攻防世界-upload1

原创

贰伍捌柒 于 2021-07-05 11:19:42 发布 63 收藏

文章标签： web 信息安全 安全 经验分享

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/u258710/article/details/118485382

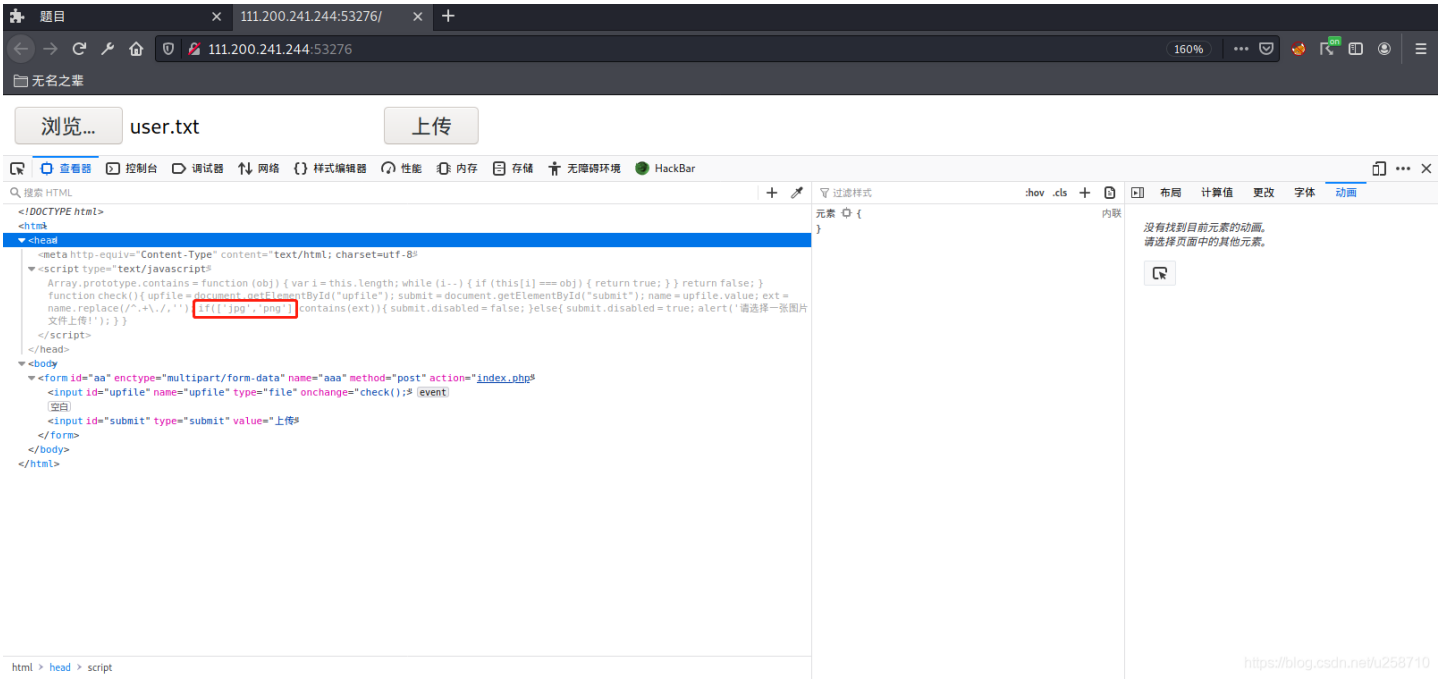
版权

攻防世界-upload1

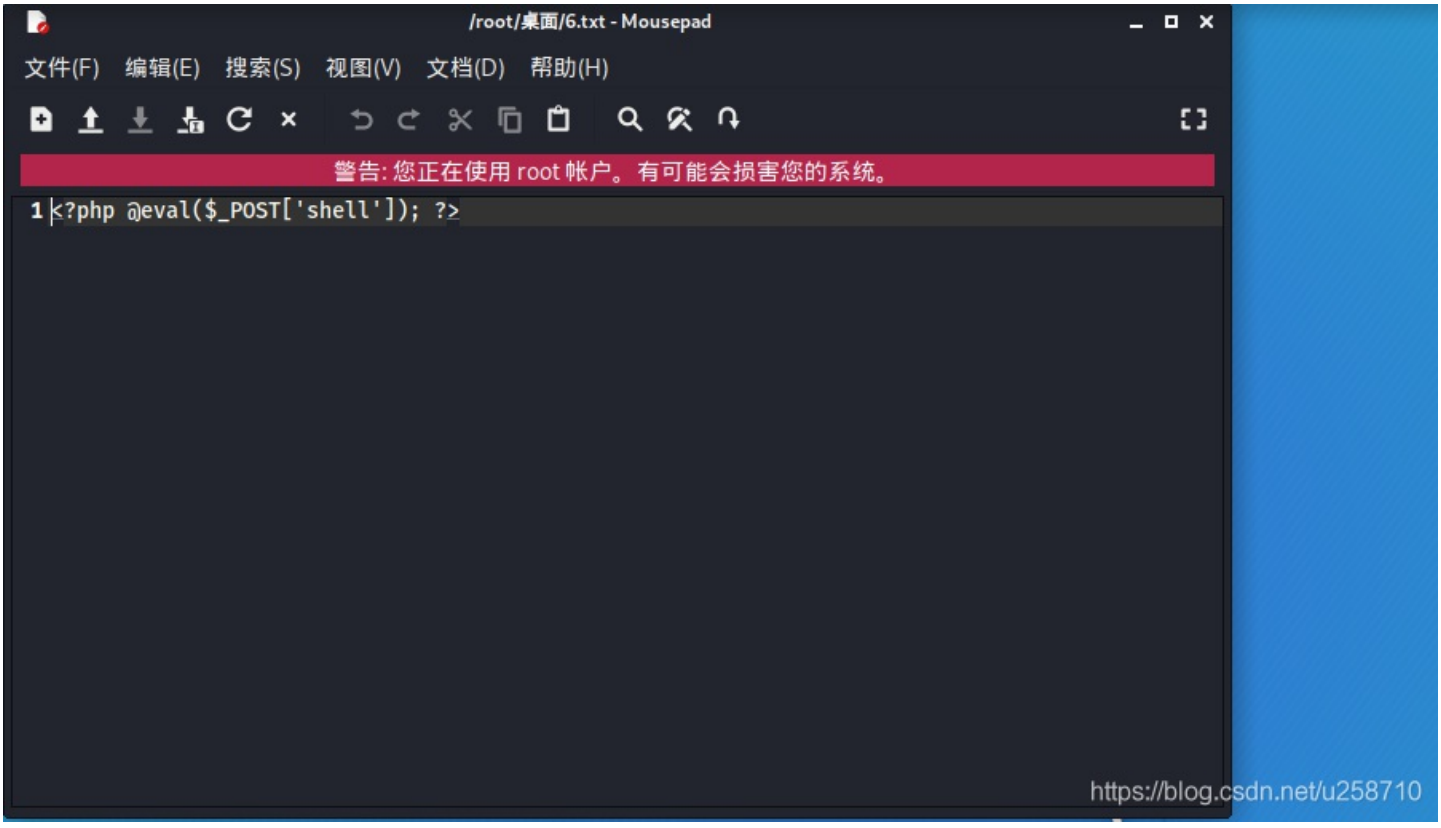
https://blog.csdn.net/u258710

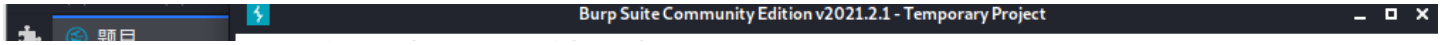
打开之后发现是一个上传页面，第一想法上传一句话木马，使用菜刀连接，尝试发现只能上传图片

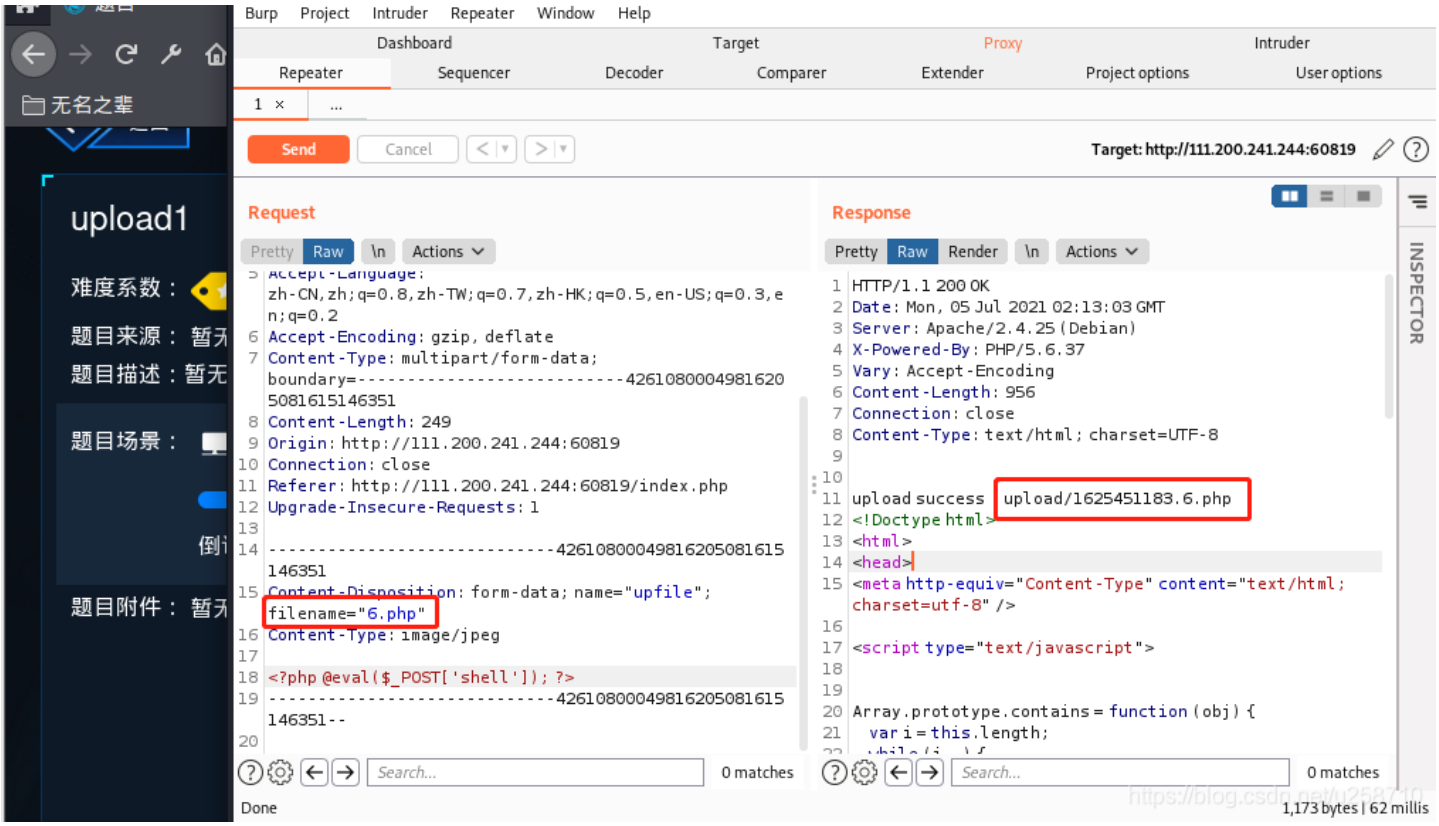
F12查看源码，发现 if(['jpg','png'].contains(ext))，就禁止报错弹窗。既然过滤是在前端，想到使用burpsuit抓包，修改后缀名



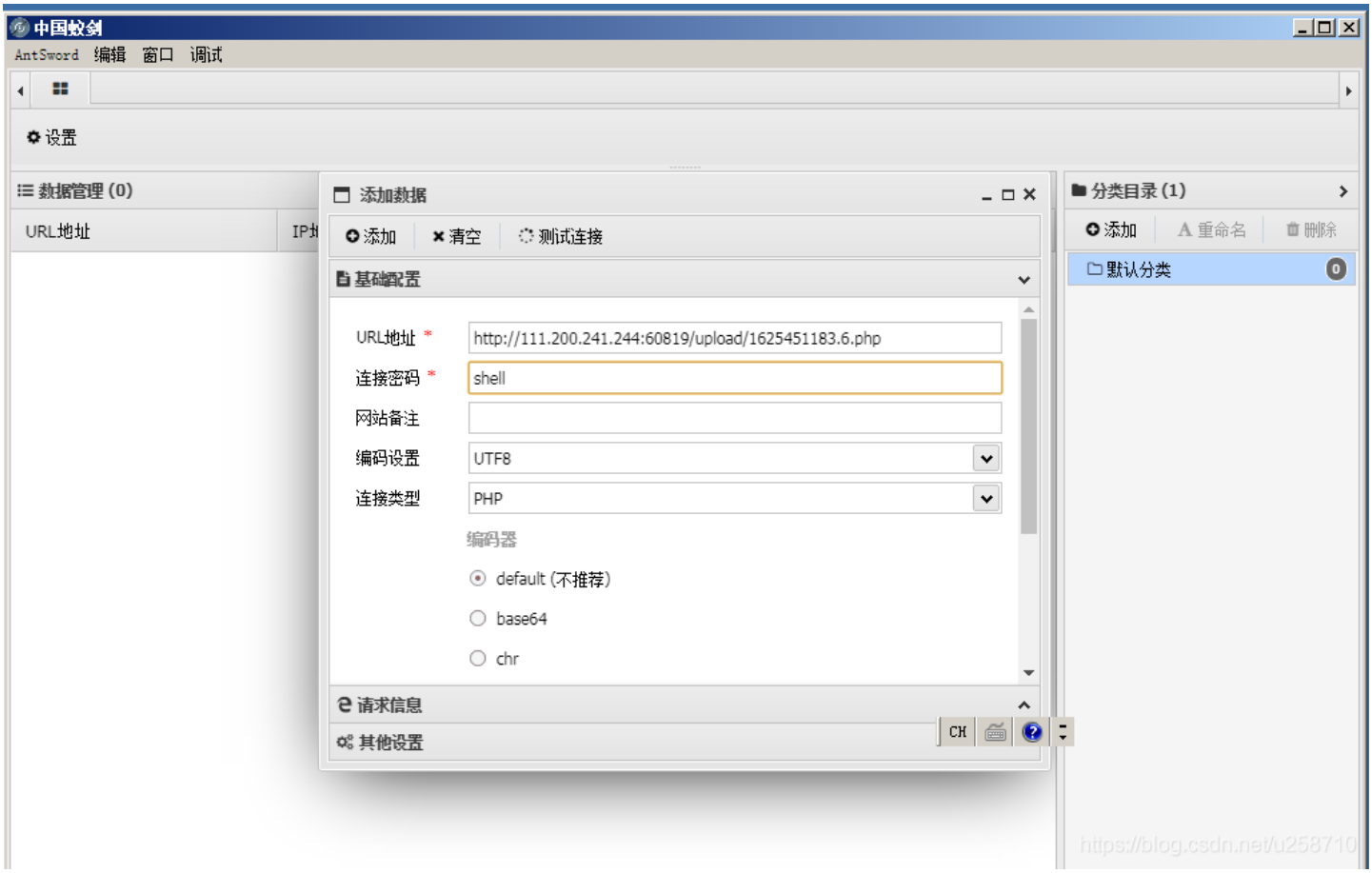
写一句话木马并保存文件格式为.jpg，使用burpsuit抓包，修改后缀名为.php。

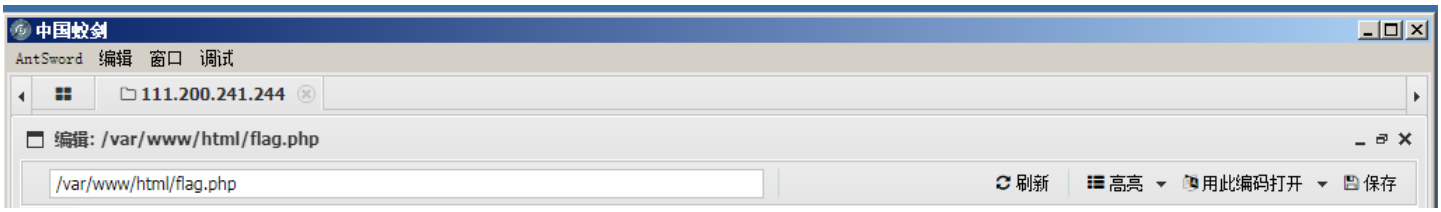






我这没装菜刀，使用御剑连接





发现flag：cyberpeace{789aee8b9c1dbec5bd9e01a8673afc9d}