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/

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,190doller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

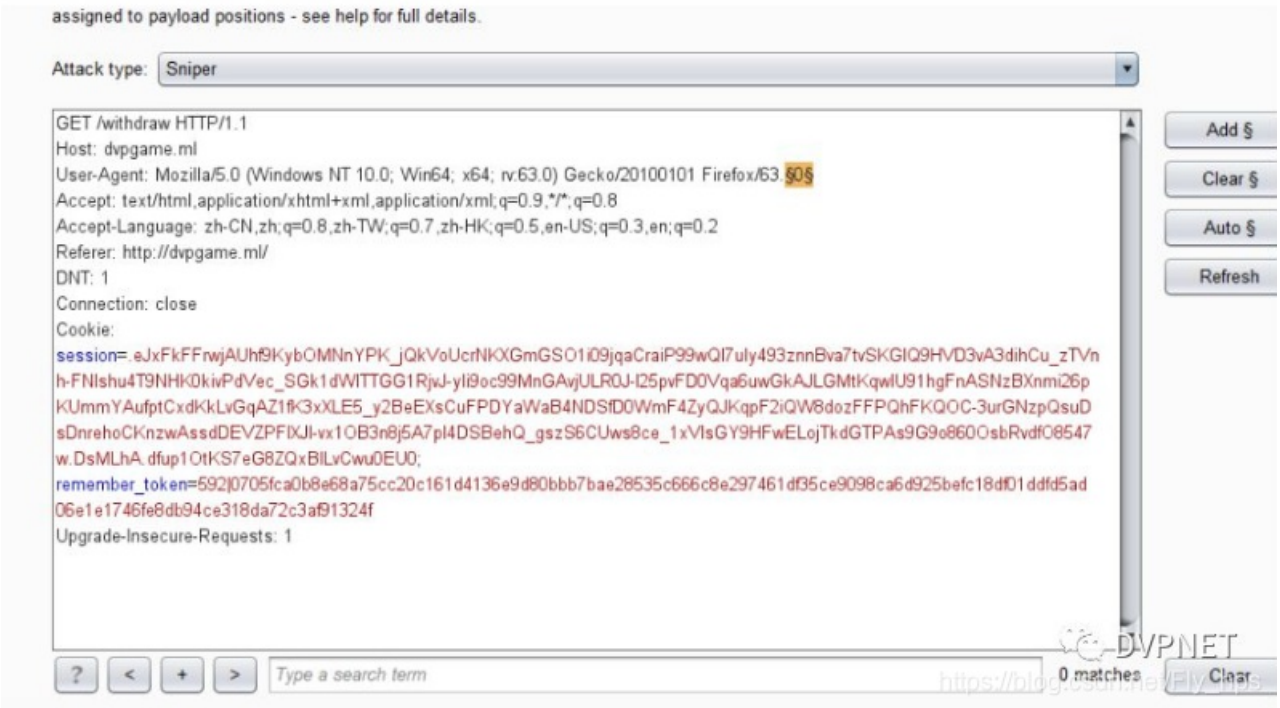
一番尝试后猜测此处或许可以通过浮点运算溢出绕过， 如(1.8+0.1)>1.9 ，如图：

```
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。

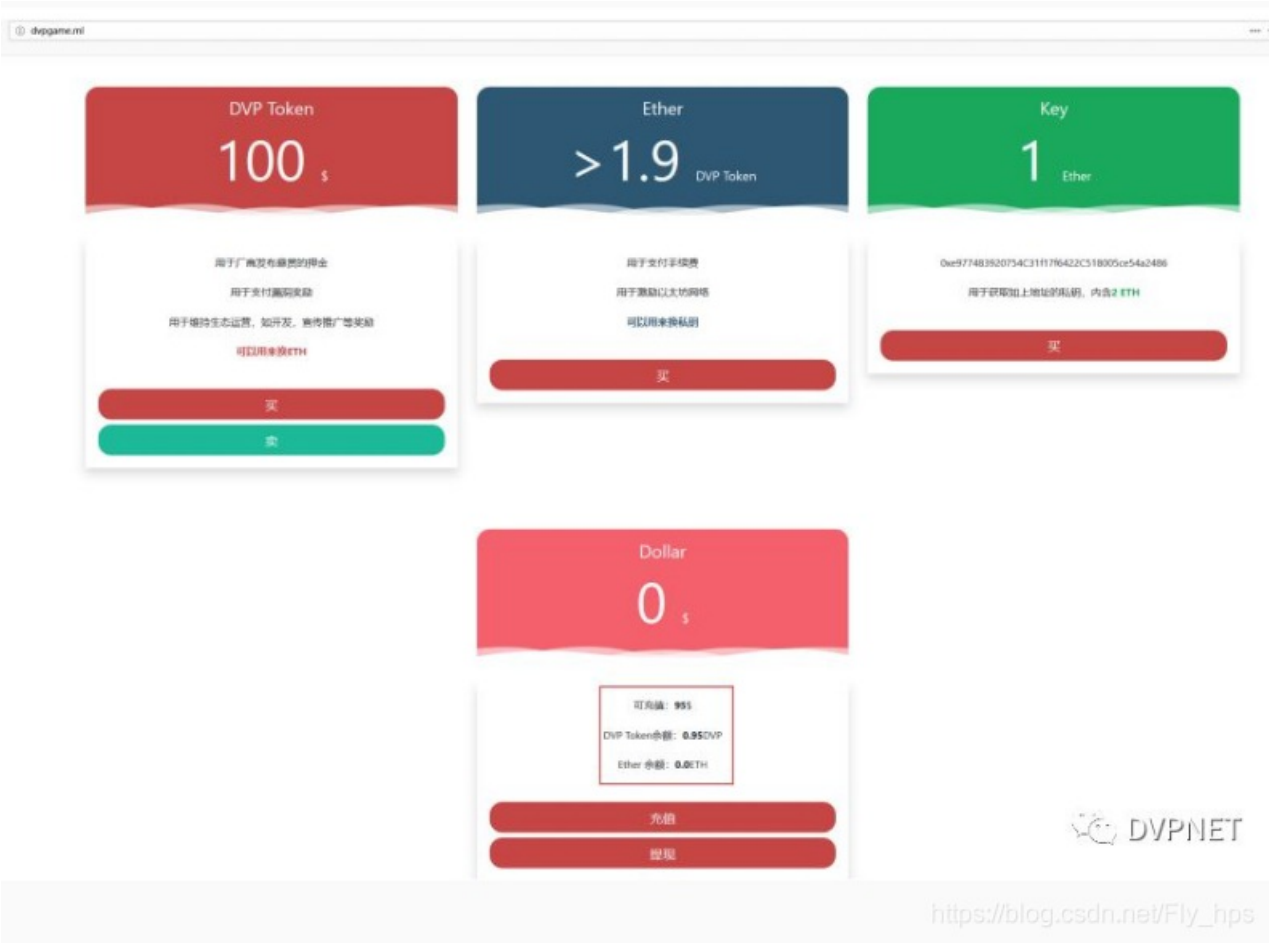
0x3 证明

1、提现数据包



2、购买DVP的数据包

3、触发条件竞争漏洞



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。