主要有两种，一种类比法，一种原子推到法。
方法名字是我自己取的，可能不是很精确。
方法的本质是我自己总结和学习别人的东西融合的，实战下来感觉还可以。

类比法，顾名思义，就是根据熟悉的问题来推演未知的问题。
人类的知识就是这么传承下来的。
也就是所谓站在巨人的肩膀上摘苹果，学习别人已经研究出来的东西。

人类是没有改造自然底层规律的能力的，有的知识发现规律，然后应用规律，组合规律。
从自然的角度上讲，一切都是已经造好的，不存在未知。
这个世界很多东西只是对于人类未知而已，因为人类智力条件限制了理解这个复杂世界的能力。
类似于早期计算机，拥有一个很差的硬件体系，cpu 性能很低，内存不到 100M，让它去跑现在的 3A 游戏，势必马上当机。
因此早期做游戏的画质都是像素画质。
人脑也是一样，世界对于人脑来说，过于复杂了， 让一个弱鸡硬件突然去跑一整组这么复杂的程序，估计大脑过热直接拜拜。
因此只能像愚公移山一样，每一代人的每一批人理解一部分，各自钻研各自的领域，然后传承知识，后人接过接力棒继续研究，传承，让时间的力量来加深人类对于世界的理解。
这就是类比法的本质。

类比法这里会有一个引申问题，那么重复的问题还需要自己再亲身从 0 开始解决一次吗？
我觉得，可以直接继承，但没必要从 0 开始推导。
就好像现在已经有一个父方法了，直接 extends 就好了，为什么还要从 0 开始写呢？
“同一个问题不值得被解决两次”---引用不知道哪里看到的话
eg:
玩英雄联盟有两种人：
1、玩了几把，然后看看对应英雄的教程，然后再玩几把，然后再看教程
这种人其实就是用了类比法，用已知（别人的教程）解决未知（实战中没遇到的情况）
2、头铁，玩盖伦，一玩就是一千把
这种人用的是从 0 推导法，也不管别人怎么玩，他只自己总结实战经验，然后改进。

哪种人段位更高，答案一目了然。
自己一个人，从 0 开始推导，不去吸收前辈的知识，如果想比别人强，不是不可能，但是得满足下面这个条件
天纵奇才，一个人推导的所有东西>以前所有人推导的方法和经验（包含以前所有天才）
“没学会走就想跑，不是不可以，但是先问问自己是不是天才”---引用不知道哪里看到的话
因此在有成熟方案的时候，如果想不直接引用就超越别人，先问问自己是不是天才。

搞安全也是一个逻辑，例如，现在市面上工具也很多，但是依然还有人在不断的写重复功能的工具（从 0 推导法）。
在这里不是抨击这些人，而是觉得有些东西直接引用成熟的工具就好了。

安全本来就是为了实战服务的学科，属于软件开发的旁支，现在安全生态最缺的不是工具，而是一种全局观，一种成熟的看待整个安全技术栈和业务走向的架构思想。

就好像打 lol，别人也用剑圣，我也用剑圣，其实工具两个人手上的工具都是一样，但是不同玩法拿到手上，打出来的实战效果天差地别。

差在哪里，差在打法上，差在思想上。

这里也不是说不需要工具开发，而是说，不需要重复的工具，已有的轮子，调优可以，为了学习技术再造一个，也可以，但是为了单纯 a 钱再造一个，耗费人力物力，其实意义真的不大，因为往前走还有更赚钱的东西，没必要一叶障目。

类比法和类比法的一些推导问题就阐述完毕了，下面阐述原子法。

原子法，这个方法是跟马斯克学习的，他叫的更加专业，叫第一原则法（First Principles Thinkings），但我觉得原子法更好记，就一直这么叫了。

这个方法本质就是把一个事物分解成小原子，然后再组合，从而引发创新。

eg:

黑色水性笔，分解为墨水，笔尖，笔帽，笔身。

正常模式：墨水换成红色 -->得到红墨水笔

魔改模式：墨水换成小型炸弹，笔尖+笔帽换成触发器，用笔写字，然后再盖上笔帽，触发电路，然后引发定时炸弹。-->得到笔形炸弹

但是这个方法需要类比法的前置，就是首先得通过类比法了解一个事物的原子组件。

比如首先我得知道一只笔有哪些组件，我才能拆分原子。

这里也可以通俗的描述为：

先传承，再创新

创新不是无端端来的，因为创新的本质就是另一种组合方式。

没用类比法学习以前的知识，就好像一个人堆积木，他手中的积木块有限（原子），无论怎么堆砌，其实都达不到想要的效果。

而先学习现有方法， 相当于增加手中的积木块个数，然后能够组合的东西就越来越多，最后才能引发创新。

eg:

代码审计，jboss 出现了一个漏洞，了解了原理。

exchange 也出现了一个漏洞，了解了原理。

飞机上如果 x 部位少了一颗螺丝就会引发远端的另外两类器械工作不正常，因为异常抖动。

组合三者，然后扰动 weblogic 的某个组件，在触发异常的条件下，代码会进行非预期跳转，进而引发反序列化逻辑，最后挖了一个 0day。

以上两种研究方法简单总结，就是先学习，后创新，先类比推导，再原子分析。

先熟悉现有规则，把现在的规则玩透了，玩烂了，再尝试改变规则，左右规则，才会有更好的效果，否则就是原地打转，类似于用初中数学推微积分，就那么几下子，用到极致了，但是跳出来一看，人家洛必达法则早给整明白了。

done