BJDCTF2nd 假猪套天下第一 Writeup

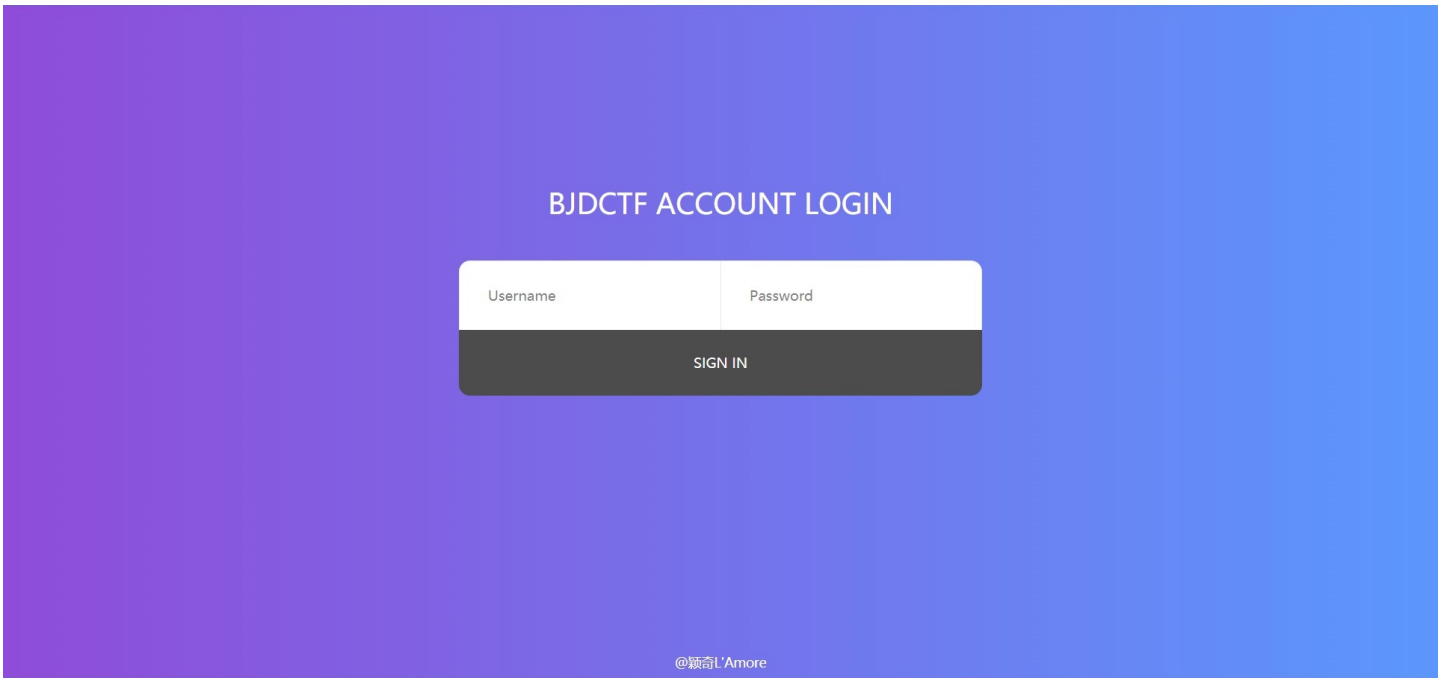
原创

Tajang 于 2021-04-11 13:51:09 发布 98 收藏

分类专栏： CTF 文章标签： php 网络安全 web html

本文链接：https://blog.csdn.net/qq_45619909/article/details/115598085

打开靶机后是一个登录页面

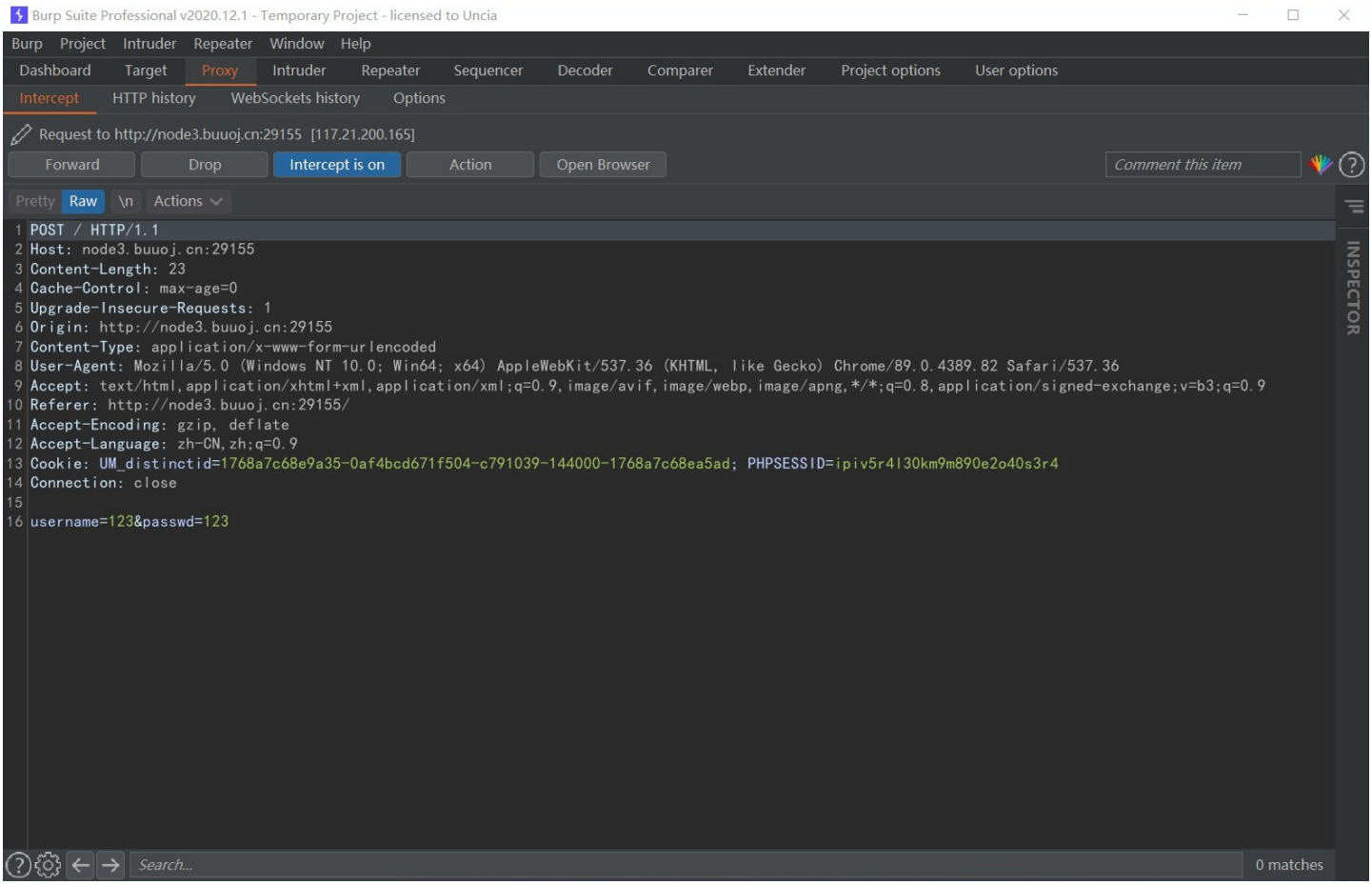


我们先输入一个admin和123456试试

真调皮，那我们什么都不输入再登录一次

我真的是越来越喜欢Y1ng师傅出的题了

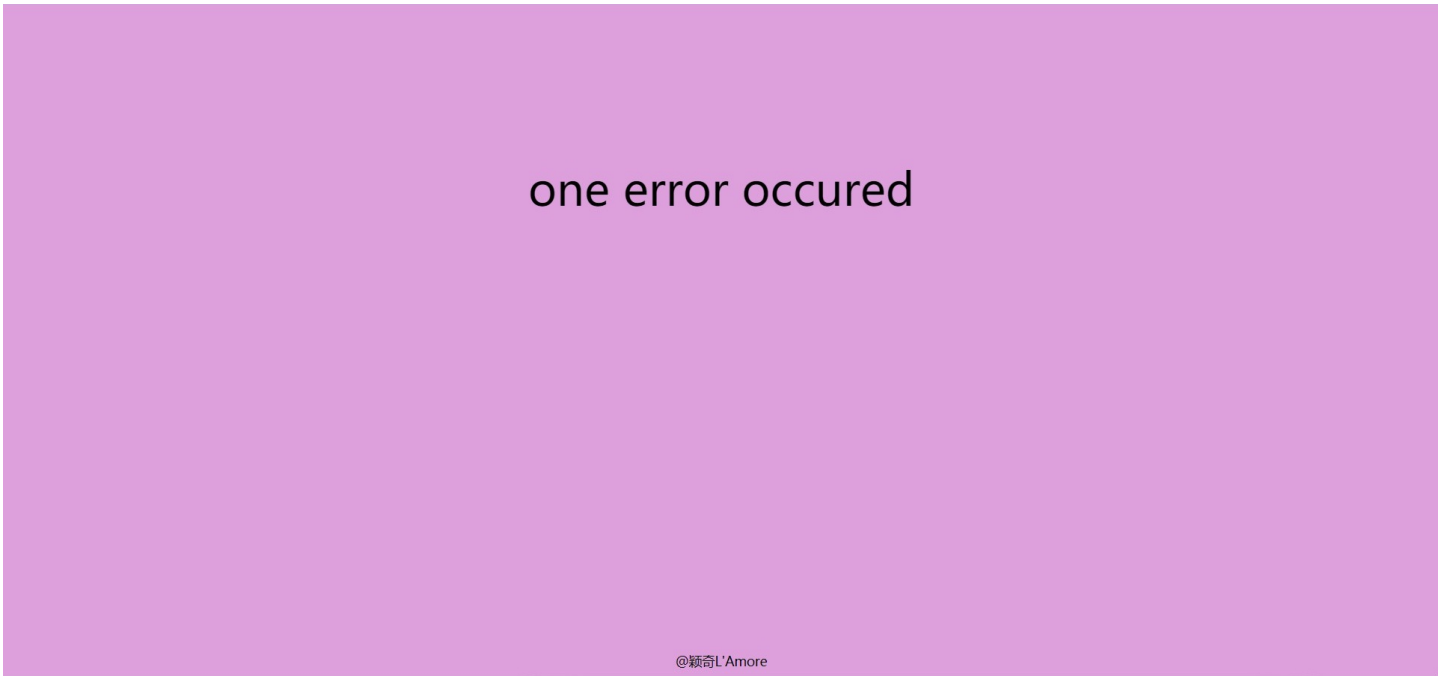
试了，F12，robots协议，看了网页源代码没发现什么重要内容。在一筹莫展的时候那就抓包。抓包如下：



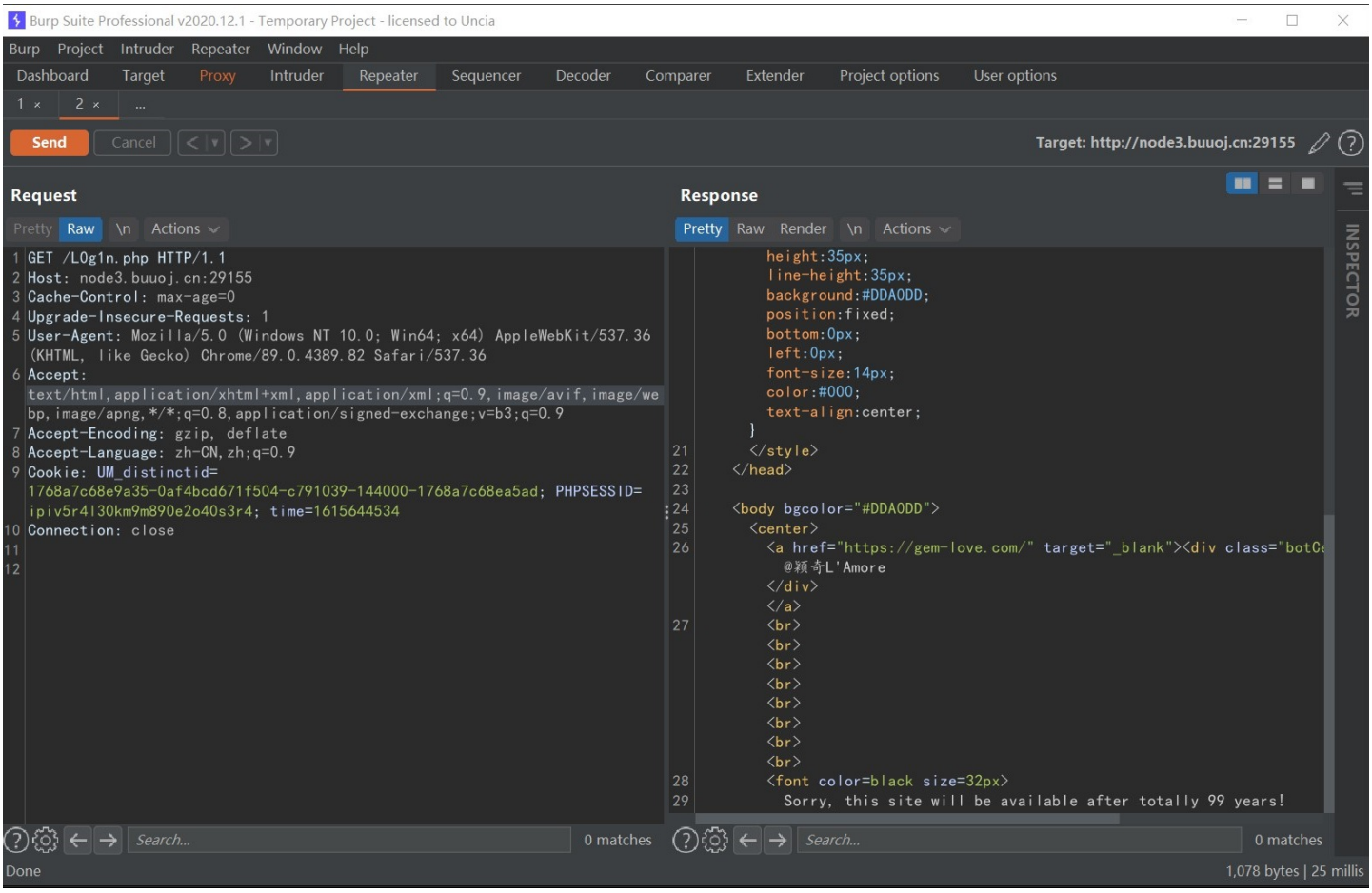
发送到Repeater,发包。发现如下：

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-h5YGqBse-1618120221358)(https://cdn.jsdelivr.net/gh/Tajang-ctf/blog_images/bjdtaowa5.png)]

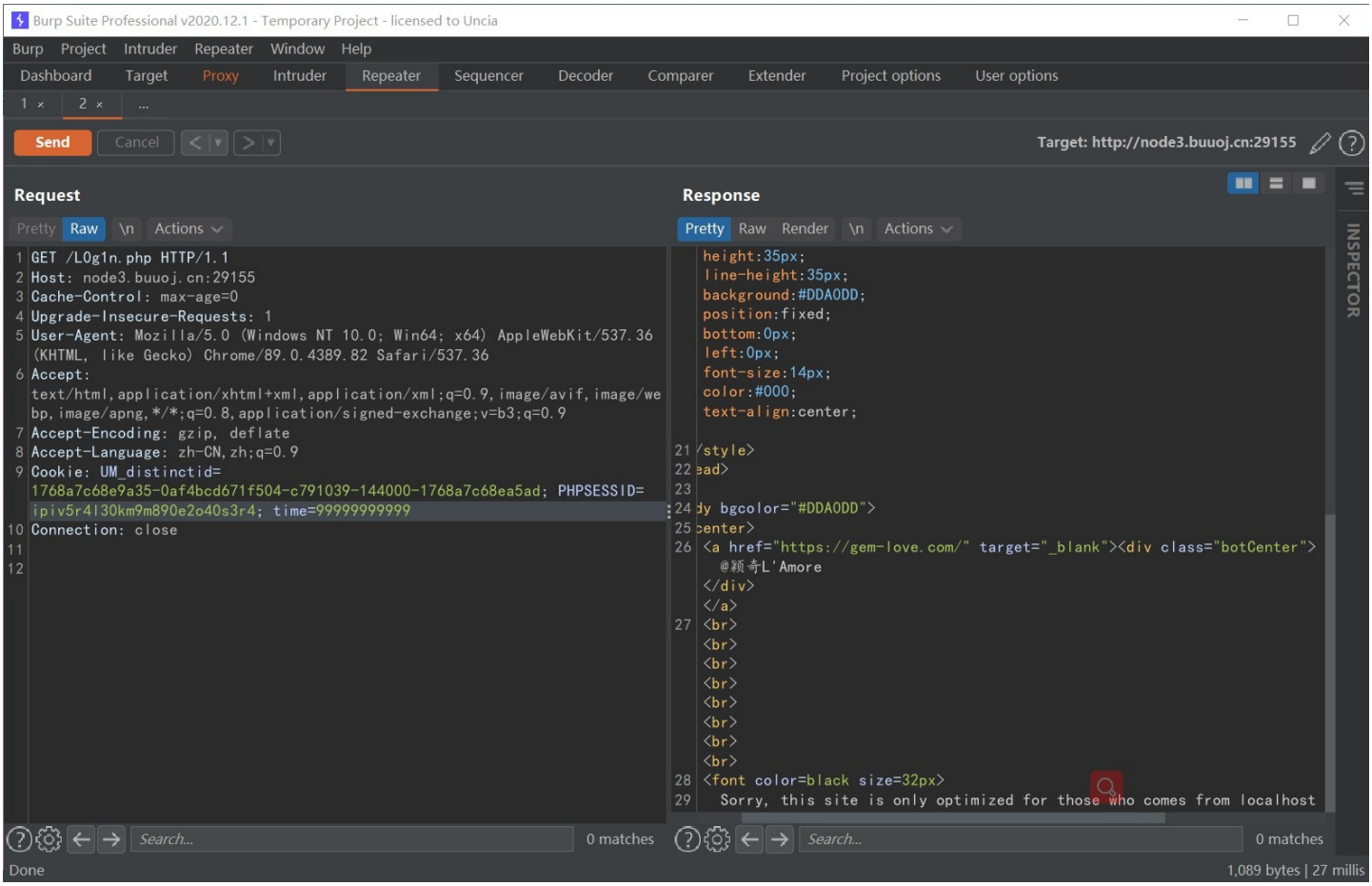
我们可以看到右边代码里倒数第二行提示了Log1n.php页面，我们关闭代理打开网页看一下



很粉的界面，没什么线索，再抓一次包，发送到Repeater，发包，内容如下：



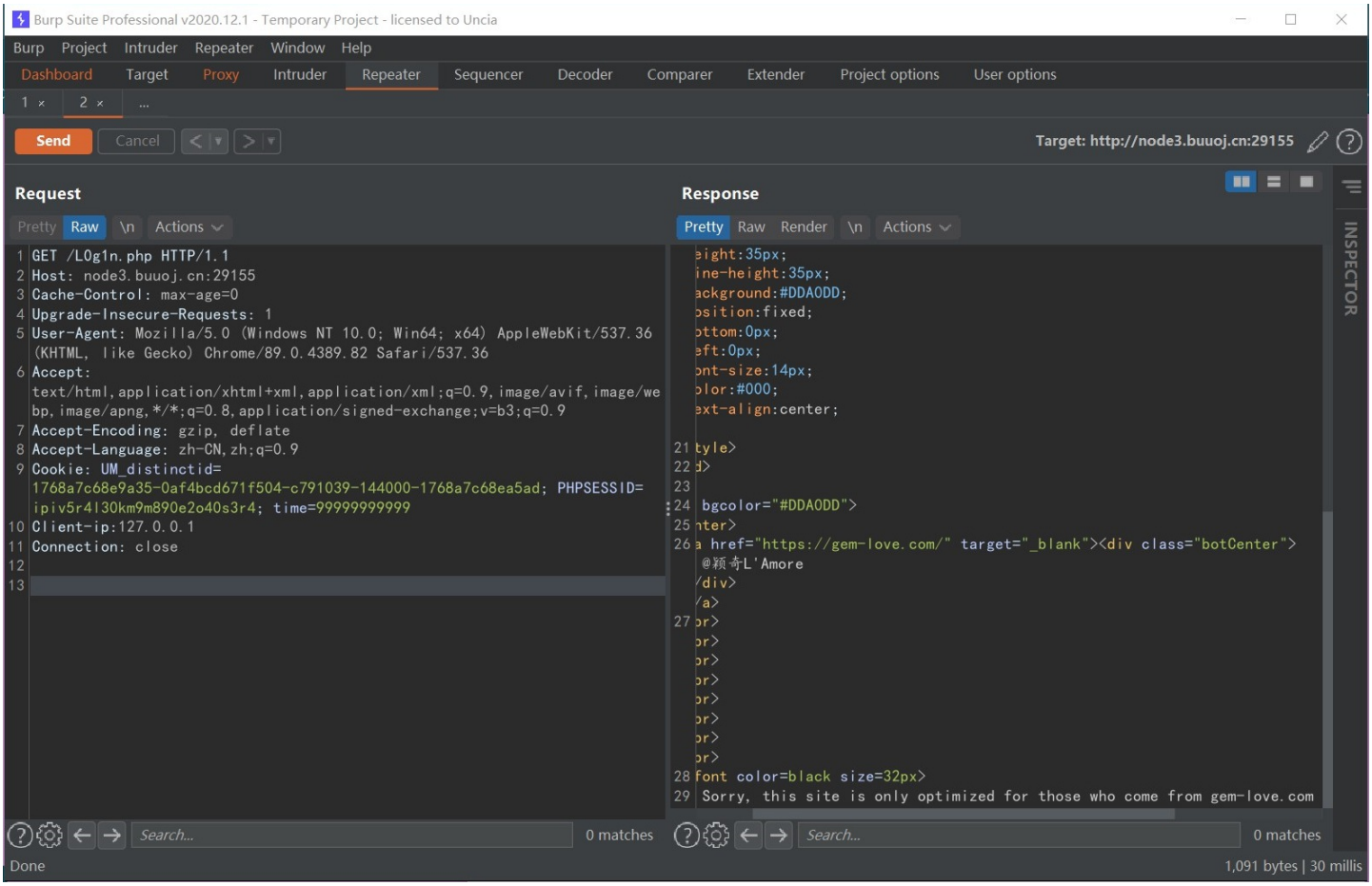
右下角给了提示，意思是这个网站99年后才能用，这时又没头绪了，注意它的提示，99年。认真看一下包，发现header里有个time项。那我们把time项数值改很大试试。发包后返回如下：



右下角又有了提示，内容意思是这个站只能让本地用户访问，我们知道127.0.0.1代表自己本地，这里可以使用XFF或者Client-ip我这里使用后者。在包内添加

```
Client-ip:127.0.0.1
```

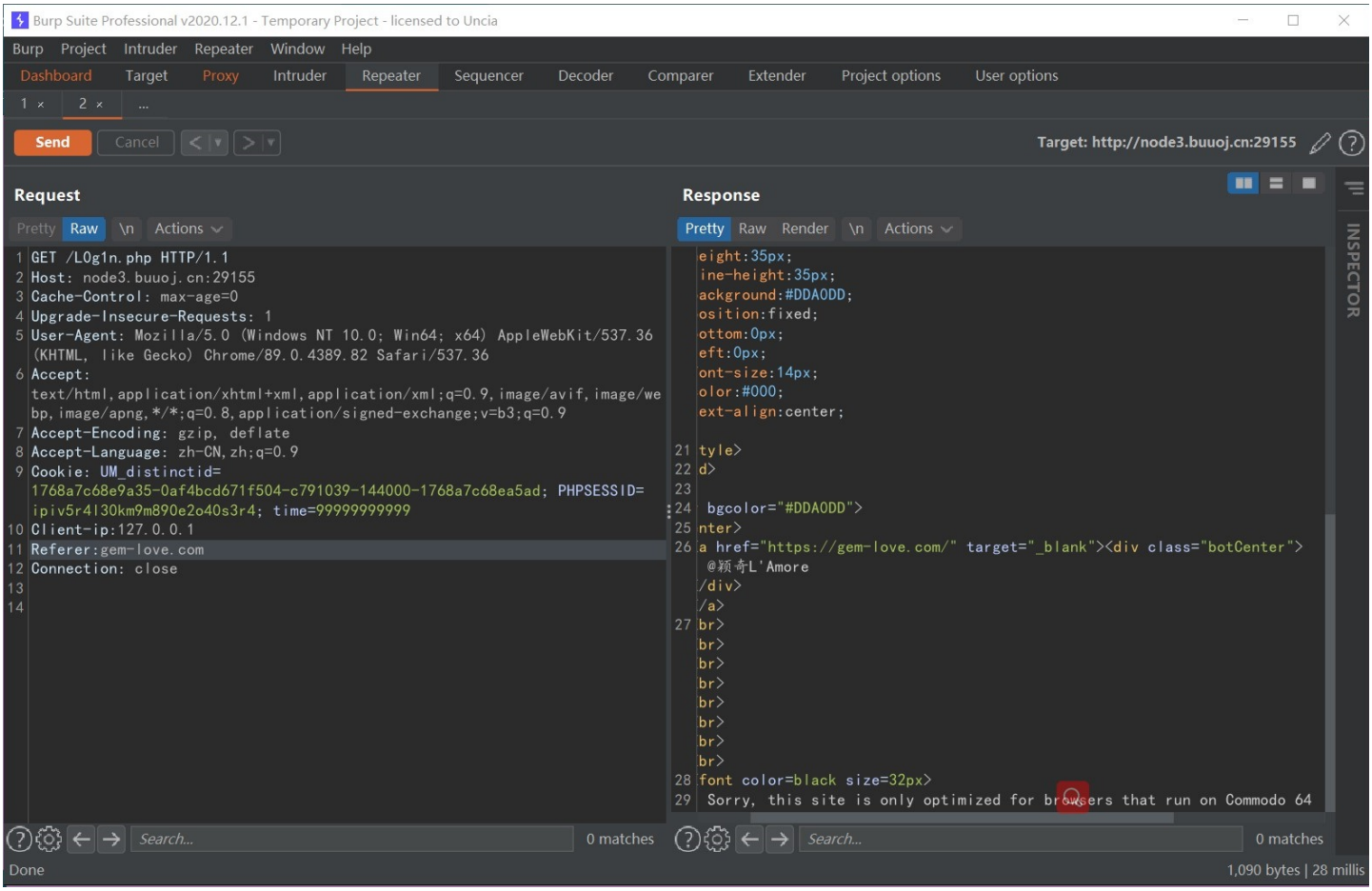
再次发包，看到如下：



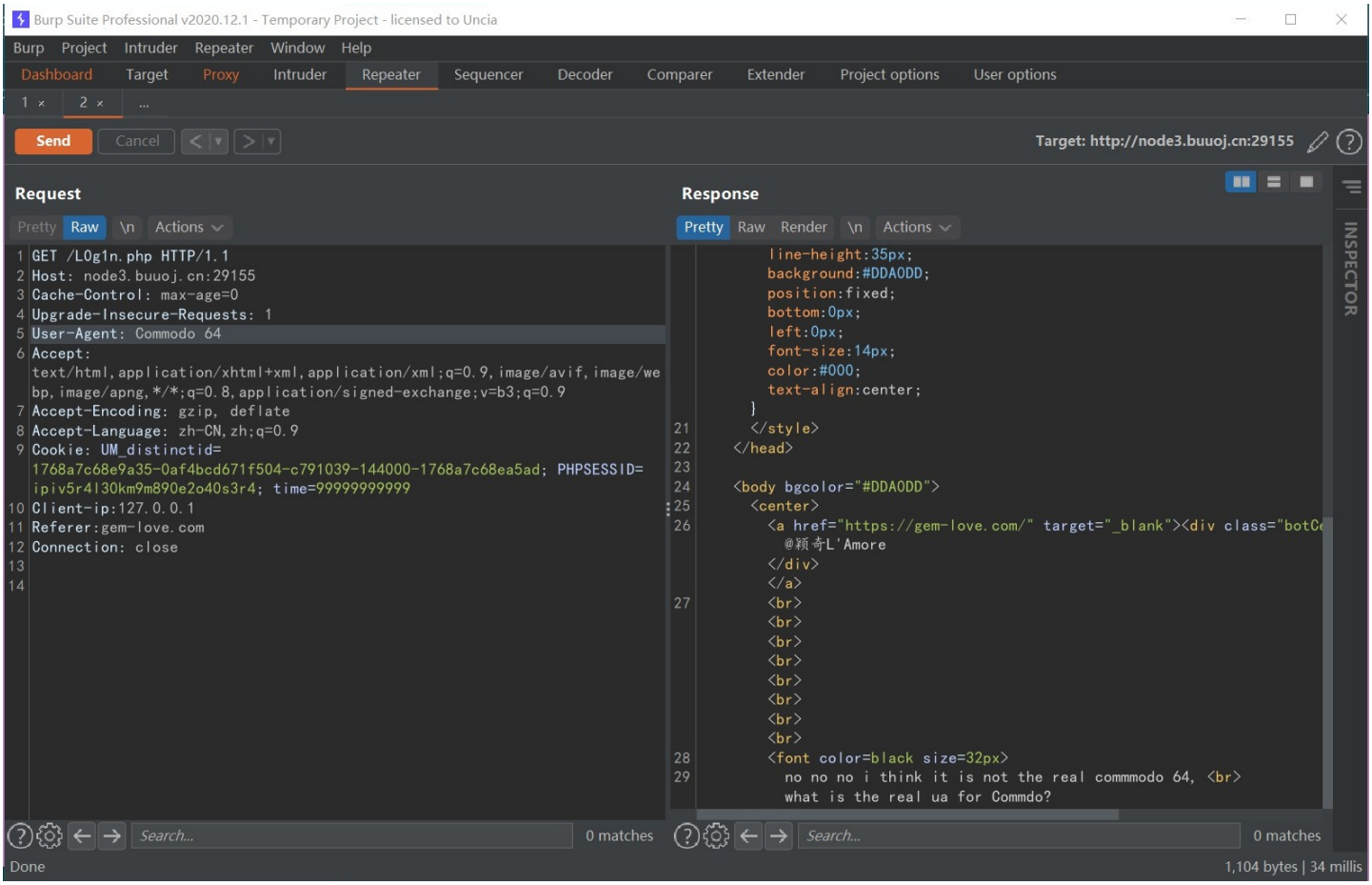
拜托把话说完行吗？提示访问要来自gem-love.com，在包内添加

```
Referer:gem-love.com
```

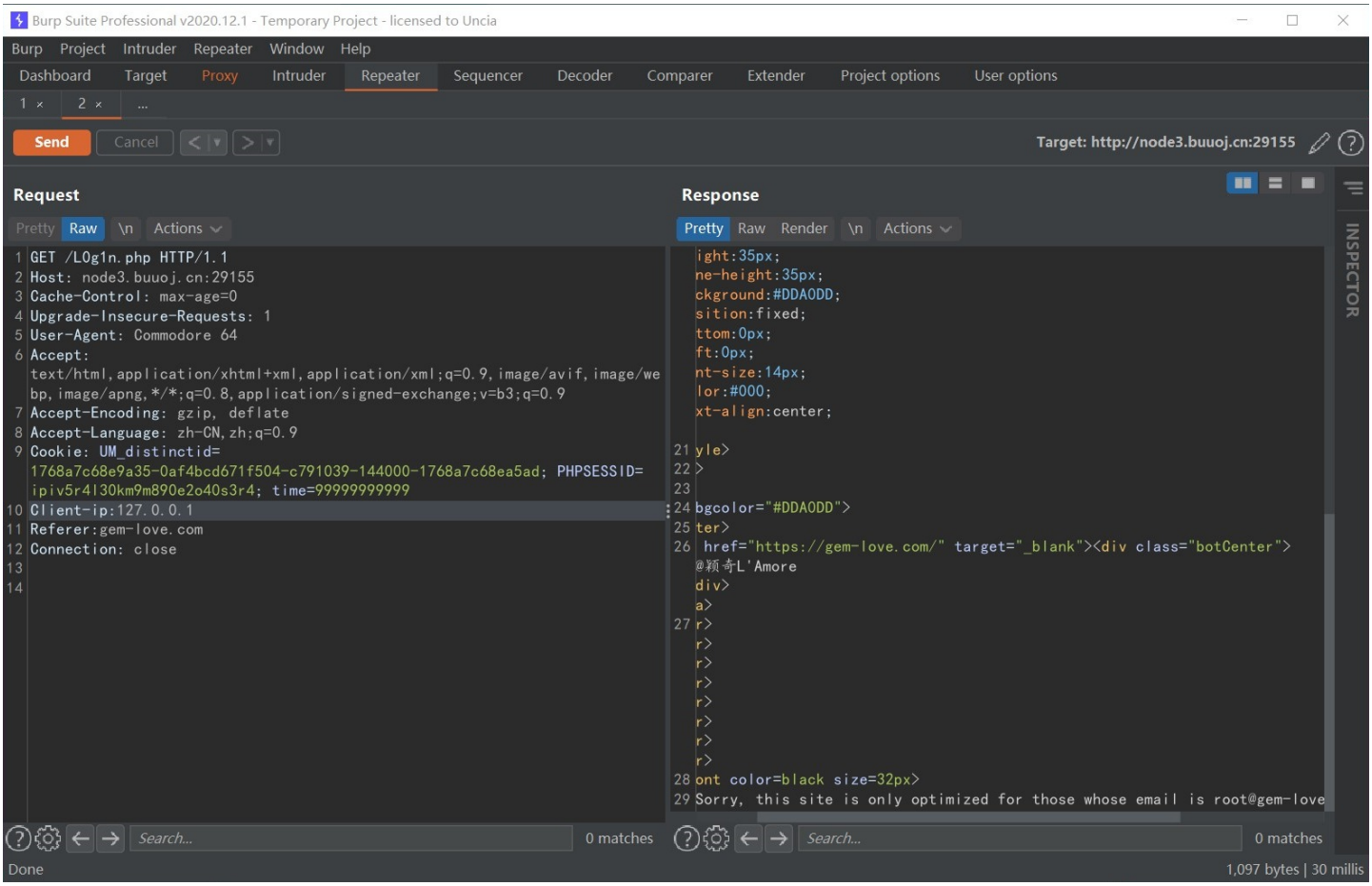
再来



还要使用的浏览器必须是Commodo 64,在User-Agent里将原来浏览器信息改为Commodo 64。

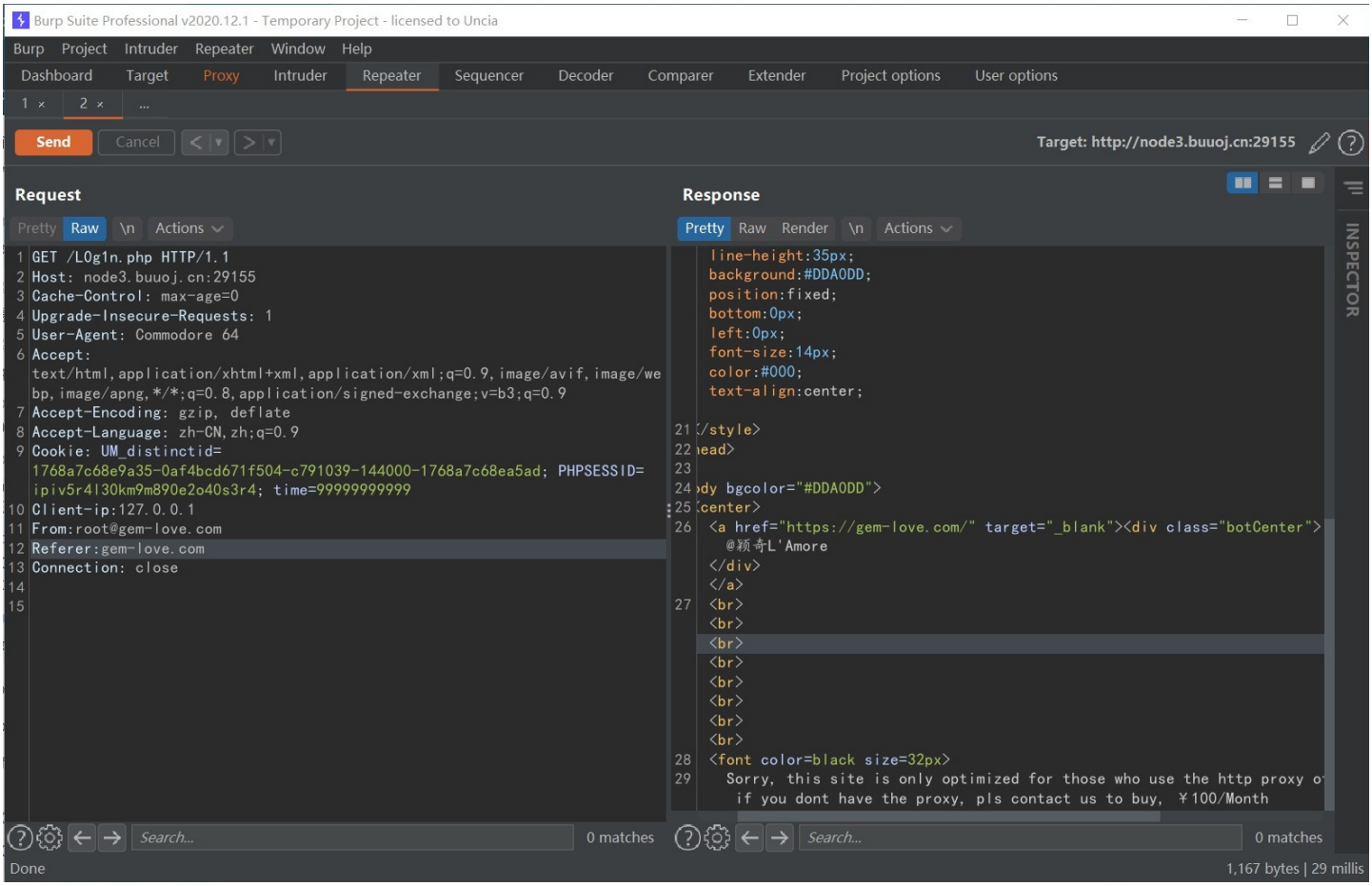


不是真的Commodo 64?百度一下，发现这个浏览器全称是Commodore 64,改正再来



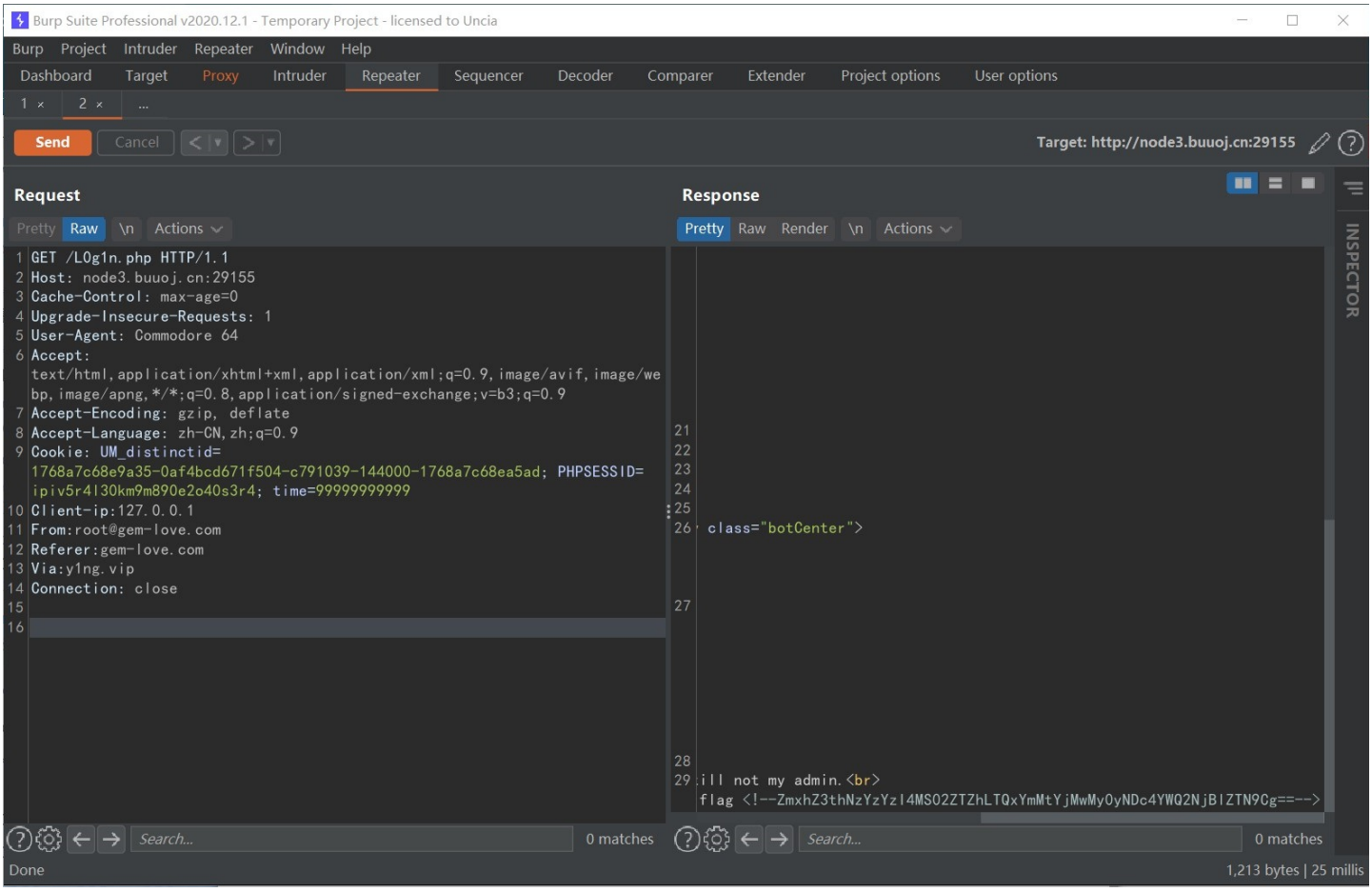
还要邮箱，在包里添加

```
From:root@gem-love.com
```



提示让我买？开玩笑，我身上搜不出10块钱。它说需要代理服务器地址是y1ng.vip，那我们加个

```
Via:y1ng.vip
```



终于给了，虽然它说不给我们flag，但是后面的注释里给了一串代码，尝试使base64进行解码!

有本事你再套几个，这题并不难主要就是考察访问头的要点。不知道的地方仍然百度了一些。希望知识积累得更多！