文件上传漏洞

文件上传本身没有问题，是一个正常的业务需求，但问题在于服务端如何对文件进行处理，如果逻辑做的不够安全，就会导致严重的后果。

上传漏洞完成的条件：

1. 上传的文件可以被web容器解释执行
2. 用户可以通过web访问到文件

在针对上传文件的检查时，许多应用通过文件的后缀名进行检查安全性。攻击者可以通过[\0] %00 来绕过。原理是%00 在许多语言函数中被认为是终止符号，比如说某个网站只允许上传.JPG格式的文件，那么攻击者可以上传hacker.php[\0].JPG 在web看来这是一个JPG文件，但是当服务器端执行时会把[\0]及以后得内容截断，视为hacker.php。

另一种常见的安全性检查是通过检查文件的文件头，这种方式要比检查后缀名靠谱一些，但是攻击者同样可以通过伪造文件头，将真实的攻击代码藏在文件头之后。但这需要php执行此文件才可以，因为服务器端会将该文件看做JPG文件，很有可能不会去执行，这样攻击代码也就无效了。