flag——writeup

原创

Child_by_dream 于 2018-01-19 20:03:09 发布 299 收藏

本文链接：https://blog.csdn.net/Child_by_dream/article/details/79110299

ctf线上赛——第五关

地址：http://106.75.26.211:3333/

提示：天下武功唯快不破

首先我们访问目标站点，看到一段代码。

这段代码的意思是，首先生成一个cookie，token他的值位hello。然后验证cookie，如果token==hello，那么就回去flag.php这个文件你去读取flag信息。生成一个u/+一个随机从1到1000中那一个数进行MD5加密的txt文件。再过十秒钟，就删除这个文件。

这题的解题思路就是，写一个python脚本来帮我们请求访问，并获得响应包中的flag信息。

或者用脚本生成1到1000所数的MD5加密。在通过burp爆破这个文件名。请求成功就会返回flag

先抓包。

选择爆破参数。

添加字典。

开始爆破。

成功爆破。查看response包，获得flag。

ok，通关。