Introduction to pigx（pigx 简介）

The pigX framework is a microservice development framework based on Spring Cloud. It integrates excellent frameworks such as Spring Boot, MyBatis, and MyBatis-Plus, and provides a complete microservice solution. PigX is committed to simplifying the microservice development process, improving development efficiency, and provides a wealth of functional modules, such as authentication and authorization, monitoring, and log management.

Vulnerability description（漏洞描述）

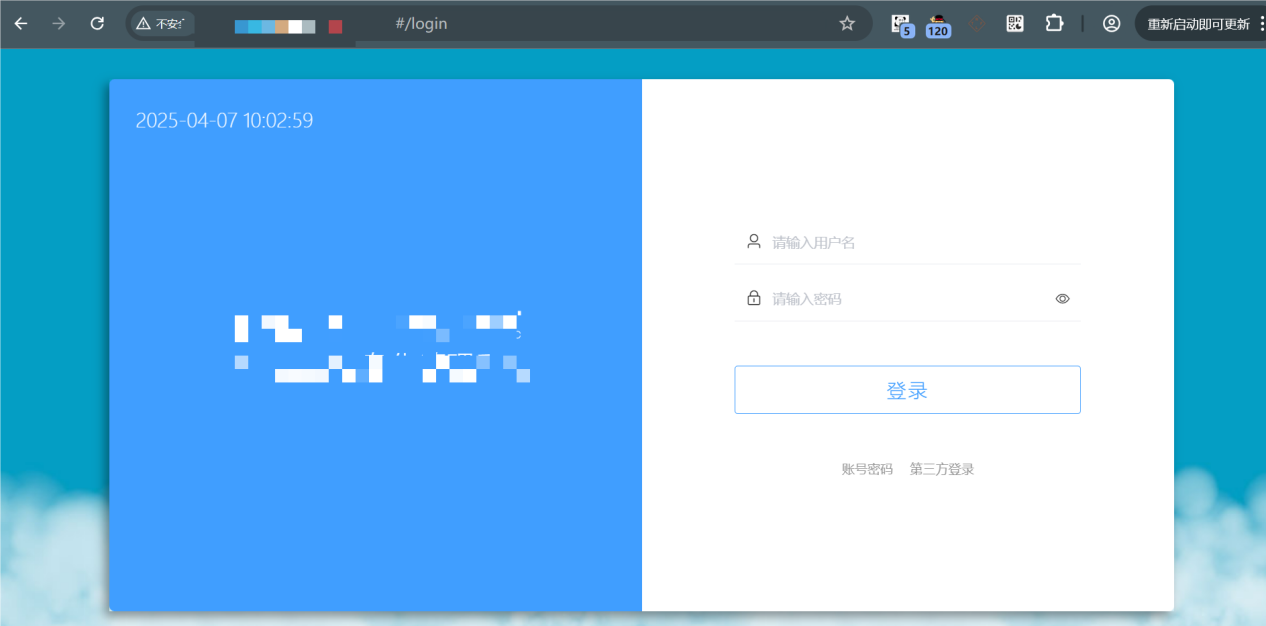
As mentioned in the previous introduction, the pigX framework is a microservice development framework based on Spring Cloud, but the pigX framework is in Spring Cloud. After enabling Actuator in the project, by default, we can access any interface without restriction. Some of these interfaces expose very sensitive information, such as: /env, /configprops, /threaddump and other interfaces, which directly display all information.

Loophole principle（漏洞原理）

When visiting a website, the brute force path method is found to exist /admin/actuator. At this time, check whether there is a heapdump file, download and decompress it, and search globally to find the key leak. After getting the file address, visit and download, and use tools to crawl the content after downloading. Found leaked ak\sk

Case reproduction（案例复现）

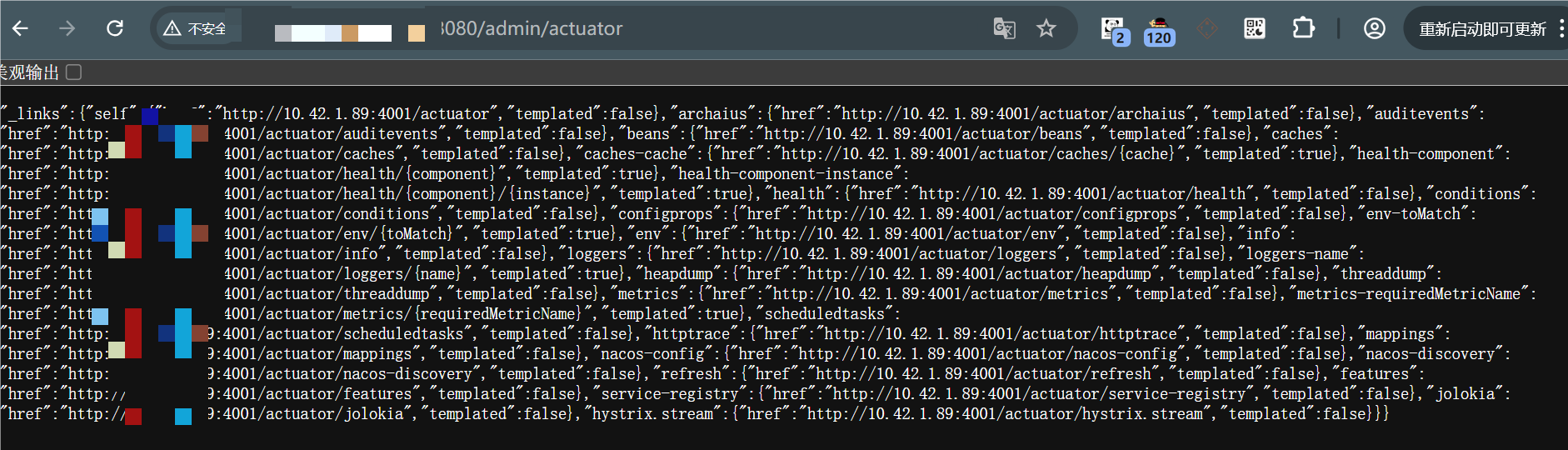
As shown, this is a test site



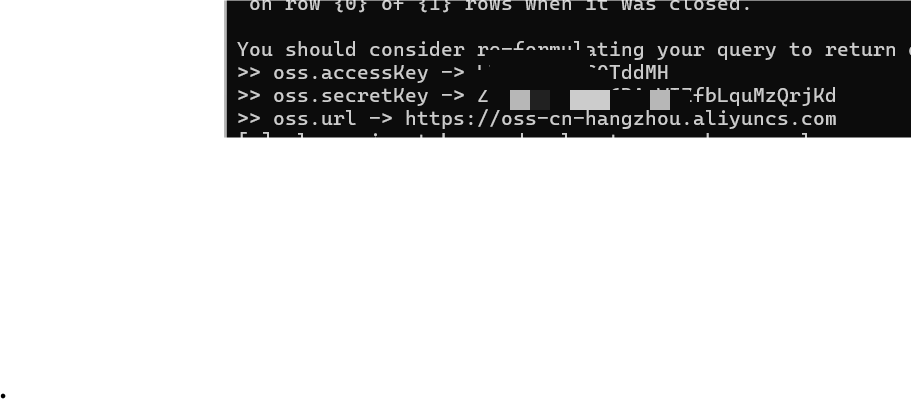
By brute-forcing the website, we found that /admin/actuator exists.

<http://ip:port/admin/actuator>

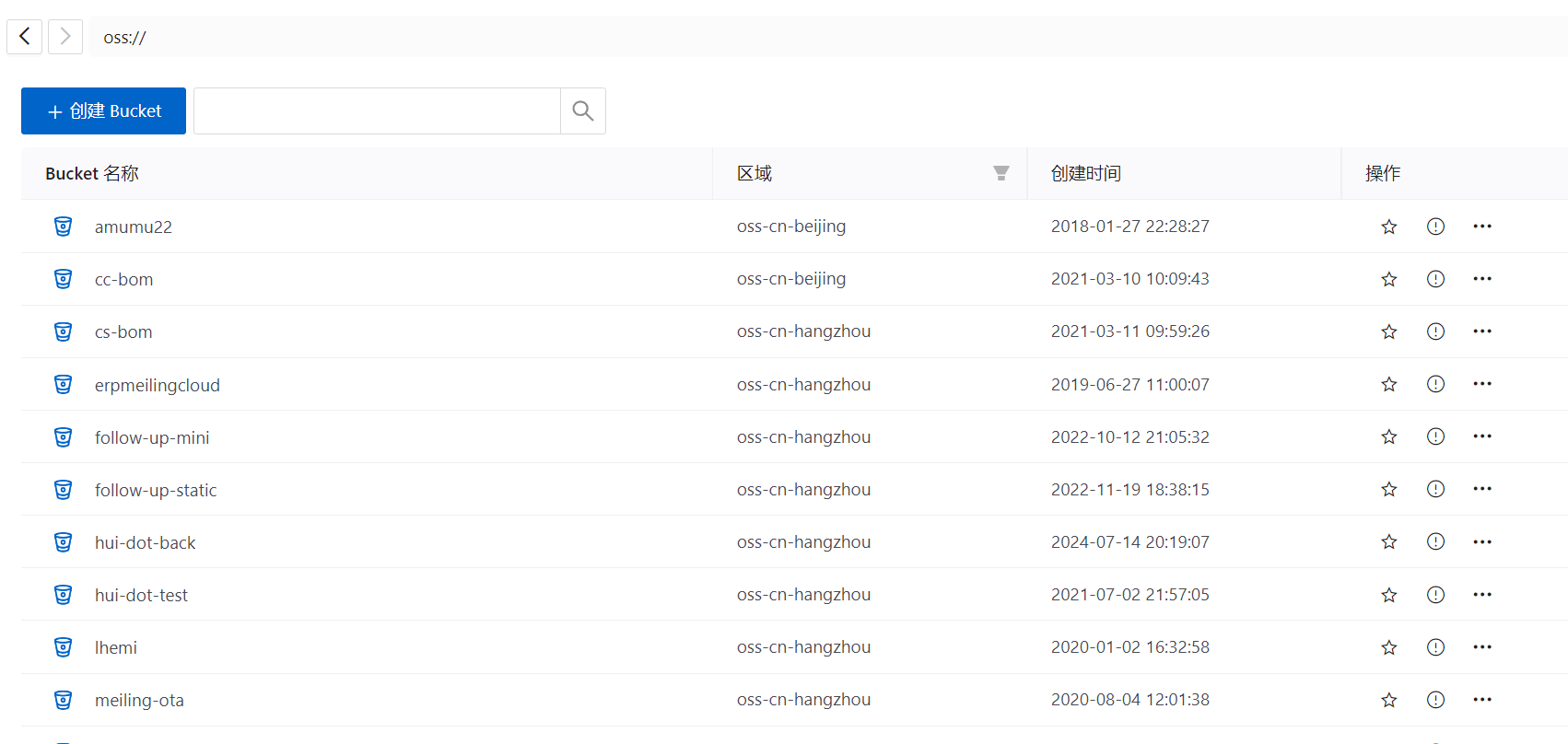
A large number of endpoints were found on this page



Then connect heapdump to http://ip:port/admin/actuator, you can download the heapdump file and decrypt it to get the aksk of the cloud storage bucket



You can take over the bucket



Tool link: <https://github.com/whwlsfb/JDumpSpider>

The affected version（受影响的版本）

PigX rapid development framework v 4.0

PigX rapid development framework v 3.0.0

PigX rapid development framework v 4.5