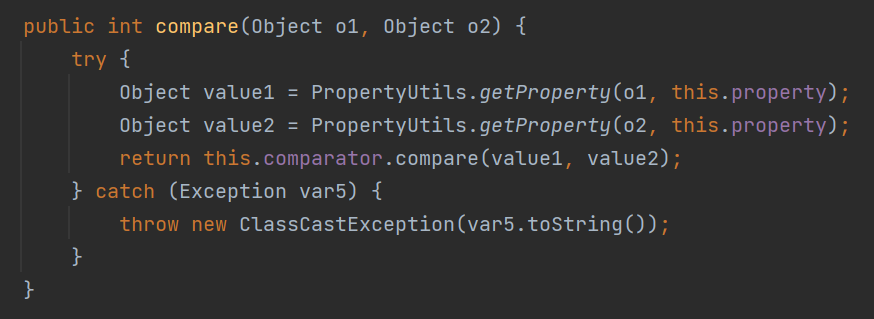
Java1.4下的CommonsBeanutils利用

wp地址：https://mp.weixin.qq.com/s/hXoUs4ZJgLHHaTvoyhwFxg

### CommonsBeanutils1利用链

##### 核心

org.apache.commons.beanutils.BeanComparator#compare，通过getProperty调用任意指定对象的特定getter方法



##### 入口

ObjectInputStream.readObject()

PriorityQueue.readObject()

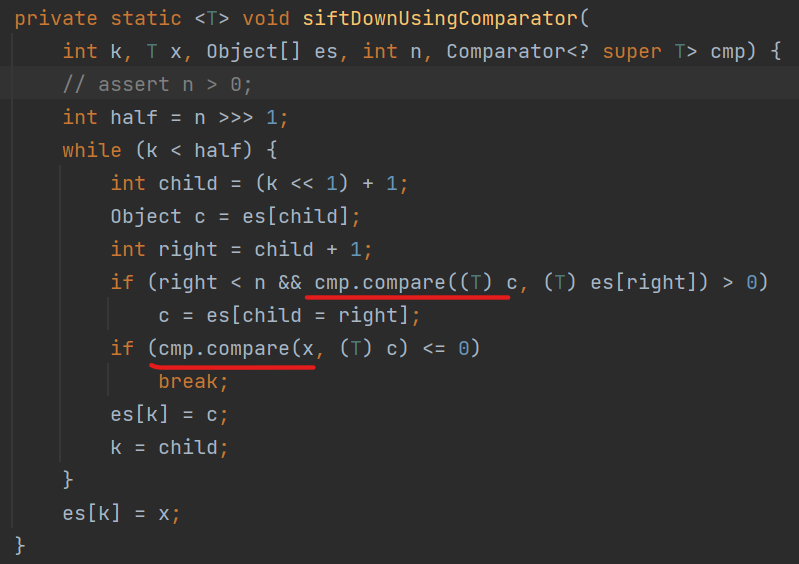
PriorityQueue.heapify()

PriorityQueue.siftDown()

PriorityQueue.siftDownUsingComparator()

BeanComparator.compare()

核心是通过PriorityQueue类反序列化readObject一系列的函数调用，直到siftDownUsingComparator方法调用指定的BeanComparator的compare方法



##### 出口

TemplatesImpl链，不是本文重点，这里不再分析

### Java 1.4下的利用

Java 1.4 的环境下，没有 PriorityQueue 这个类（入口），TemplatesImpl 和 JdbcRowSetImpl这两个类（出口）也没有，在本题中，作者发现了新的可利用类

##### 入口

java.util.HashMap#readObject

java.util.HashMap#putForCreate

java.util.HashMap#eq

java.util.AbstractMap#equals

java.util.TreeMap#get

java.util.TreeMap#getEntry

org.apache.commons.beanutils.BeanComparator#compare

首先是TreeMap#get方法中调用getEntry方法，其中会调用指定比较器类的compare方法

