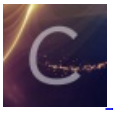
bugku-writeup-web-game1

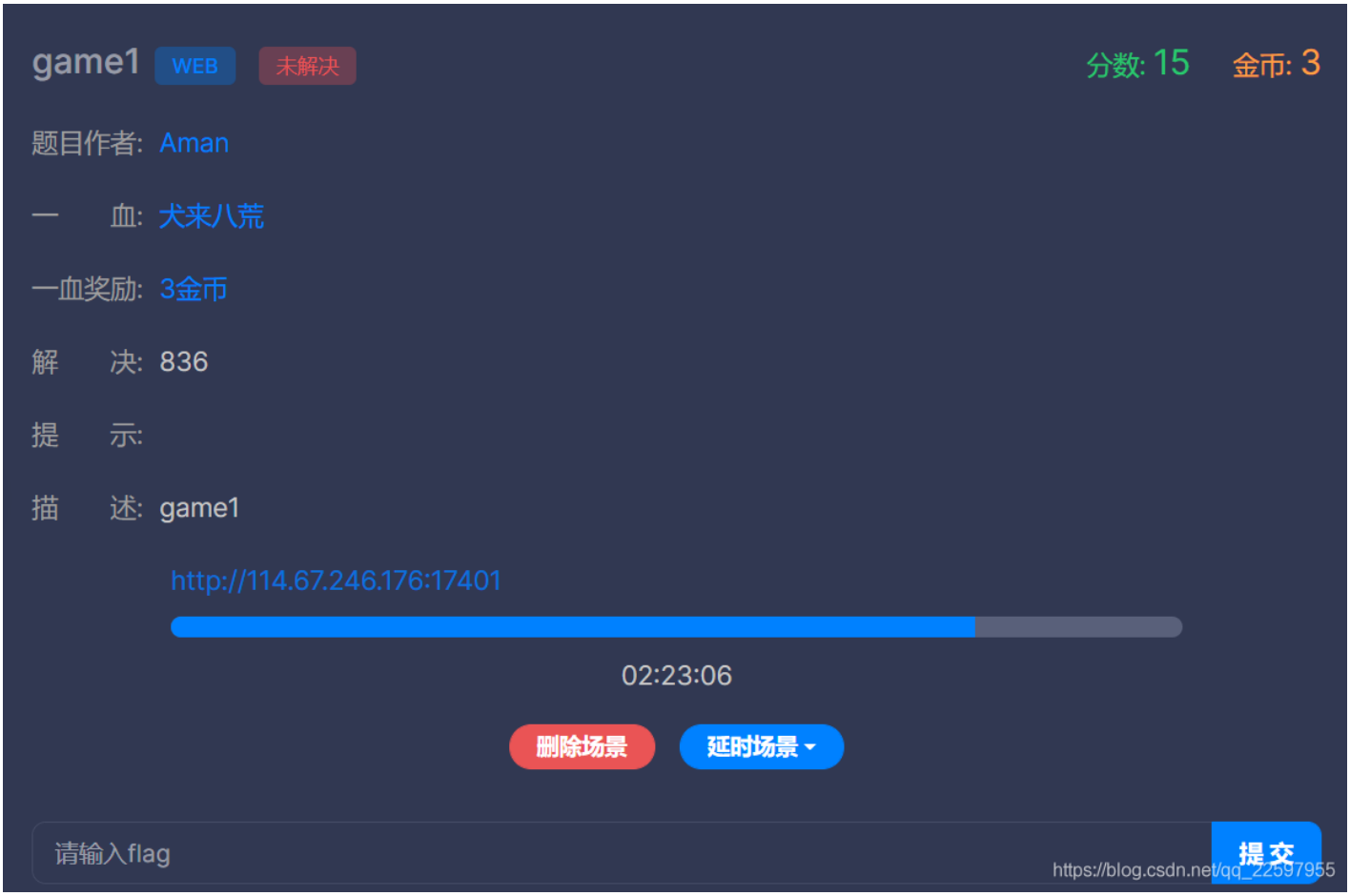
原创

dark2019 于 2021-06-27 12:00:48 发布 17 收藏
分类专栏： wp 信息安全 文章标签： php

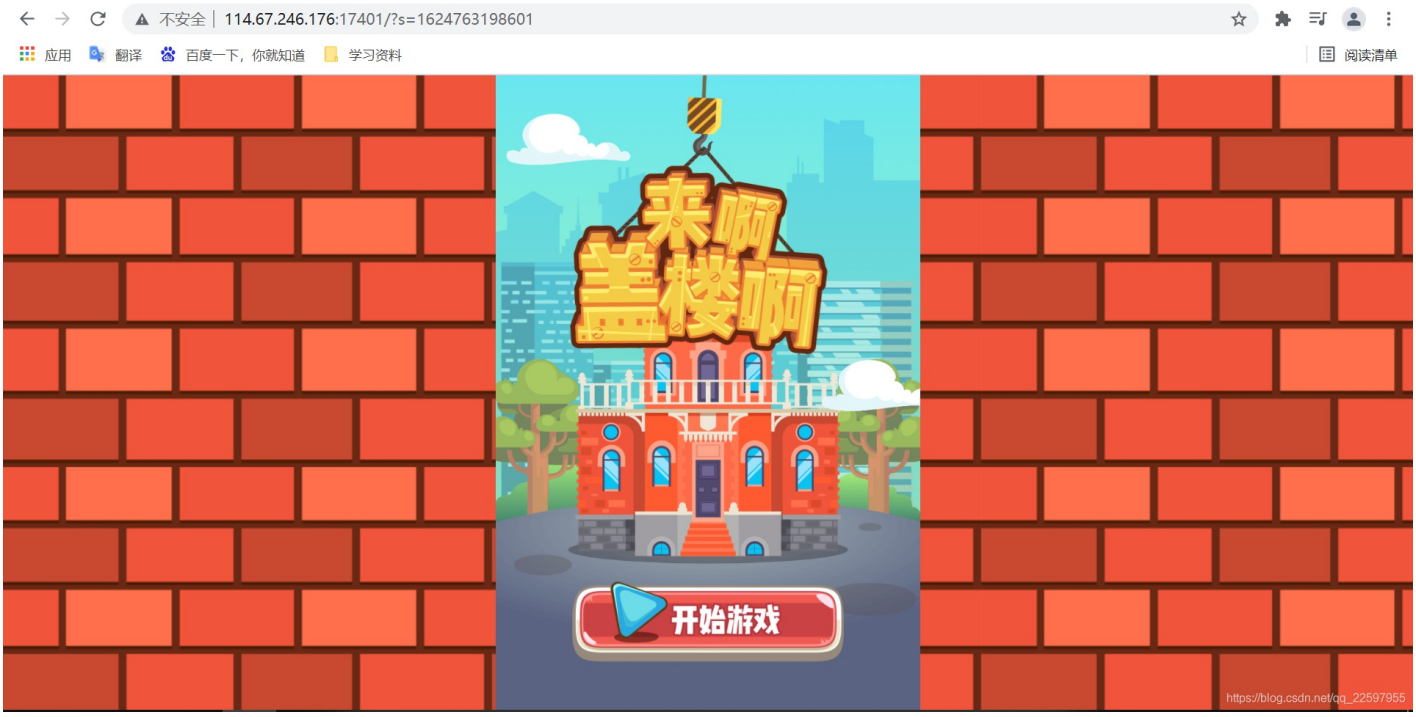

wp 同时被 2 个专栏收录
31 篇文章 0 订阅
订阅专栏


信息安全
53 篇文章 1 订阅
订阅专栏

题目： **game1**

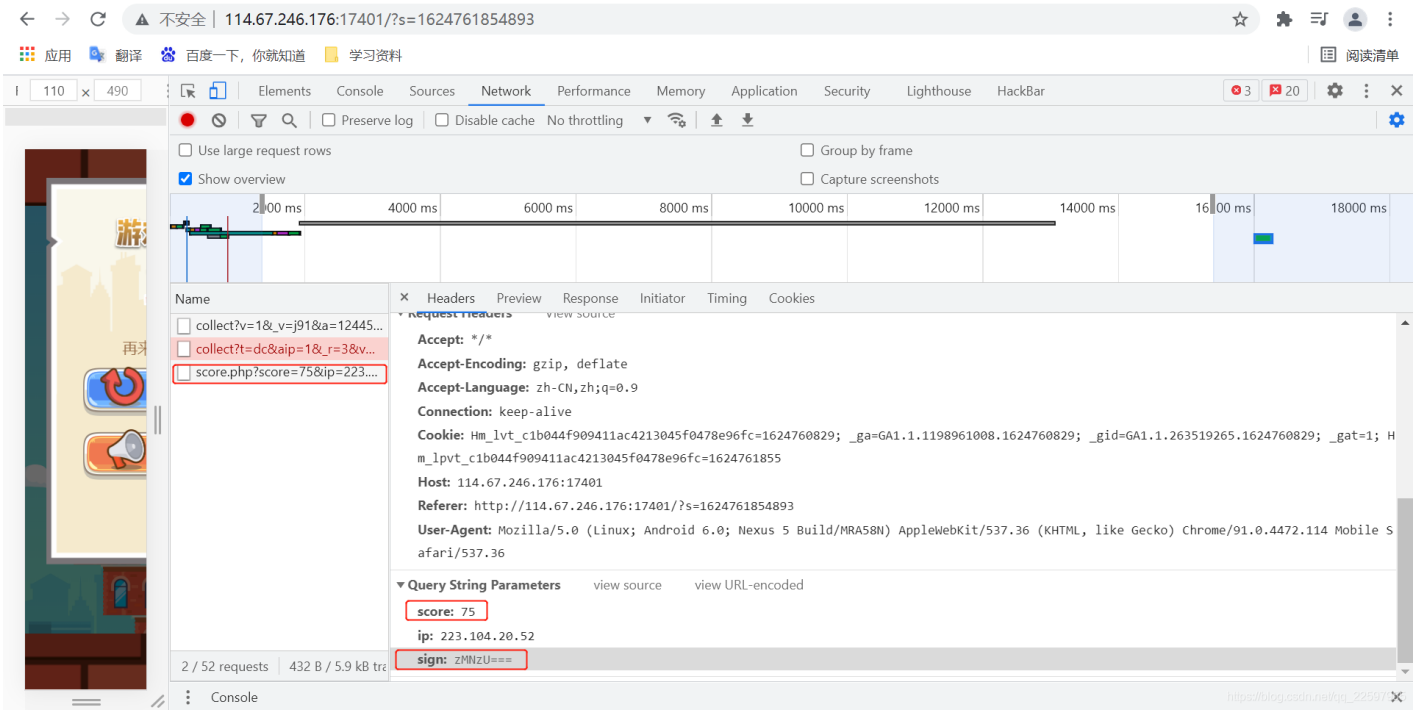


01—看源码

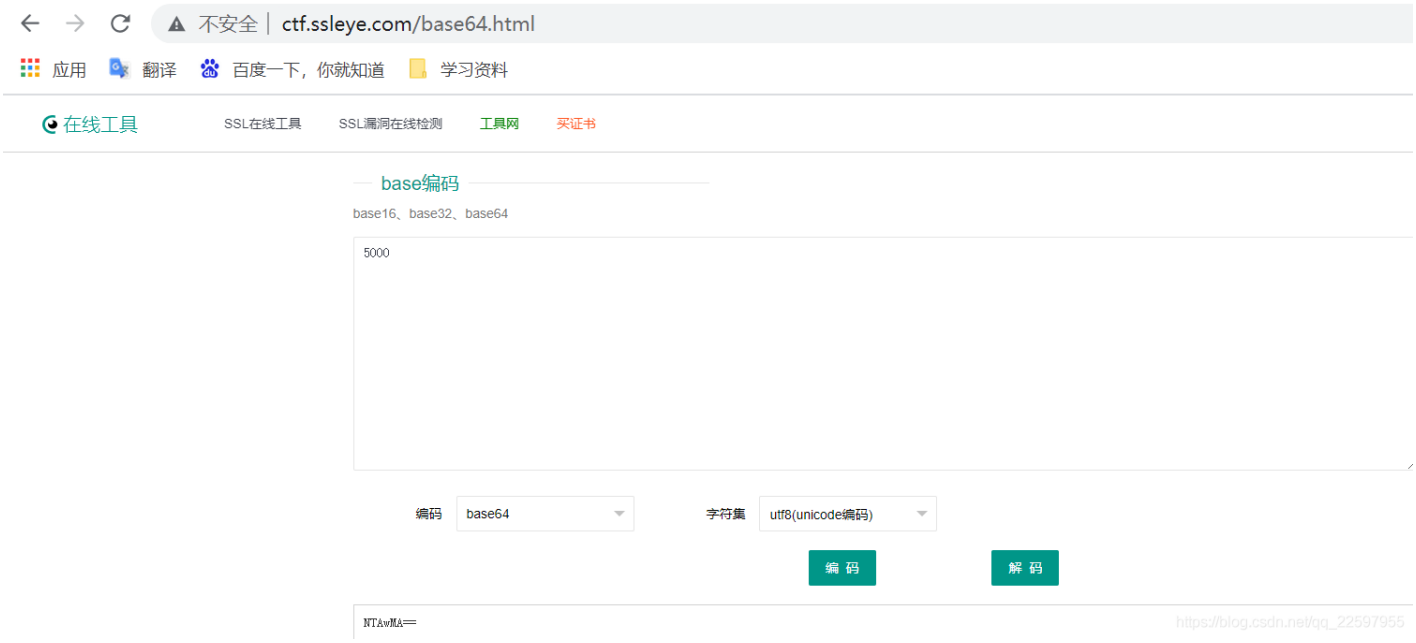


a.启动场景，是一个盖房子的游戏，先来玩一下吧！

b.纯靠玩游戏是找不到flag的，可能要通关才行，但是通关好难啊，看看源代码吧！

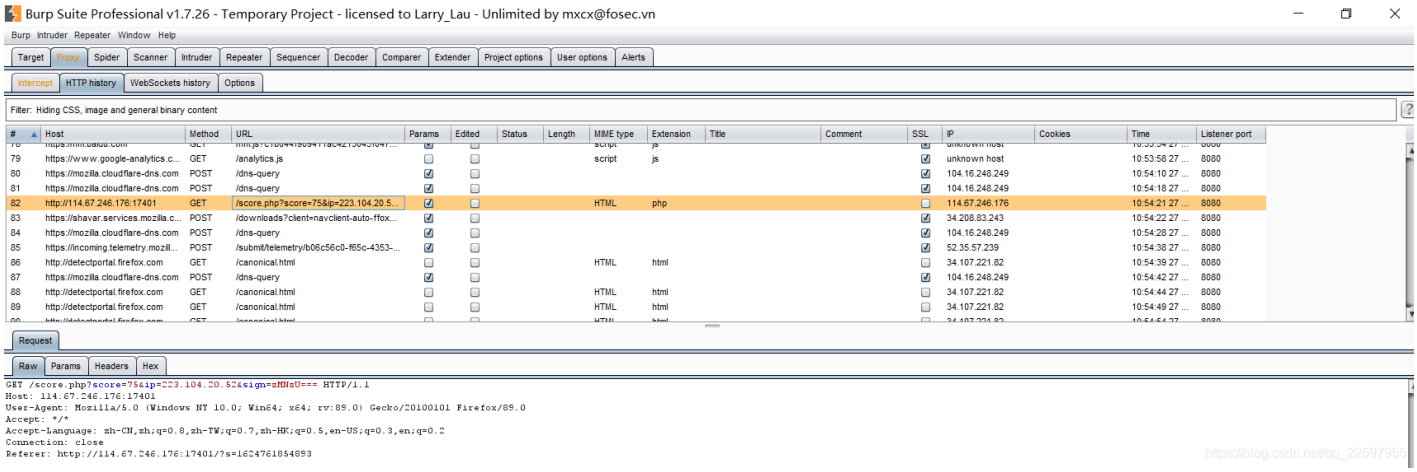


c.**F12-Network-ctrl+r** 发现有一个score.php文件，score=75时，sign为zMNzU===，75的base64编码为NzU=，因此sign表示在zM+score的base64编码。

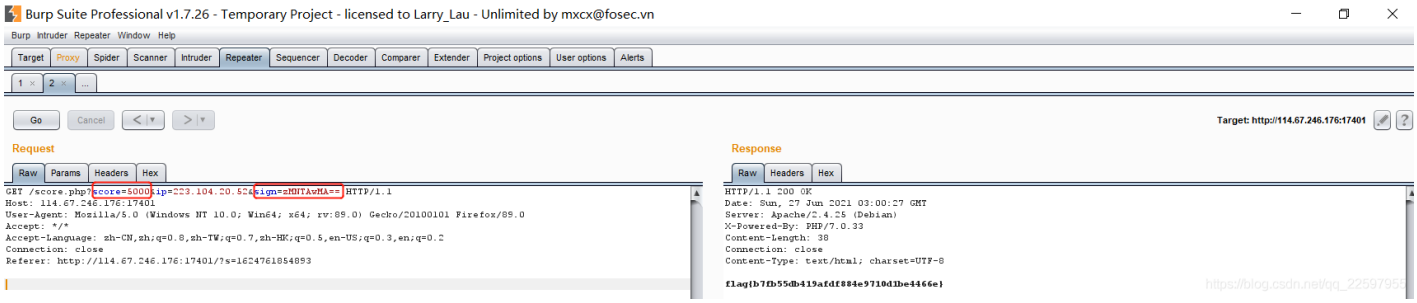


将score改为5000，同时base64编码得到sign:zMNTAwMA==

02—burp抓包



将score.php抓包并发送repeater



修改score和sign, go,得到flag。（试过9999也可以，尝试大一点的分数即可）