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

本文链接：https://blog.csdn.net/qq_51954912/article/details/116128478

文章目录

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

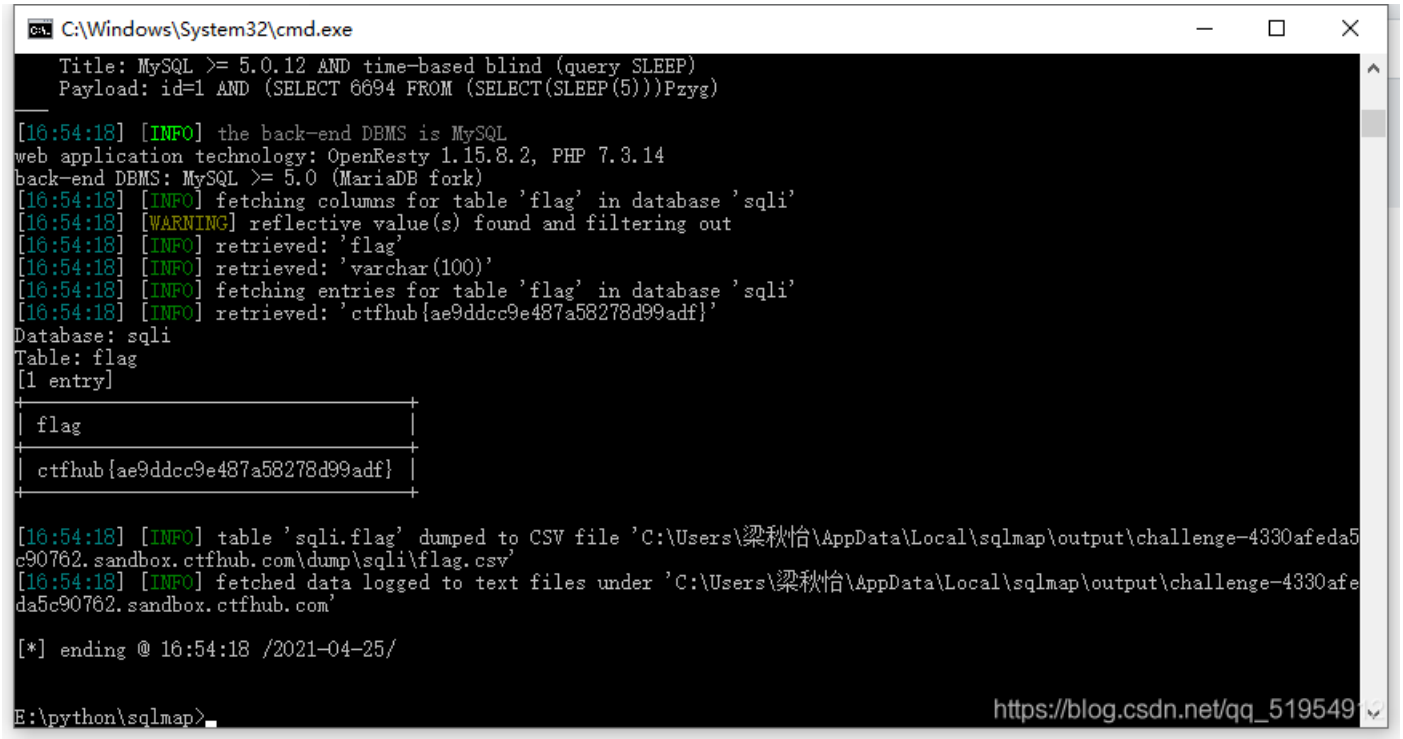
sql整型注入

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



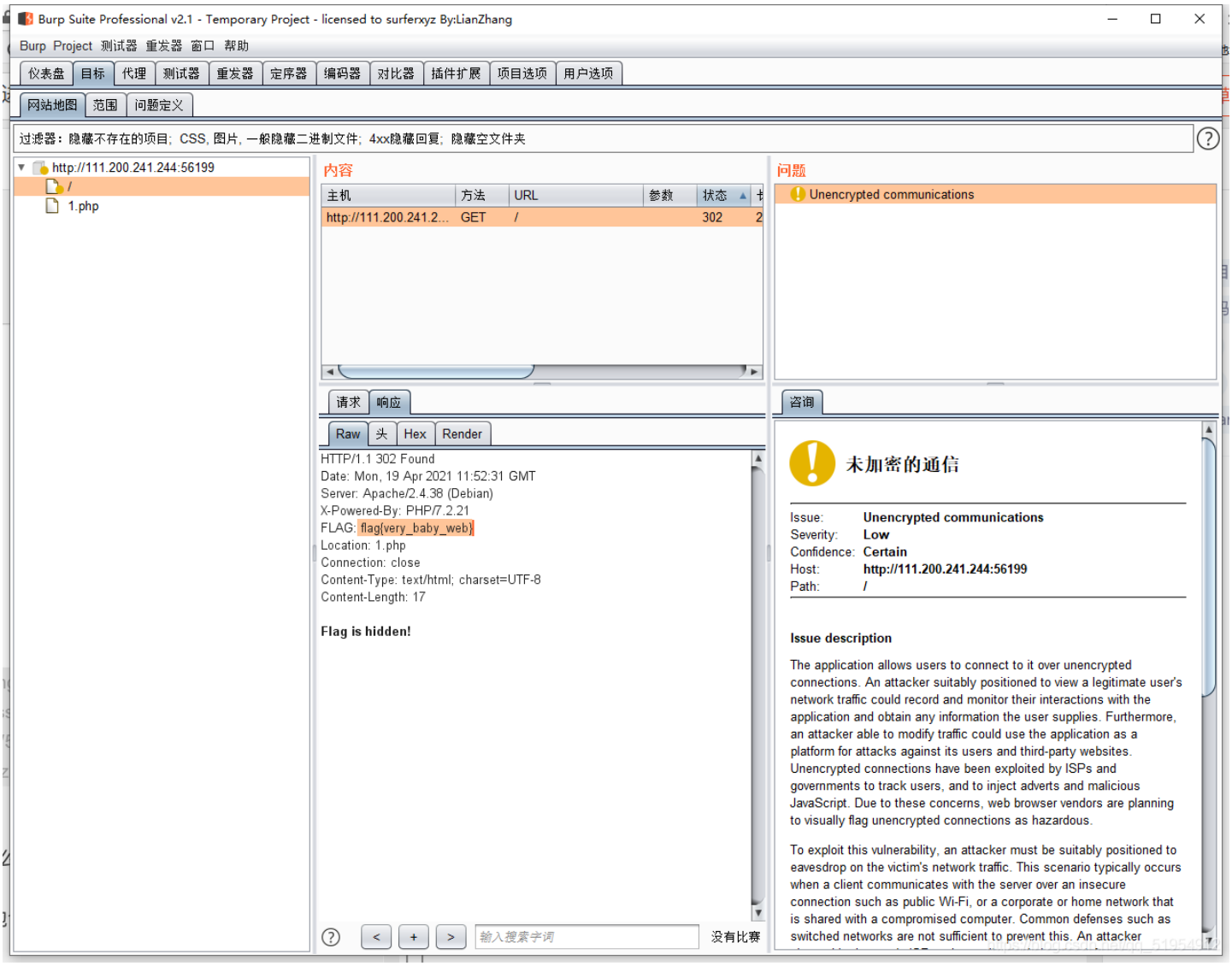
跑sqlmap，依旧是sqli，得到flag

baby_web

首先得到一个在线场景

HELLO WORLD

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

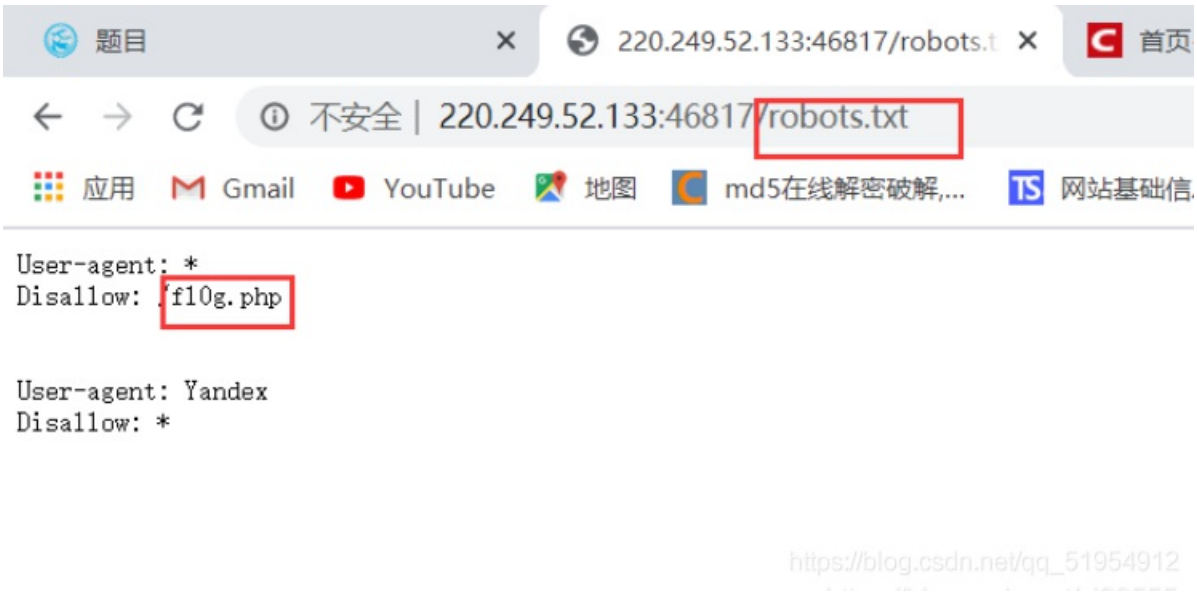


Training-WWW-Robots

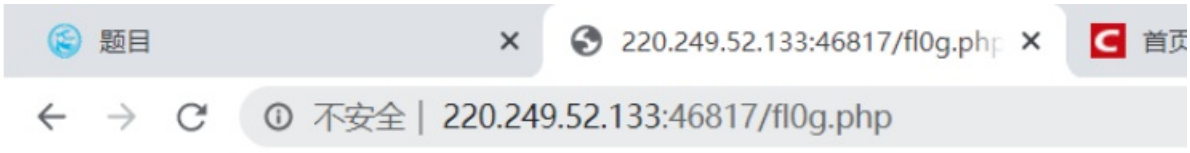
首先，看到robots，想到是在url后面改东西

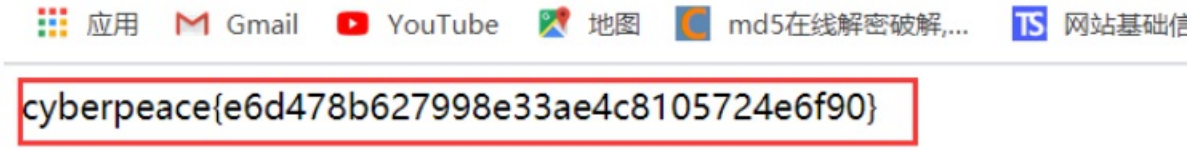
加上翻译

把.txt文件名放在url后面可以得到



然后





得flag