java序列化漏洞基础

那些可以被序列化的对象要实现Serializable

常见的创建的序列化和反序列化协议

• JAVA内置的writeObject()/readObject()

• JAVA内置的XMLDecoder()/XMLEncoder

• XStream

• SnakeYaml

• FastJson

• Jackson

反序列化漏洞条件

1.被反序列化的对象存在重写readObject方法，且这个方法中存在攻击方法

2.被反序列化的对象存在toString方法，且这个方法中存在攻击方法，而且被反序列化的对象被输出

学习java反射机制

反射就是加载类，获取类的各种信息并操作他们 可以通过修改变量的值去达到利用漏洞，如：

public class cmd_shell{ public String cmd="calc"; public void shell(){ Runtime.getRuntime().exec(cmd); } }

1.反射第一步：加载类，获取类的字节码：Class对象

2.获取类的构造器：Constructor对象

3.获取类的成员变量：Field对象

4.获取类的成员方法：Method对象

学习js逆向动态调试

1. 找到发包时提交的那个地址
2. 搜索那个地址在js文件中
3. 找到调用的函数

学习vue.js框架与打包器

这个框架比较安全一般只存在xss漏洞

使用v-html可能会存在这个漏洞 使用文本插值（{{}}）代替 v-html可以修复漏洞

这个框架会有个默认的打包器， vite.config.ts

webpack存在.js.map文件的泄露，通过.js.map的查找可以找到js源码。