BUUCTF [ACTF2020 新生赛] Upload

原创

Senimo_ 于 2021-01-09 00:21:11 发布

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF ACTF2020 新生赛 Upload writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/112386060

BUUCTF [ACTF2020 新生赛] Upload

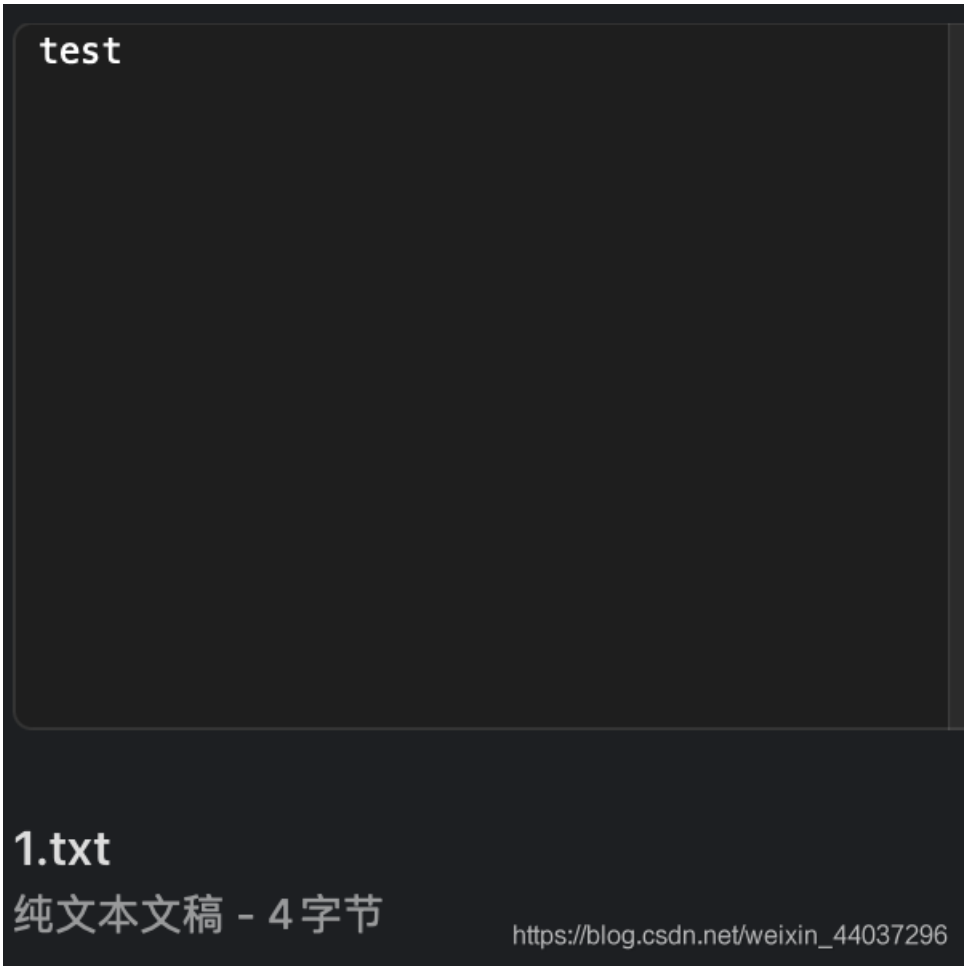
考点：

1. `.phtml`文件上传
2. 前后端限制绕过

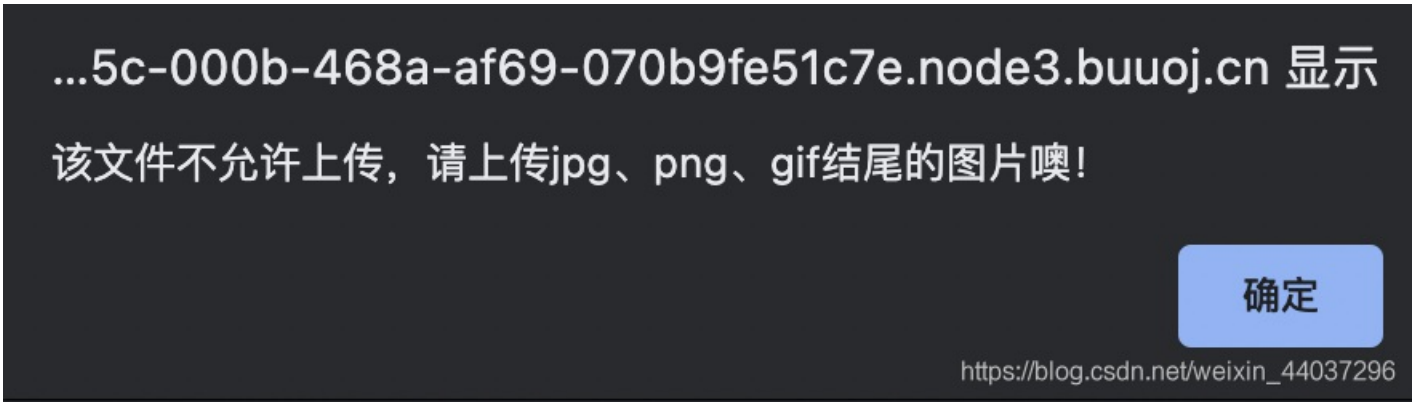
启动环境：

一个灯泡图标，点击的话会出现文件上传点：

随便上传点东西试试：



得到提示：



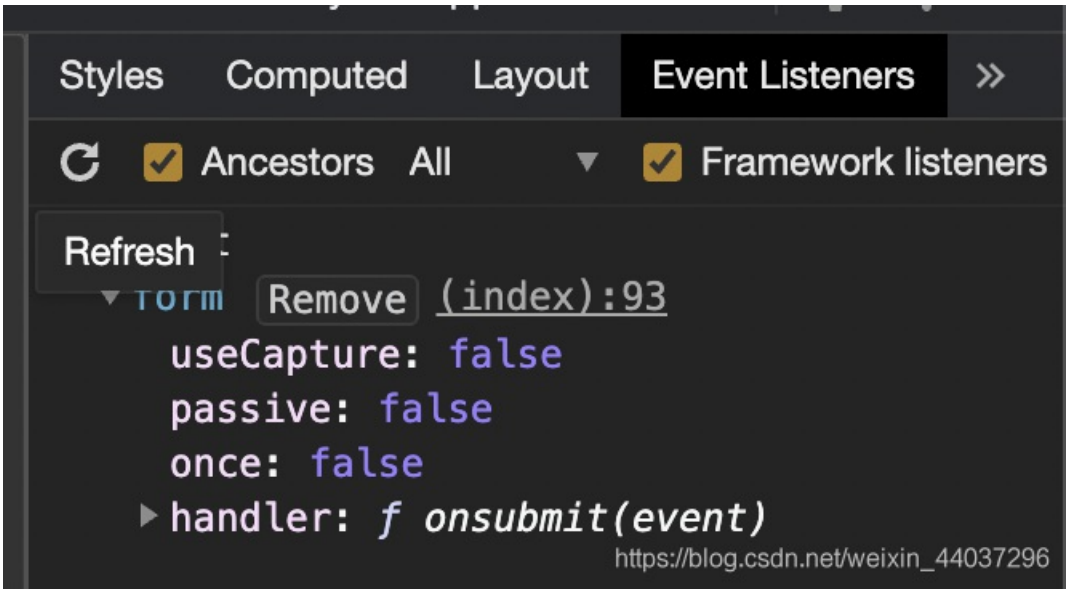
查看网页源码：

```
<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
```

表单提交后会执行`checkFile()`函数，在`main.js`中查看该函数：

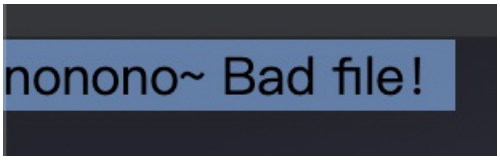
```
function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("请选择要上传的文件!");
        return false;
    }
    //定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));
    //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;
    }
}
```

只是做了前端校验，在上传文件时，将**js属性**删除（Remove）即可：

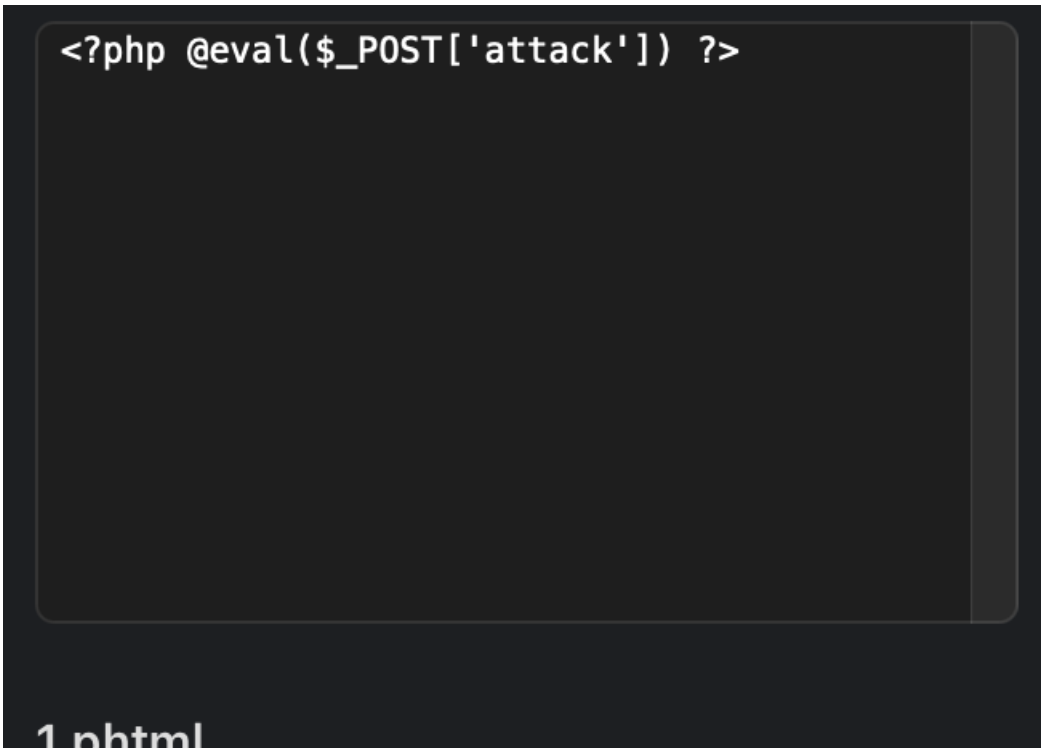


上传写好的一句话木马：

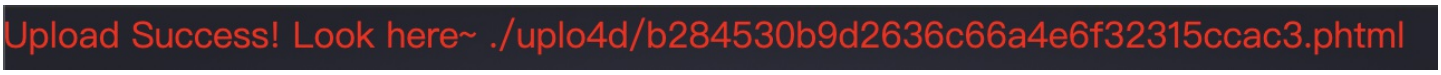
得到回显：



不允许的文件，后端可能也存在验证，尝试`.phtml`文件：



上传成功，回显给出了文件路径：



使用**中国蚁剑**链接：

在根目录下发现flag：