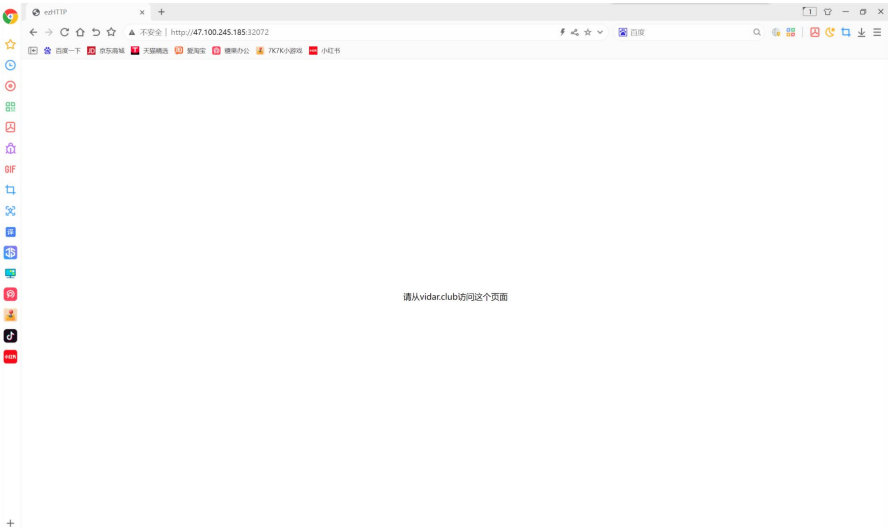
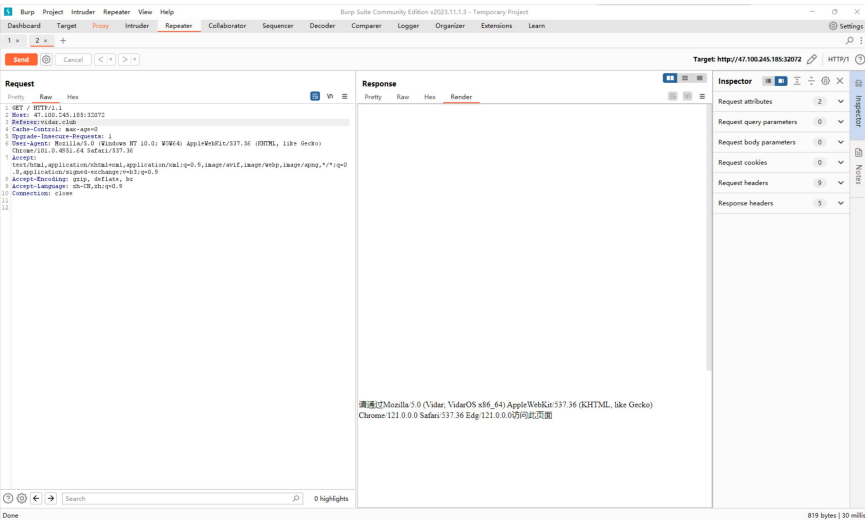


# EzHTTP

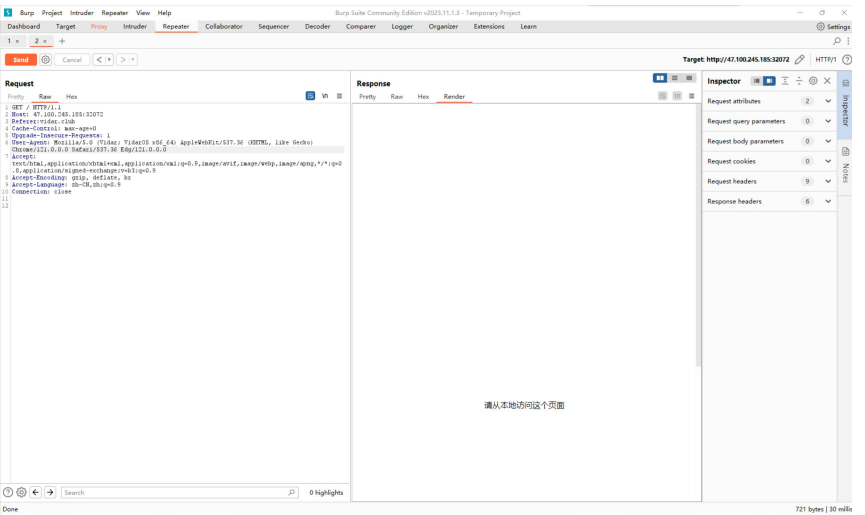
先打开网址



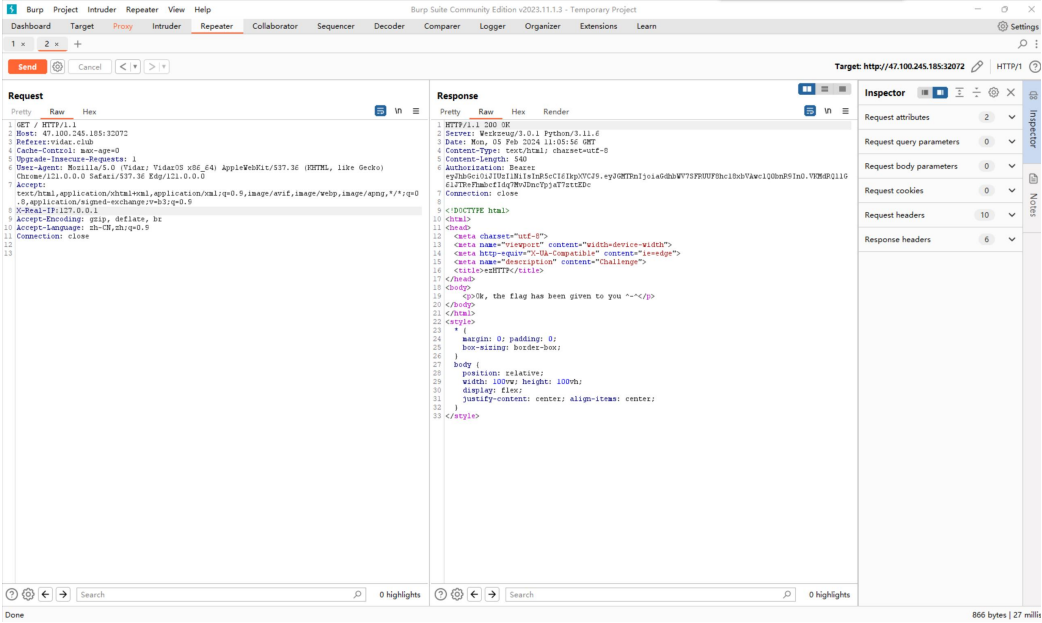
从 vidar.club 访问说明要改 referer，那就先打开 burp， 改 Referer 为 127.0.0.1，显示



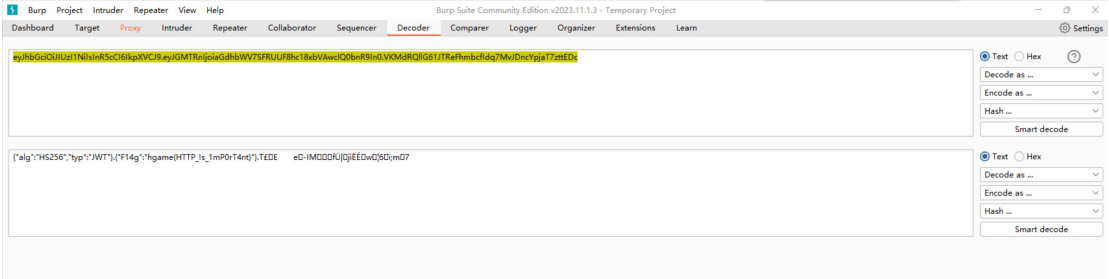
然后看格式将 User-Agent 改为了



从本地访问，说明要伪造 IP 为 127.0.0.1 后来发现用 X-forwarded-For 还是原来的页面，我就去搜，发现了其他与 xff 类似的表达，最后为



最后将 Authorization: Bearer 后的一串字符提取，用 base64 解码可得 flag



# Bypass it

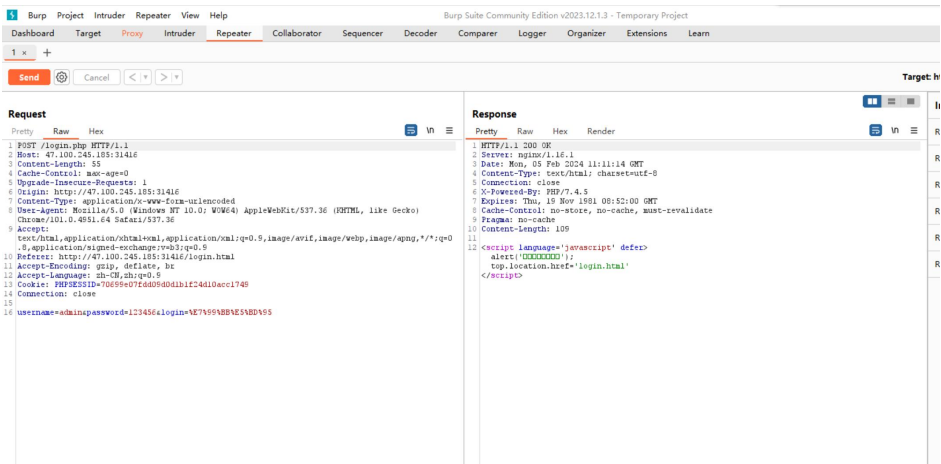
先打开网址



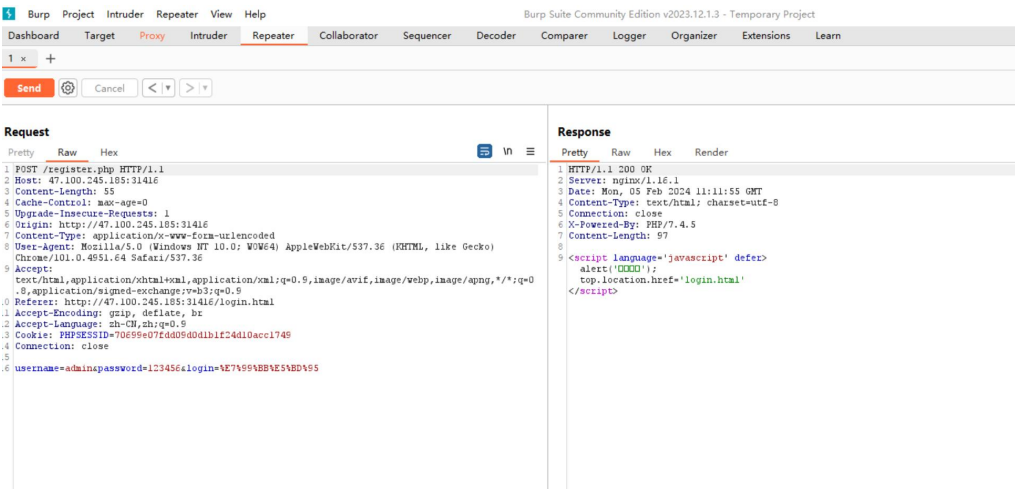
再随便填个用户名密码发现错误，然后尝试点击注册



说明应该尝试绕过这个注册弹窗，先打开 burp



将 POST 的网址改为 register.php



说明注册成功了再将注册的用户名密码填入

个人主页 | <http://47.100.243.103:31410/user/index.php>

京东商城  天猫精选  爱淘宝  糖果办公  7K7K小游戏  小红书

## 你好! 欢迎来到个人中心!

- [~Click here~](#)
- [注销](#)

就可得 flag

hgame{69e7985990c325cda128d9c491d2f287139774c2}