

地球OL真实盗币游戏，Web题WriteUp

转载

FLy_鹏程万里 于 2018-12-18 08:56:44 发布 267 收藏
分类专栏: # 智能合约安全



[智能合约安全 专栏收录该内容](#)

35 篇文章 0 订阅
订阅专栏

0x1 原题

挑战1: Web

题名: **Crypto Exchange Bug**

奖励: 2 Ether (≈2900¥)

地址:<http://dvpgame.ml/>



https://blog.csdn.net/FLy_hps

0x2 解题思路

1、登陆

随便输入个账号就能登录，这里用asd:asd登录，发现初始有95dollar可用。

2、猜想

走一遍系统的各个功能点，猜测可能出现漏洞的地方。经过一番尝试后，觉察参数中的值0.95和系统中1.9的值有某种联系，猜测可能存在条件竞争。

3、测试

1.条件竞争

各个功能中只有提现功能和购买DVP功能互相存在条件竞争。burp抓取提现的数据包和购买DVP的数据包，同时请求，一段尝试后即可触发漏洞。成功使余额变为190dollar,190dollar可以兑换1.9dvp，但是eth购买条件是需要大于1.9dvp。

2.浮点运算溢出

一番尝试后猜测此处或许可以通过浮点运算溢出绕过，如 $(1.8+0.1)>1.9$ ，如图：

```
C:\Users\Administrator>python
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:25:58) [MSC v.1500 64 bit
Type "help", "copyright", "credits" or "license" for more information.
>>> 1.8+0.1
1.9000000000000001
```

分别进行两次购买，第一次购买1.8dvp，第二次0.1dvp。成功绕过。

0x3 证明

1、提现数据包



2、购买DVP的数据包

? **Payload Positions** Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /buydvp?amount=0.95 HTTP/1.1
Host: dvpgame.ml
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0$
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://dvpgame.ml/
DNT: 1
Connection: close
Cookie:
session=.eJxFkFFrWjAUhf9KybOMNnYPK_jQkVoUcrNKXGmGS01i09jqacraip99wQI7uly493znnBva7tvSKGIQ9HVD3vA3dihCu_zTVn
h-FNlshu4T9NHK0kiPdvVec_SGk1dWITTGG1RjvJ-yI9oc99MnGAyJLROJ-i25pvFD0Vqa6uwGkAJLGMtKqwlU91hgFnASNzBXnmi26p
KUmmYAufptCxdKkLvGqAZ1fK3xLE5_y2BeEXsCuFPDYaWaB4NDSD0Wmf4ZyQJKqF2iQW8dozFFPQhFKQOC-3urGNzPQsuD
sDnrehoCKnzWAssdDEVZPFIXJ-vx10B3n8j5A7pI4DSBehQ_gszS6CUws8ce_1xVIsGY9HFwELojTkdGTPAs9G9o8600sbRvdf08547
w.DsMLhA.dfup10tKS7eG8ZQxBILvCwu0EU0;
remember_token=592jD705fca0b8e68a75cc20c161d4136e9d80bb7bae28535c666c8e297461df35ce9098ca6d925befc18df01ddf5ad
06e1e1746fe8db94ce318da72c3af91324f
Upgrade-Insecure-Requests: 1
```

0 matches Clear

1 payload position Length: 994

3、触发条件竞争漏洞

The screenshot shows a web application interface with the following elements:

- DVP Token:** Balance of 100. Description: 用于广告发布商提供的押金, 用于支付手续费, 用于维持生态运营, 加好友, 邀请推广等奖励. 可以用来换ETH. Buttons: 买 (red), 卖 (green).
- Ether:** Balance of >1.9. Description: 用于支付手续费, 用于奖励以太坊网络, 可以用来换私钥. Button: 买 (red).
- Key:** Balance of 1. Description: 用于获取以太坊地址的私钥, 内含2 ETH. Button: 买 (red).
- Dollar:** Balance of 0. Description: 可充值: 95\$, DVP Token余额: 0.95DVP, Ether余额: 0.0ETH. Buttons: 充值 (red), 提现 (red).

Watermark: DVPNET https://blog.csdn.net/Fly_hps

4、触发浮点运算溢出漏洞

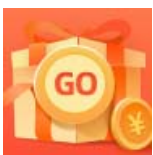
分两次购买dvp, 先购买0.1个DVP, 再购买1.8个DVP, 此时我账户下的DVP数应该溢出为1.9000000000000001了, 大于1.9, 成功购买ETH。



5、购买key



可以看到打印出来的字符串是base64后的，解码一下就是真实的私钥了，然后把私钥导入钱包即可转账走人。



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)