**北京科技大学实验报告**

学院：计算机与通信工程学院 专业：信息安全 班级：信安182

姓名： 王泽辰 学号：41824180 实验日期： 2020年11月15日

**实验名称：**

XXE

**实验目的：**

了解XXE，学习使用其在pikachu进行简单的实战。

**实验仪器：**

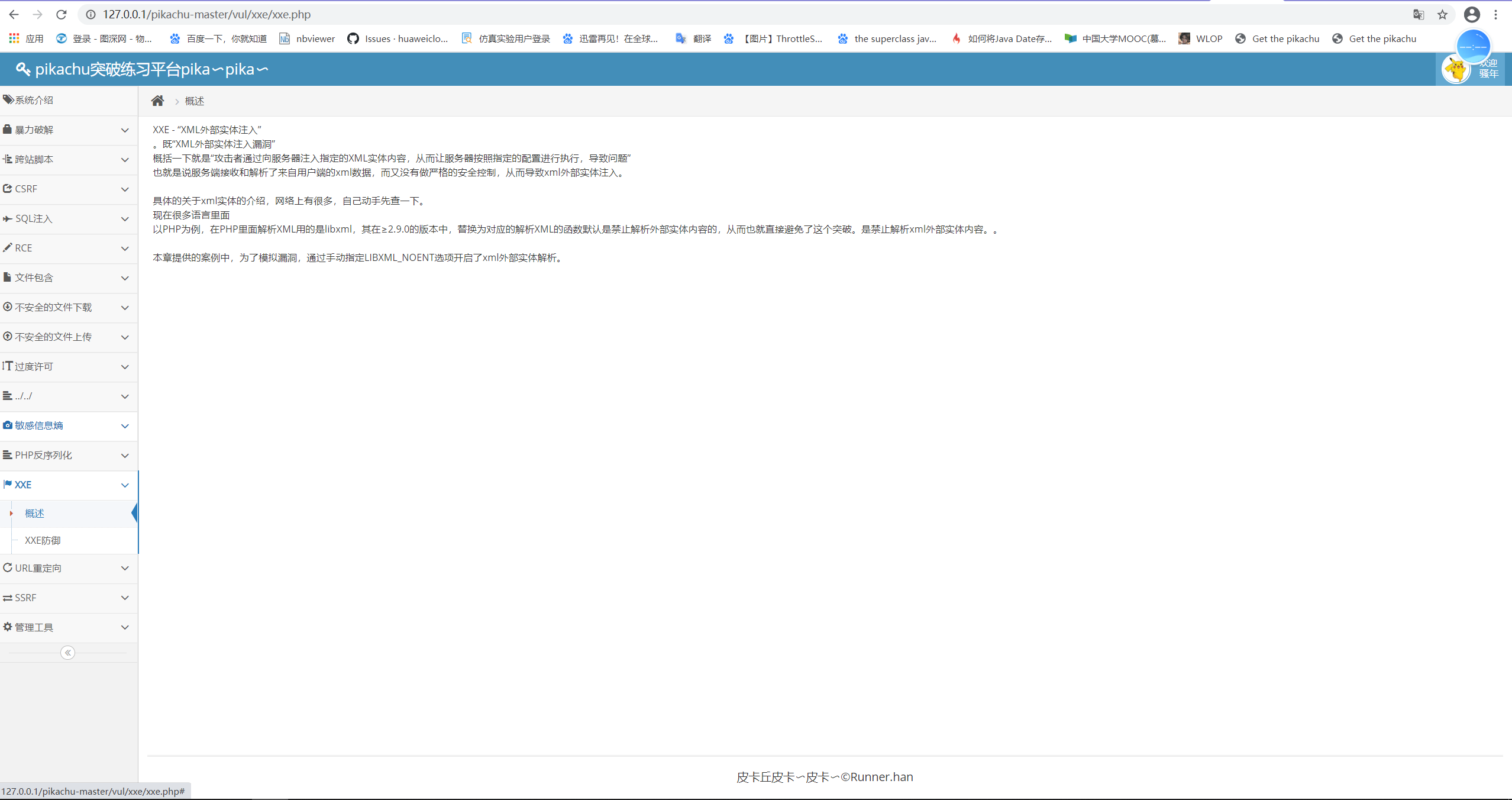
PC\*1

**实验原理：**

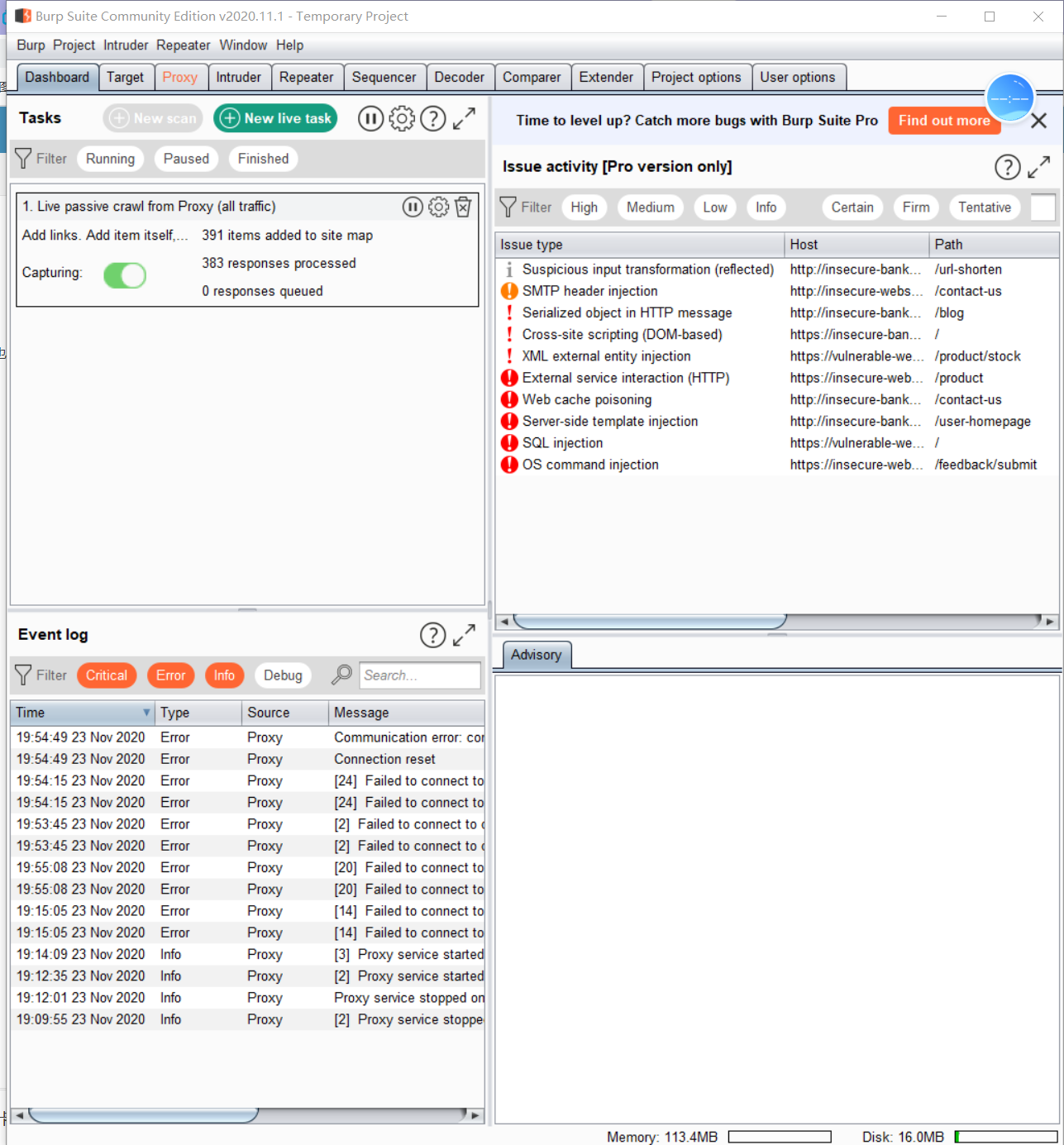
XXE漏洞全称(XML External Entity Injection)即xml外部实体注入漏洞，XXE漏洞发生在应用程序解析XML输入时，没有禁止外部实体的加载，导致可加载恶意外部文件，造成文件读取、命令执行、内网端口扫描、攻击内网网站、发起dos攻击等危害。xxe漏洞触发的点往往是可以上传xml文件的位置，没有对上传的xml文件进行过滤，导致可上传恶意xml文件。

**实验内容与步骤：**

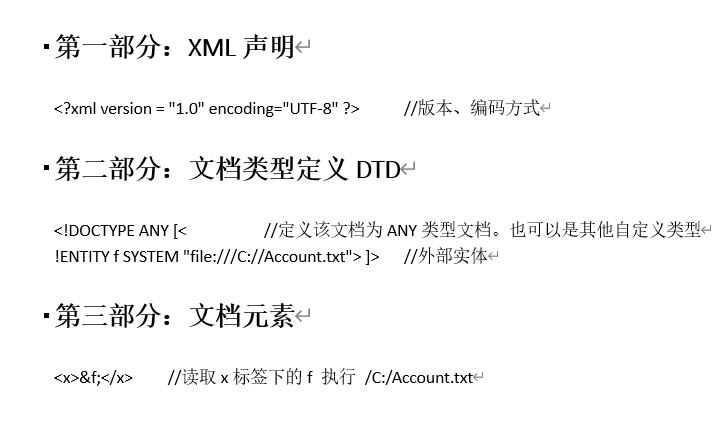
1. 配置pikachu实验环境。



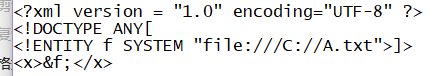
1. 下载安装Burp Suite。



1. 学习XML语言，编写xml文档。



此次使用的xml内容：

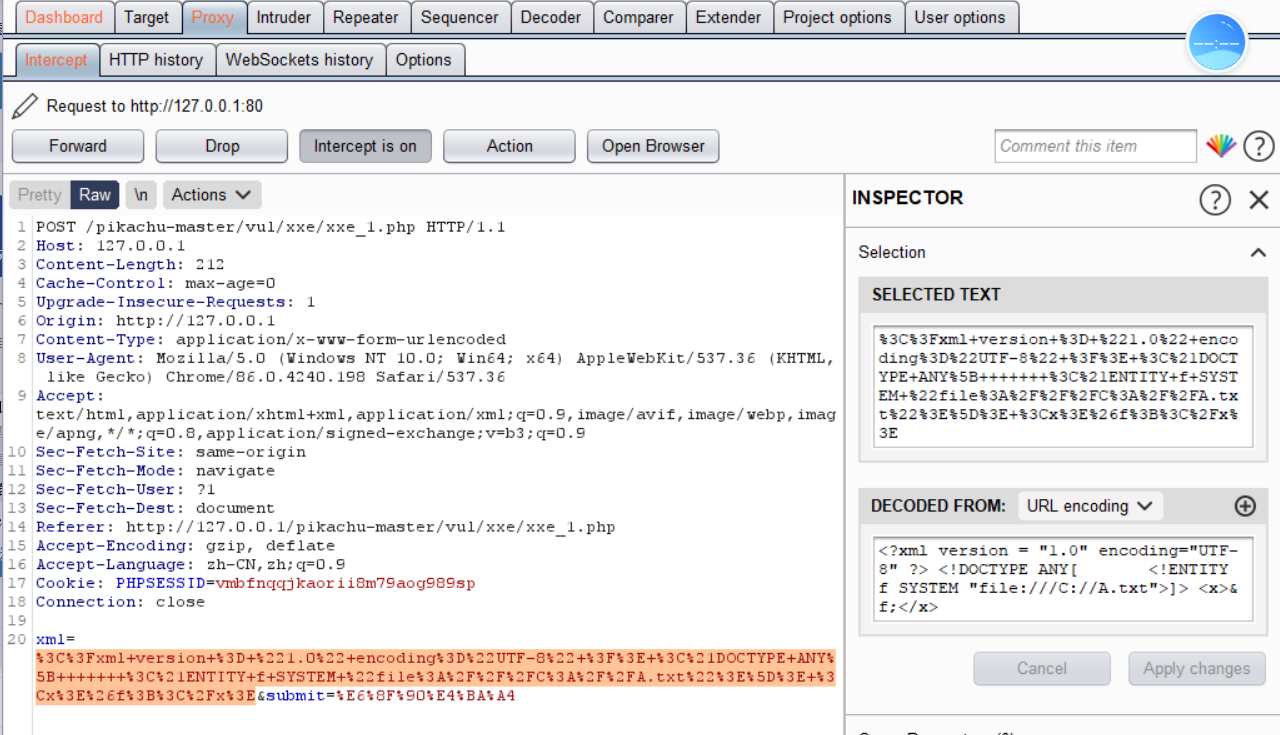


1. 将xml内容写入pikachu提供的api



可以看到文件内容被读取了

1. 使用burp suite抓包转发



可以看到这是一个POST请求与其请求内容，可以在右下角的文本框进行更改，之后使用重新加密后的字符串替代原来的字符串即可进行更改。

**实验总结与收获：**

学会了使用pikachu漏洞测试平台和burp suite，步入了信安门槛，有一个可以实战的网站。