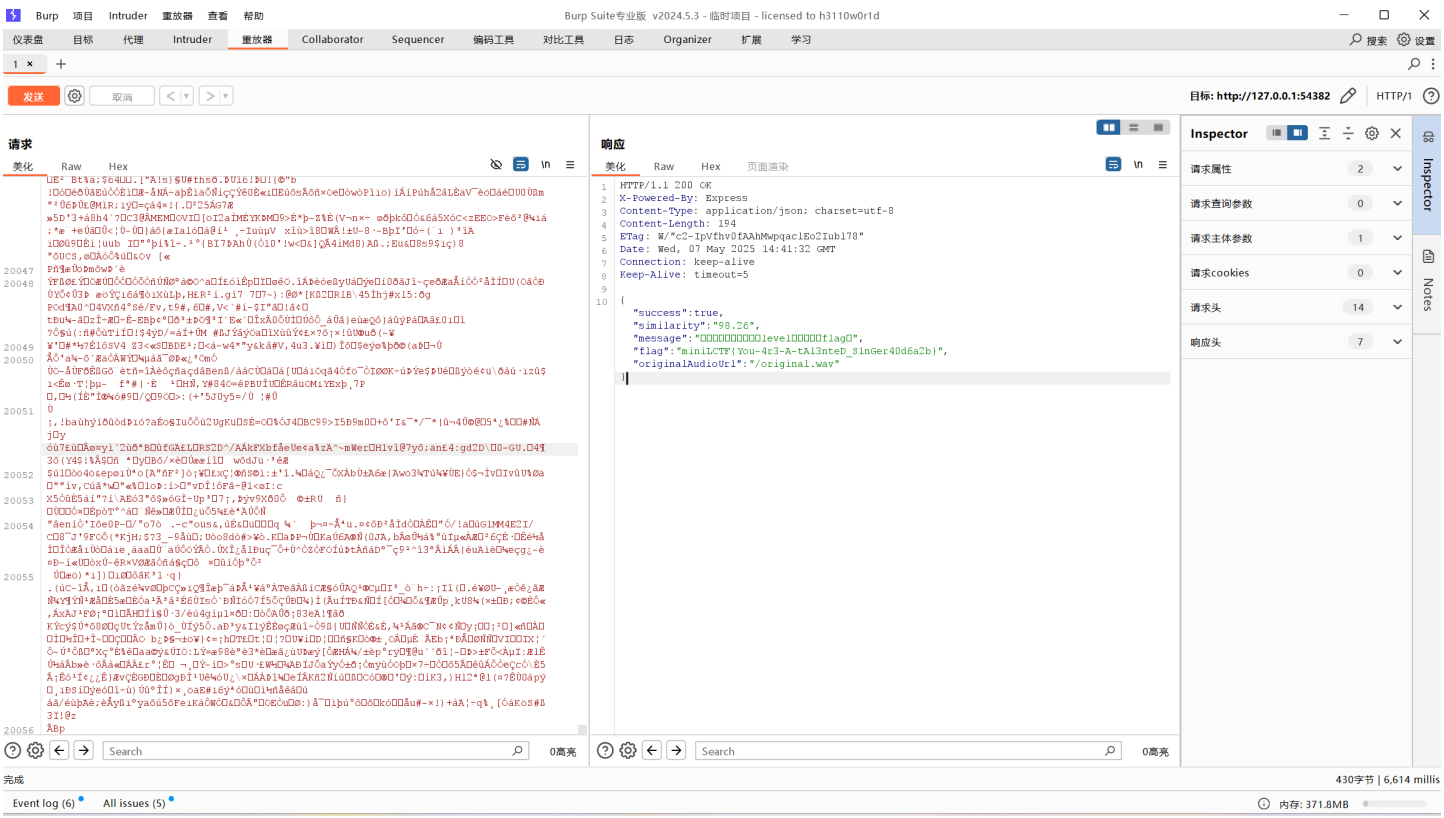
Lub的miniLCTFwp

misc

麦霸评分

点开后是一个网页，网页里能看到一段音频和录制音频的按键，先把原音频下载下来，然后开启录制音频和burpsuite拦截，结束录制拦截到上传的文件，将原来录制的文件替换成刚刚下载的原音频后拿到flag

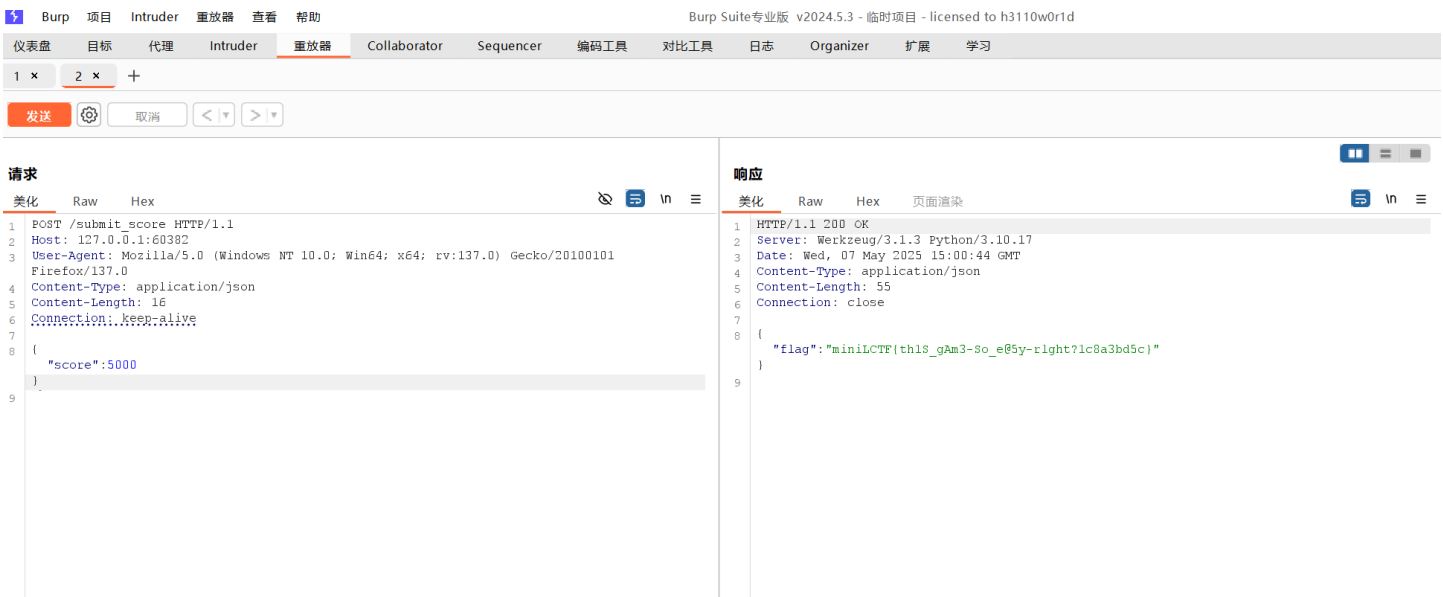


吃豆人

打开后是个网页，看小游戏的源代码发现获得flag需要的请求报文的格式

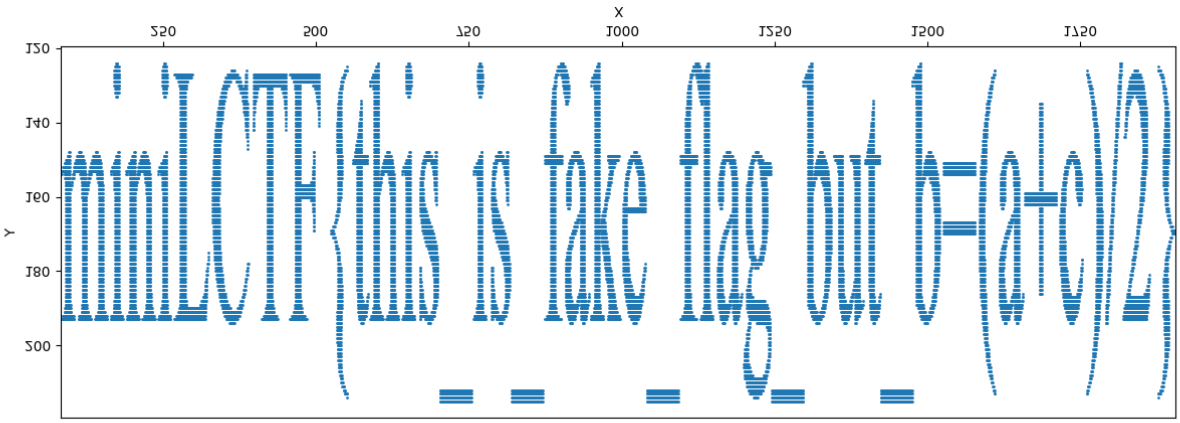
```
// 胜利检测
if (score >= 5000 && !hasGotFlag) {
    fetch('/submit_score', {
        method: "POST",
        headers: { "Content-Type": "application/json" },
        body: JSON.stringify({ score: score })
    })
        .then(response => response.json())
        .then(data => {
            if (data.flag) {
                alert("🎉 恭喜！你的flag是: " + data.flag);
            } else {
                alert("未达到指定分数！");
            }
        });
    hasGotFlag = true;
}
```

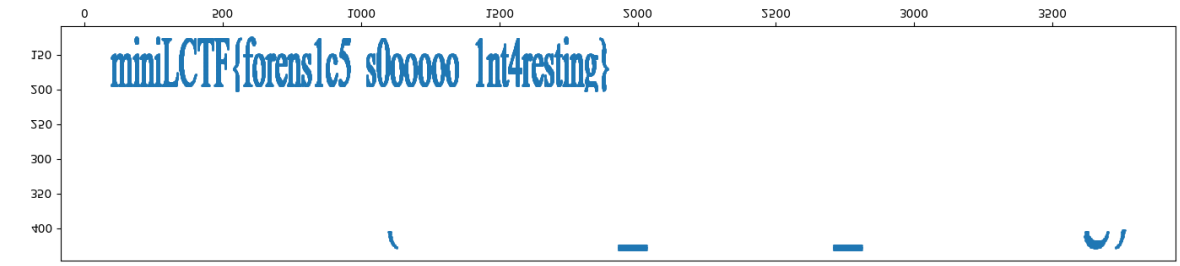
用这个修改请求，用burpsuite发送获得flag



MiniForensics I

打开虚拟机后发现桌面有一个流量包和一个“b.txt”，再打开c盘，找到user/document目录下的隐藏文件夹“nihao”，里面有压缩包和一个pwd.txt，从pwd.txt得知ai.rar的密码是七位数字，直接用hashcat爆破得知密码是1846287，打开后里面是一张图片，一个ssl.log和hahaha.txt，配置ssl.log到wireshark，解密流量包，提取出d盘的恢复密钥521433-074470-317097-543499-149259-301488-189849-252032，打开d盘，有一个看不到的文件夹，打开里面是c.txt，用c.txt的数据画散点图，然后转180°，再镜像得到提示“b=(a+c)/2”，用这个公式得到a，再用a画出散点图得到flag


X
Y
miniLCTF{this is fake flag but hahaha}


miniLCTF{forens1c5 s0oooo 1nt4resting}