

# 实验二 报文监听

## 实验目的

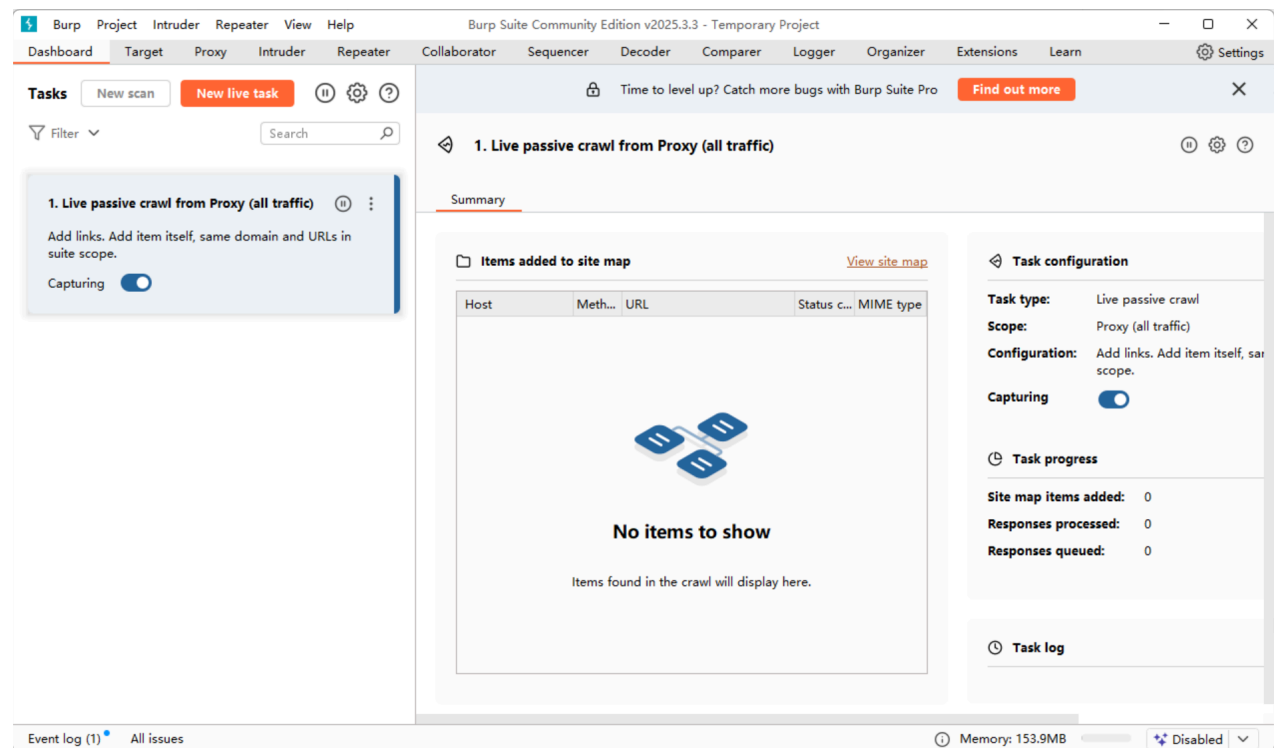
- 掌握 Burp Suite 工具的基本使用方法，能够独立完成抓包、分析HTTP请求与响应数据。
- 理解HTTP协议基本原理，包括请求头、响应头、状态码等核心概念。
- 理解抓包原理，了解中间人代理的工作机制及数据拦截过程。
- 学会使用 Burp Suite 进行简单的弱口令漏洞测试，掌握暴力破解基本操作与防护意识。
- 通过靶场实践，提高网络安全基础技能，培养攻防思维。

## 实验要求

- 熟悉 Burp Suite 界面布局及各主要模块（Proxy、Intruder、Repeater、Decoder等）的基本功能。
- 能够独立完成通过配置代理，实现浏览器与 Burp Suite 之间的流量劫持。
- 能正确分析一个完整的HTTP请求与响应，并能够指出关键字段。
- 成功完成对 Pikachu 靶场弱口令模块的暴力破解实验，并总结破解过程与防御措施。
- 撰写实验报告，总结操作步骤、遇到的问题、解决方法以及个人收获。

## 实验内容

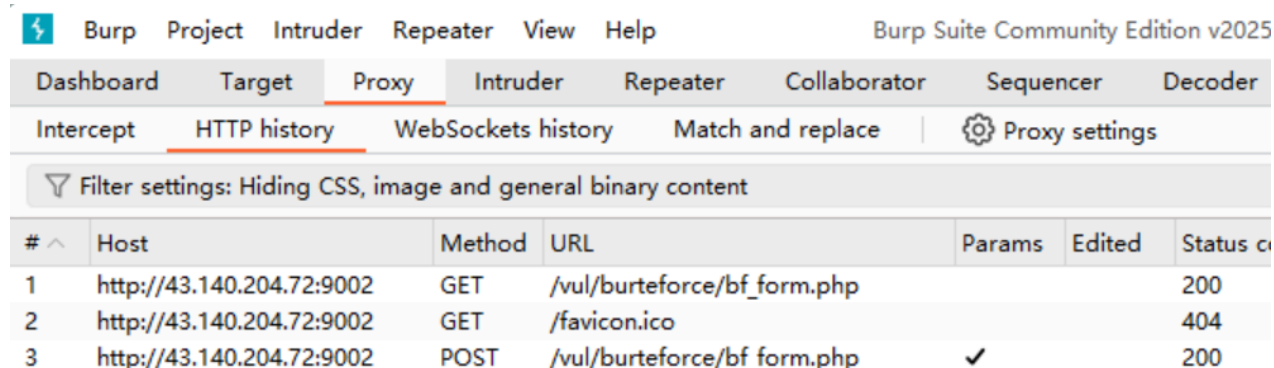
- 安装、配置 Burp Suite 抓包工具。（见附件1：Burp Suite 抓包工具安装与配置）  
[Burp Suite 抓包工具安装与配置](#)
- 熟悉 Burp Suite 界面布局及各主要模块（Proxy、Intruder、Repeater、Decoder等）的基本功能。



- 通过配置代理，实现浏览器与Burp Suite之间的流量劫持。  
配置好代理后使用浏览器访问 "百度一下" 官网页面，分别对 Burp Suite中拦截到的HTTP请求和响应截图。



- 正确分析一个完整的HTTP请求与响应，并能够指出关键字段。  
对拦截到的 HTTP 请求和响应进行分析，分别指出请求、响应的关键字段。  
需要有对 Get 请求和 POST 请求两种类型的分析。



- 完成对 Pikachu 靶场弱口令模块的暴力破解实验，并总结破解过程与防御措施。
- 访问 Pikachu [靶场地址](#)，进入 暴力破解页面。

Pikachu 漏洞练习平台 pika~pika~

 欢迎  
骚年

🔍 系统介绍

📁 暴力破解

▶ 概述

基于表单的暴力破解

验证码绕过(on server)

验证码绕过(on client)

token防爆破?

🔗 Cross-Site Scripting

🔗 CSRF

🔗 SQL-Inject

🔗 RCE

🔗 File Inclusion

🏠 暴力破解 > Burte Force概述

**Burte Force（暴力破解）概述**

“暴力破解”是一攻击手段，在web攻击中，一般会使用这种手段对应用系统的认证信息进行获取。其过程就是使用大量的认证信息在认证接口进行尝试登录，直到得到正确的结果。为了提高效率，暴力破解一般会使用带有字典的工具来进行自动化操作。

理论上来说，大多数系统都是可以被暴力破解的，只要攻击者有足够强大的计算能力和时间，所以断定一个系统是否存在暴力破解漏洞，其条件也不是绝对的。我们说一个web应用系统存在暴力破解漏洞，一般是指该web应用系统没有采用或者采用了比较弱的认证安全策略，导致其被暴力破解的“可能性”变的比较高。这里的认证安全策略,包括：

- 1.是否要求用户设置复杂的密码；
- 2.是否每次认证都使用安全的验证码（想想你买火车票时输的验证码～）或者手机otp；
- 3.是否对尝试登录的行为进行判断和限制（如：连续5次错误登录，进行账号锁定或IP地址锁定等）；
- 4.是否采用了双因素认证；

...等等。

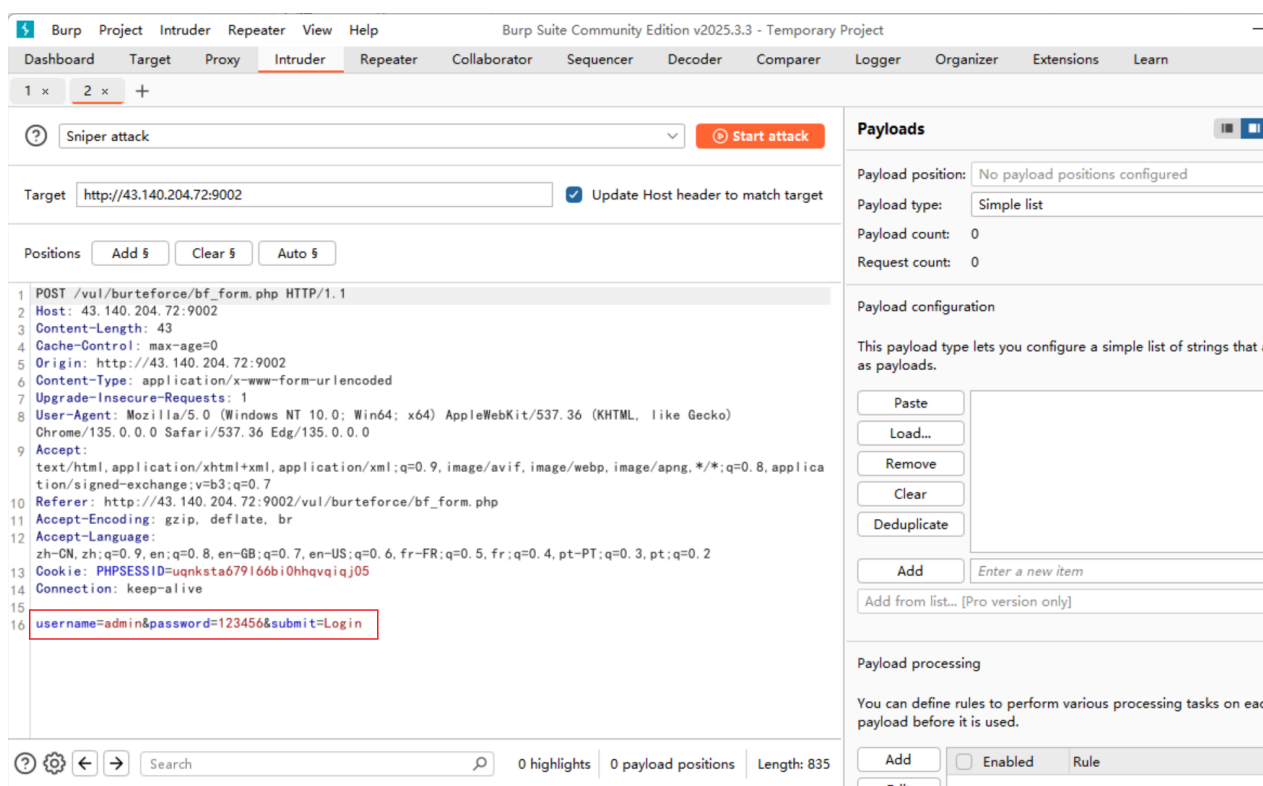
千万不要小看暴力破解漏洞,往往这种简单粗暴的攻击方式带来的效果是超出预期的!

你可以通过“BurteForce”对应的测试栏目，来进一步的了解该漏洞。

从来没有哪个时代的黑客像今天一样热衷于猜解密码 ---奥斯特洛夫斯基

利用Burp Suite 工具抓包后，使用“Intruder 模块”完成“基于表单的暴力破解”。

弱口令字典下载地址 [弱口令字典](#)



- 撰写实验报告，总结操作步骤、遇到的问题、解决方法以及个人收获。

## 参考资料

- [《Burp Suite官方用户手册》](#)
- [Pikachu靶场官网及相关文档](#)