巅峰极客CTF writeup[上]

转载

weixin_30273175 于 2018-07-23 11:28:00 发布 242 收藏
文章标签： php runtime shell
原文链接：http://www.cnblogs.com/null1/p/9353759.html

经验教训

> 1.CTF不比实战，最好不要死磕。死磕就输了。我就是死磕在缓存文件死的。真的惭愧；
>
> 2.对于flag的位置不要太局限于web目录下，如果是命令执行直接上find / -name flag*；
>
> 3.善用搜索引擎；
>
> 4.刷题很重要，推荐刷题：https://www.ichunqiu.com/battalion?t=1；
>
> 比赛技巧总结：
>
> 虽然只做出了签到题，但是收货还是不少。认识到了自己真的菜的连狗都不如。
>
> 1.平台如果是被搞坏了，可以重新下发环境的。这点是之前没注意到的，不然有些时候被前人把环境搞坏了后面的人就没办法做出来了。所以这时候可以重新下发容器环境。
>
> 2.绝对不能慌，哪怕到了最后一分钟。冷静很重要。

题目名称：A Simple CMS

经过搜索这个CMS是存在缓存文件漏洞的，也就是说你注册的账号密码会保存在一个php文件当中，进而写shell

参考链接：https://www.cnblogs.com/Ragd0ll/p/8734841.html

由文中可得分别注册两个名为

账号一：%0a$a=$_GET[a];//

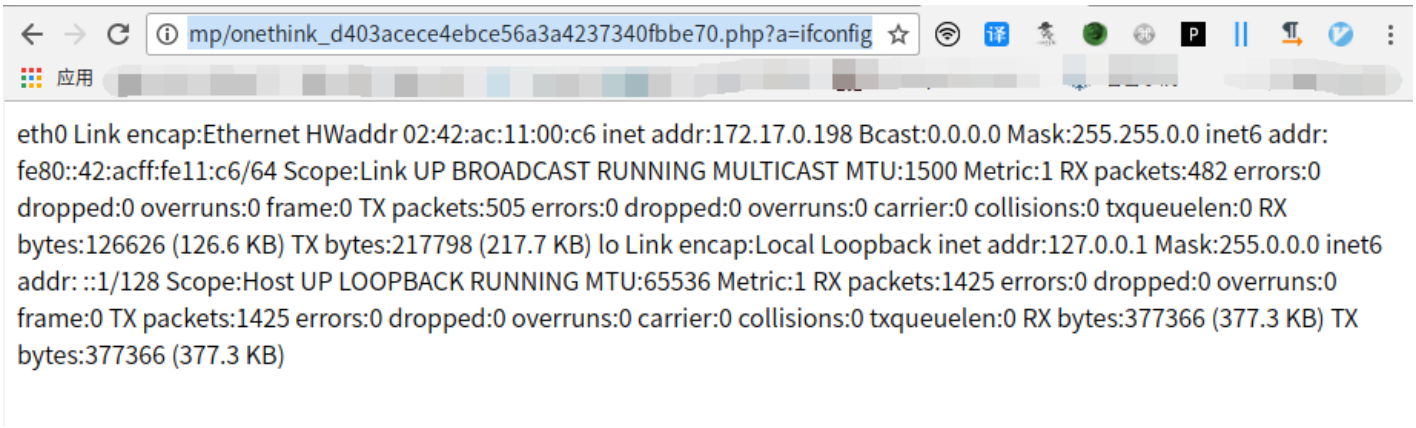
账号二：%0aecho `$a`;//

的用户然后登录即可缓存到php文件当中（这个缓存文件是不变的），但是我在做题的过程中一直命令执行不成功（最后才知道出题人把缓存文件改了）

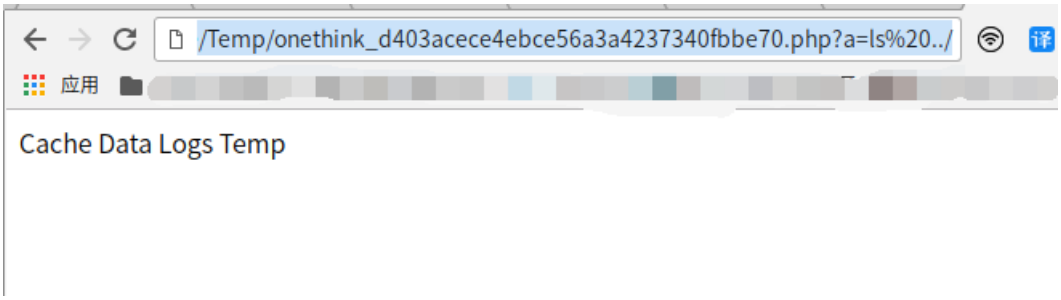
经过扫描是网站有一个www.zip的压缩文件。

然后通过使用这个下载到的备份源码进行复现发现缓存文件被改成了：/Runtime/Temp/onethink_d403acece4ebce56a3a4237340fbbe70.php

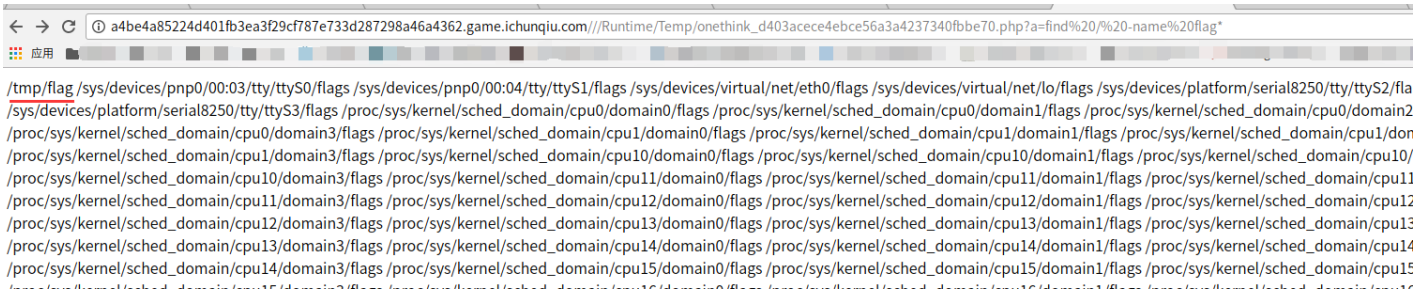
然后直接通过该php文件执行命令

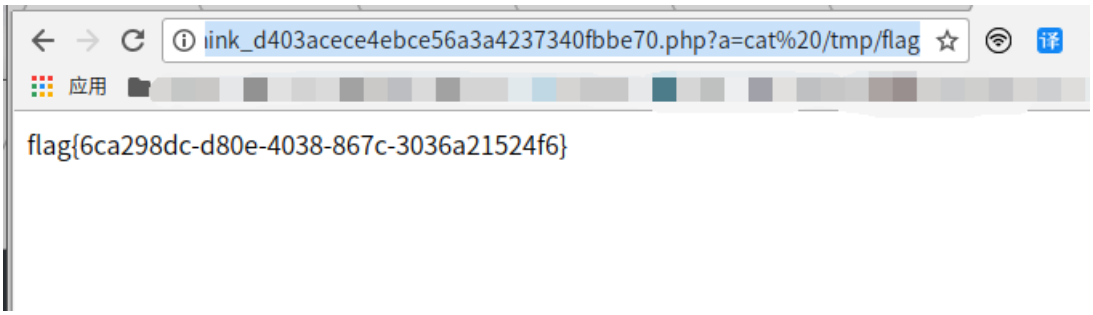


然后通过../查看（执行别的命令都行，就是这个会显示"缓存数据日志"）本以为是跟那个文章中说的一样，是权限问题，然后我就把这个目录下的所有文件cp到/var/www/html目录下，发现全是php文件。



后来通过find / -name flag* 查找到flag。经过测试，flag在/tmp/flag





转载于:https://www.cnblogs.com/nul1/p/9353759.html