一、 文件上传漏洞与 WebShell 的关系

文件上传漏洞是指网络攻击者上传了一个可执行的文件到服务器并执行。这里上传的文件可以是木马，病毒，恶意脚本或者 WebShell 等。这种攻击方式是最为直接和有效的，部分文件上传漏洞的利用技术门槛非常的低，对于攻击者来说很容易实施。

文件上传漏洞本身就是一个危害巨大的漏洞，WebShell 更是将这种漏洞的利用无限扩大。大多数的上传漏洞被利用后攻击者都会留下 WebShell 以方便后续进入系统。攻击者在受影响系统放置或者插入 WebShell 后，可通过该 WebShell 更轻松，更隐蔽的在服务中为所欲为。

这里需要特别说明的是上传漏洞的利用经常会使用 WebShell，而 WebShell 的植入远不止文件上传这一种方式。

1 Webshell 简介

WebShell 就是以 asp、php、jsp 或者 cgi 等网页文件形式存在的一种命令执行环境，也可以将其称之为一种网页后门。攻击者在入侵了一个网站后，通常会将这些 asp 或 php 后门文件与网站服务器 web 目录下正常的网页文件混在一起，然后使用浏览器来访问这些后门，得到一个命令执行环境，以达到控制网站服务器的目的（可以上传下载或者修改文件，操作数据库，执行任意命令等）。

WebShell 后门隐蔽较性高，可以轻松穿越防火墙，访问 WebShell 时不会留下系统日志，只会在网站的 web 日志中留下一些数据提交记录，没有经验的管理员不容易发现入侵痕迹。攻击者可以将 WebShell 隐藏在正常文件中并修改文件时间增强隐蔽性，也可以采用一些函数对 WebShell 进行编码或者拼接以规避检测。除此之外，通过一句话木马的小马来提交功能更强大的大马可以更容易通过应用本身的检测。<?php eval($_POST[a]); ?>就是一个最常见最原始的小马，以此为基础也涌现了很多变种，如<script language="php">eval($_POST[a]);</script>等。

2 文件上传漏洞原理

大部分的网站和应用系统都有上传功能，如用户头像上传，图片上传，文档上传等。一些文件上传功能实现代码没有严格限制用户上传的文件后缀以及文件类型，导致允许攻击者向某个可通过 Web 访问的目录上传任意 PHP 文件，并能够将这些文件传递给 PHP 解释器，就可以在远程服务器上执行任意 PHP 脚本。

当系统存在文件上传漏洞时攻击者可以将病毒，木马，WebShell，其他恶意脚本或者是包含了脚本的图片上传到服务器，这些文件将对攻击者后续攻击提供便利。根据具体漏洞的差异，此处上传的脚本可以是正常后缀的 PHP，ASP 以及 JSP 脚本，也可以是篡改后缀后的这几类

脚本。

m 上传文件是病毒或者木马时，主要用于诱骗用户或者管理员下载执行或者直接自动运行；

m 上传文件是 WebShell 时，攻击者可通过这些网页后门执行命令并控制服务器；

m 上传文件是其他恶意脚本时，攻击者可直接执行脚本进行攻击；

m 上传文件是恶意图片时，图片中可能包含了脚本，加载或者点击这些图片时脚本会悄无声息的执行；

m 上传文件是伪装成正常后缀的恶意脚本时，攻击者可借助本地文件包含漏洞(Local File Include)执行该文件。如将 bad.php 文件改名为 bad.doc 上传到服务器，再通过 PHP 的 include，include_once，require，require_once 等函数包含执行。