解析漏洞

什么是解析漏洞?

解析漏洞又称中间件（容器）解析漏洞。是指中间件（容器）解析了预期之外类型的文件。

利用方式?

与文件上传功能联用

解析漏洞有何危害?

绕过后端对上传文件类型的限制并得以执行其中的脚本。

解析漏洞有哪些？各自利用条件有哪些?

IIS

历史上有，太过古老，暂且不表

Apache

xx.php.kjhsdf：2.0.x <= 2.0.59、2.2.x <= 2.2.17、2.2.2 <= 2.2.8

1.php%0a.jpg：2.4.0-2.4.29

Nginx

xx.xx/xxx.php，访问时在上传文件名后面添加斜杠和随意php文件名，比如nginx1.11.5

a.jpg%00.php，0.5.,0.6., 0.7 <= 0.7.65, 0.8 <= 0.8.37

a.jpg\0.php， 0.8.41 ~ 1.4.3， 1.5 <= 1.5.7 （CVE-2013-4547）