**江苏科技大学**

**课 设 报 告**

课 程： 渗透扫描与测试课程设计

课 题： Burp Intruder暴力攻击

学 院： 计算机学院

专 业： 信息安全

学 号： 182210710119

姓 名： 陈四贵

指导老师： 刘噶琼

设计时间： 2021-11-15至2021-11-19

# 实践目的

1.掌握渗透测试的工作流程，能对所需测试的类型，制定工作方案。

2.理解渗透测试各环节的工作原理和实施目的。

3.了解渗透测试相关法律法规，做到依法依规工作。

4.熟练掌握渗透测试各种工具软件的使用方法。

5.掌握主机加固和网络加固的基本方法。

6.对未来自己的职业生涯有个比较清晰的规划。

# 实践内容

1.利用Burp Suite进行请求的拦截和修改,扫描web应用程序漏洞，以暴力破解登录表单，执行会话令牌等多种的随机性检查。

2.做一个Burp Suite完全的演练，进行暴力破解，破解登陆密码。

3.尝试使用以下模块：代理、Spider、Scanner(扫描器)、Intruder(入侵)、epeater(中继器)、Sequencer、Decoder(解码)、Comparer

# 实践工具及实践原理

1.关于实践工具：Burp Suite 是用于攻击web 应用程序的集成平台，包含了许多工具。Burp Suite为这些工具设计了许多接口，以加快攻击应用程序的过程。所有工具都共享一个请求，并能处理对应的HTTP 消息、持久性、认证、代理、日志、警报。

◎Proxy——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——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]——高级工具，执行后，它能自动地发现web 应用程序的安全漏洞。

◎Intruder——高度可配置工具，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——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——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——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——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”。

2.关于实践原理：本次课程设计主要聚焦于对一个具体网站的暴力破解，通过Burp suite从多个技术维度深度剖析网站可能存在的漏洞，并最终成功爆破登录账号与密码。

3.涉及的相关知识：

①现代网络通信采用TCP/IP协议，在访问web服务器的过程中，通常是客户端发送请求报文-服务端发送响应报文。Burp Suite正是利用了这点，通过Proxy模块开启代理后，利用代理的原理（代理服务器，也称网络代理，是一种特殊的网络服务，允许一个网络终端（一般为客户端）通过这个服务与另一个网络终端进行非直接的连接）截获通信报文，并可就此修改，以达到暴力破解或中间人攻击的目的。

②爬虫时通过模拟浏览器行为爬取信息的程序，由于其能通过相关算法获取有用的信息，我们可以使用爬虫获取有用的信息，如登录表单的executeid和token等常见参数，以及一些加密算法。

# 实验步骤及运行结果

①搭建简易登录测试平台，设有参数username、password、token。其中username与password为用户输入；token为服务器端自动返回的数据，需动态更新。

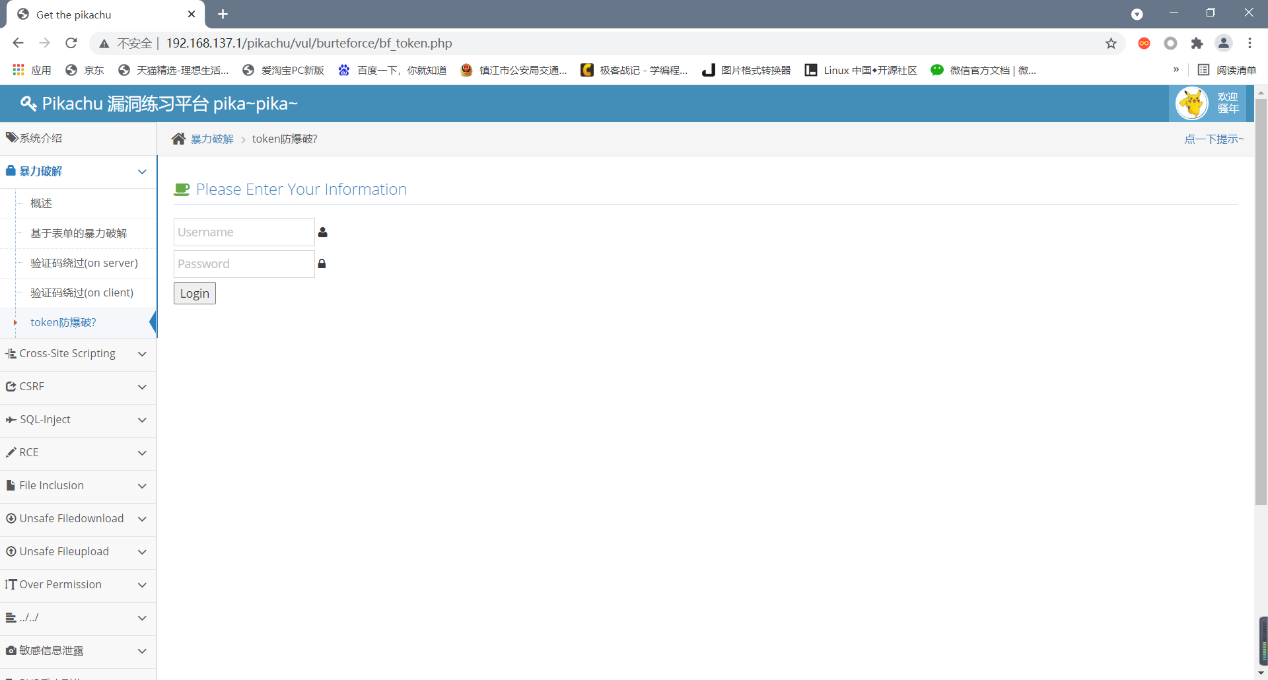


图1-1简易登录测试平台界面

②开启代理，设置代理为127.0.0.1:8080端口。其中，127.0.0.1是环路地址，这意味着将本机作为代理（相当于将本机作为代理。如果设置后不开启代理服务器，则无法正常访问网络）；8080端口常用于WWW代理服务，可以实现网页浏览。

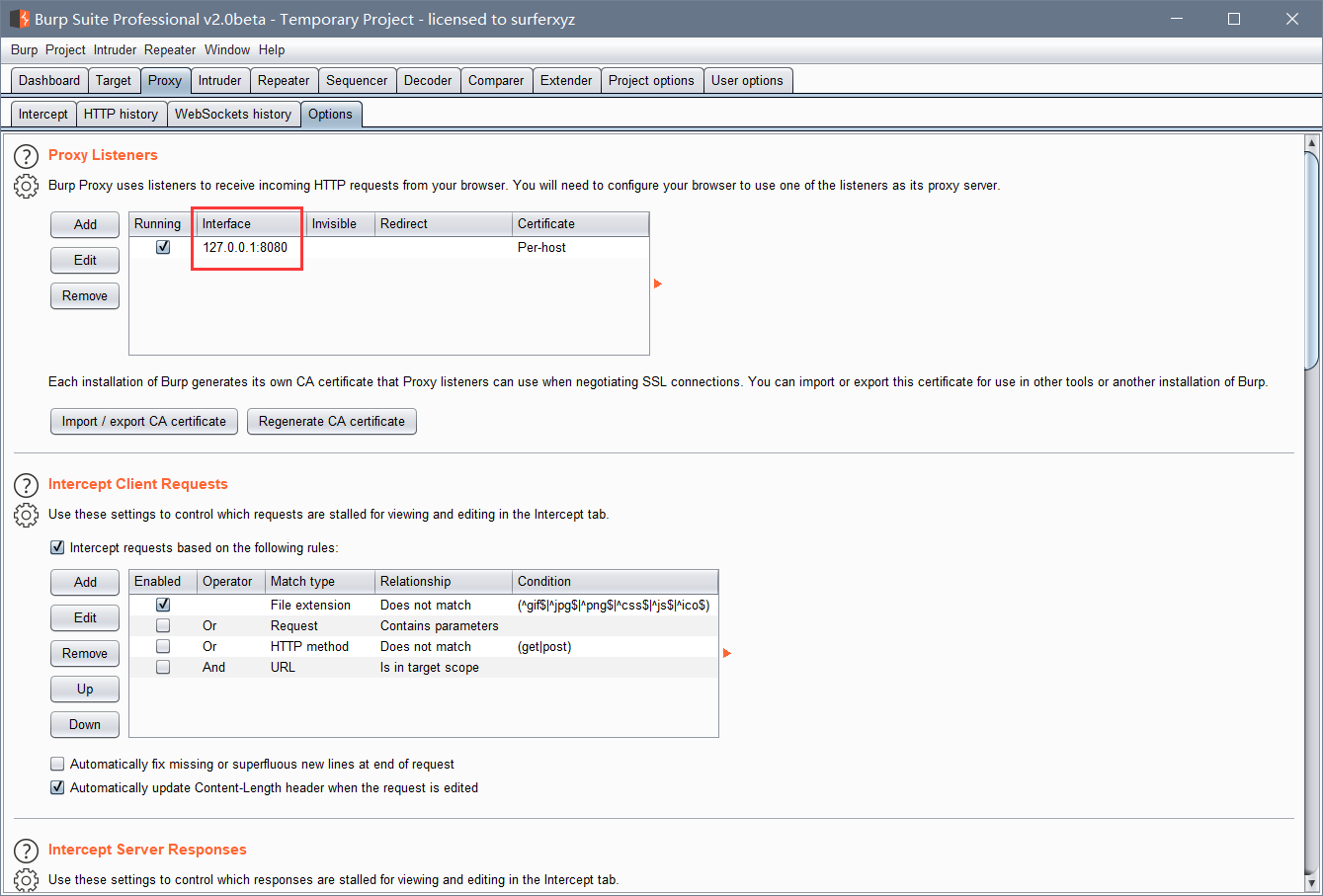


图2-1 设置代理地址

③任意输入用户名和密码后提交表单。由于数据包经由代理服务器转发，我们可以在Proxy模块的Raw（原生的）选项中查看经过的数据包，并由此判断目标服务器基本类型，挖掘可能出现的漏洞。

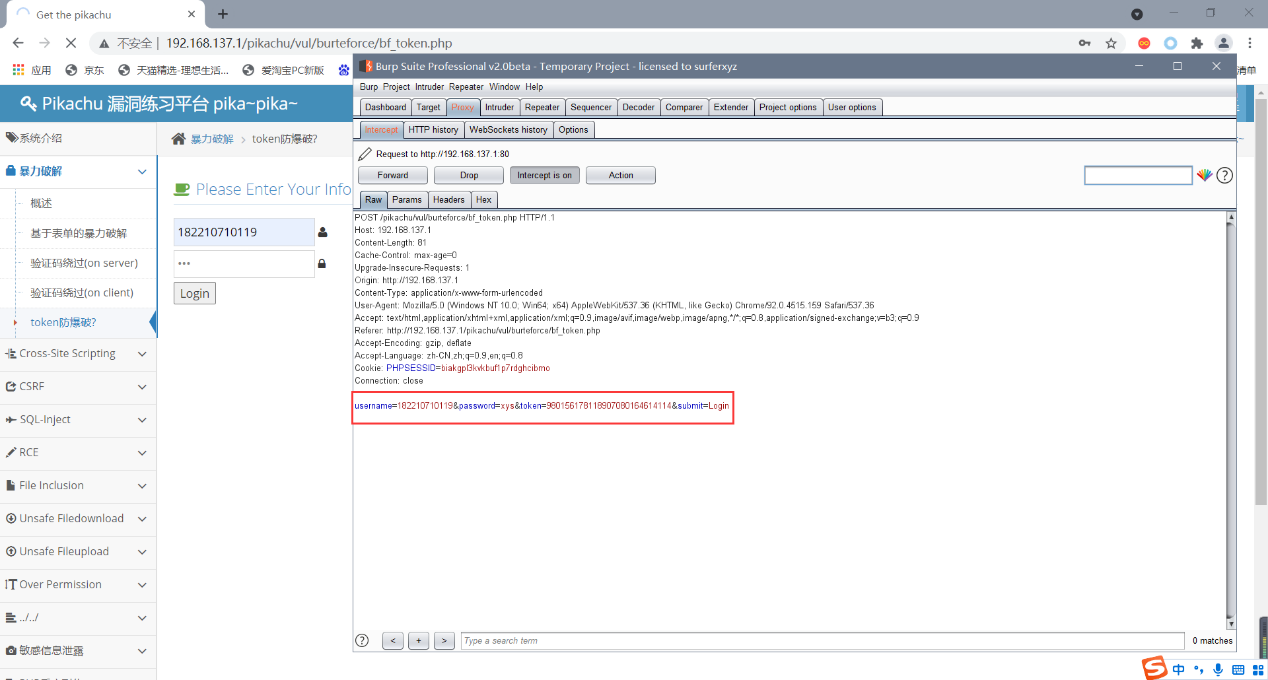


图3-1 监控到的原生数据包

由此我们可以判断出：目标IP地址为192.168.137.1，登录提交参数有username、password、token以及submit。经由常识知，token 是在服务端产生的，前端在每次请求时需带上 token 以证明自己的合法地位。由此我们在爆破时需注意token问题。

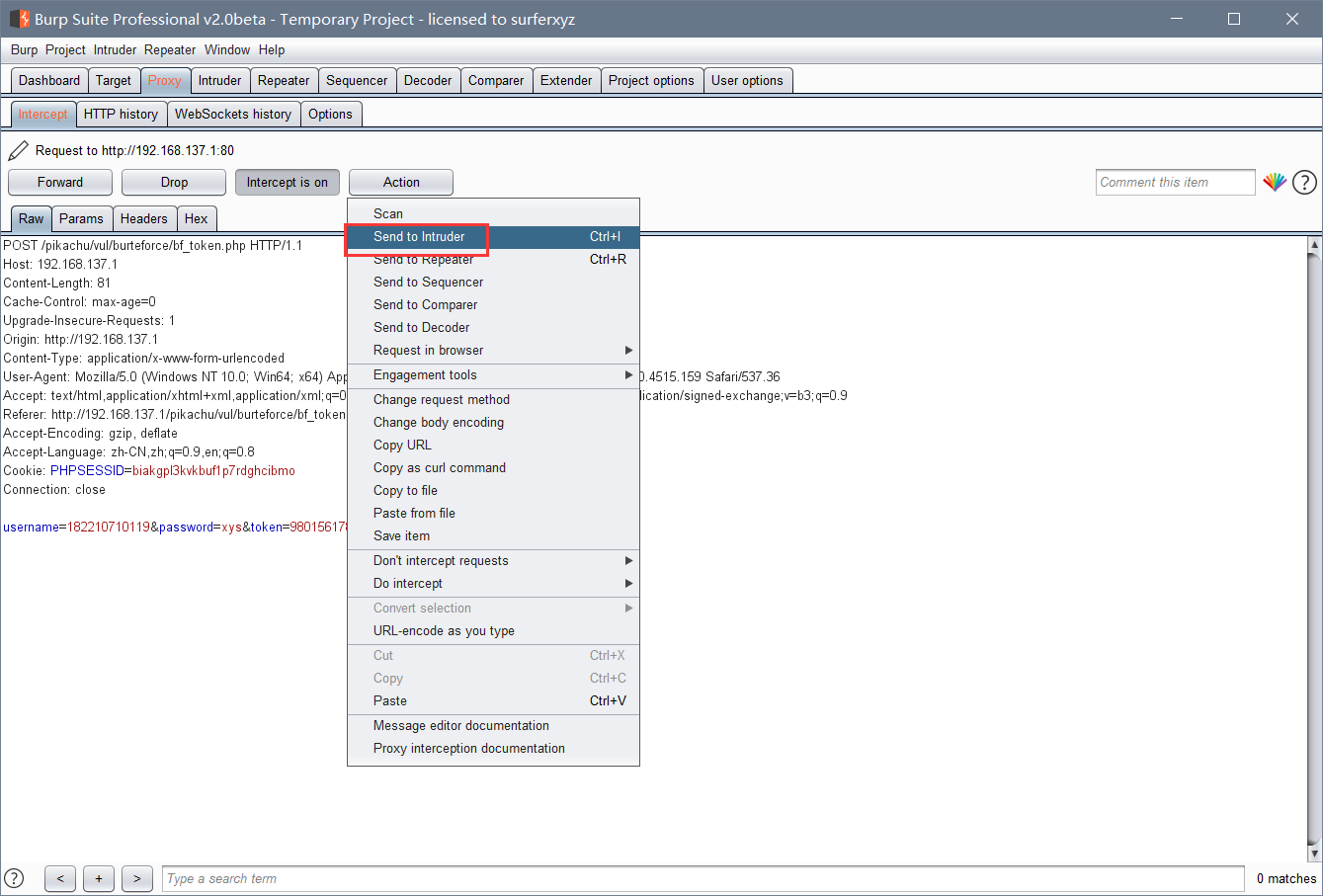


图3-2 操作示意图，将其Send to Intruder（入侵）或Send to Repeater（中继器）

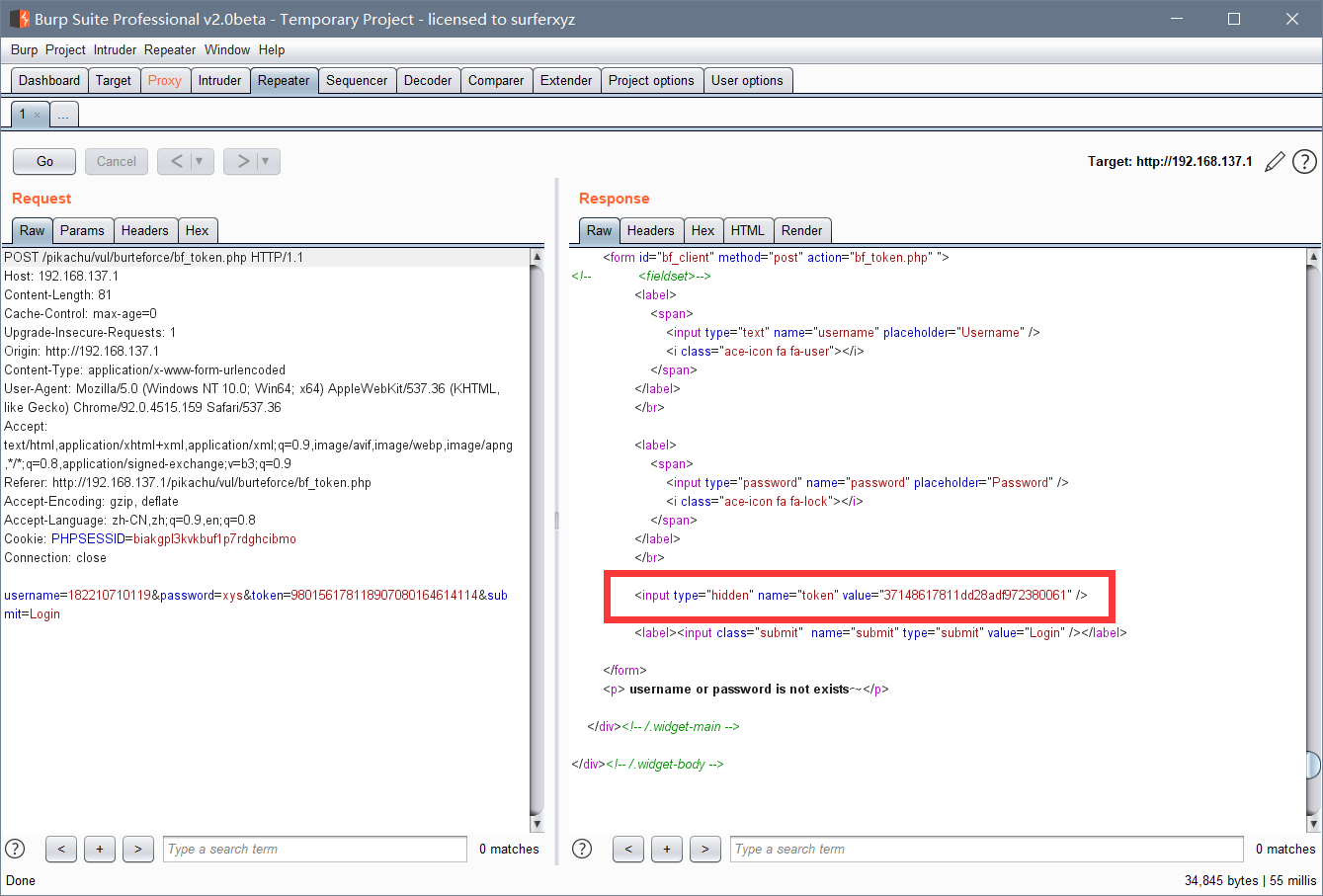


图3-3 使用Reapter功能查看经由的数据包

据此可以看出，提交参数中的token初始值是静态的，内嵌自html的Input标签，由于其属性为hidden，我们无法在登录界面中看见该输入框。

④使用Intruder模块进行爆破（暴力破解）。

点击Clear，清除相关符号（submit参数无需爆破）

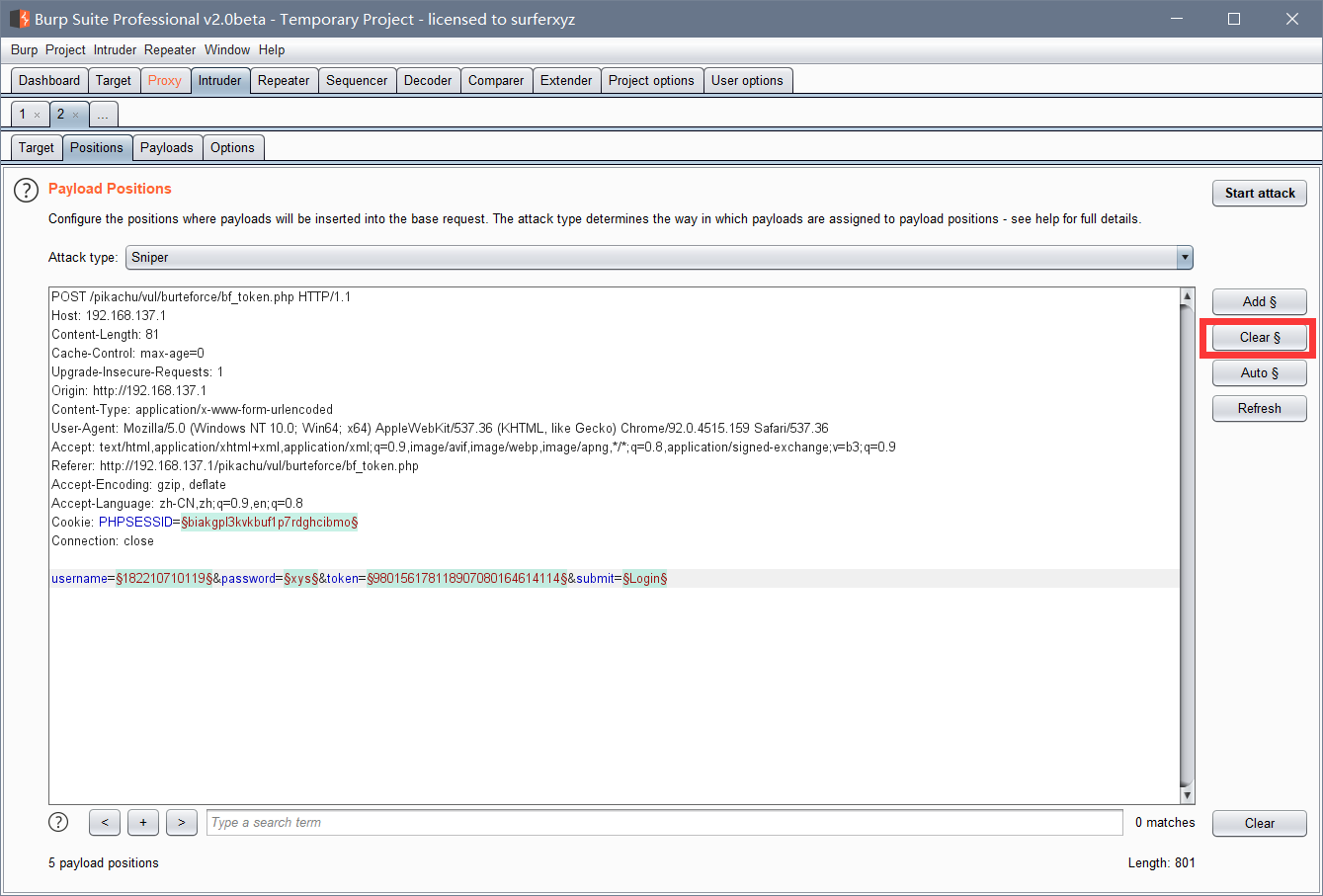


图4-1 演示图

点击Add，对username、password以及token等需要爆破的参数添加相应符号

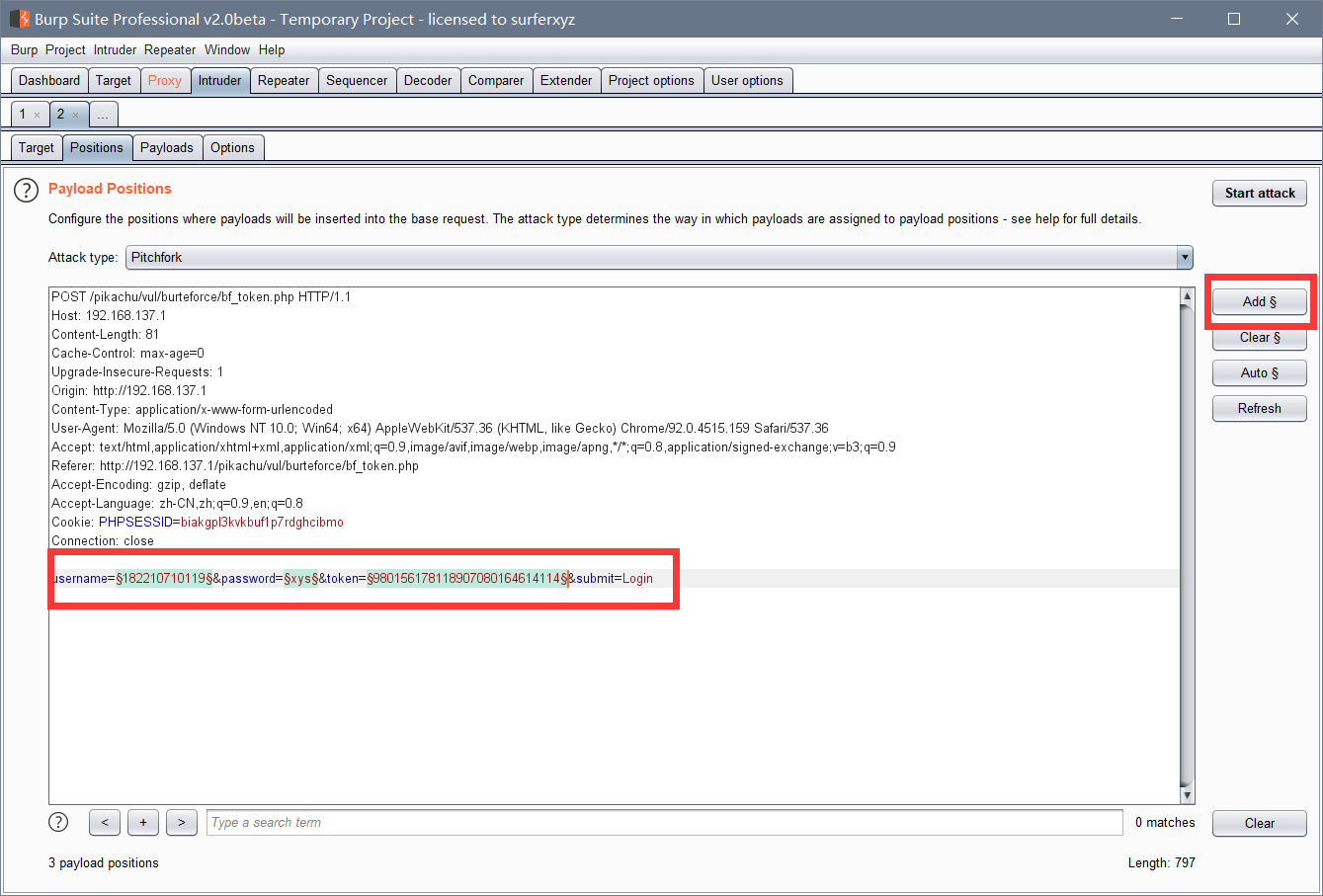


图4-2 演示图

在Payloads选项中添加爆破用的用户名、密码字典。

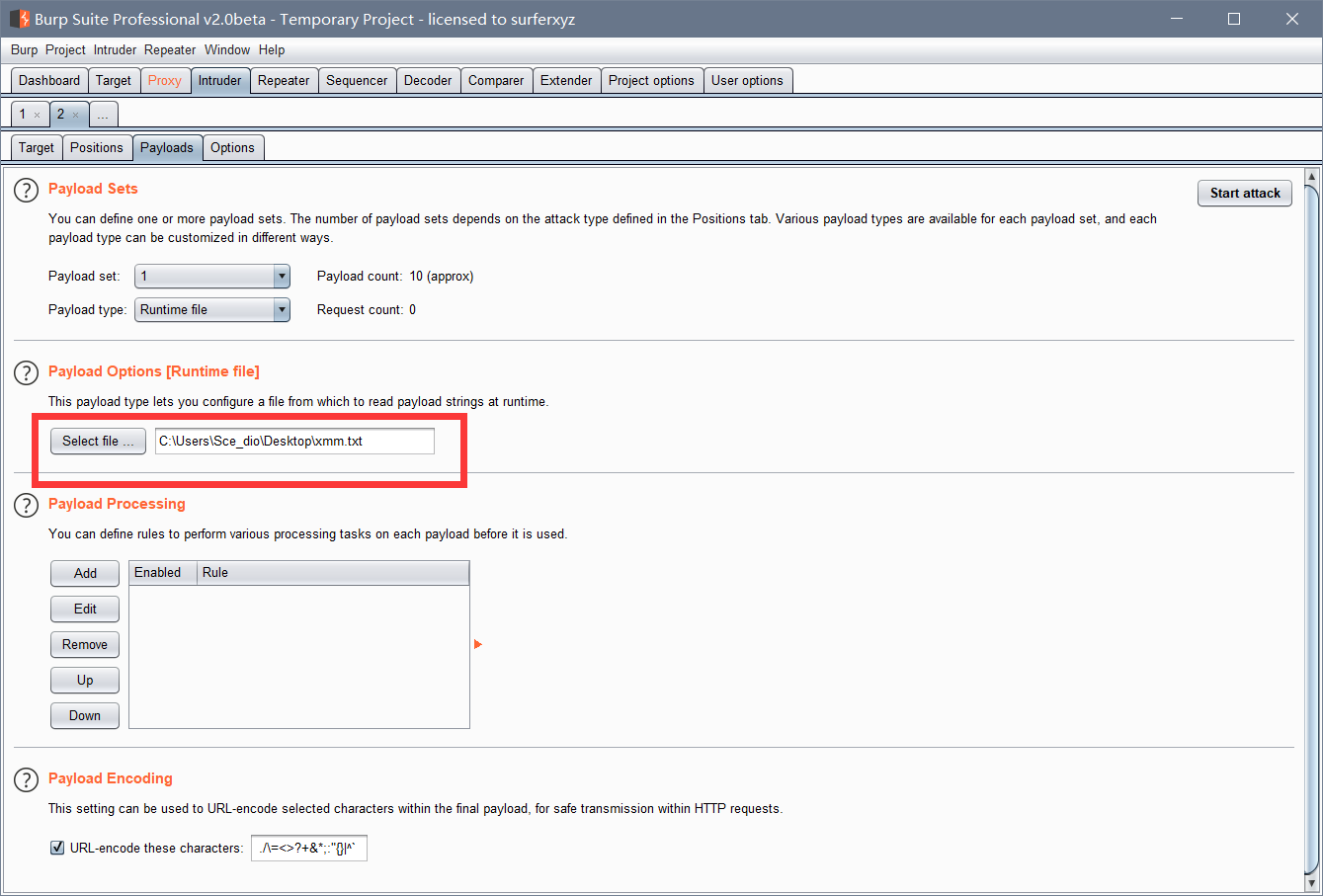


图4-3 添加字典演示图

设置爆破各项参数（Payload set：3；Payload type：Recursive grep以及初始token值）

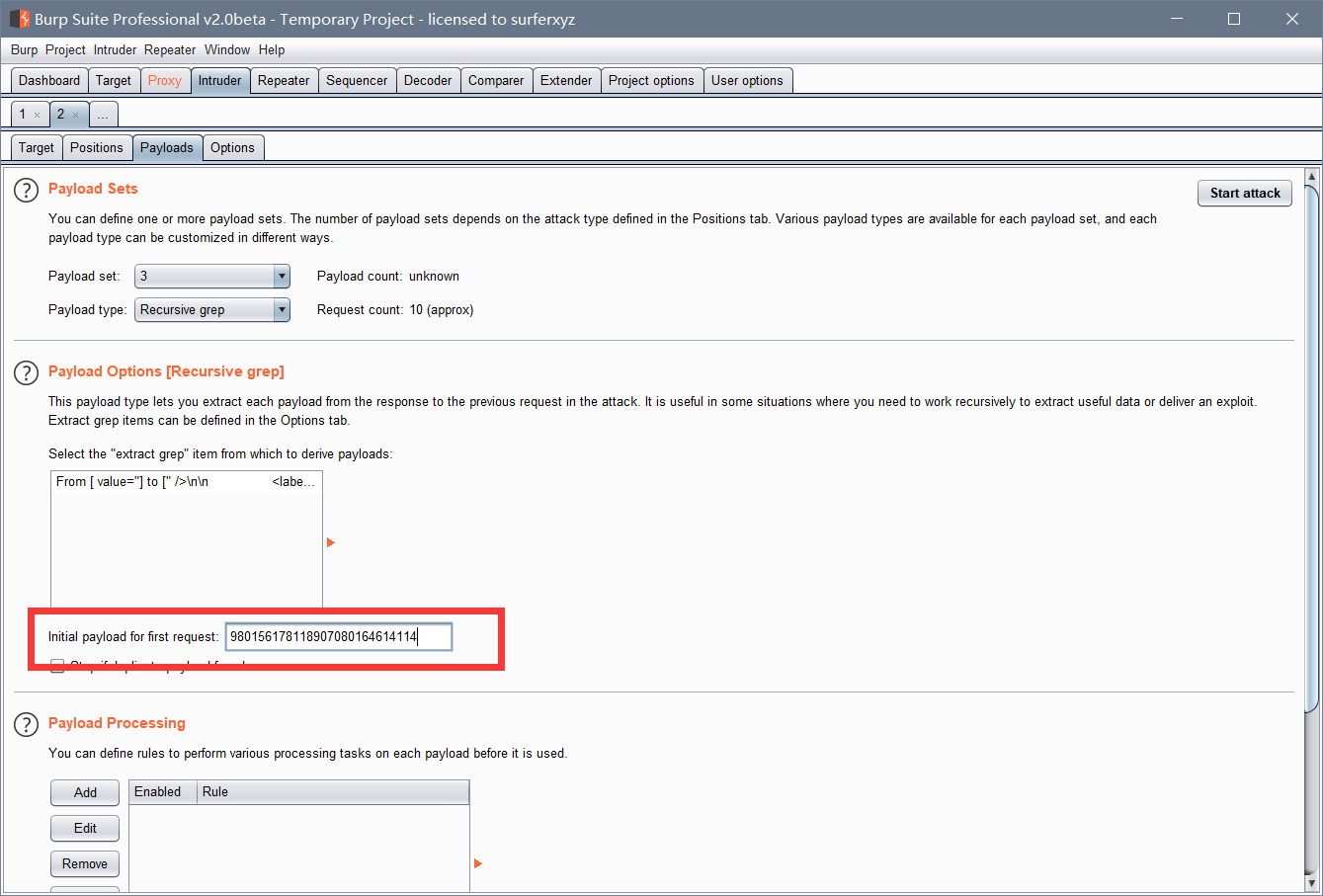


图4-4 参数设置演示图

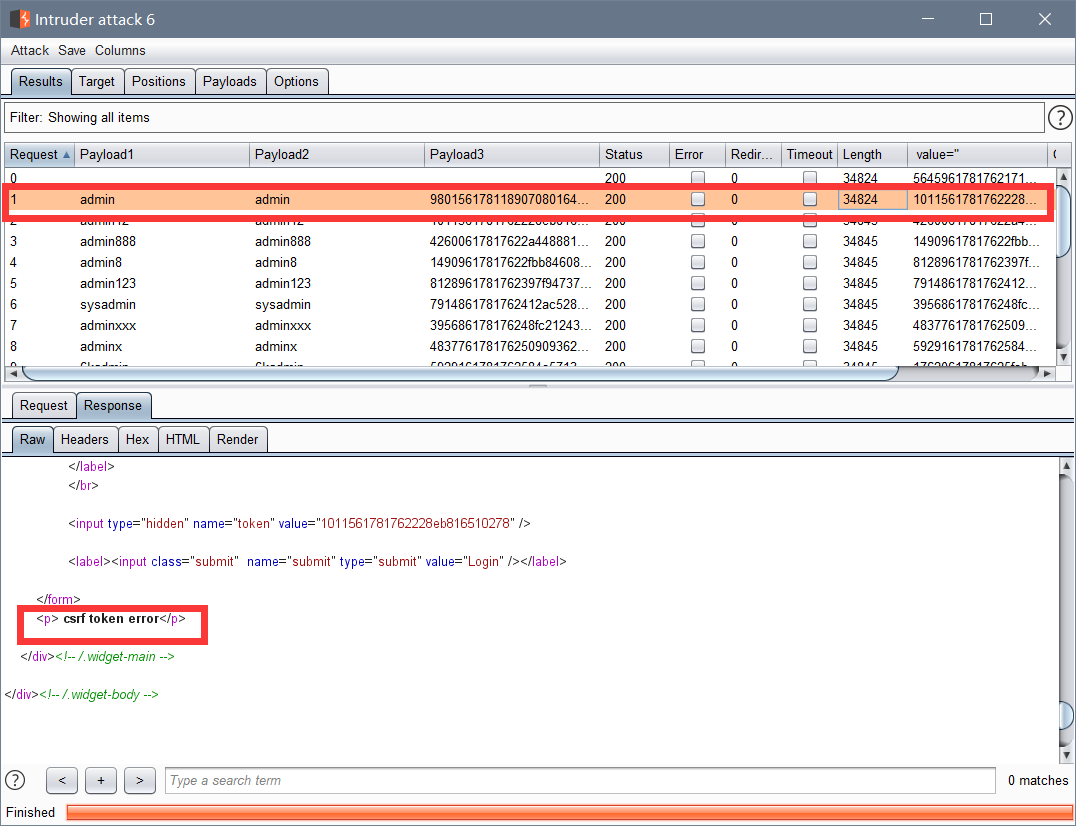


图4-5 错误结果

然而，结果显示爆破失败。经分析，原因在于提交了错误的token初始值。改正后重复上述步骤，得到了正确结果，返回的response也显示Login success。用户名为admin、密码为123456.

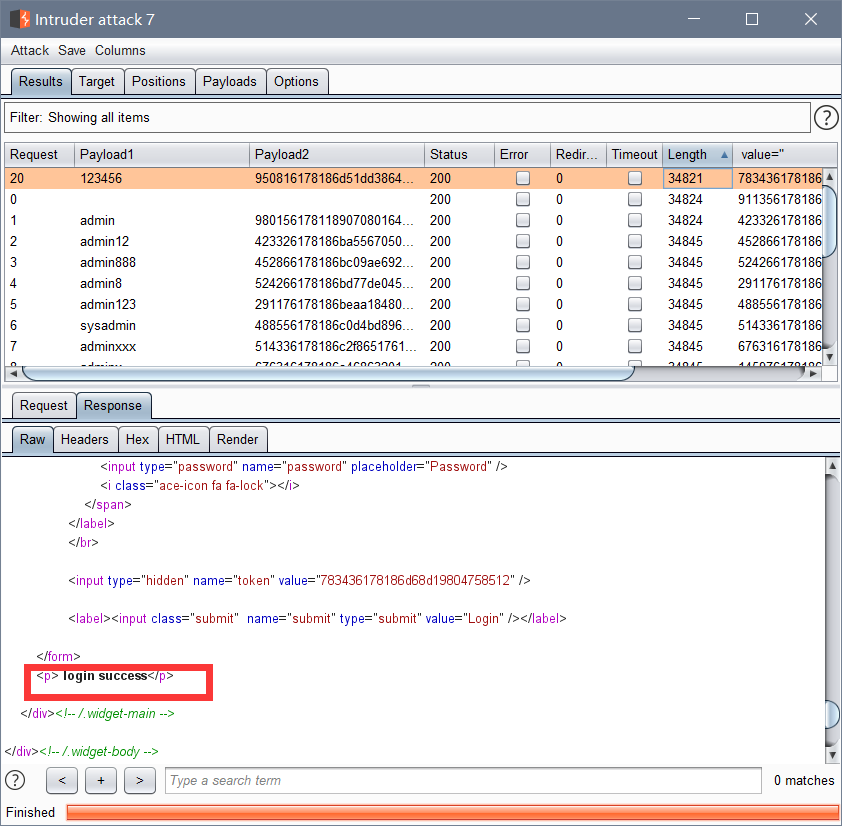


图4-6 正确结果

# 实践小结

①关于工具Burpsuite：Burpsuite 是用于攻击web 应用程序的集成平台，包含了许多工具。Burp Suite为这些工具设计了许多接口，以加快攻击应用程序的过程。所有工具都共享一个请求，并能处理对应的HTTP 消息、持久性、认证、代理、日志、警报。

②127.0.0.1 是回送地址，指本地机，一般用来测试使用。回送地址（127.x.x.x）是本机回送地址（Loopback Address），即主机IP堆栈内部的IP地址，主要用于网络软件测试以及本地机进程间通信，无论什么程序，一旦使用回送地址发送数据，协议软件立即返回，不进行任何网络传输。类比计算机组成中的五大层次：

|  |  |
| --- | --- |
| M4：虚拟机器（使用高级程序设计语言） | 将127.0.0.1作为代理地址相当于在“实际机器”间新增了一台虚拟机（实际并不是），若是不开启代理服务器，其仍然不能向外收发。在计算机看来，其就是把数据包发现了目标地址为127.0.0.1的（代理）机器。 |
| M3：虚拟机器（用汇编语言程序） |
| M2：虚拟机器（用机器语言程序执行操作系统） |
| M1：实际机器（机器指令） |
| M0：实际机器（用微指令执行机器指令） |

③token常用于主机与服务器间的通信验证参数，通常是动态更新的。我们在仿造相应的请求时也应作出相应调整。

④爆破即暴力破解，即使用字典来进行穷举，看返回的数据包Length长度是否不同。通常情况下，匹配成功与否返回的数据包长度是不一样的。通过找特殊，我们也可以判断是否爆破出些许信息。