JEEWMS Shipper Information Leakage

http://192.168.244.1:8080/jeewms\_war/wmOmNoticeHController.do?exportXls

1. Vulnerability Description

Guangzhou Huayi Intelligent Technology Co., Ltd.'s main business scope includes technology promotion and application services, software development, digital content services, information technology consulting, animation and comics design, data processing and storage, information system integration, and wholesale and retail of computer and communication equipment. Its intelligent warehouse management system JEEWMS has an information leakage vulnerability in the wmOmNoticeHController.do path. Attackers can download relevant shipping information by accessing wmOmNoticeHController.do?exportXls, which leaks important information such as the shipper's address, name, and contact information.

2. Impact of the vulnerability

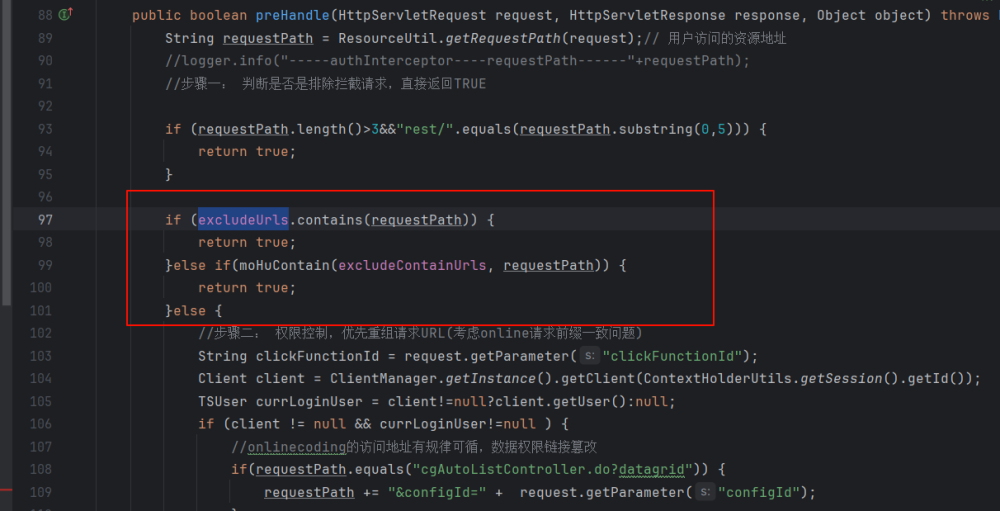
wmOmNoticeHController.do?exportXls leaks relevant shipper information

3. Vulnerability location

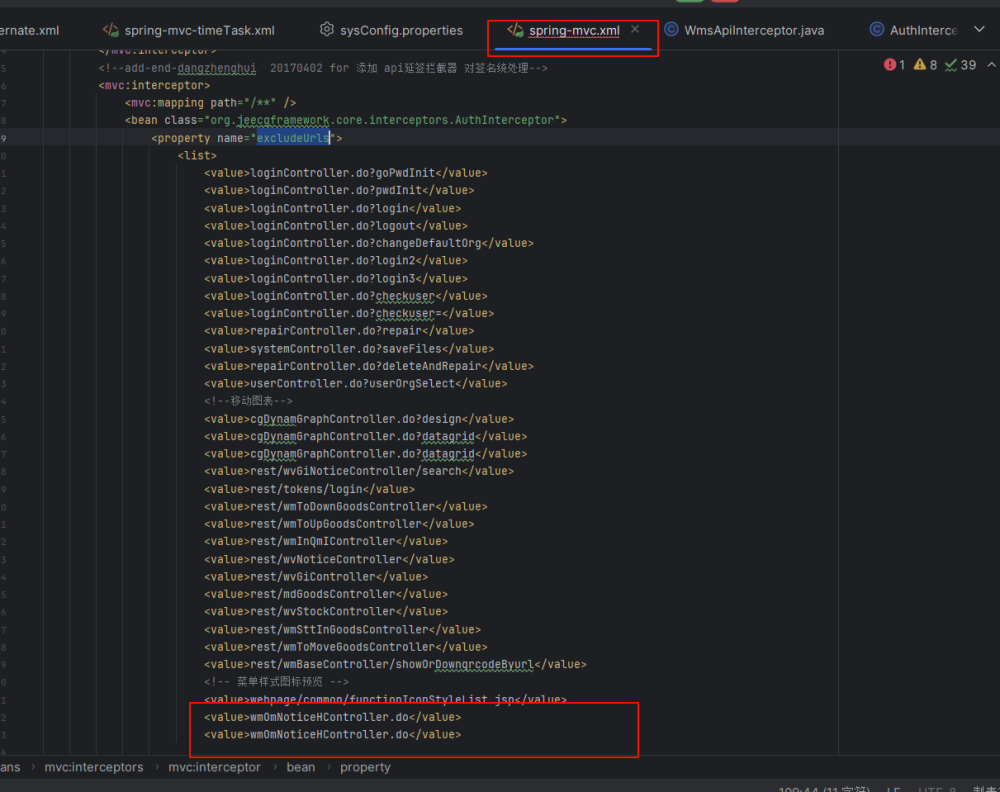
src/main/java/com/zzjee/wm/controller/WmOmNoticeHController.java

4. Code analysis

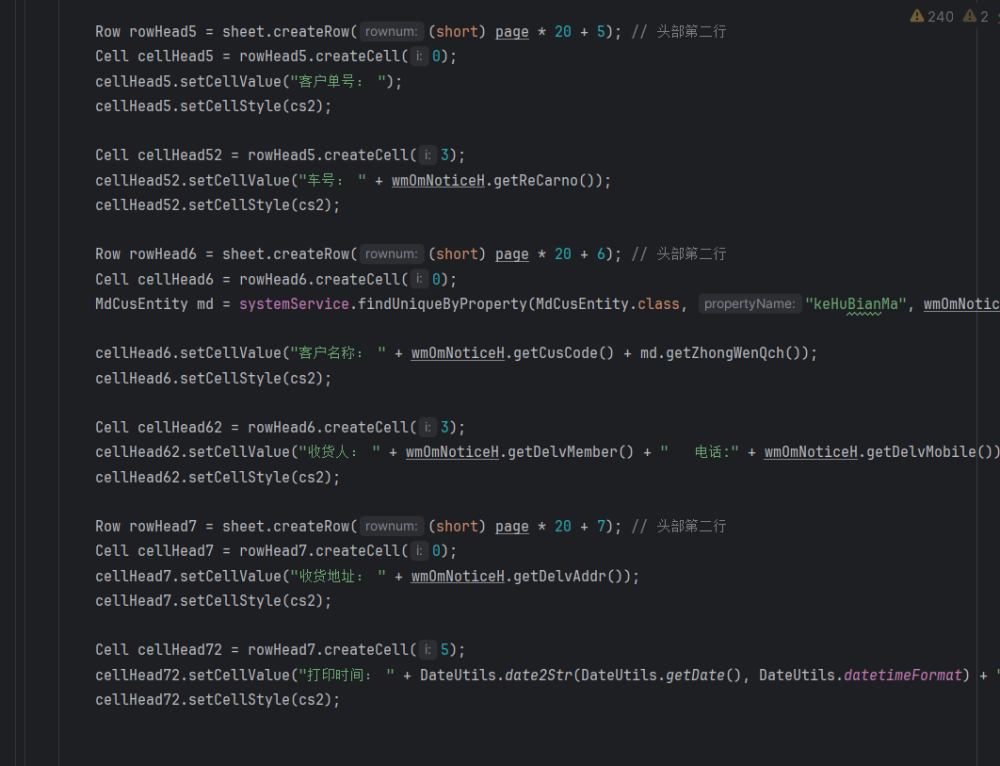
src/main/java/org/jeecgframework/core/interceptors/AuthInterceptor.java sets the path that does not require authorization in excludeUrls.



src/main/resources/spring-mvc.xml allows wmOmNoticeHController.do unlimited authorization to access



Export related information in exportXls

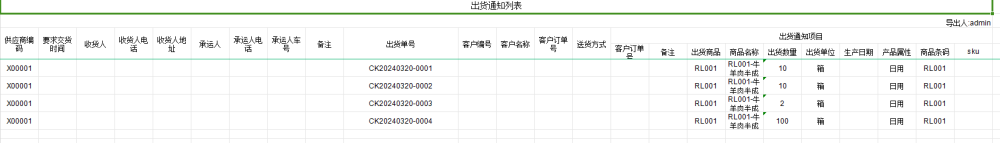


5. Vulnerability Reproduction

Project address: <https://gitee.com/erzhongxmu/JEEWMS>

Download code and build:

Visit<http://192.168.0.102:8080/jeewms_war/wmOmNoticeHController.do?exportXls>



Project test website reproduction:

<http://47.113.229.131:9080/jeewms/wmOmNoticeHController.do?exportXls>

