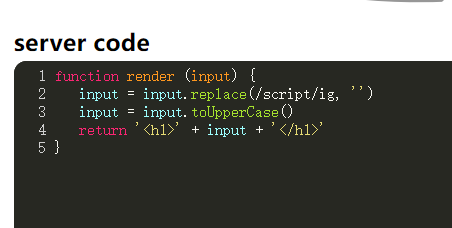
0x0C

过滤条件:



分析:先正则判断提交的字符串里有没有script,如果有替换成空;然后将替换后的字符串全部转成了大写, html标签不区分大小写,但是js代码区分大小写,而html标签属性内的字符使用html实体编码也能正常解析运行,

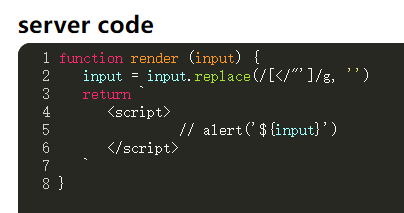
解题:双写script,然后将js代码进行html实体编码后提交

<a href="javascrscriptipt:&#97;&#108;&#101;&#114;&#116;&#40;&#49;&#41;">点我有奖</a>

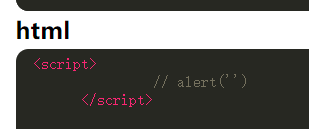
通关

0x0D

过滤条件:

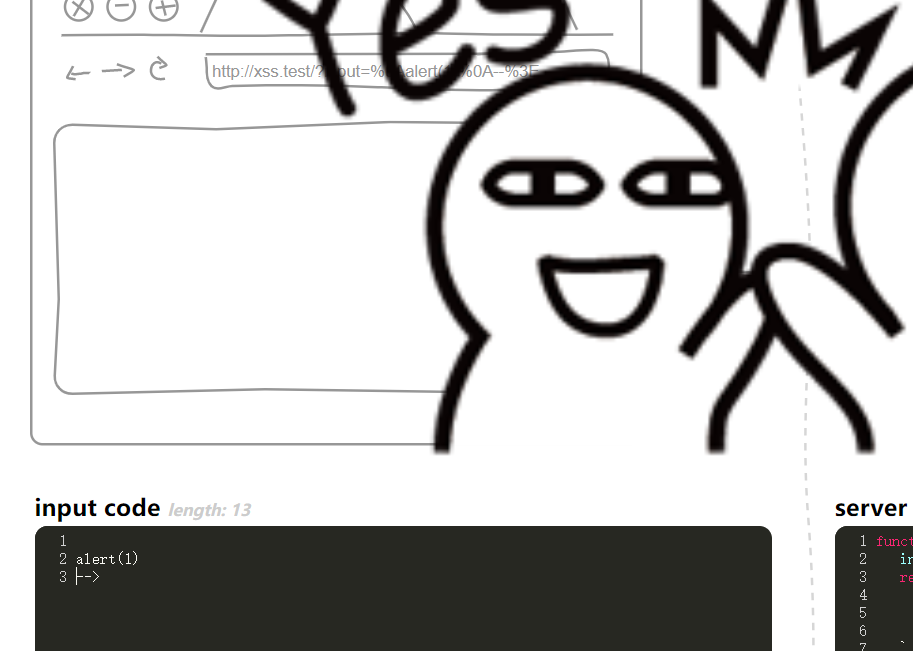


前端内容:



分析:

输出位置在单行注释符后,直接输出会被注释掉,所以在提交字符串的行首添加一个换行符,让js代码在下一行正常运行,但是换行后会有')未闭合,由于过滤条件中包含单双引号,无法闭合,所以选择使用单行注释把多余的字符注释掉,由于注释符正斜杠/也被过滤,所以使用-->当做单行注释,但是他会把那一行全部代码都注释,所以再次换行



通关

0x10

过滤条件:



HTML已有内容:



题目分析:

可以看出,后端并没有过滤前端的任何输入,所以可以直接闭合window.data="";

alert(1);

通关

后来发现,直接window.data=alert(1)也可以通关,猜测是只要语法正确,正常调用了alert(1)即可通关