实验二 报文监听

实验目的

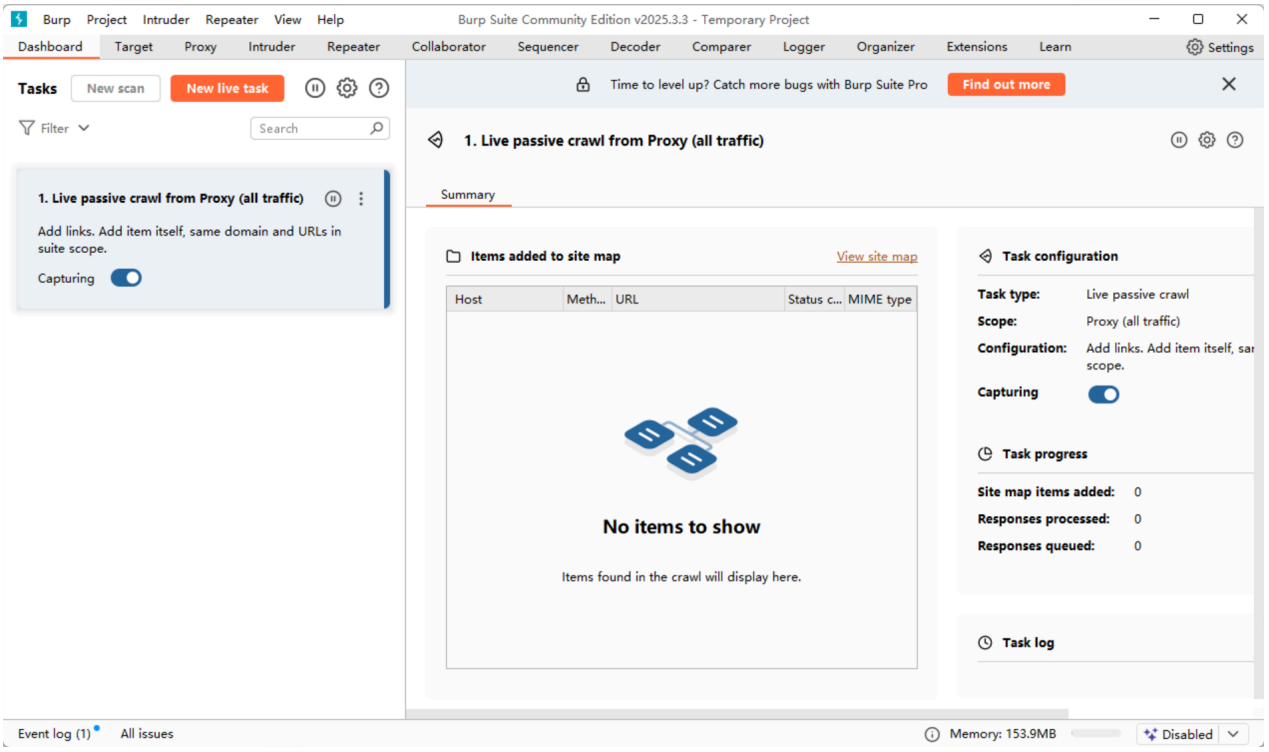
- 掌握 Burp Suite 工具的基本使用方法，能够独立完成**抓包**、分析**HTTP请求与响应**数据。
- 理解HTTP协议基本原理，包括**请求头、响应头、状态码**等核心概念。
- 理解抓包原理，了解中间人代理的工作机制及数据拦截过程。
- 学会使用 Burp Suite 进行简单的**弱口令**漏洞测试，掌握**暴力破解**基本操作与防护意识。
- 通过靶场实践，提高网络安全基础技能，培养攻防思维。

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。

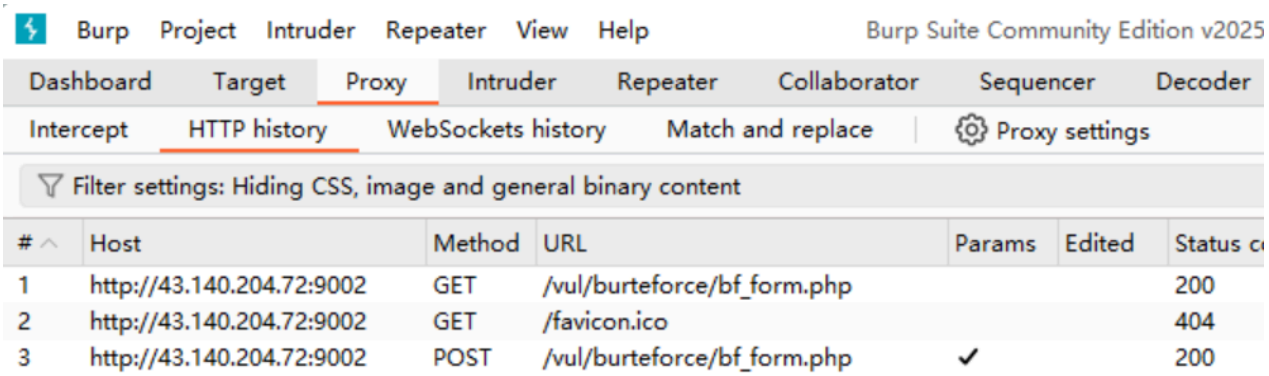
实验内容

- 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。



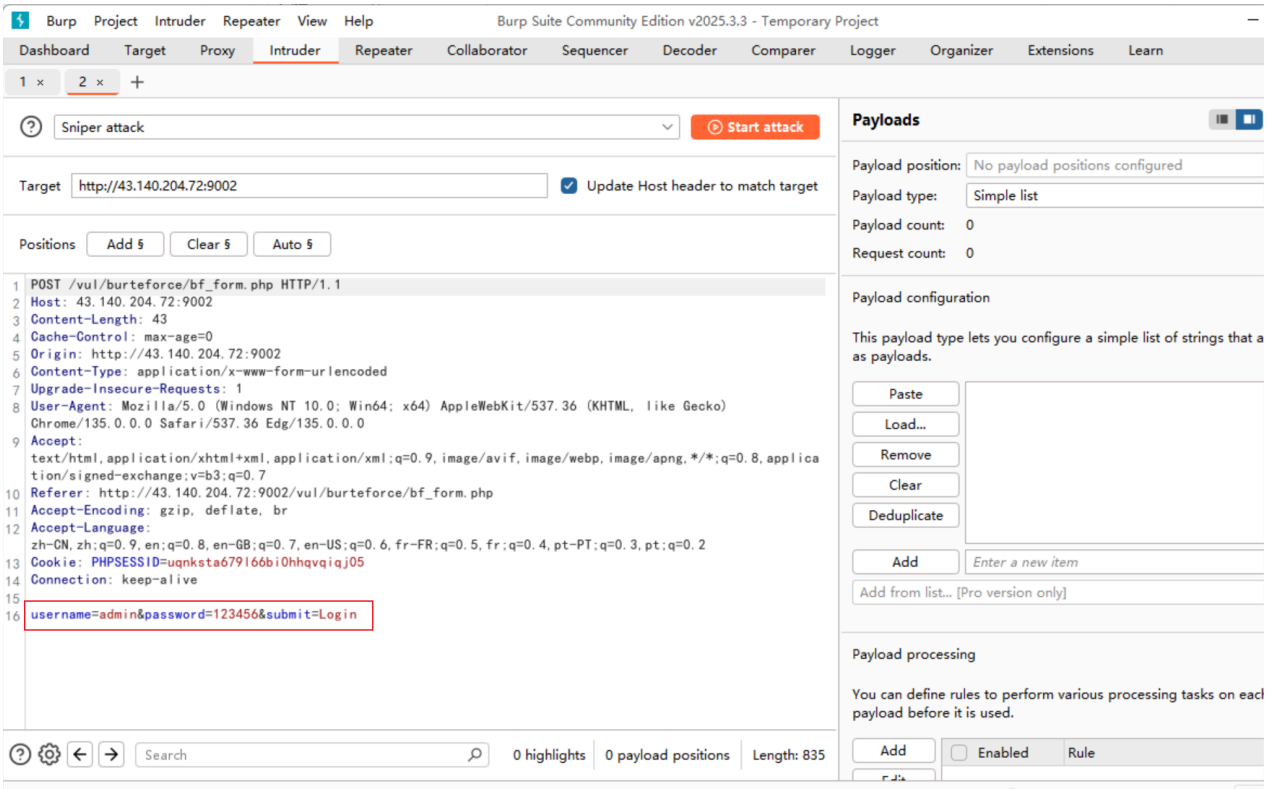
- 通过配置代理，实现浏览器与Burp Suite之间的流量劫持。
  配置好代理后使用浏览器访问 "百度一下" 官网页面，分别对 Burp Suite中拦截到的HTTP请求和响应截图。

- 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。

  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