bugku 求getshell(后缀黑名单检测和类型检测) writeup

转载

xuchen16 于 2018-09-27 16:37:41 发布 4600 收藏 1
分类专栏： ctf 文章标签： bugku 求getshell 后缀黑名单检测 类型检测 writeup 求getshell


ctf 专栏收录该内容
66 篇文章 6 订阅
订阅专栏

这道题是后缀名黑名单检测和类型检测

1. 把请求头里面的Content-Type字母改成大写进行绕过
2. .jpg后面加上.php5其他的都被过滤了好像

如果是walf严格匹配，通过修改Content-type后字母的大小写可以绕过检测，使得需要上传的文件可以到达服务器端，而服务器的容错率较高，一般我们上传的文件可以解析。然后就需要确定我们如何上传文件，在分别将后缀名修改为php2, php3, php4, php5, phps, pht, phtm, phtml（php的别名），发现只有php5没有被过滤，成功上传，得到flag