Bugku ctf writeup--web篇-文件包含2

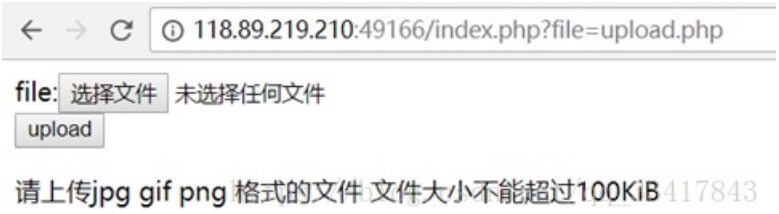
转载

byjfsj 于 2019-09-30 16:10:21 发布 433 收藏

原文链接：https://blog.csdn.net/qq_33417843/article/details/79756682

Step1:查看源码

发现注释文件upload.php,访问下来到文件上传页面



Step2：上传一句话

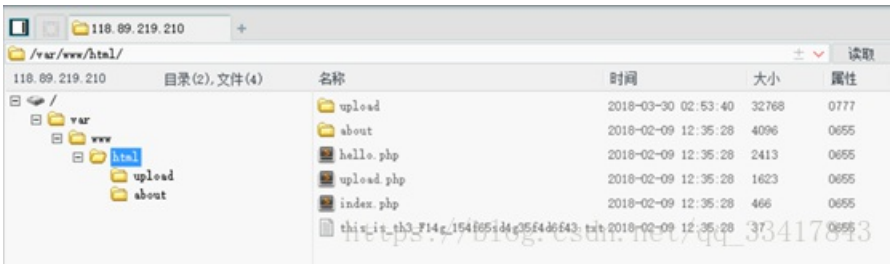
普通一句话会被过滤，这里构造<?=eval($_POST['shell']);>

保存文件修改后缀为1.php;.jpg,成功上传

根据提示是文件包含，直接访问文件路径无效，菜刀无法连接

包含文件进行访问是空白页面，再进行菜刀连接

Step3：上菜刀



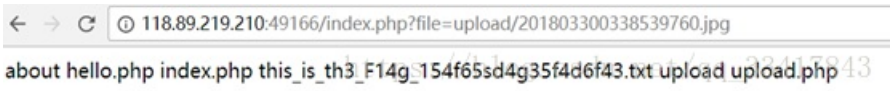
发现一个文件名很长的txt文件，打开就是flag

另一种思路是简书上看到的，在这里也po出来以供参考

在php文件里写入<script language=php>system("ls")</script>,列当前目录

同理,修改后缀名为jpg,如1.php;.jpg,上传成功

访问直接可以看到flag文件



包含或者直接访问都可以得到flag