0x01 最简单的文件上传

未进行文件类型和格式做合法性校验，任意文件上传

漏洞代码示例：

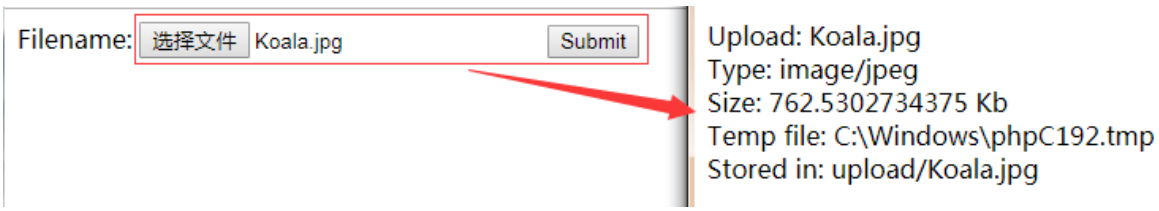
新建一个提供上传文件的 upload.html

```
<html>
<body>
<form action="upload_file.php" method="post" enctype="multipart/form-data">
<label for="file">Filename:</label>
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

创建上传脚本 upload_file.php

```
<?php
if ($_FILES["file"]["error"] > 0)
  {
  echo "Error: " . $_FILES["file"]["error"] . "<br />";
  }
else
  {
  echo "Upload: " . $_FILES["file"]["name"] . "<br />";
  echo "Type: " . $_FILES["file"]["type"] . "<br />";
  echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
  echo "Temp file: " . $_FILES["file"]["tmp_name"] . "<br />";
  move_uploaded_file($_FILES["file"]["tmp_name"],"upload/" . $_FILES["file"]["name"]);
  echo "Stored in: " . "upload/" . $_FILES["file"]["name"];
  }
?>
```

漏洞利用：可上传任意文件



这是一种非常简单文件上传方式。

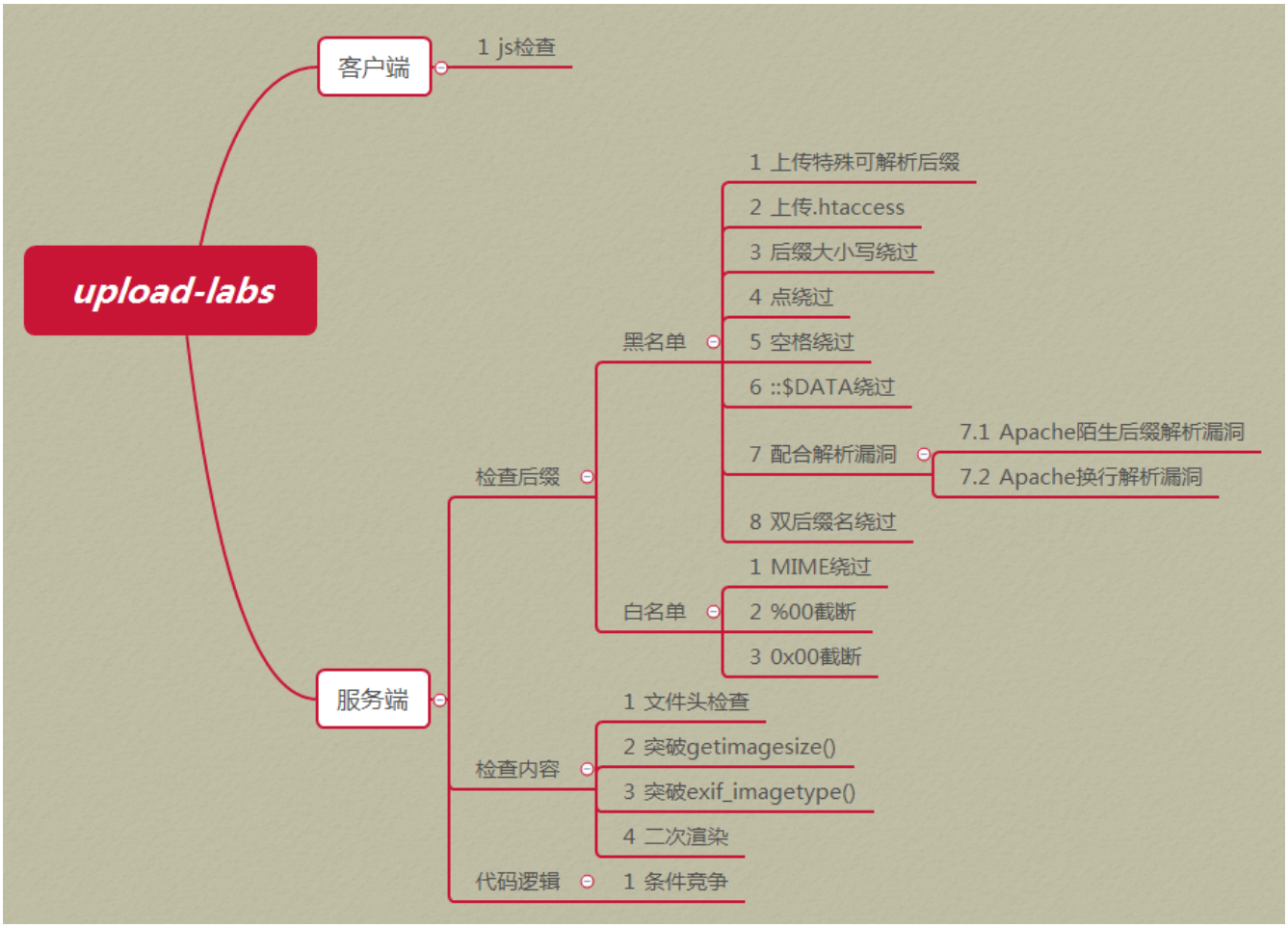
基于安全方面的考虑，应增加用户上传文件的限制，比如检查文件类型、限制文件大小，限定文件路径，文件名重命名、白名单限制文件上传类型等。

0x02 upload-labs

推荐一个很不错的项目，提供了各种上传漏洞的靶场，可以从upload-labs总结上传漏洞及其绕过的技巧。

GitHub项目地址：https://github.com/c0ny1/upload-labs

```
Pass-01
    js判断文件上传文件类型，抓包绕过

Pass-02
    文件类型匹配，抓包修改Content-Type: image/jpeg

Pass-03~Pass10
    黑名单过滤

Pass11~Pass12
    白名单，上传路径拼接，可截断

Pass13~Pass16
    文件头判断，图片马绕过

Pass17~Pass18
    先上传后删除，条件竞争

Pass19
    文件名可控，move_uploaded_file()函数 00截断绕过

Pass20
    文件名可控，数组方式绕过
```


upload-labs
客户端
1 js检查
服务端
检查后缀
黑名单
1 上传特殊可解析后缀
2 上传.htaccess
3 后缀大小写绕过
4 点绕过
5 空格绕过
6 ::$DATA绕过
7 配合解析漏洞
7.1 Apache陌生后缀解析漏洞
7.2 Apache换行解析漏洞
8 双后缀名绕过
白名单
1 MIME绕过
2 %00截断
3 0x00截断
检查内容
1 文件头检查
2 突破getimagesize()
3 突破exif_imagetype()
4 二次渲染
代码逻辑
1 条件竞争