# 未初始化结构（US）

## 0. 参考《8种智能合约蜜罐》中“3.2 开放地址彩票 OpenAddressLottery” 和下面这个链接

<https://www.reddit.com/r/ethereum/comments/7xvoui/exposing_ethereum_honeypots/>

## 1. 指向storage的指针未初始化

合约地址：

0x01b21934ba28dfd8a22c4d21c710290500a5081f

0x04baddfb21723ec467e9993b715c5e0d673bac96

0x0d83102ec81853f3334bd2b9e9fcce7adf96ccc7

0x13b87fb8e6152032fd525f64f158c129a230b6ee

0x2075d158924f5030aece55179848c2bd7ec5833f

0x29d6cf436c893c7e44ea926411d5fd4dd763d9b3

0x2f069a1d7a052052458e8b5511e91221eb337c52

0x3268ecb4fcba1ca9f43da8ed05ffc80382cef1da

0x36f726e01cc85fdb0d998dfc442856379c569274

0x37541ebf8b4e25d36fbaa9b4c4eaad8c06314d6f

0x413c8657b6e6fa2b433db62271e662a470de4ba0

0x4fdc2078d8bc92e1ee594759d7362f94b60b1a3d

0x559be9a89db88794645abb93e3bfc1af2ee0be40

0x559cc6564ef51bd1ad9fbe752c9455cb6fb7feb1

0x6324d9d0a23f5ddba165bf8cc61da455350895f2

0x650734bfd0465b7c6cd2932ea555e721308fd0b3

0x6a2e025f43ca4d0d3c61bdee85a8e37e81880528

0x741f1923974464efd0aa70e77800ba5d9ed18902

0x74808c86c6f0bc6f59a3a1430ddfcd2e29952eac

0x783cf9c6754bf826f1727620b4baa19714fedf8d

0x787b9a8978b21476abb78876f24c49c0e513065e

0x8685631276cfcf17a973d92f6dc11645e5158c0c

0x96830139e44251ddbe3d1c4c4110262b47cf6d34

0xad1aa68300588aa5842751ddcab2afd4a69e9016

0xadccea0b14d26d786b99cf3ba3e9812cd4d23a81

0xb1f4ca3c6256f415e420de511504af8ea8a9c8e0

0xc57fc2c9fd3130933bd29f01ff940dc52bc4115b

0xe19ca313512e0231340e778abe7110401c737c23

0xe6f245bb5268b16c5d79a349ec57673e477bd015

0xefba96262f277cc8073da87e564955666d30a03b

0xf6c61cb3b0add944ac53c9c2decaf2954f0515cb

0xfb6e71e0800bccc0db8a9cf326fe3213ca1a0ea0

0xf5b72a62d7575f3a03954d4d7de2a2701da16049

0x1f7725942d18118d34621c6eb106a3f418f66710

0x94602b0e2512ddad62a935763bf1277c973b2758

0x652eb151869c2e8fa354f29321ba192d5d9f84dc

0x656610729fc13e8283d96aa69cdf56c112222951

0x9823e4e4f4552cd84720dabbd6fb2c7b67066c6c

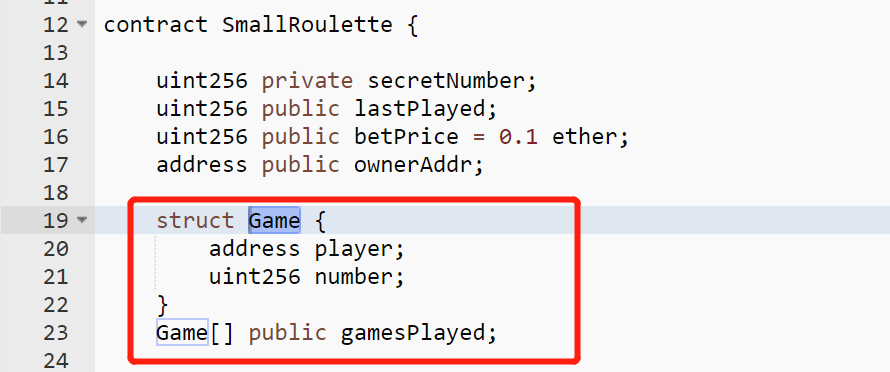
（1）重要特征：

首先，存在struct关键字；

其次，编译器的版本在0.4.25（或0.5.0）之前，或者是0.4.x版本的编译器都存在这个问题。

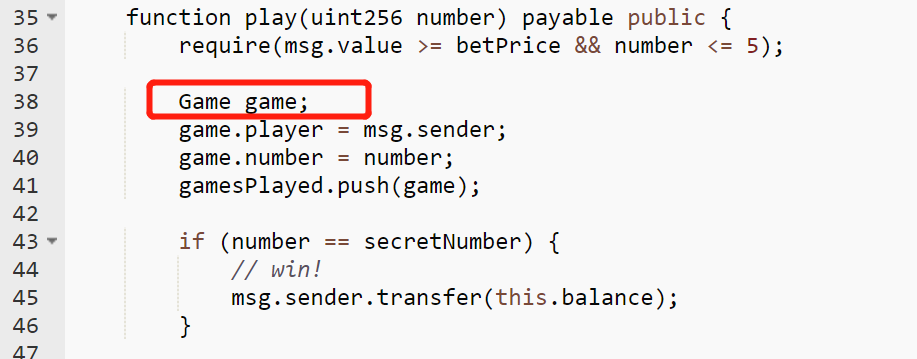
再者，一定要有声明的其他状态变量。

之后，一定要有转账指令。



Game game；声明了一个未初始化的storage指针。

（对于未初始化的 storage 指针（类似传统语言中的空指针），Solidity 默认其指向 storage 的起始地址，即指向合约开头定义的状态变量。）



## 2. 关注可能制造蜜罐的点：

当我们把一个storage类型的变量赋值给另一个storage时，只是修改了它的指针（引用传递）。