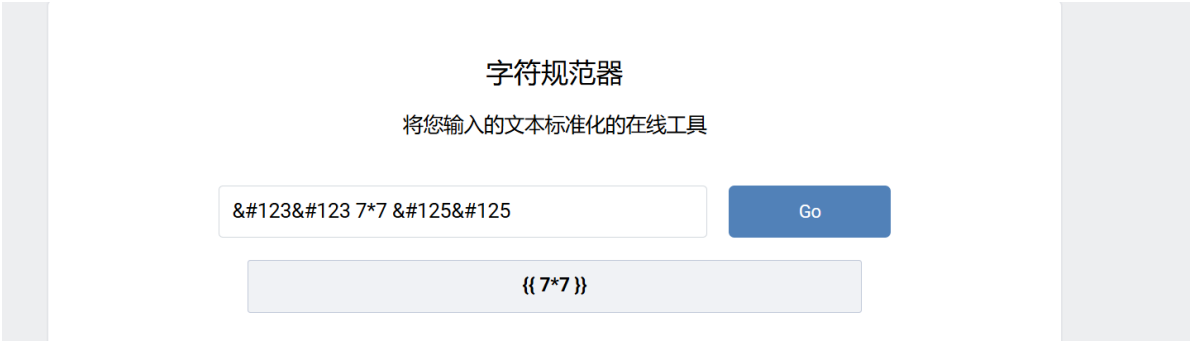
easy_web

首先打开页面是一个有回显的输入框，那么能联想到的就是xss，ssti了，结合adworld很喜欢ssti，首先检测是否是ssti

首先会发现输入的都可以回显，但是在注入{构造ssti的时候却发现有禁止。那么肯定是ssti无疑了。

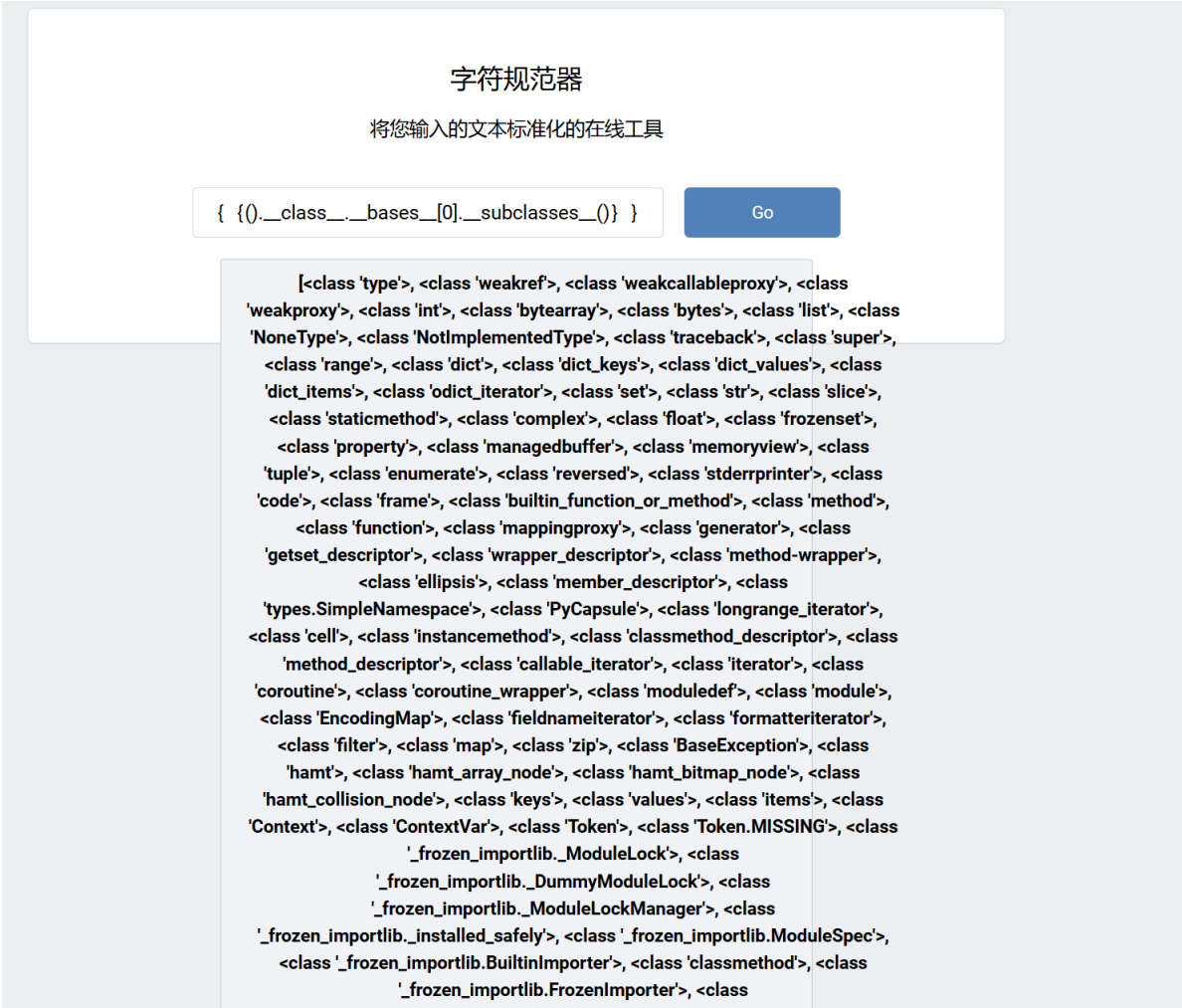
首先思考能否通过url编码构造

没有识别，再尝试Unicode编码，只是纯粹的文字内容而已没有任何注入



使用全角标点可以绕过识别

并且在wp中提到的特殊字符网站http://www.fhdq.net/，可以使用﹏绕过，但我不明白这个是如何能做到{闭合的同等效果的?



之后进行简单的ssti注入，配合脚本找关键函数就好了

```
{ {().__class__.__bases__[0].__subclasses__()[127].__init__.__globals__.popen('cat /flag').read()} }
```

但是这里遇到问题是`"`和`'`都被过滤，无法构造出popen的命令shell，如何绕过呢，在刚才的网站找到`'`，就直接找到flag了