buuctf [ACTF2020 新生赛]Upload 1

原创

hint=flag 于 2021-06-15 14:00:19 发布 93 收藏

分类专栏： 文件上传 web

本文链接：https://blog.csdn.net/hintll/article/details/117922613

文件上传 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏

web

32 篇文章 0 订阅

订阅专栏

看题目的标题应该还是一道文件上传的题目:

打开看看

找到了上传点，先上传一个.php的一句话木马试一下
显示该文件不允许上传，请上传jpg、png、gift结尾的图片
看一下有没有白名单或者黑名单
足迹F12看源码：

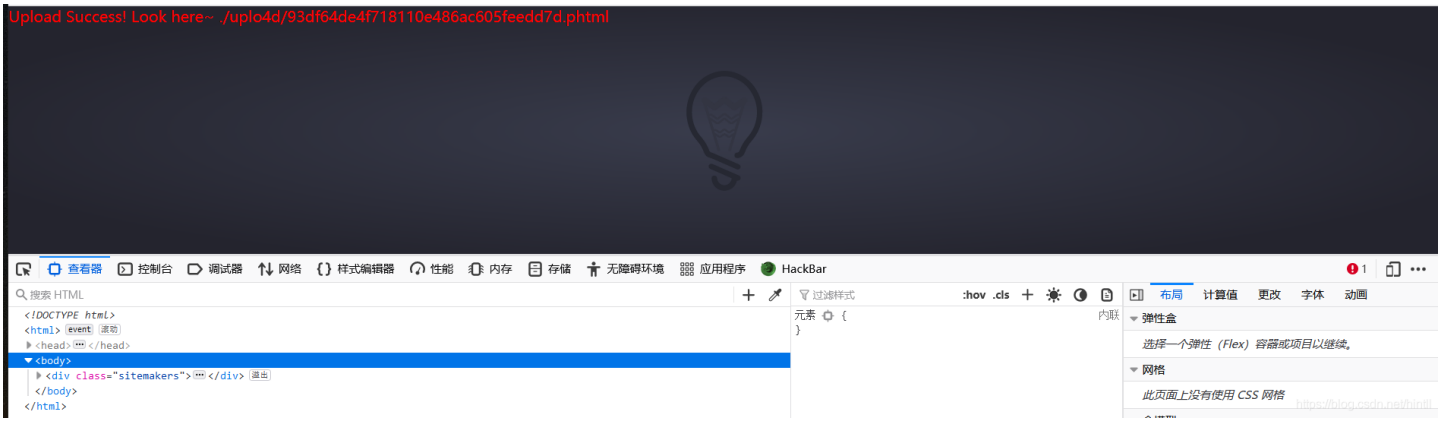
```
<div class="light">
<span class="glow">
 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"> event
    嘿伙计，你发现它了！
    <input class="input_file" type="file" name="upload_file">
    <input class="button" type="submit" name="submit" value="upload">
  </form>
 </span>
```

看到有
个checkfile的函数
看看能不能直接删掉
还真的能被删掉
然后传了一个php文件
但是什么回显都没有
一个是后端也被过滤了一遍
那就试一下这个东西能不能传上去


.htaccess

也不行
那就burpsuit抓包fuzz一下
分析phtml可以有回显
那就写一个phtml的一句话木马
可以参考之前的文章：https://blog.csdn.net/hintll/article/details/117922290?spm=1001.2014.3001.5501
这个html的一句话木马也是加了文件头幻术的

传一下试试：



有回显

直接中国蚁剑去连接：

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	2021-06-15 05:27:53	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	2021-06-15 05:48:43	6 b	1777
usr	2019-01-22 15:00:00	19 b	0755
var	2019-01-22 21:56:12	17 b	0755
.dockerenv	2021-06-15 05:27:53	0 b	0755
flag	2021-06-15 05:27:54	43 b	0644

去交flag