

# ctf入门题库\_【CTF】10个经典的CTF-web题目学习

原创

半生瓜Cc 于 2020-12-31 01:27:56 发布 3356 收藏 2

文章标签: [ctf入门题库](#)

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/weixin\\_42635849/article/details/112810002](https://blog.csdn.net/weixin_42635849/article/details/112810002)

版权

对CTF不是很感兴趣, 但是从中一些php的安全知识还是不错的, 从这个项目中找了10个案例, 自己本地搭建环境尝试分析, 这篇文章记录一下

## extract

extract函数是把数组里面的键、值映射为变量、值。

该题条件是`$shiyan==$content`

`$shiyan`是可控的, 而`$content`为读取一个文件名为`$flag`的文件内容。

尝试网上的payload: `?shiyan=&flag=1`

这个思路是覆盖`$flag`为1, `file_get_contents`读取1这个不存在的文件内容为空, 然后满足条件, 读出了flag:

我想到一个加强版:

我在条件里面加了一个 `$shiyan=='mkdd'`, 这个时候上面的方法就不可用了, 因为问题在于怎么让 `file_get_contents`读取一个文件, 内容为mkdd?这时候需要用到php://input伪协议, 直接把post的内容传给 `$content`即可

## strcmp

`strcmp`是对两个变量进行比较, 完全相同才返回0, 题目的意思就是你传入一个和flag完全相同的值, 我就告诉你flag...这不扯淡吗

那肯定还有某些情况下也能返回0? 是的, `strcmp`传入数组的话, 会返回null, 而`null==0` 是true

绕过过滤的空白字符



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)