《Java反序列化漏洞》

基础环境

JDK解压版：包含Java运行时环境
IDEA： 开发工具
Maven： jar包依赖管理
Tomcat： HTTP服务器
Burp Suite： 发送HTTP请求
Kali： 启动相关服务

总体规划

1、Java反序列化漏洞
2、Apache Commons Collections反序列化漏洞
3、Alibaba Fastjson反序列化漏洞
4、Apache Shiro反序列化漏洞

Java反序列化漏洞

Java序列化和反序列化

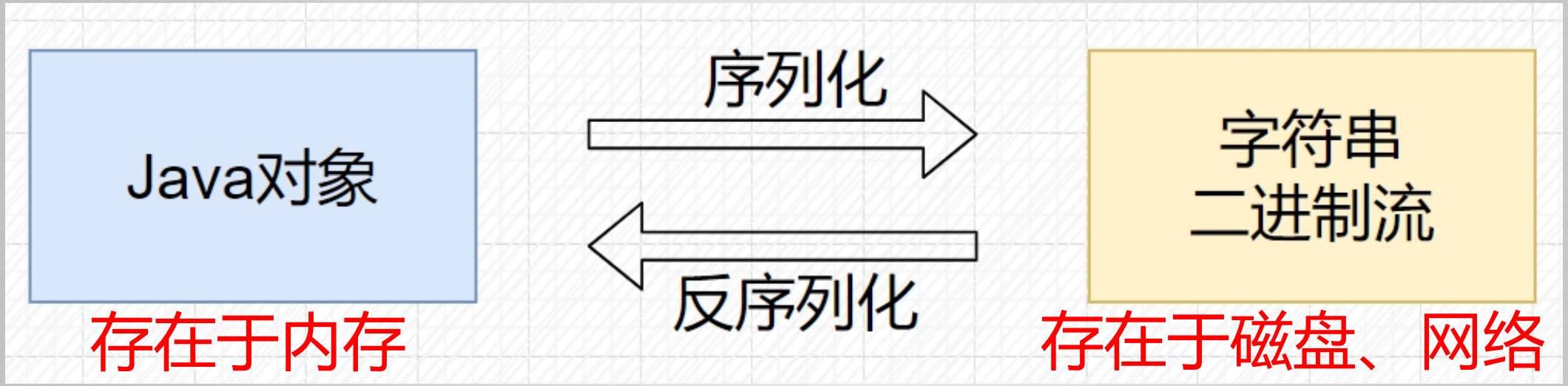
课程目录

1、序列化和反序列化的含义和用途
2、Java序列化演示
3、反序列化漏洞的出现

01

序列化和反序列化的含义和用途

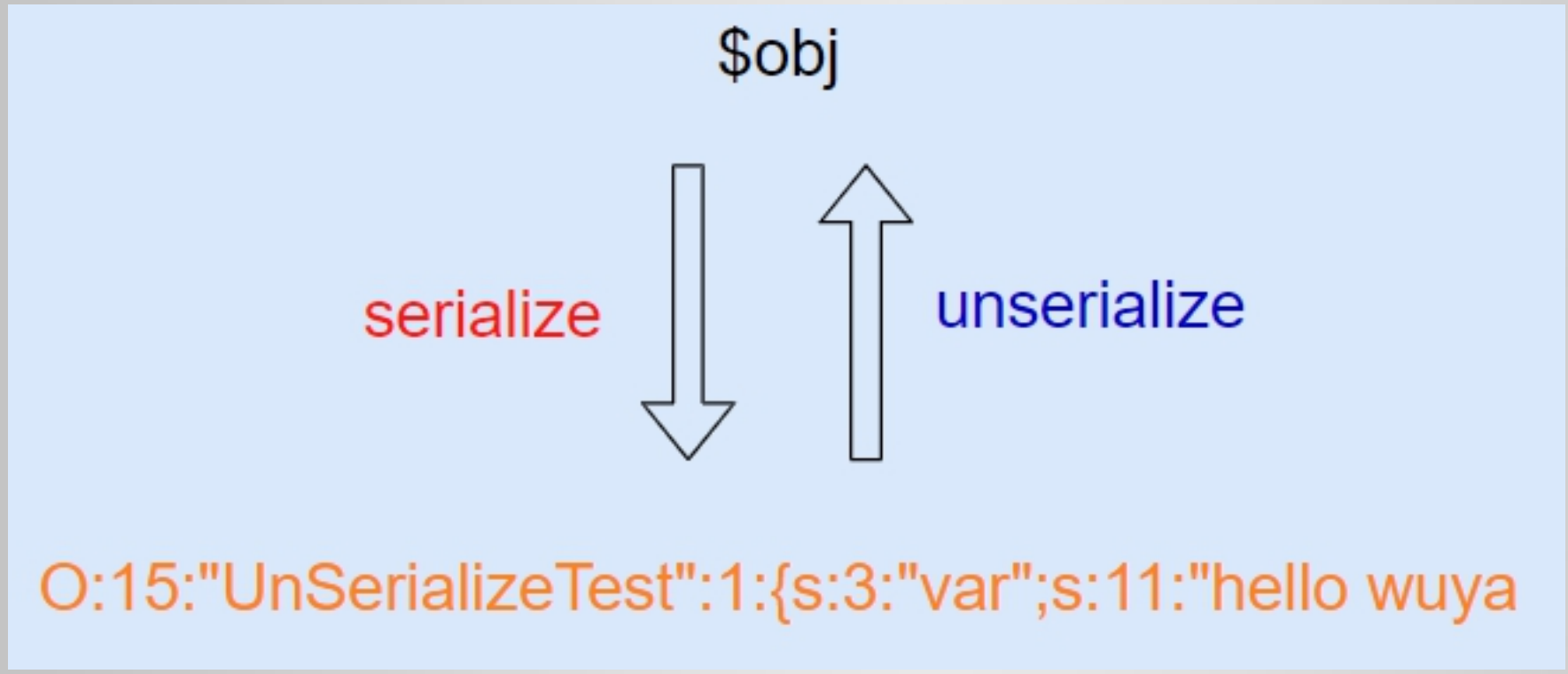
Java序列化和反序列化



序列化主要使用场景

1、持久化内存数据
2、网络传输对象
3、远程方法调用(RMI)
……

PHP反序列化



JSON格式


```
{
    name = 'wuya', age = 66, flag = true, gender = 'male', address = 'cs'
}
```

```
{
    "name": "网站",
    "num": 3,
    "sites": [{
            "name": "baidu",
            "info": ["putian", "广告", "贴吧"]
        },
        {
            "name": "谷歌",
            "info": ["打不开", "技术", "资料"]
        },
        {
            "name": "淘宝",
            "info": ["买了吗", "购物"]
        }
    ]
}
```

02 Java序列化演示

Java序列化和反序列化

Person对象，实现Serializable接口

序列化格式

参考：
https://docs.oracle.com/javase/8/docs/platform/serialization/spec/serialTOC.html

https://docs.oracle.com/javase/8/docs/platform/serialization/spec/protocol.html#a10258

Java序列化和反序列化

序列化
java.io.ObjectOutputStream.writeObject()

反序列化
java.io.ObjectInputStream.readObject()

03 反序列化漏洞的出现

自定义反序列化

1、重写类的readObject()方法
2、反序列过程中会执行自定义的readObject()

利用思路

1、利用自定义的readObject()方法执行代码
2、寻找重写了readObject()方法的类

利用

有没有重写了readObject()的现成的类?

package sun.reflect.annotation;
AnnotationInvocationHandler

package javax.management;
BadAttributeValueExpException

……

Thank you for watching

无涯老师