

[ACTF2020 新生赛]Upload -wp

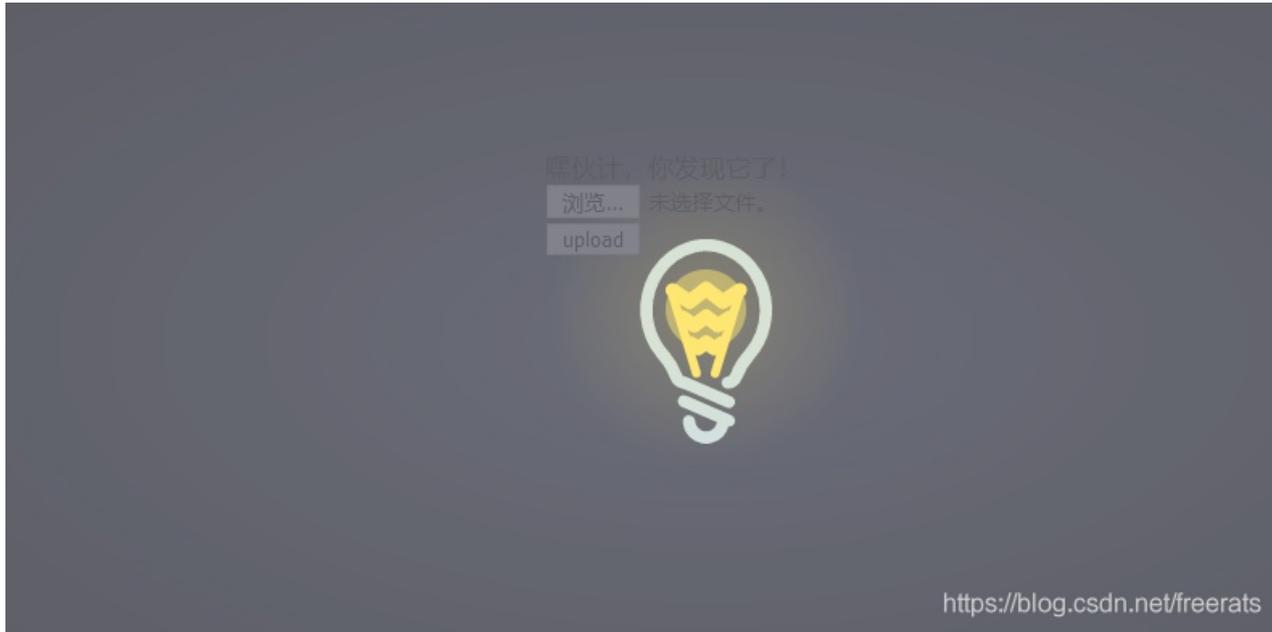
原创

冰可乐不加可乐 于 2020-06-29 19:38:35 发布 1272 收藏 2

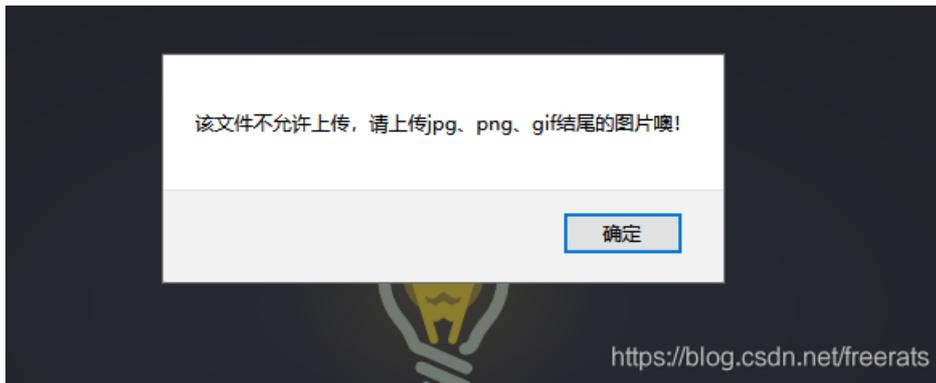
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/freerats/article/details/107026806>

版权



把鼠标移到灯泡处的时候发现上传处



任意传了个文件上去，弹窗只能穿图片格式，本来是想抓个包看看，发现挂了代理还是会弹窗提示，意识到是前端过滤

```
搜索 HTML
<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>
```

删除check就可以绕过了



上传php文件发现还存在后端过滤
把后缀改为phtml即可上传
没其他过滤，直接上传一句话
接下来蚁剑或菜刀连接即可

