网络攻防平台网络安全实验

----------Burpsuite 网站密码破解

一、实验名称

- **名称：**
  Burpsuite 网站密码破解

二、实验目的

- **目的：**
  利用 burpsuite 破解某网站后台密码

三、实验工具

- **工具：**
  Burpsuite、firefox

三、实验基础知识

- **基础知识：**

  Burpsuite 功能很强大，主要用于 web 渗透方面。

  BurpSuite 是用于攻击 web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。所有的工具都共享一个能处理并显示 HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。

  利用 Burp suite 破解网站后台密码就是暴力破解，利用用户名和密码的组合去无数次的尝试。

- **知识拓展：**

  Burpsuite 工具箱：

  Proxy----是一个拦截 HTTP/S 的代理服务器，作为一个在浏览器和目标应用程序之间的中间人，允许你拦截，查看，修改在两个方向上的原始数据流。

  Spider----是一个应用智能感应的网络爬虫，它能完整的枚举应用程序的内容和功能。

  Scanner[仅限专业版]——是一个高级的工具，执行后，它能自动地发现 web 应用程序的安全漏洞。

  Intruder----是一个定制的高度可配置的工具，对 web 应用程序进行自动化攻击，如：枚举标识符，收集有用的数据，以及使用 fuzzing 技术探测常规漏洞。

  Repeater----是一个靠手动操作来补发单独的 HTTP 请求，并分析应用程序响应的工具。

  Sequencer——是一个用来分析那些不可预知的应用程序会话令牌和重要数据项的随机性的工具。

  Decoder----是一个进行手动执行或对应用程序数据者智能解码编码的工具。

  Comparer----是一个实用的工具，通常是通过一些相关的请求和响应得到两项数据的一个

可视化的“差异”。

➢ **注意事项：**

在输入密码登录时开启代理 burpsuite 抓取登录信息。

四、实验步骤

➢ **实验地址：**

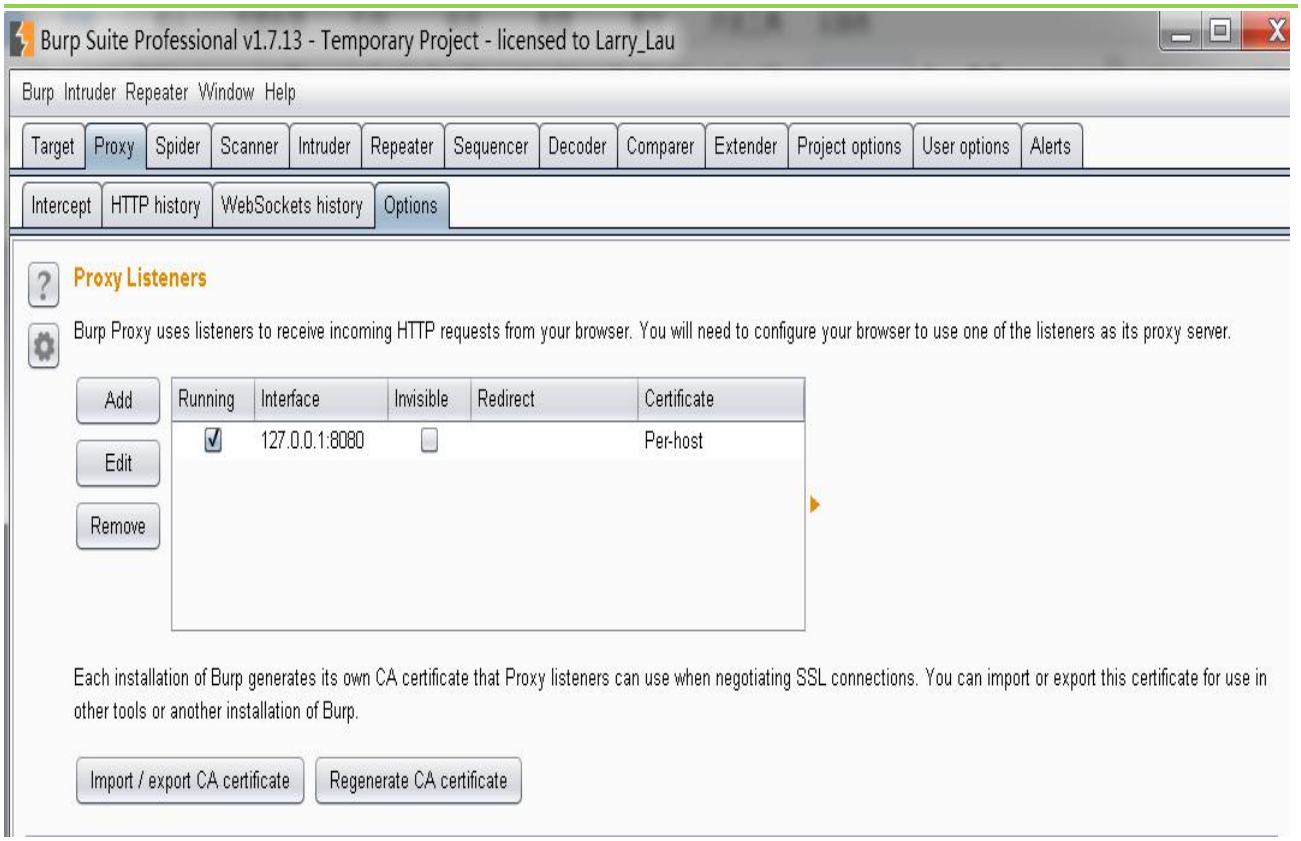
www.example.com

➢ **实验：**

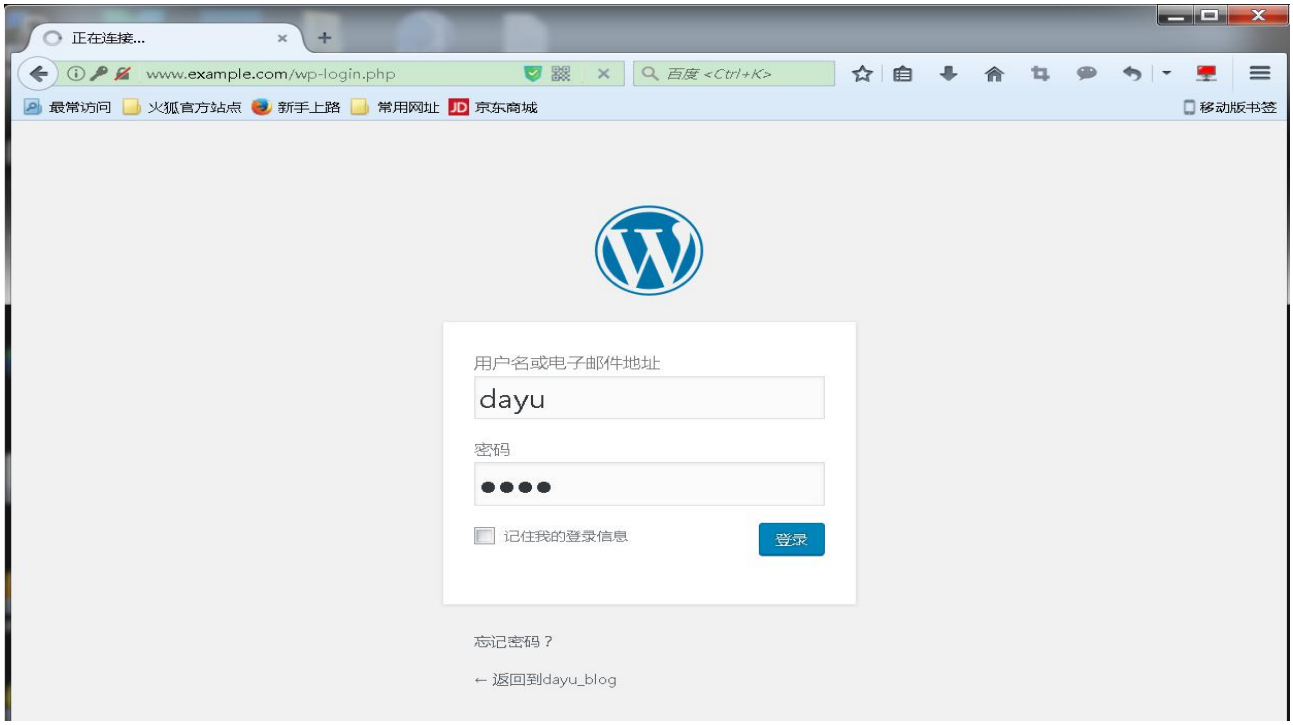
1.1 开启代理，启动 Burpsuite

打开 firefox，点击【工具】--->【选项】--->【高级】--->【网络】--->【设置】，手动配置代理，IP 地址为【127.0.0.1】端口号为【8080】

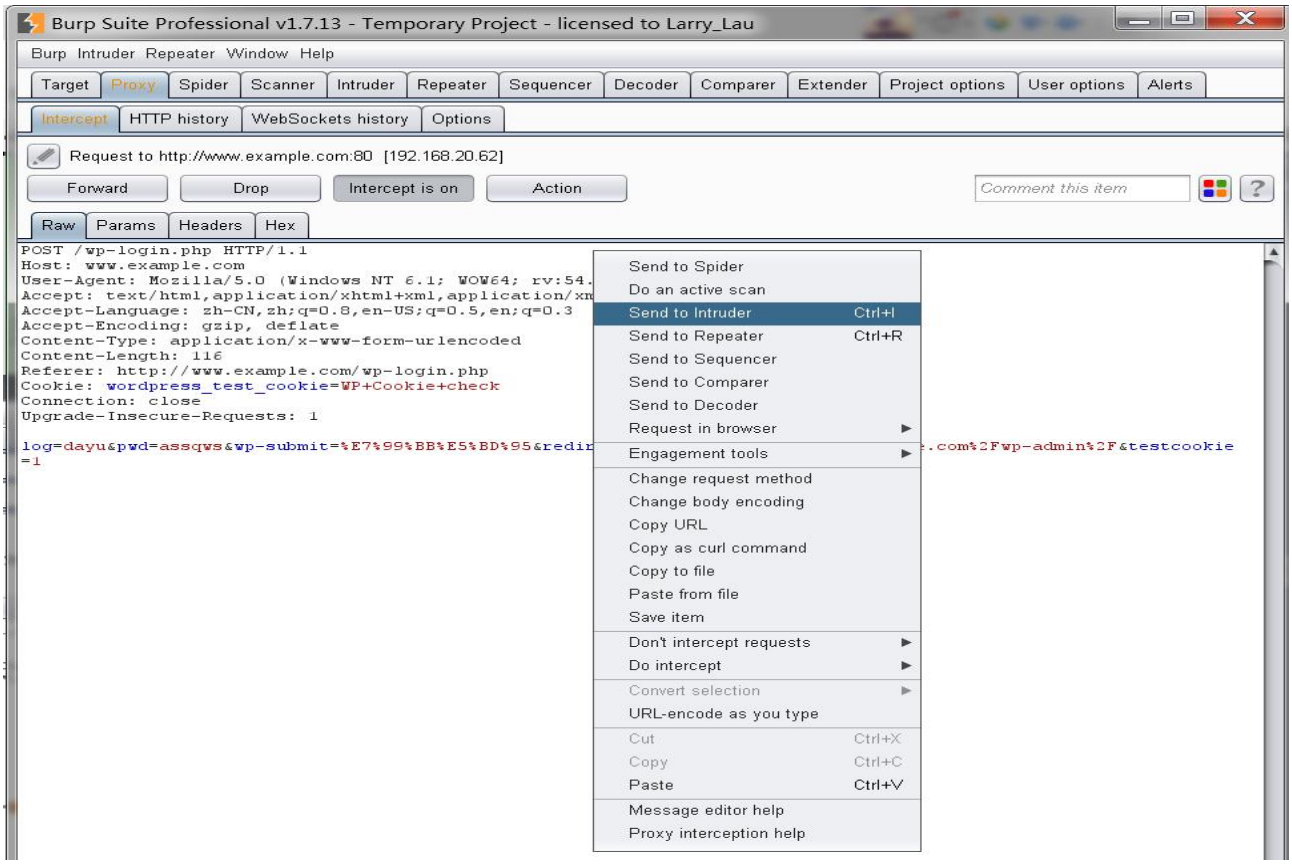
1.2 打开 burpsuite 点击【proxy】-->【options】开启代理



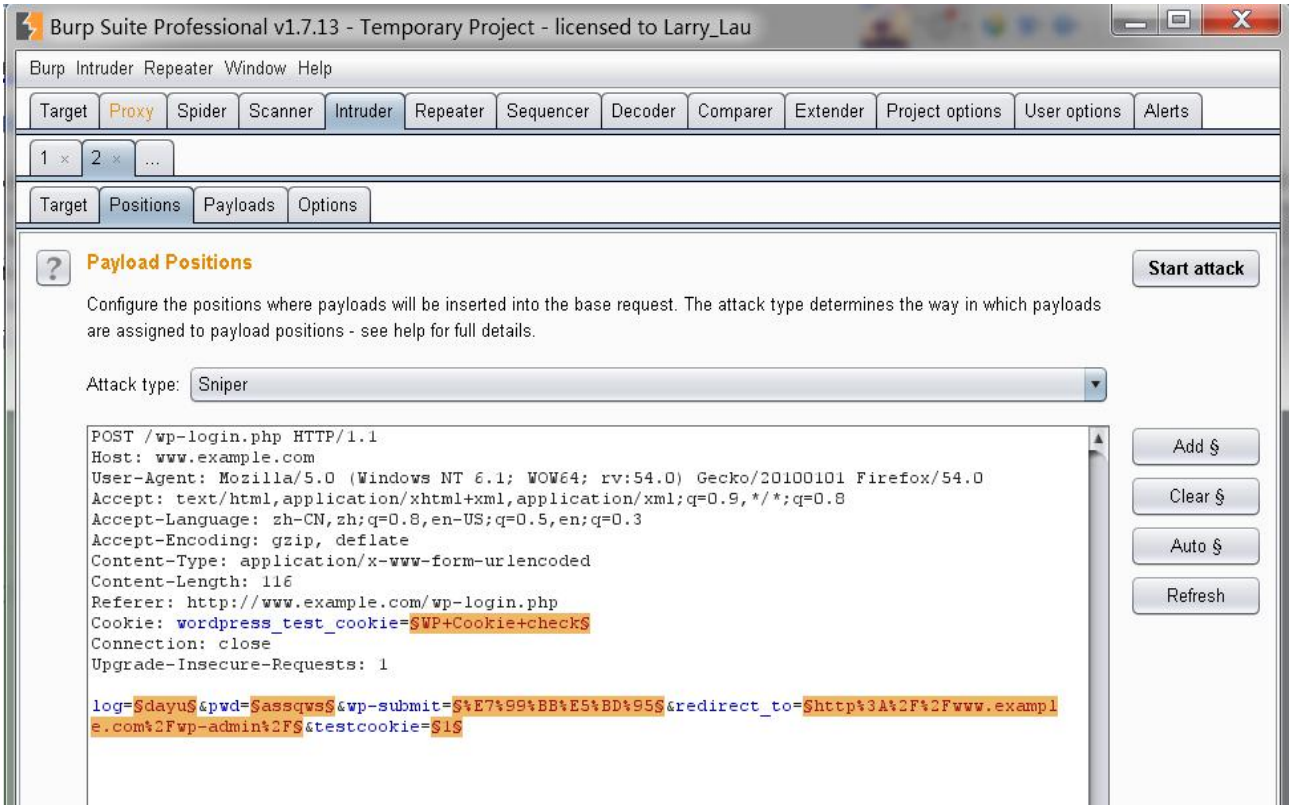
1.3 打开 firefox 代理输入地址 http://example.com 登录 wordpress 博客系统，输入错误密码登录。



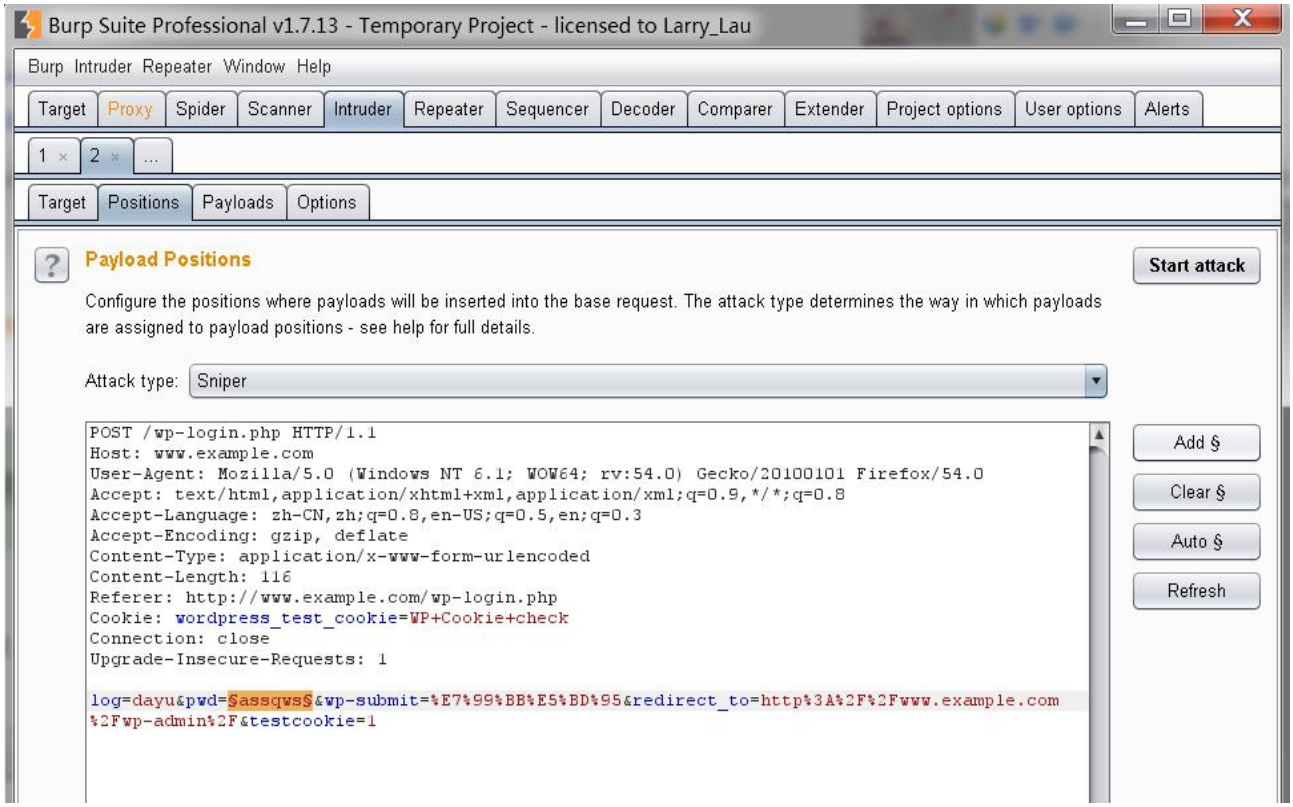
1.4【proxy】-->【intercept】-->【intercept is on】-->【raw】查看抓包内容，鼠标右键选择【send to intruder】。



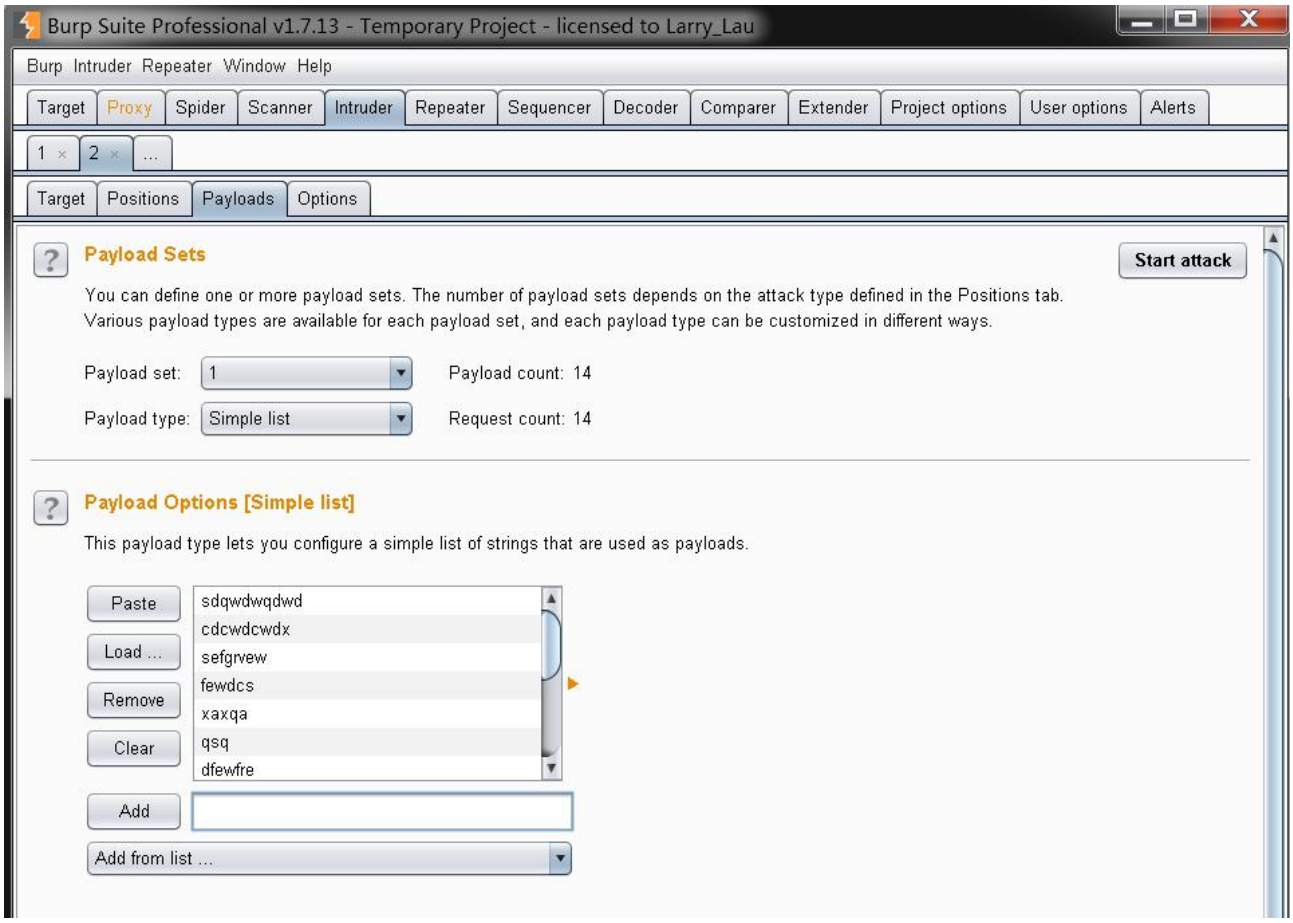
1.5 【intruder】-->【positions】列出了关键字段，右侧点击 clear 擦除标注。



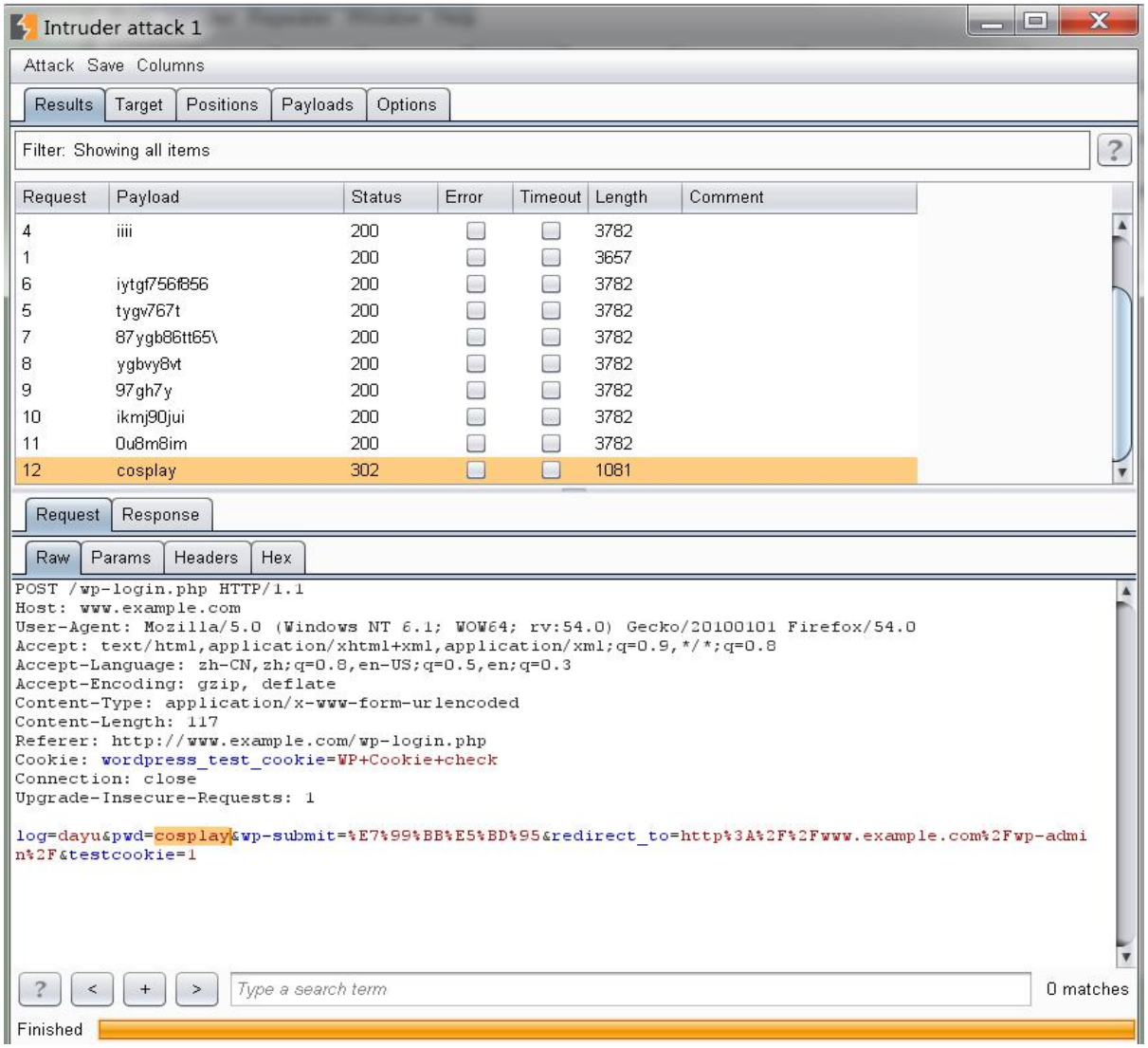
1.6 重新鼠标双击选择需要爆破的字段点击右侧【add】添加。



1.7【intruder】-->【payloads】添加字典，点击右上角 start attack 开始爆破。



1.8 爆破完毕，查看密码。【status：（302 说明页面跳转）】、【error（没有返回错误）】、【timeout（没有超时）】、【length（返回长度与其他不一样）】，又上几点可以确定 wordpress 的密码就是“cosplay”。



五、实验结论

- **结论：**

  利用 burpsuite，黑客可以在不需要知道网站用户密码的情况下即可登录网站，进行一些非法操作。

- **漏洞修复：**

  设置高难度密码。