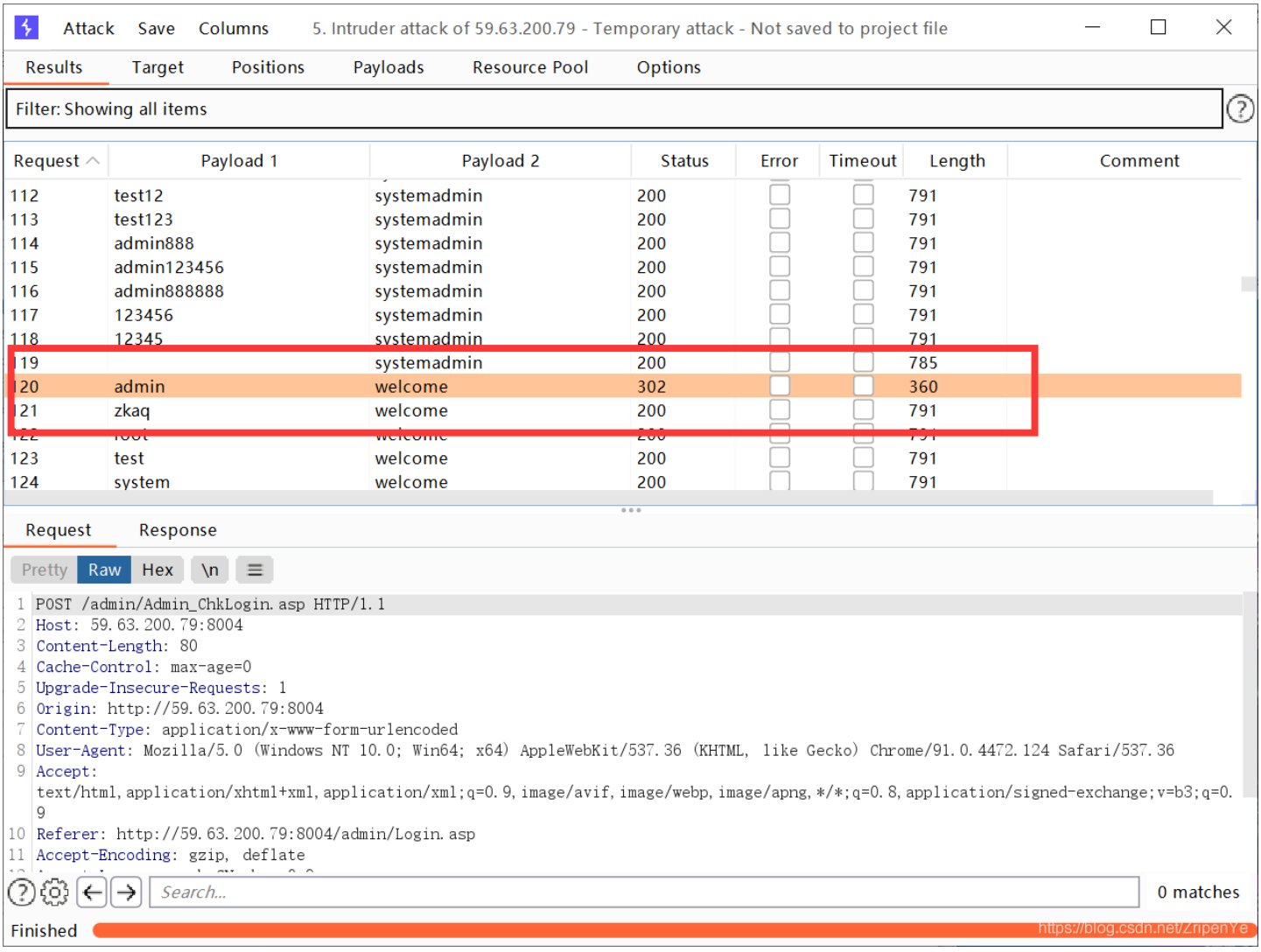


开始爆破

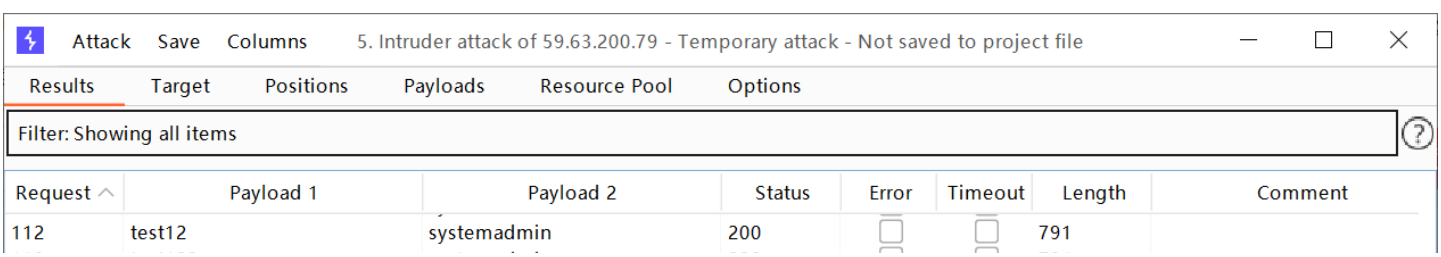


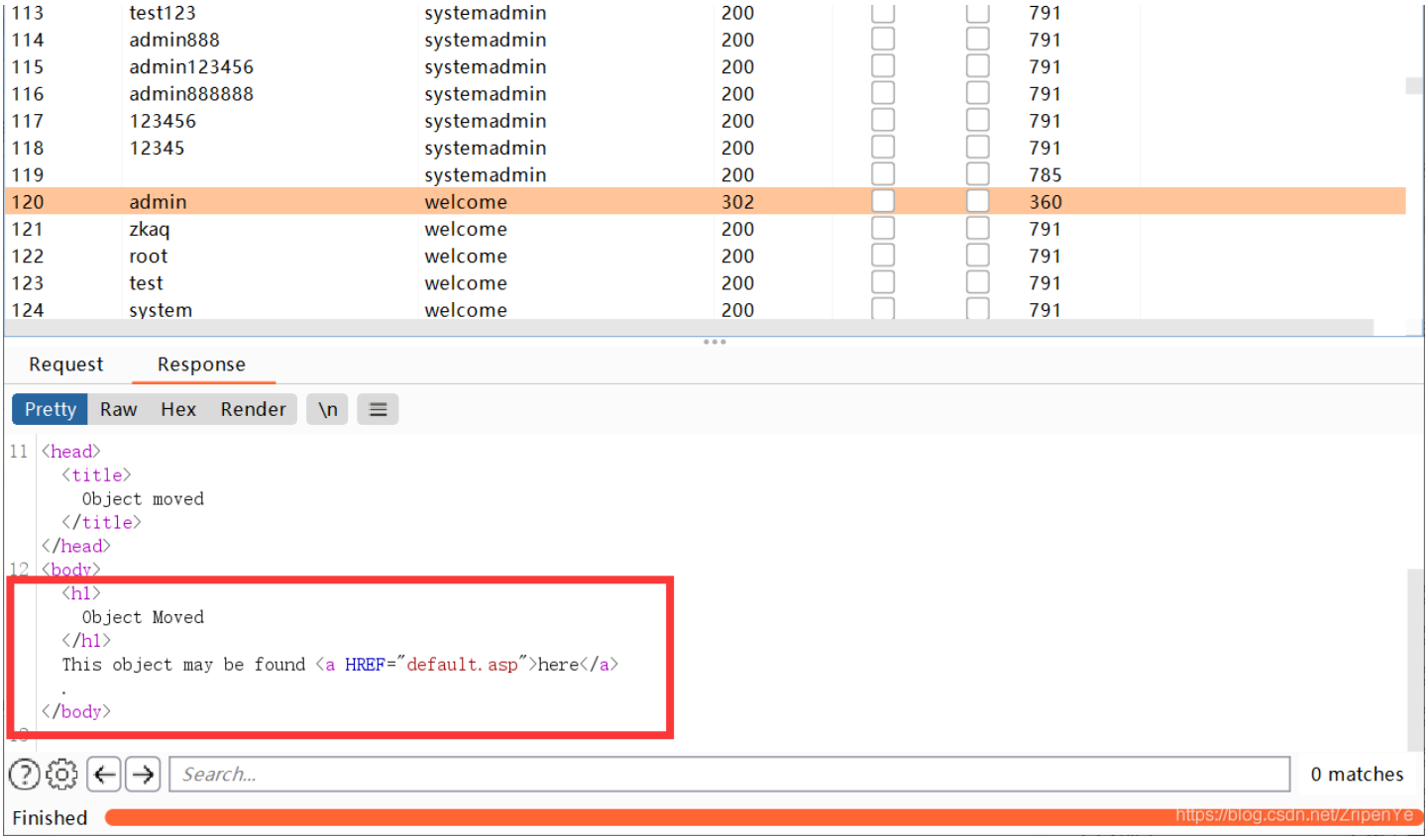


发现了什么不太一样的东西



观察响应





说明爆破成功。

最简单的爆破方法了，以后更新别的。