

攻防世界web baby_web writeup

原创

[Sprint#51264](#) 于 2020-07-08 18:37:18 发布 225 收藏

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_45837896/article/details/107212287

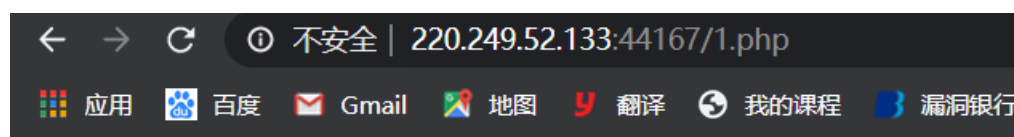
版权

题目提示：

想想初始页面是哪个

根据题目要求应该是让我们打开该网站下的index.php

我们进入在线场景发现进入的是1.php



HELLO WORLD

https://blog.csdn.net/qq_45837896

将1.php改为index.php再次进入发现，页面直接跳转到1.php

f12打开开发人员工具查看network项

Name	Status	Type	Initiator	Size	Time	V
index.php	302	text/h...	Other	277 B	132 ms	
1.php	200	docu...	index.php	240 B	70 ms	

发现index.php页面的状态码是302，

(302 Found, 原始描述短语为 Moved Temporarily, 可以简单的理解为该资源原本确实存在, 但已经被临时改变了位置)

查看它的头部返回包:

× Headers Preview Response Initiator Timing Cookies

index.php
1.php

Remote Address: 220.249.52.133:44167
Referrer Policy: no-referrer-when-downgrade

▼ Response Headers view source

Connection: Keep-Alive
Content-Length: 17
Content-Type: text/html; charset=UTF-8
Date: Wed, 08 Jul 2020 10:20:53 GMT
FLAG: flag{very_baby_web}
Keep-Alive: timeout=5, max=100
Location: 1.php
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.21

▼ Request Headers view source https://blog.csdn.net/qq_45837896

一个是flag

另一个是location参数（用来重定向接收方到非请求URL的位置来完成请求或标识新的资源）

所以题目知识点是HTTP请求中参数的含义。