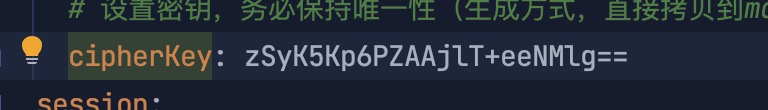
Shiro的反序列化

Shiro两个常见漏洞 一个是密钥硬编码、一个是权限绕过

若依版本 4.6.0

硬编码密钥

关键字setCipherKey



可以查看到代码里的硬编码密钥

shiro的流程

1：生成cookie：序列化 => 使用密钥进行AES加密 => Base64编码，最后返回客户端 remebreme Cookie；

2： 识别cookie：得到rememberMe的cookie值=>Base64解码=>使用密钥进行AES解密=>反序列化。

攻击者只要找到AES的key

构造恶意的对象 加密、编码之后发送给服务器 服务器进行解码用key解密就会执行反序列化漏洞

复现

未授权访问（不存在）

找到shiro的过滤器配置文件

anon表示匿名访问也就是无需认证即可访问

authc表示需要认证才可访问

文本

描述已自动生成

看下该处代码配置有没有authc

因为代码里存在这个 所以不存在权限绕过

文本

描述已自动生成