Buuctf [ACTF2020 新生赛]Upload

原创

*小瑶 于 2021-06-10 20:29:15 发布 116 收藏 2

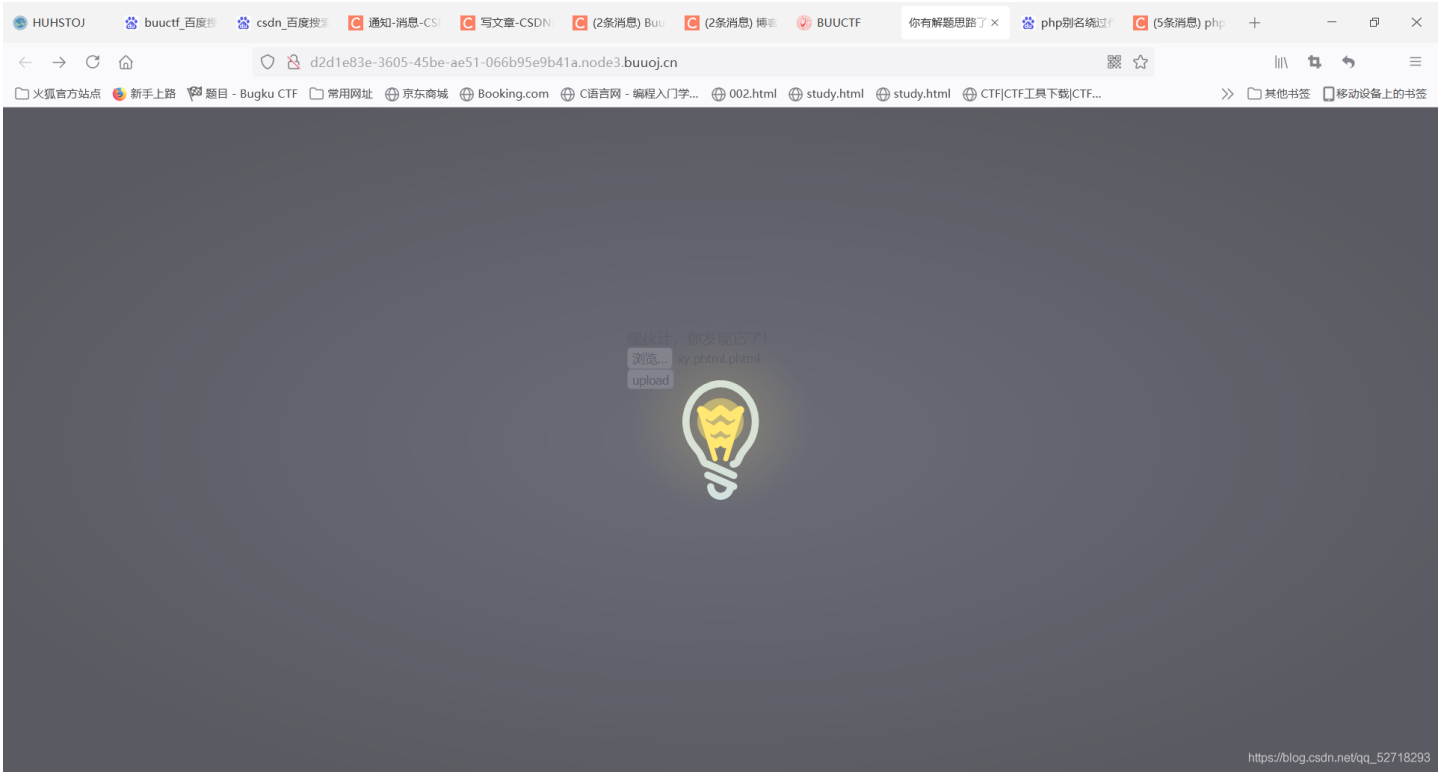
分类专栏： web

本文链接：https://blog.csdn.net/qq_52718293/article/details/117789342

web 专栏收录该内容

32 篇文章 0 订阅

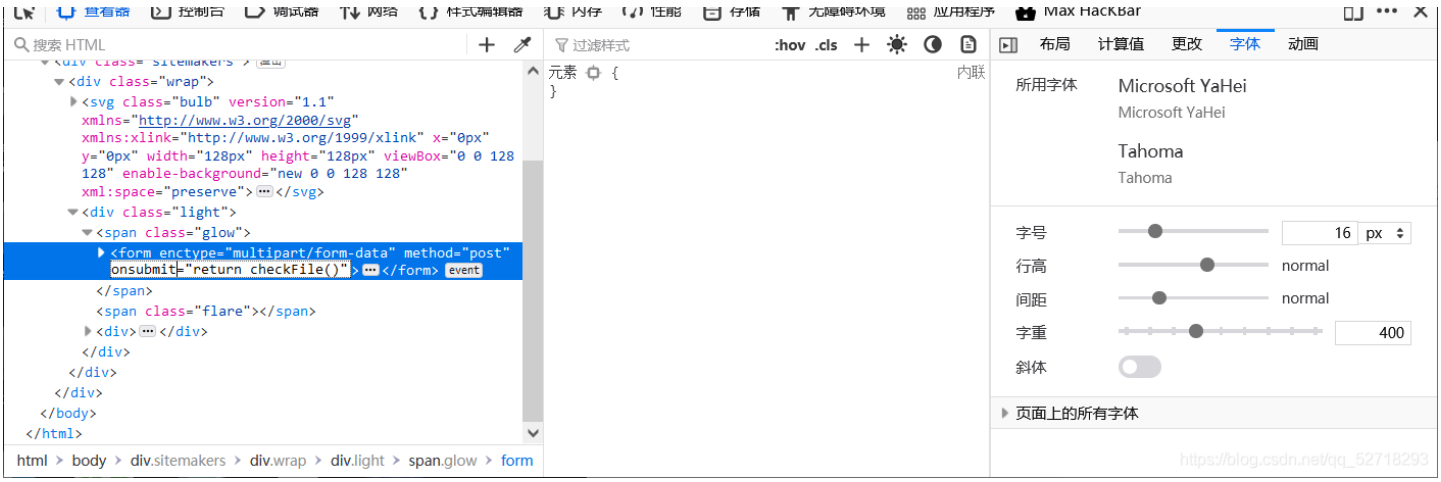
订阅专栏



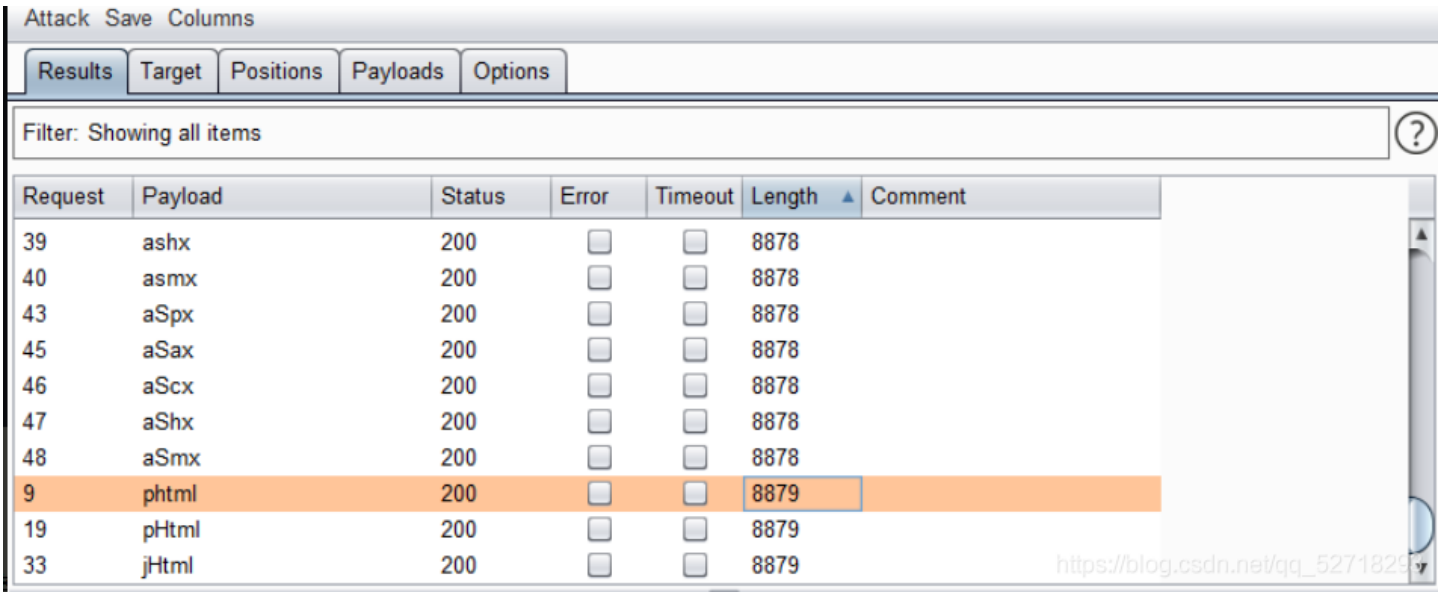
先说本题考点吧：php别名绕过

打开是一个灯泡，要我们上传一个文件（文件上传）发现有上传要求

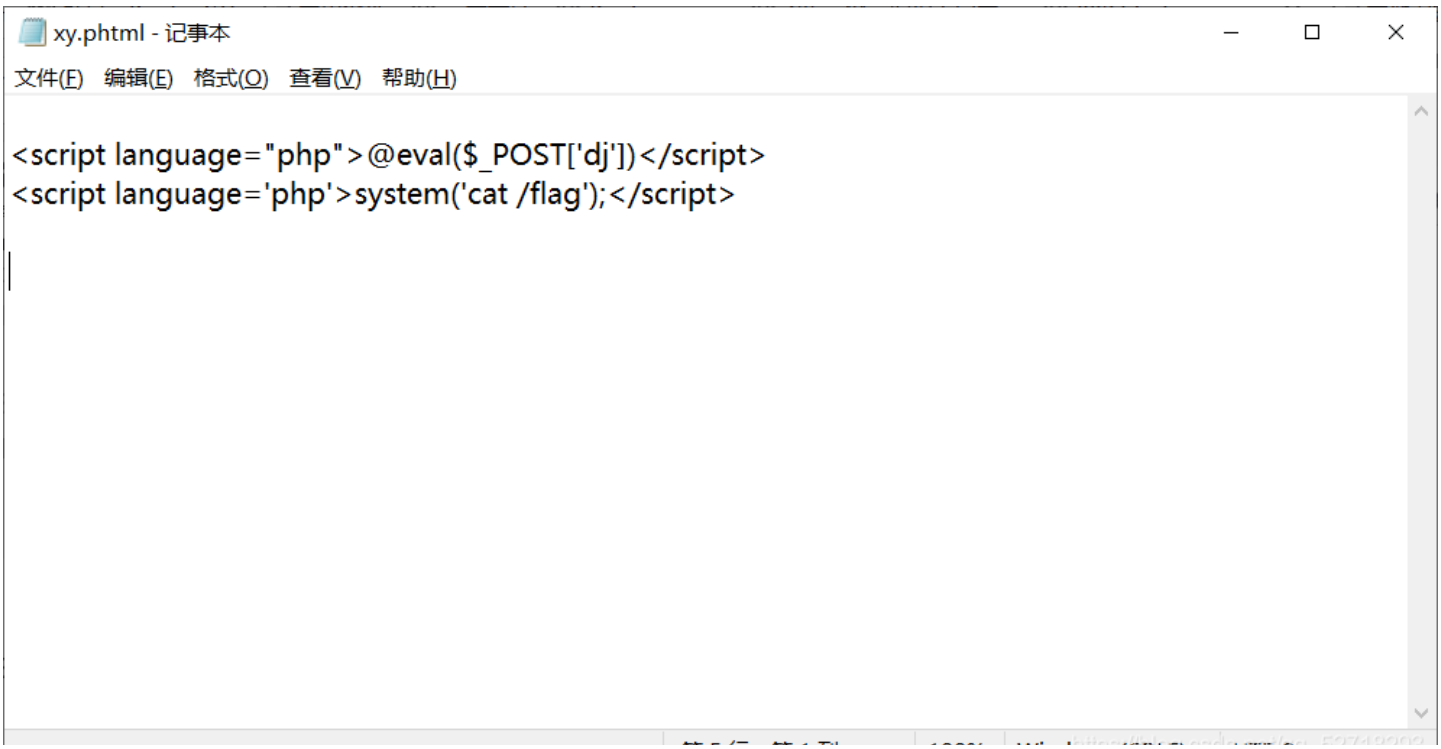
我们可以在前端的html中将下图我标记的白色部分删除即可没有要求

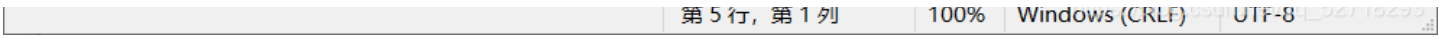


然后我们开始可以试着上传一个php文件，发现上传php文件会被拦截。这种时候我们可以用burpsuite fuzz一下（不会的在文章最后会给大佬的教程） fuzz后发现phtml类型的文件可以上传

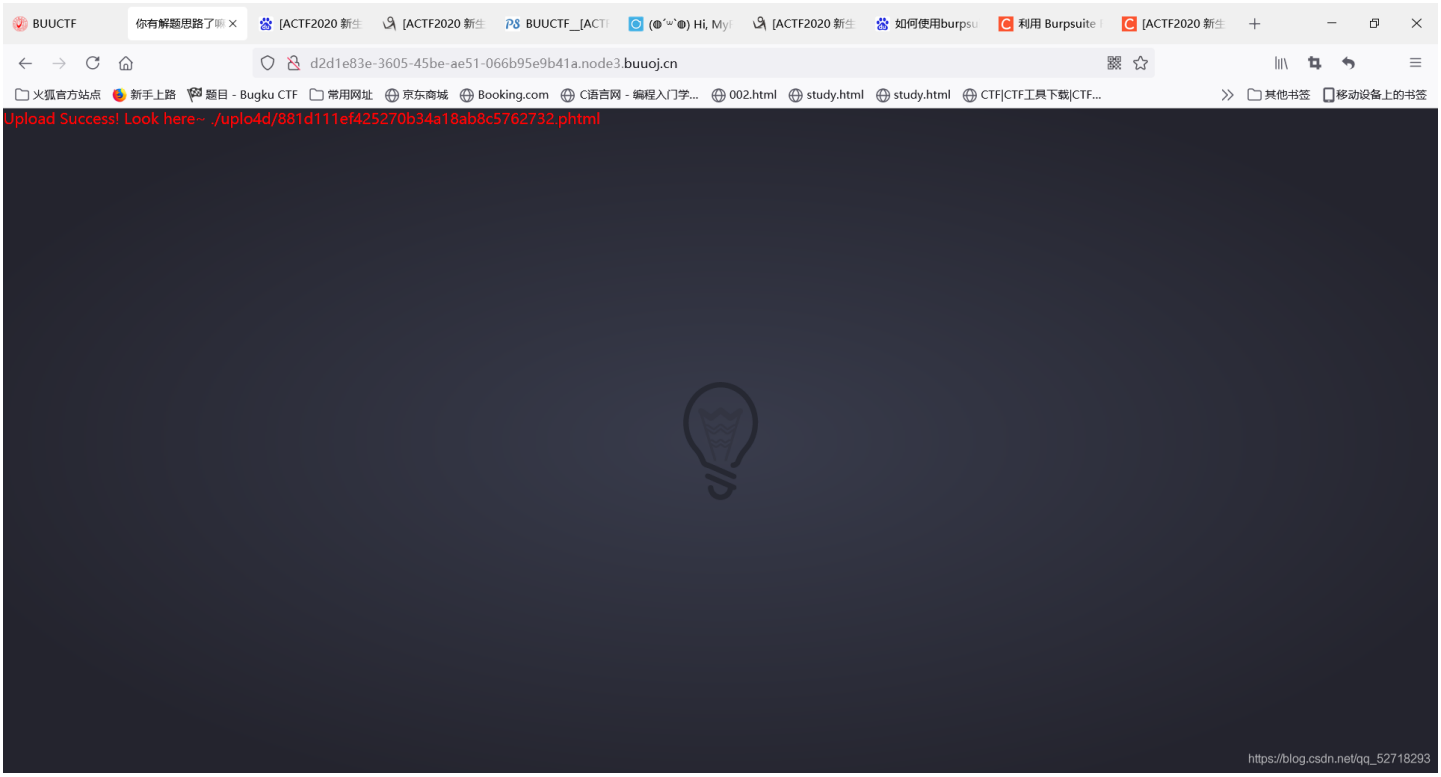


文件里我们写一句话木马，和cat flag

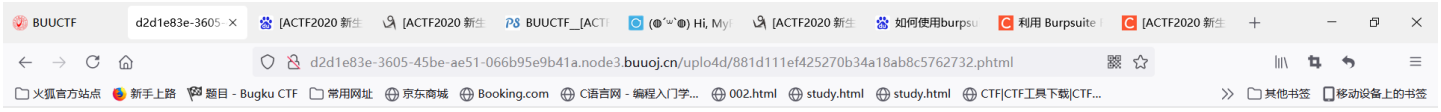




上传成功后即可看到



然后我们url/uplo4d/881d111ef425270b34a18ab8c5762732.phtml
即可看到flag



当然如果我们在文件里不加入cat flag的内容，也可以后续连接蚁剑，同样可以在根目录下找到flag

其实这道题还有很多别的方式拿到flag，但是今天小瑶太累了，你们大致看看就好，说不定以后哪天后再编辑一下这篇文章

最后的最后搬运小能手小瑶小能手又上线了

附赠一个大佬的php函数绕过

大佬的php代码审计之文件上传漏洞

大佬手把手教你如何fuzz