记xctf_web upload1

原创

fly夏天 于 2019-09-30 10:49:54 发布 1794 收藏 2
分类专栏： ctf 文章标签： xctf-web
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/xiayu729100940/article/details/101756727
版权


ctf专栏收录该内容
17 篇文章 1 订阅
订阅专栏

题目一打开就只有上传界面

习惯性的后台扫描一下没有可以页面，看来目标就在这个上传功能上面了。

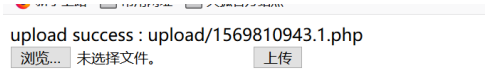
尝试上传php文件，报错。

这里我尝试传了一个图片马，能成功上传但是菜刀无法执行。

f12检查源码，发现前端有一个js验证，有一个白名单过滤，只允许上传png或jpg文件。

这里我们可以直接前端删除这段js函数。

然后选择上传一个php文件，刷新即可成功上传。

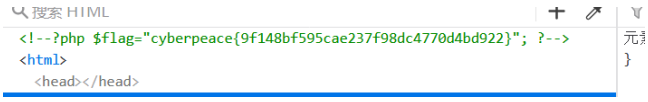


网站直接给出了上传地址。访问该链接，由于php文件中尝试了 system("ls")

发现php代码成功执行。

访问上级目录 ls ../ 发现flag.php 文件

直接 cat ../flag.php 即可源码中发现flag



ps：由于需要多次构造php指令，可以用brupsuite抓包，直接修改php文件内容，这样方便很多。