# Java

1. 身份验证绕过
    1. 拦截器
    2. 过滤器
    3. 常见身份验证绕过模式
    4. https://tttang.com/archive/1899/
2. 服务器端模板注入
3. JDBC
    1. 常见驱动程序及其利用
    2. 反序化+mysql
4. Struts 框架相关漏洞
5. JDNI
6. Java 反序列化
    1. Ysoserial 构建的原理 https://tttang.com/archive/1683/
    2. 自己写个吊毛工具链 https://tttang.com/archive/1729/
7. 最后是shiro https://tttang.com/archive/1592/
    1. 权限绕过思路比较值得学习
8. 补充一下codeql的知识就行

## 必看文章

https://tttang.com/archive/1899/

https://tttang.com/archive/1831/

https://tttang.com/archive/194/

https://tttang.com/archive/1511/

https://tttang.com/archive/1462/

https://tttang.com/archive/1645/

https://tttang.com/archive/1405/

https://tttang.com/archive/1441/

# Python

1. Flask 密钥硬编码

# PHP