无回显 SSRF(时间判断)
中

点击保存头像,开启 burpsuite 抓包

可以看到 avatar 的一个参数,采用的是请求其他地方的图片,此时我们对这条 URL 进行修改
凭借 dnslog 并用#注释掉后面的 URL 地址

DNS Query Record	IP Address	Created Time
9jrw2m.dnslog.cn		2022-07-02 11:12:32

发现这边收到了请求

此时查看回显包发现响应的时长 0.3 秒
然后替换地址为 127.0.0.1 也就是本地的地址

发现响应的时长为 1.125 秒
此时依次替换为 172.16.1.1 和 192.168.1.1
发现响应的时长都为 6 秒以上

也就是说我们可以用时长来判断内网中是否存在这个地址