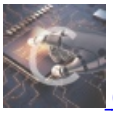
【XCTF高手进阶区】web1_baby_web writeup

转载

J0hnson666 于 2021-07-25 17:23:01 发布 20 收藏

分类专栏： # CTF 文章标签： ctf web http

原文链接：https://blog.csdn.net/Mitchell_Donovan/article/details/112894150



web1_baby_web

原题链接

key:php重定向

```
题目描述：想想初始页面是哪个
```

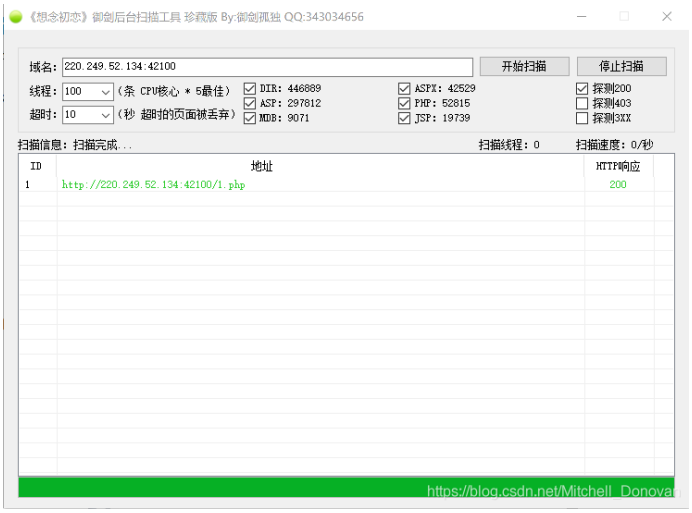
①进入环境后页面显示只有HELLO WORLD

抬头看URL地址栏里访问的是1.php

根据题目描述，由初始页面想到index.php

尝试访问index.php，然而却又跳转到1.php

②思路碰壁，不妨先御剑扫描一下



发现只有一个1.php可以访问

猜测index.php应该是被重新定向到了1.php

③F12打开开发者模式查看“网络”模块

查看返回包发现确实有index.php

其中的location参数被设置为了1.php，这就不难解释index.php自动跳转到1.php的问题了

同时发现了flag

④另外也可以在请求index.php后用burpsuite抓包

随后Ctrl+R发送到Repeater

Go一下也发现了flag

知识补充：

- **index.php的状态是302什么意思？**

302 Found，原始描述短语为 Moved Temporarily(临时搬家），是HTTP协议中的一个状态码(Status Code)。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；换而言之，就是请求的资源暂时驻留在不同的URI下，故而除非特别指定了缓存头部指示，该状态码不可缓存。

- **访问index.php跳转到1.php这种情况又是什么原理呢？**

一般原网页被换地方后，有人访问该网页是会被自动定向到另一个设置好的网页，且临时URI应该由响应头部中的 Location 字段给出。