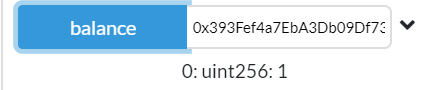
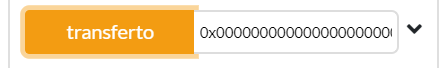
为了获取flag，我们需要让自己的余额大于1000000，可以看到存在空投函数，也可以给合约转账获取余额，一个比特币对应1个余额。当然我们可以来执行risegame，如果我们猜对secret的话，可以让我们的余额增加转账\*倍率的值，否则不仅不加，还会把余额清0。在转账函数中存在一个storage覆盖漏洞，可以覆盖referee和secret，我们可以把referee覆盖为我们自己，然后去修改倍率，实现余额暴增的目的。

首先领一个空投，让自己的余额不是0。





给0地址转账 触发漏洞



此时我们可以将倍率设置为1000000



此时我们的balance又变成了0，因此我们需要通过deposit来获取新的余额。然后进行risegame，附带2个eth，此时secret也是刚才的余额就是1。此时我们将获得大量余额，可以购买flag

