XCTF-baby_web

原创

auxein 于 2020-08-04 19:24:56 发布 96 收藏

分类专栏： CTF-Web入门

本文链接：https://blog.csdn.net/weixin_45613760/article/details/107795894

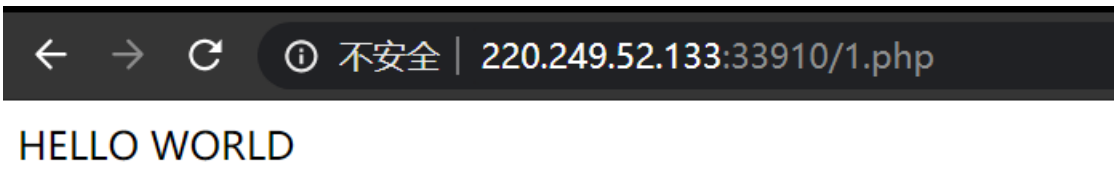
XCTF-baby_web

- 查看题目描述
- 打开链接，跳转到1.php
- 输入index.php后发现跳转到1.php
- 使用dirsearch扫描没有其他地址
- F12查看index.php的响应包，找到了flag

查看题目描述

想想初始页面是哪个

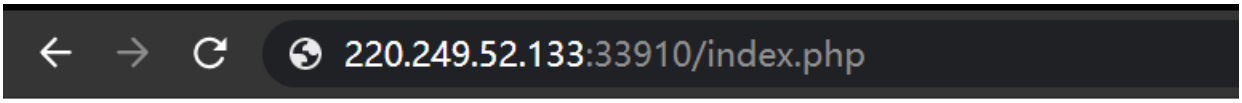
打开链接，跳转到1.php



HELLO WORLD

根据题目推测需要转到index.php

输入index.php后发现跳转到1.php



HELLO WORLD

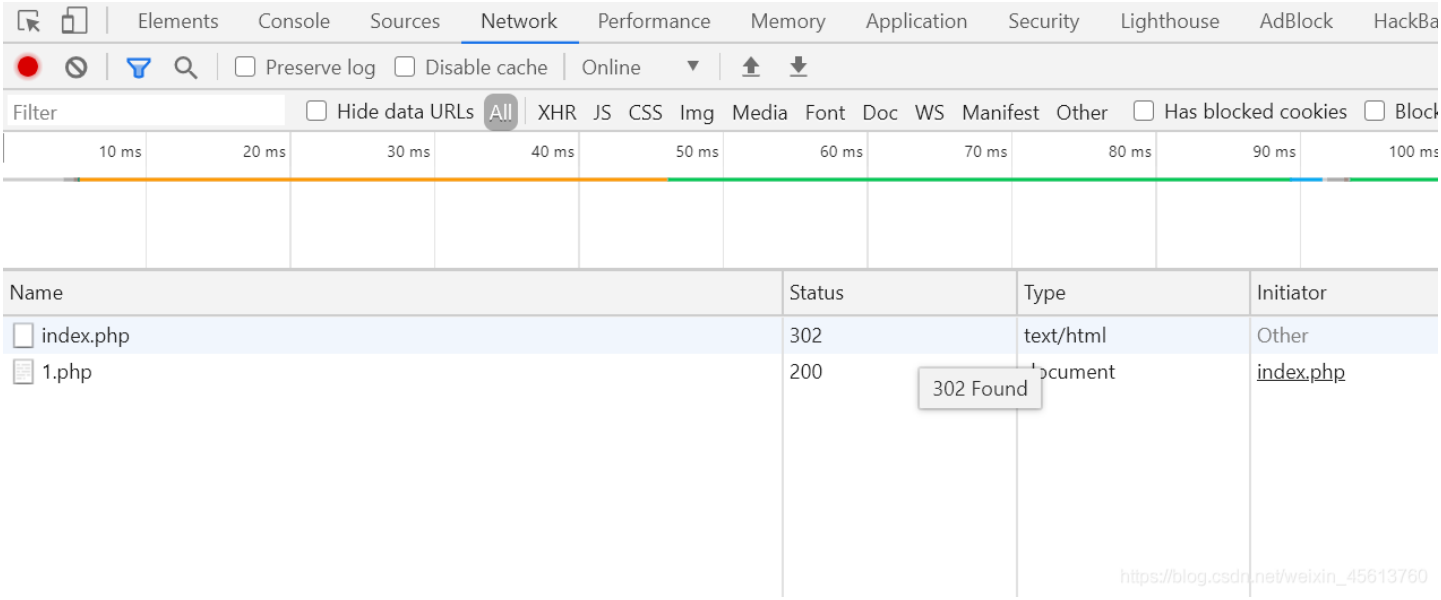
使用**dirsearch**扫描没有其他地址

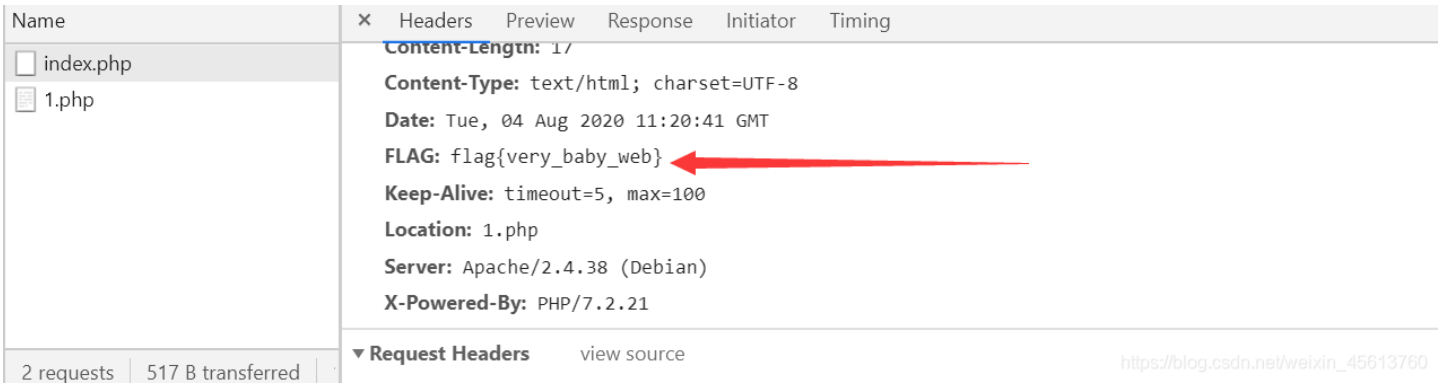
```
Target: http://220.249.52.133:33910/

Output File: D:\Python\Python3.7.0\dirsearch\reports\220.249.5

[19:09:04] Starting:
[19:09:07] 403 -  305B  - /.htaccess-dev
[19:09:07] 403 -  307B  - /.htaccess-local
[19:09:07] 403 -  307B  - /.htaccess-marco
[19:09:07] 403 -  306B  - /.htaccess.bak1
[19:09:07] 403 -  305B  - /.htaccess.old
[19:09:07] 403 -  306B  - /.htaccess.orig
[19:09:07] 403 -  308B  - /.htaccess.sample
[19:09:07] 403 -  306B  - /.htaccess.save
[19:09:07] 403 -  305B  - /.htaccess.txt
[19:09:07] 403 -  304B  - /.htaccessBAK
[19:09:07] 403 -  305B  - /.htaccessOLD2
[19:09:07] 403 -  304B  - /.htaccessOLD
[19:09:07] 403 -  305B  - /.htpasswd-old
[19:09:07] 403 -  303B  - /.httr-oauth
[19:09:09] 200 -   11B  - /1.php
[19:09:22] 302 -   17B  - /index.php  ->  1.php
[19:09:22] 302 -   17B  - /index.php/login/  ->  1.php
[19:09:29] 403 -  305B  - /server-status
[19:09:29] 403 -  306B  - /server-status/
```


F12查看**index.php**的响应包，找到了**flag**


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
AdBlock
Preserve log
Disable cache
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Has blocked cookies
10 ms
20 ms
30 ms
40 ms
50 ms
60 ms
70 ms
80 ms
90 ms
100 ms
Name
Status
Type
Initiator
index.php
302
text/html
Other
1.php
200
index.php
302 Found


Name
index.php
1.php
2 requests
517 B transferred
Headers
Preview
Response
Initiator
Timing
Content-Length: 17
Content-Type: text/html; charset=UTF-8
Date: Tue, 04 Aug 2020 11:20:41 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