Buuctf [ACTF2020 新生赛]Upload

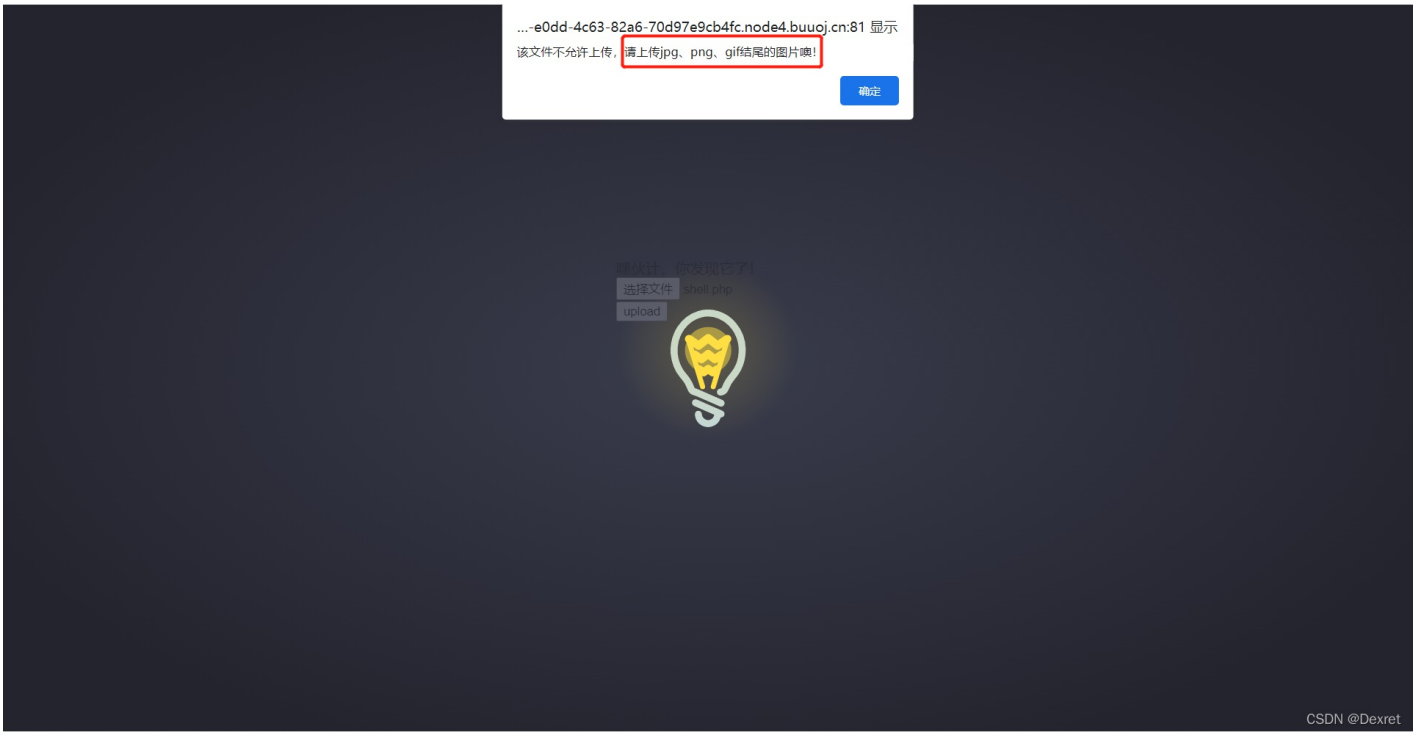
原创

Dexret 于 2021-12-07 17:26:08 发布 205 收藏
分类专栏： buuctf Web 文章标签： php 后端 web buuctf

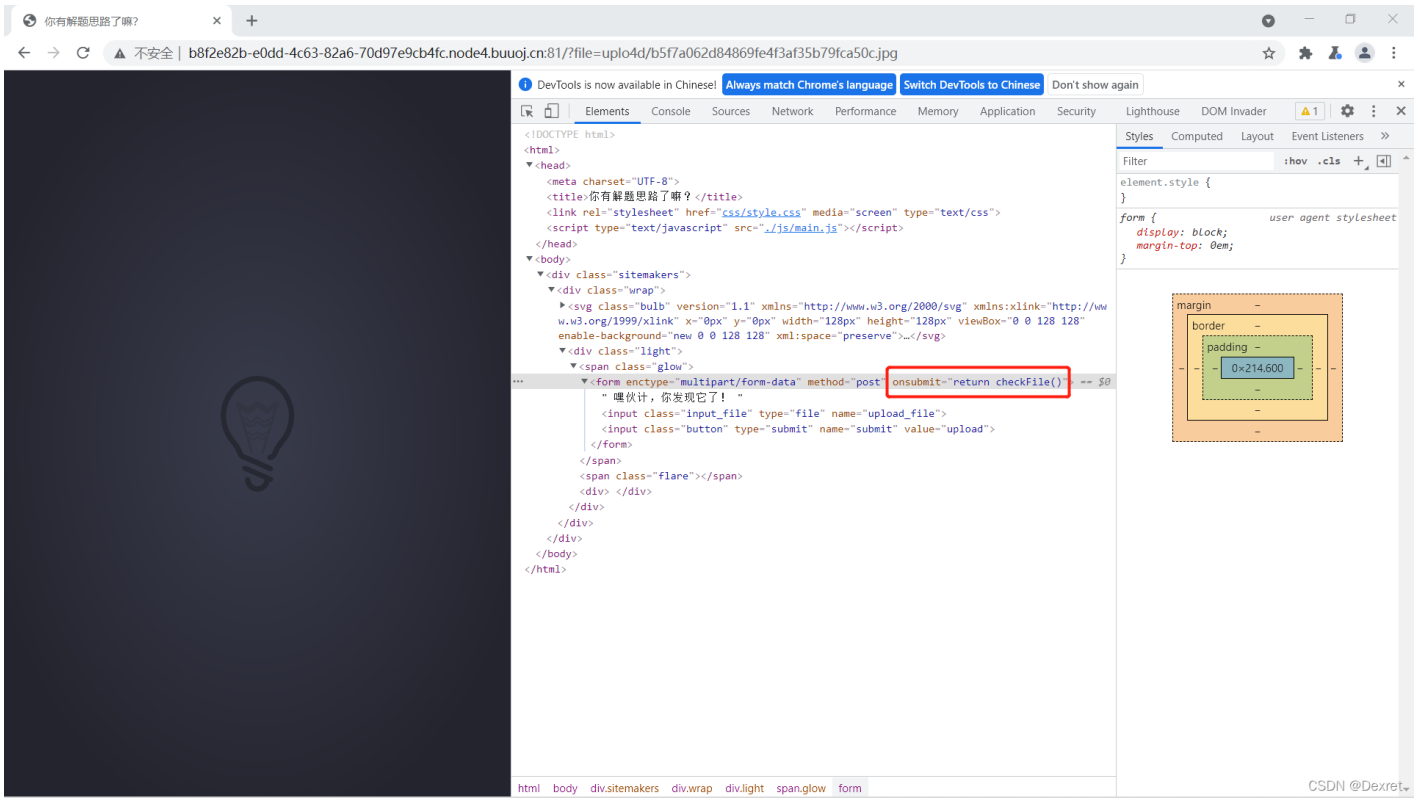
本文链接：https://blog.csdn.net/Dexret/article/details/121774289

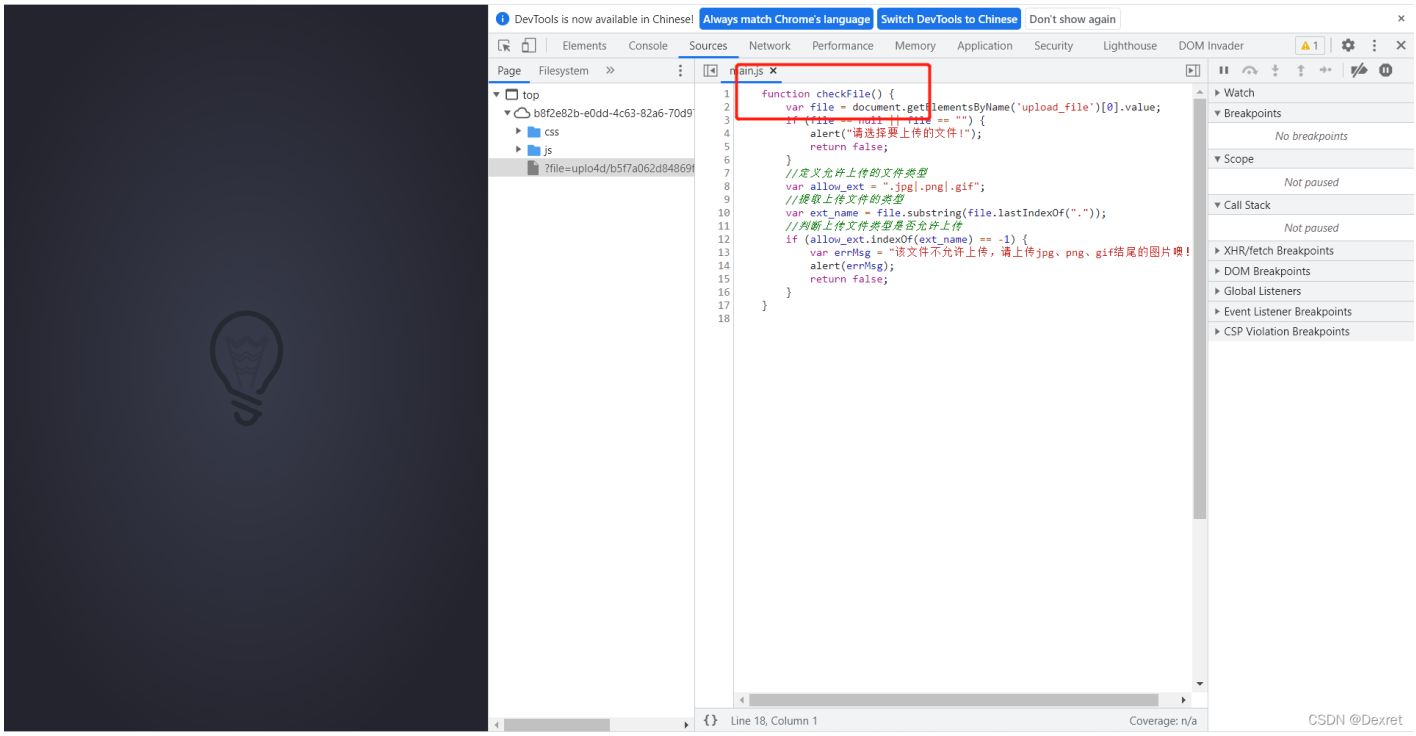
打开该靶机，发现为一个上传图片的网页

尝试上传一个php文件



发现该网页有前端验证，尝试上传.htaccess和ini文件都被拦截





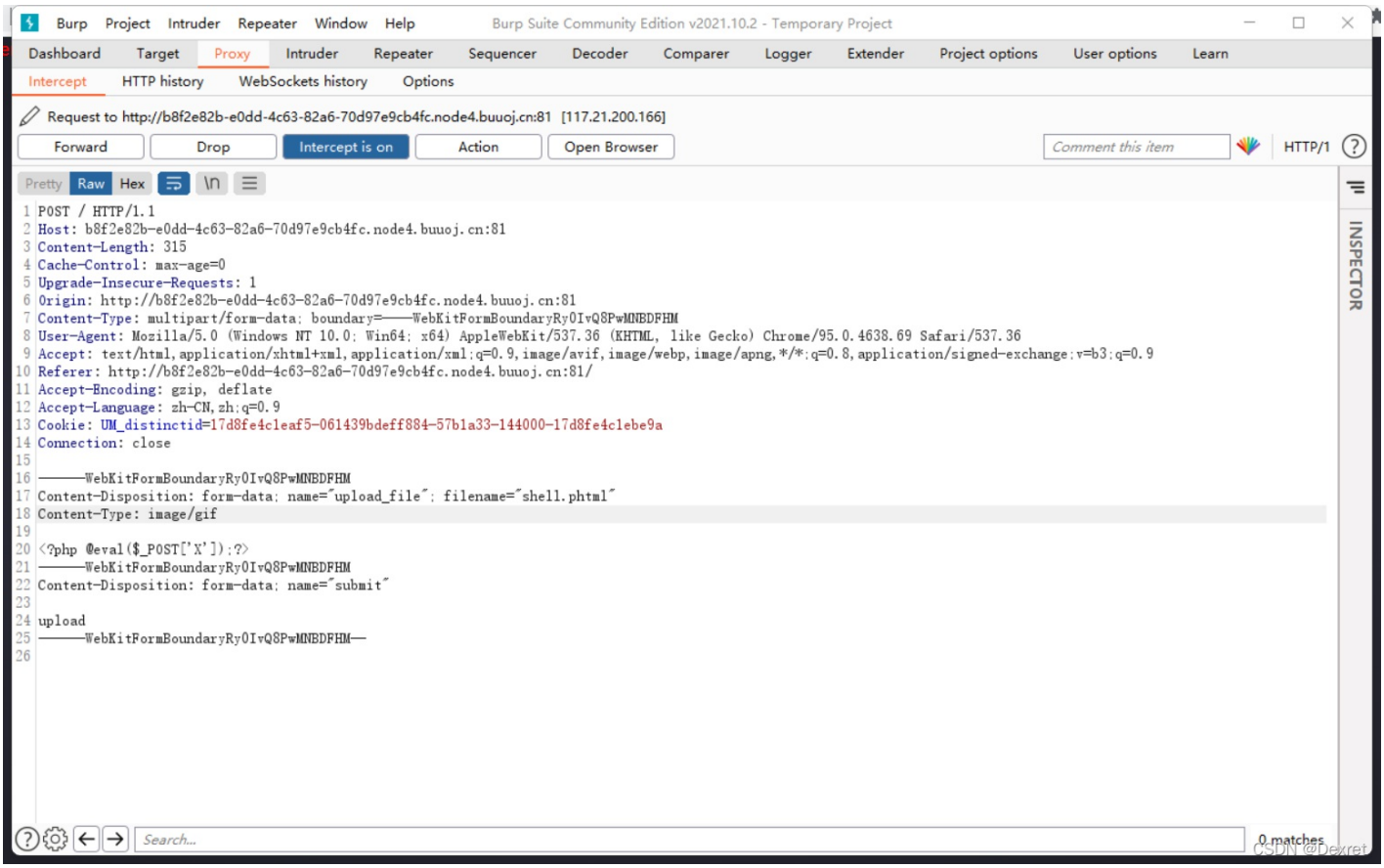
上传一个png文件，利用BurpSuite修改后缀为php，无法上传成功

应该还有个后端验证，那么这道题应该和极客大挑战那个差不多，多了个前端验证

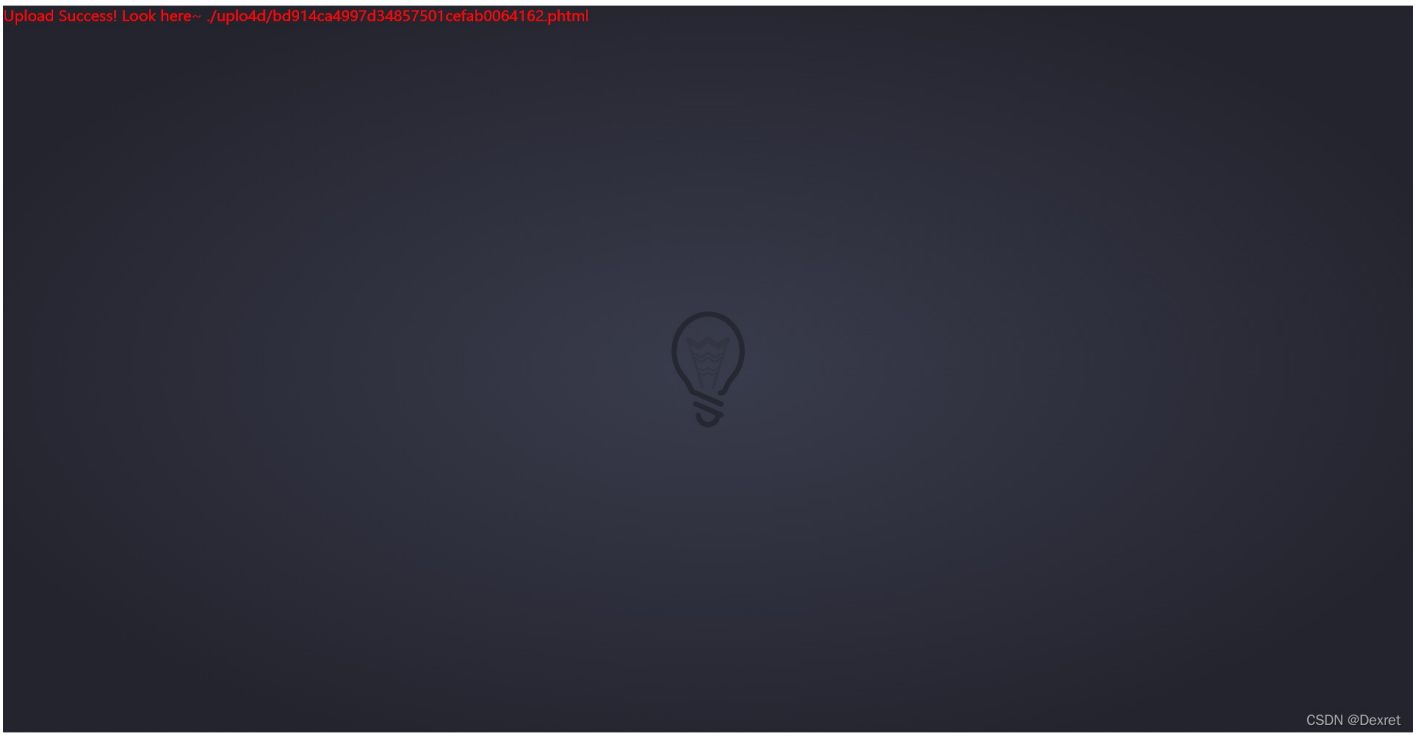
上传一句话木马，将其后缀名改为png进行上传

在上传过程中利用BurpSuite进行抓包

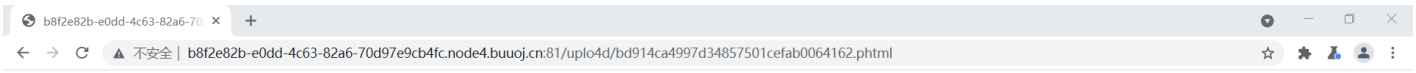
修改后缀名为phmtl



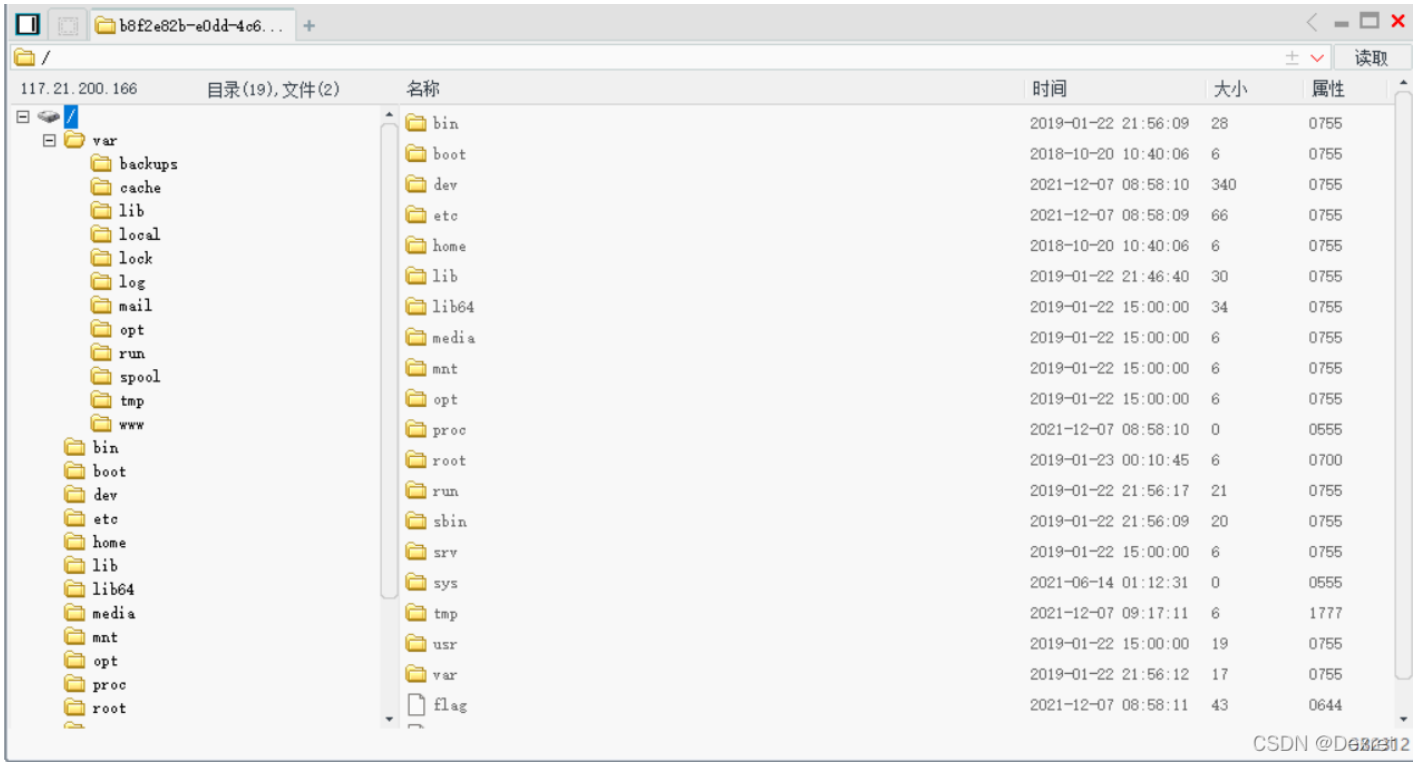
修改后上传，能够上传成功



连接一下上传文件路径



验证该路径存在后，利用中国菜刀对其进行连接



找到其flag文件并打开

得到该题的flag为

```
flag{88ea9a2f-0f90-4f7a-b75b-e6b3438edfc3}
```