

【XCTF高手进阶区】web1_baby_web writeup

原创

Mitch311 于 2021-01-20 17:36:02 发布 133 收藏

分类专栏: [CTF](#) 文章标签: [unctf](#) [网络](#) [python](#) [nginx](#) [http](#)

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/Mitchell_Donovan/article/details/112894150

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

订阅专栏

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

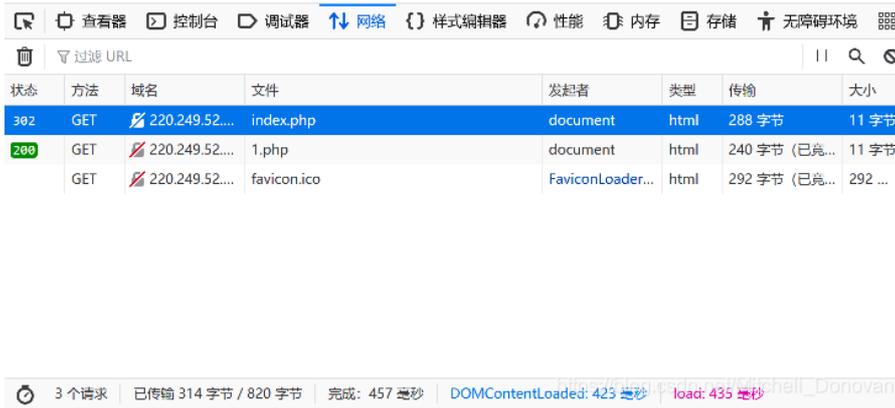
②思路碰壁, 不妨先御剑扫描一下



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

Response

Raw

Headers

Hex

```
HTTP/1.1 302 Found
Date: Wed, 20 Jan 2021 09:50:44 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.21
FLAG: flag{very_baby_web}
Location: 1.php
Content-Length: 17
Connection: close
Content-Type: text/html; charset=UTF-8
```

Flag is hidden!

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。