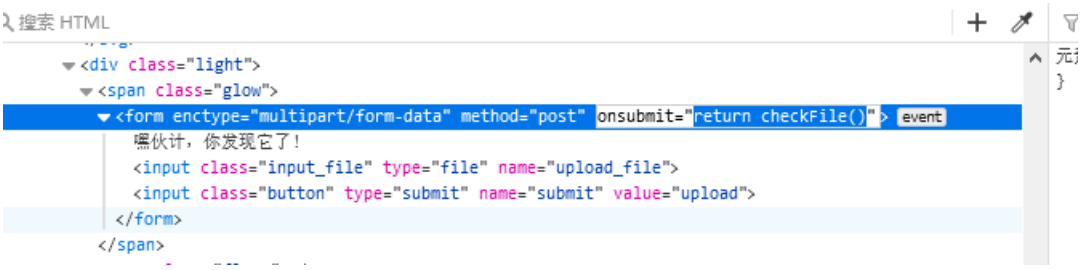
[ACTF2020 新生赛]Upload -wp

原创

冰可乐不加可乐 于 2020-06-29 19:38:35 发布 1272 收藏 2

把鼠标移到灯泡处的时候发现上传处

任意传了个文件上去，弹窗只能穿图片格式，本来是想抓个包看看，发现挂了代理还是会弹窗提示，意识到是前端过滤



删除check就可以绕过了

上传php文件发现还存在后端过滤
把后缀改为phtml即可上传
没其他过滤，直接上传一句话
接下来蚁剑或菜刀连接即可