DAO 的具体攻击方式之前研究生学长学姐们已经分享过了，我就不赘述了。

我就稍作一些补充：

本课程 ppt《典型的公有链系统——以太坊》上 P52 页开始的 DAO 攻击的代码的 Solidity 版本比较老，部分代码在我们平时做实验的版本是不支持的，如：

P55

```
if (_recipient.call.value(_amount)()){
    ...
}
```

当前语法应更新为：

```
(bool flag, ) = _recipient.call{value: _amount}();
require(flag);
```

而这一段代码是DAO攻击的漏洞之处。当单纯使用 message call 或者 send 函数发送以太币给合约的时候，没有指明调用合约的某个方法，这种状况下就会调用该合约的 fallback() 函数，致使嵌套漏洞。若是一个合约接收了以太币可是内部没有 fallback() 函数，那么就会抛出异常，而后将以太币退还给发送方。

但是当前版本的 Solidity 强制要求一个合约的 fallback() 函数需要添加 external 字段，有该字段的函数不能被所在合约内函数调用。因此我运行攻击合约中 msg.sender.call{value: 1 ether}("") 的时候会有报错，表示以太币交易因错误中断并回滚到错误发生前状态：

```
dase@ubuntu:~/Desktop/DAO$ python3 DAO.py
eth connect: True
contract address: 0xD07d841f4faCe0945a10fdD67d5a145446048A1A
contract address: 0x33f95F9e8235Cc10a6407B53B5009968d6541F5F
DAO deposit 5 Wei success!
DAO current wallet balance: 5000000000000000000
Attacker deposit 1 Wei success!
DAO current wallet balance: 6000000000000000000
execution reverted: VM Exception while processing transaction: revert
Attack wallet failed!
DAO current wallet balance: 6000000000000000000
Attacker current wallet balance: 0
dase@ubuntu:~/Desktop/DAO$
```

DAO 攻击模拟可以参考博客：[深入分析攻击原因，详解 The DAO 事件 - 区块链网 NFTs (qklw.com)]