

一、平台

服务器：211.69.198.56 端口：22

账号：fabric 或者 root 密码：jocelyn987+

二、数据集

以 000000correctDataSet 表格为准，对应的合约和 patch 均在 partSrc 文件夹中。

Patch 以合约地址名+合约名命名，一个 patch 可能包含多个函数的 patch。

合约的漏洞行在文件 0x0a0a0a0reBugInfo – partSrc 标识。

优先测试标识能够链上修复的合约，如果有时间再将不能链上修复的合约修改后再测试看看

三、执行的流程和记录的数据

1、启动 geth: 路径/home/fabric/ethereum1005/go-ethereum

2、remix 连接

3、部署漏洞合约（记录漏洞合约的部署开销） 漏洞合约部署的 nonce 需记录用于步骤 6

4、构造攻击交易和正常交易（每个漏洞点先一个，有的一个漏洞点涉及多个漏洞，就得构造多个了），攻击漏洞合约看是否成功 （分别记录攻击/正常交易案例并分别记录正常和不正常交易的执行开销）

5、部署 patch 合约 （记录 patch 合约的部署开销）

6、调用 SpecialTxCreator()函数，依次在 65~68 行填入漏洞合约地址、目标合约地址、漏洞合约部署 nonce，漏洞函数签名，构造特殊交易部署到 geth 上

在控制台发送特殊交易，命令如下：

```
personal.unlockAccount("coinbase 地址","123")
```

```
eth.sendTransaction({from:'coinbase 地址',  
to:'0x1000000000000000000000000000000000000000',data:'SpecialTxCreator 编  
码的 data 字段'})
```

- 7、再次发送正常交易（记录是否正常执行以及执行开销）
- 8、再次发送攻击交易（记录是否拦截成功，及原因）