[ACTF2020 新生赛]Upload 1

原创

火火火与霍霍 于 2021-08-01 15:07:42 发布 557 收藏

分类专栏： 每周学习

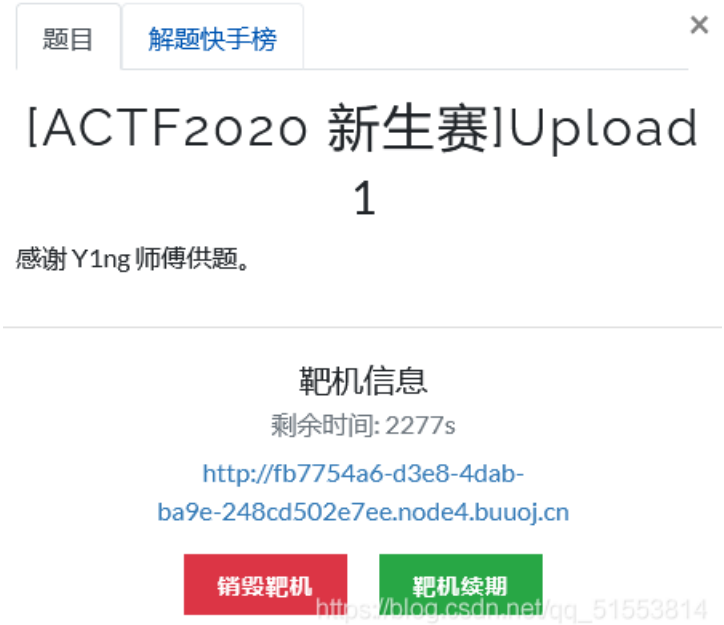
本文链接：https://blog.csdn.net/qq_51553814/article/details/119298215

每周学习 专栏收录该内容

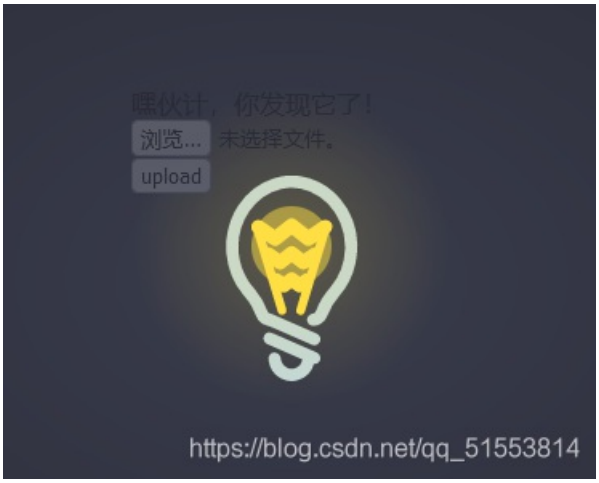
24 篇文章 0 订阅

订阅专栏

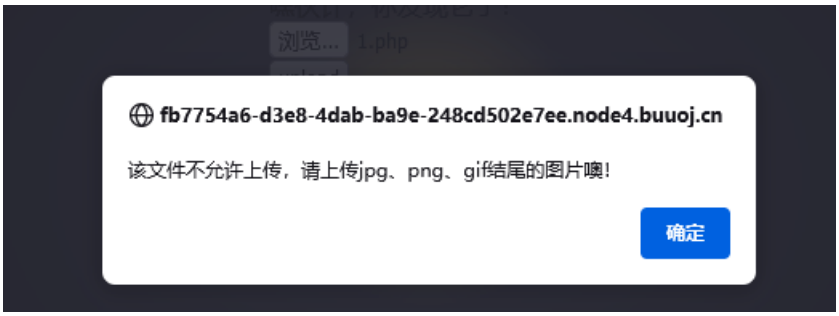
[ACTF2020 新生赛]Upload 1



要给关于文件上传题，进入靶场



可以上传文件，先上传1.php试试



未上传成功，且bp没有抓到包，很明显需要一个前端绕过

我们把文件名改成1.jpg后，在抓包工具中讲文件名改为1.php

```
Content-Disposition: form-data; name="upload_file"; filename="1.php"
Content-Type: image/jpeg
```

但是同样没有上传成功

```
        </span><span class="flare"></span><div>
    </div>
    </div>
    nonono~ Bad file!
```

怀疑是可能后端对其进行了过滤

那么换成Php试试

```
</div>
<div style="color:#F00">Upload Success! Look here~
./uplo4d/a93764746f978bca3598c4d6028f54b3.phP</div></body>
```

成功上传，但是访问该网页时，发现我们写的php代码都显示了出来

可能后端又进行了二次过滤

经过一番苦试，发现phtml可以用，

最终连接蚁剑，就得到了flag