白帽子昵称：毕竟话少

漏洞描述

漏洞URL：如果是Web就填写此项

http://xxx.bxxxx.top/xx/x/actuator/env

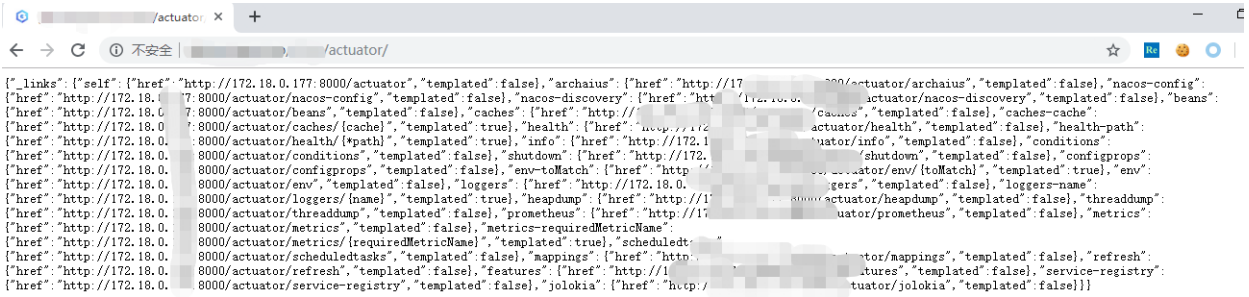
http://xxx.bxxxx.top/xx/x/actuator/heapdump

简要描述：漏洞说明、利用条件、危害等

此站点使用了Spring Actuator组件，无需授权即可访问，通过JVM分析工具可以获取到应用对应的邮件系统、SMS系统、Redis、Mysql账户密码、阿里云Access_Key等等敏感配置信息，最终导致大量敏感内容泄漏

漏洞证明：

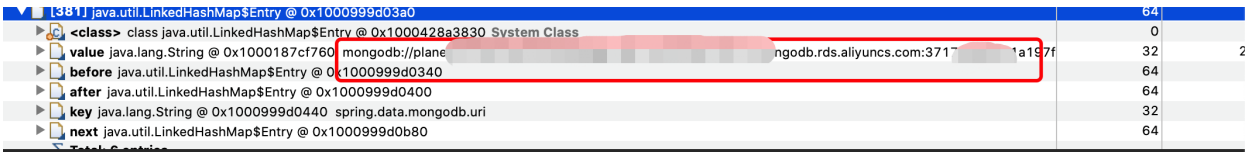
http://xxx.bxxxx.top/xx/x/actuator/



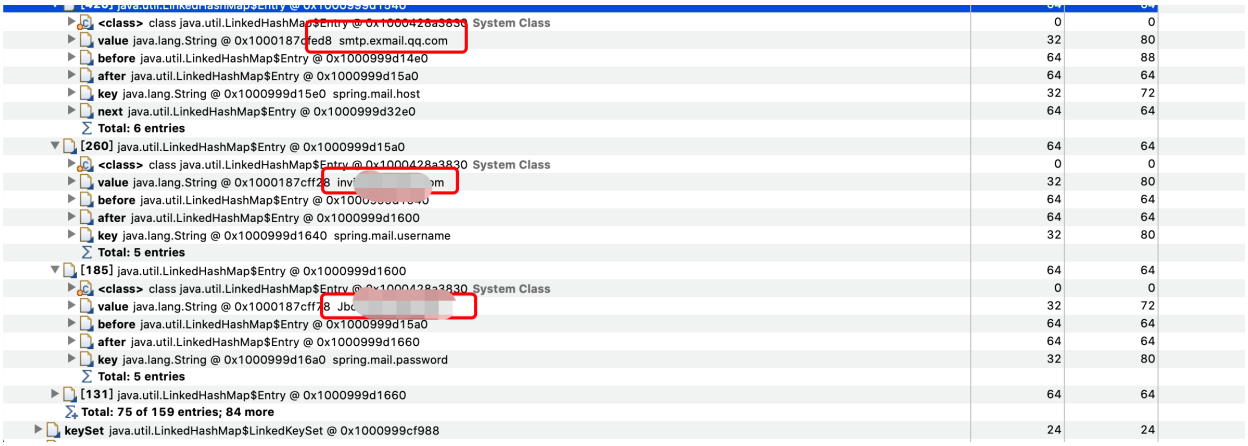
浏览器直接访问http://xxx.bxxxx.top/xx/x/actuator/heapdump 可下载到JAVA HeapDump数据

进一步使用MAT分析根据对heapdump进行分析，可以发现应用内部各类配置信息，如：

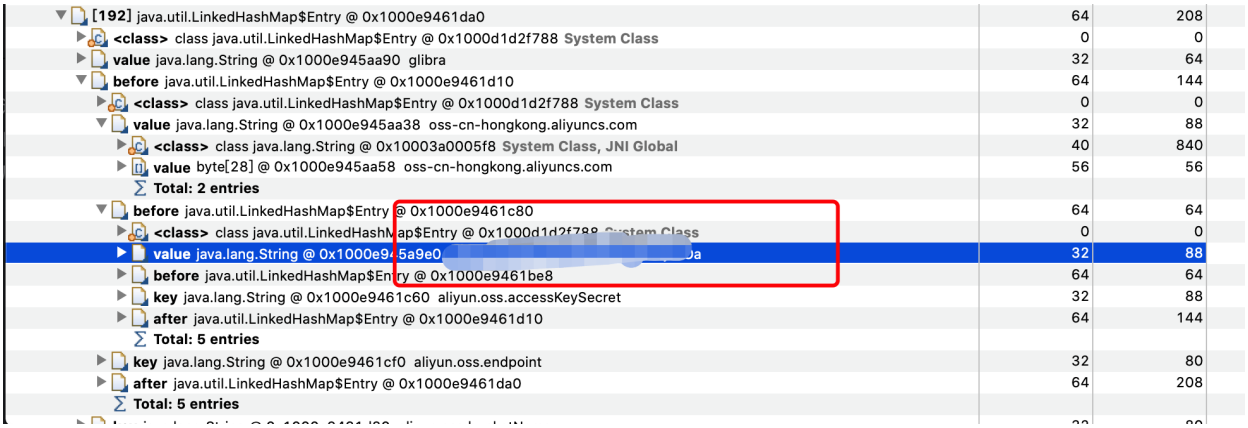
1.mongodb数据库账户密码



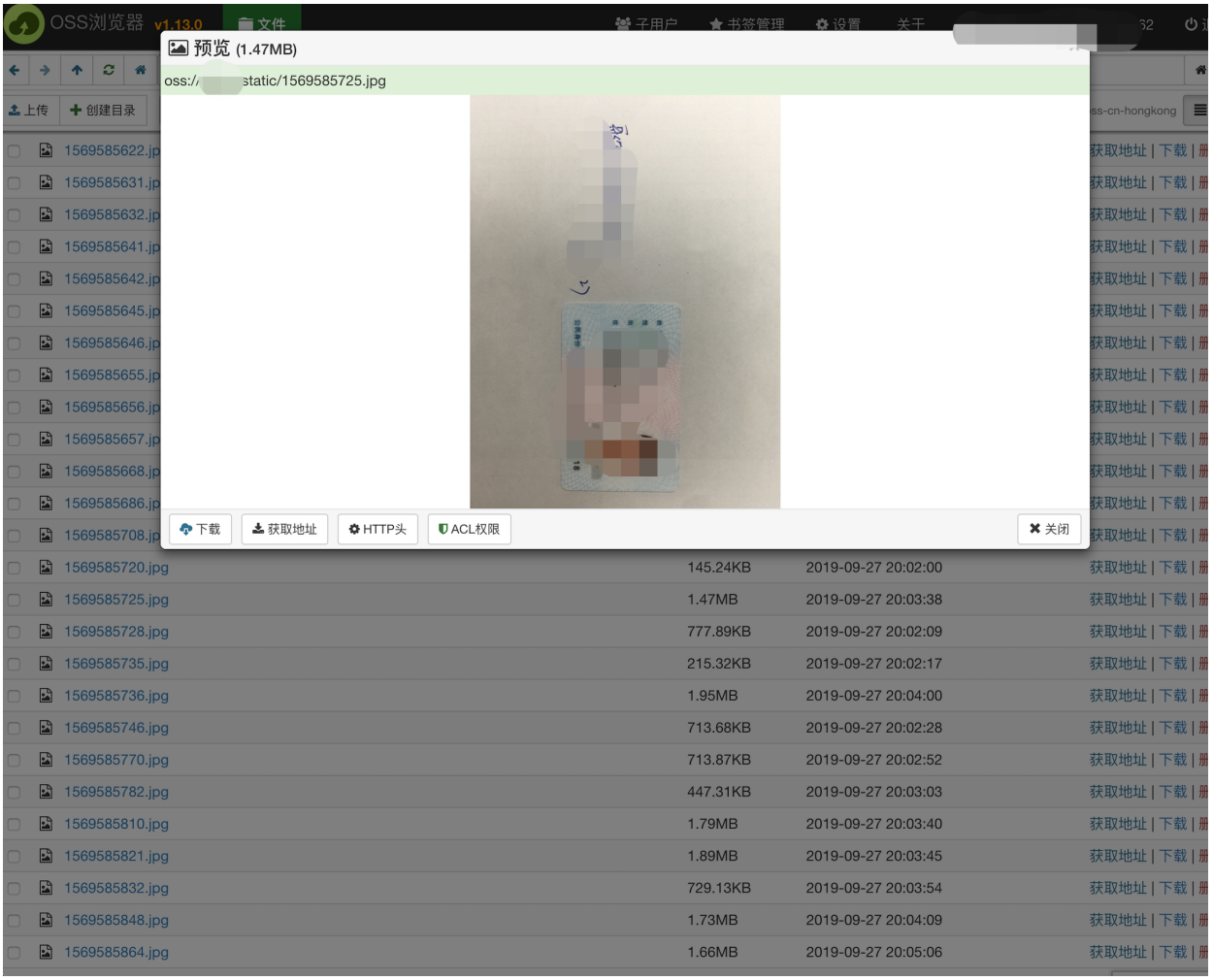
2.企业邮箱账户密码

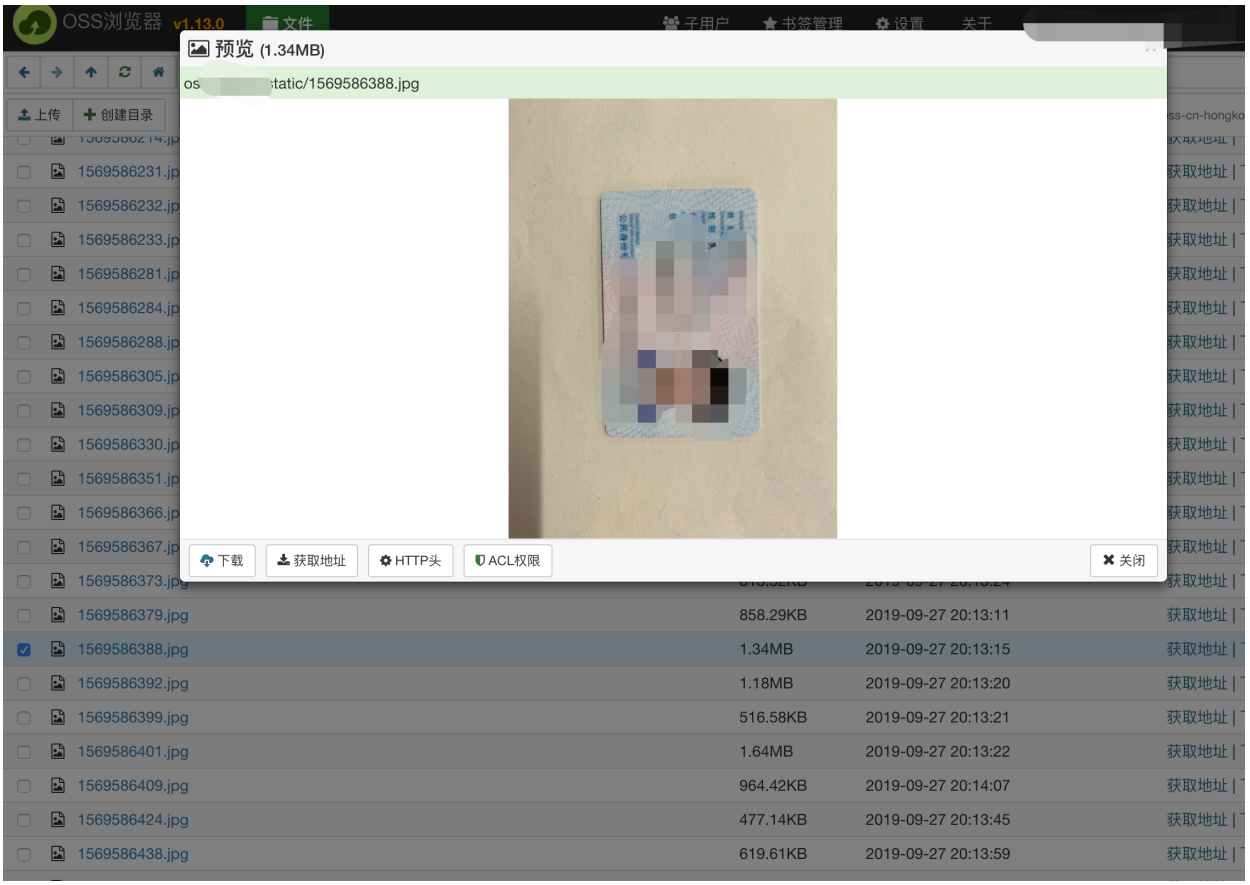


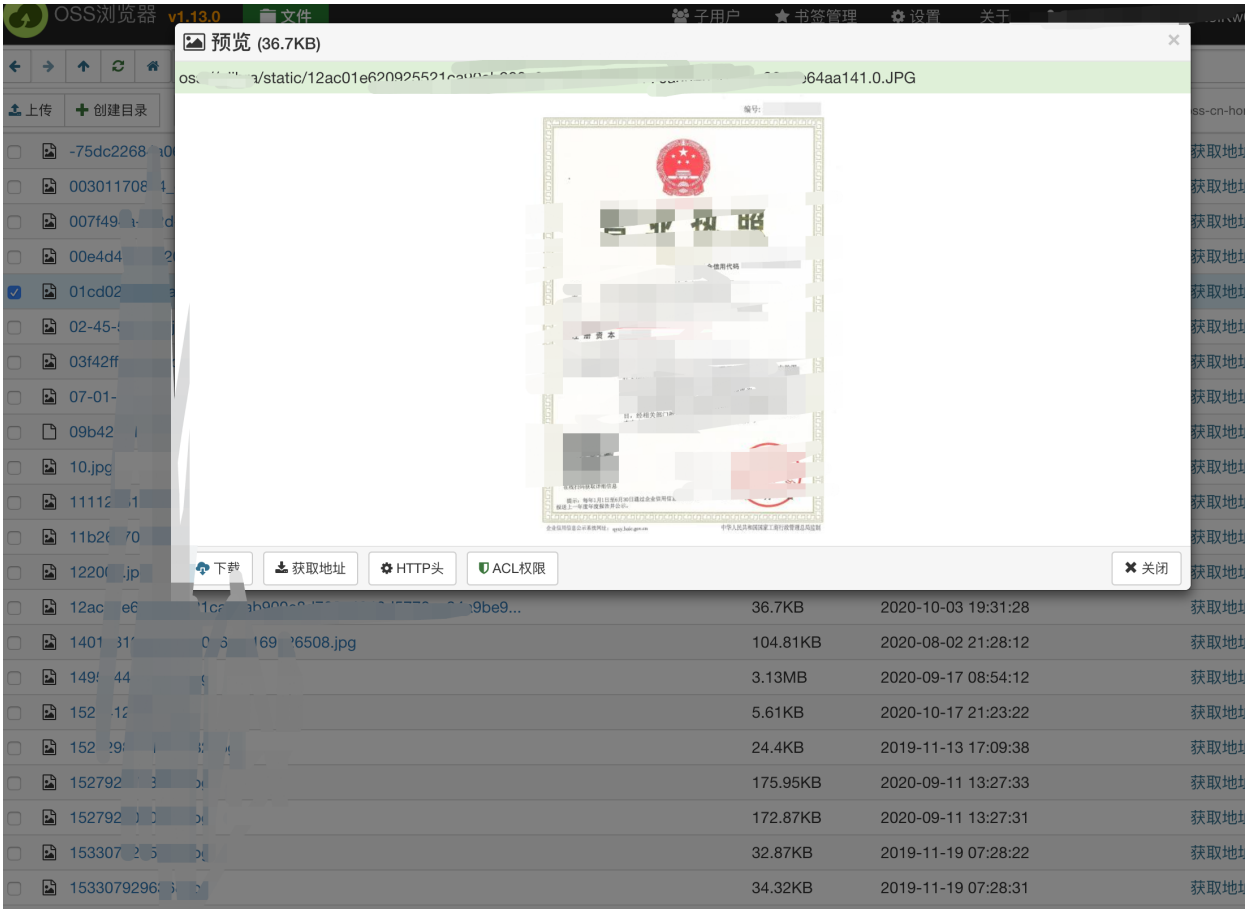
3.阿里云OSS云存储的Access_key



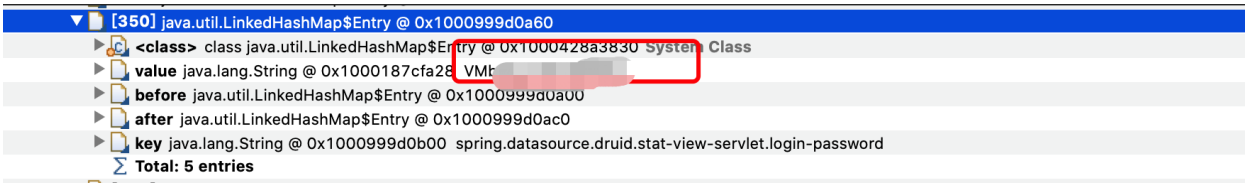
使用阿里云OSS浏览器连接后，可以读取大量用户的敏感数据（身份证信息，营业职照等）：


OSS浏览器 v1.13.0
文件
子用户
书签管理
设置
关于
预览 (1.47MB)
oss://static/1569585725.jpg
下载
获取地址
HTTP头
ACL权限
关闭
上传
创建目录
1569585720.jpg 145.24KB 2019-09-27 20:02:00
1569585725.jpg 1.47MB 2019-09-27 20:03:38
1569585728.jpg 777.89KB 2019-09-27 20:02:09
1569585735.jpg 215.32KB 2019-09-27 20:02:17
1569585736.jpg 1.95MB 2019-09-27 20:04:00
1569585746.jpg 713.68KB 2019-09-27 20:02:28
1569585770.jpg 713.87KB 2019-09-27 20:02:52
1569585782.jpg 447.31KB 2019-09-27 20:03:03
1569585810.jpg 1.79MB 2019-09-27 20:03:40
1569585821.jpg 1.89MB 2019-09-27 20:03:45
1569585832.jpg 729.13KB 2019-09-27 20:03:54
1569585848.jpg 1.73MB 2019-09-27 20:04:09
1569585864.jpg 1.66MB 2019-09-27 20:05:06

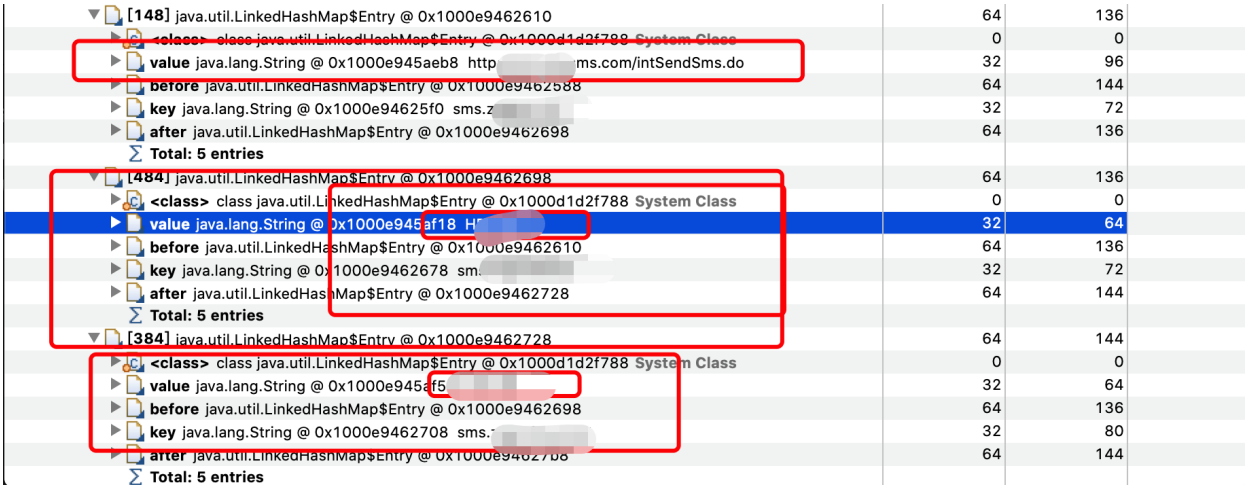


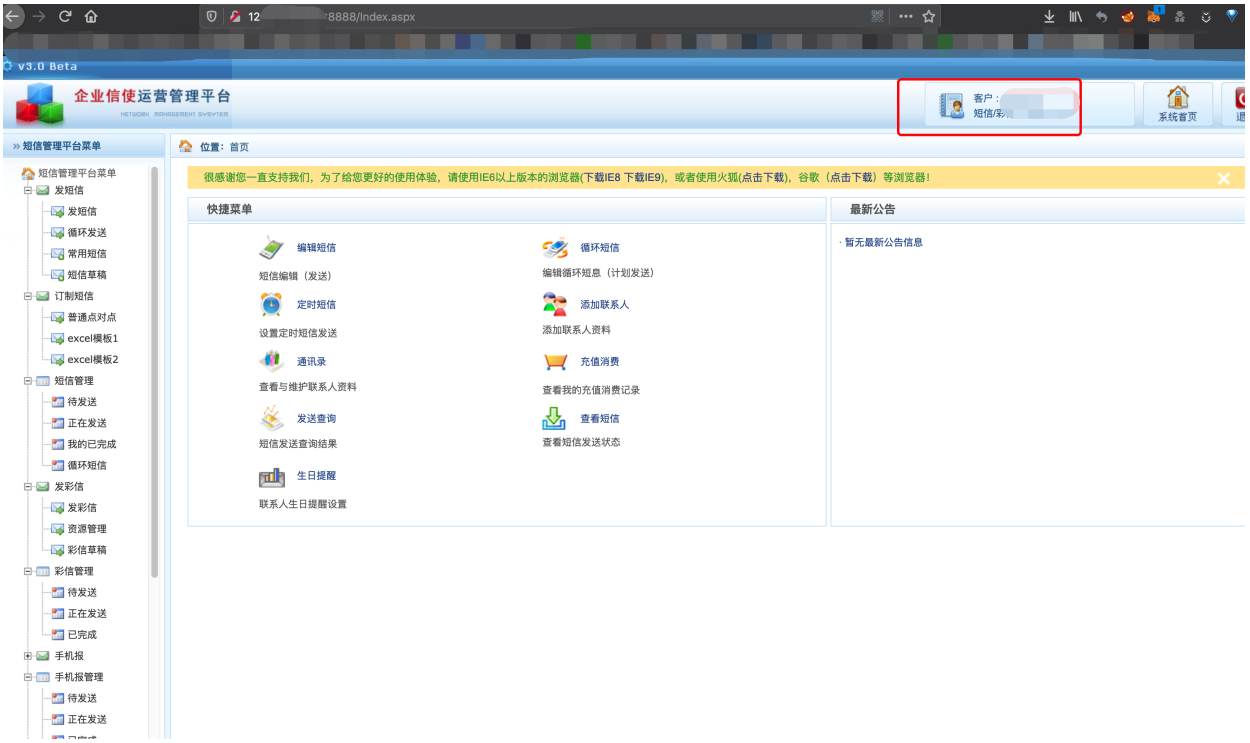


3.Alibaba Druid组件登录密码

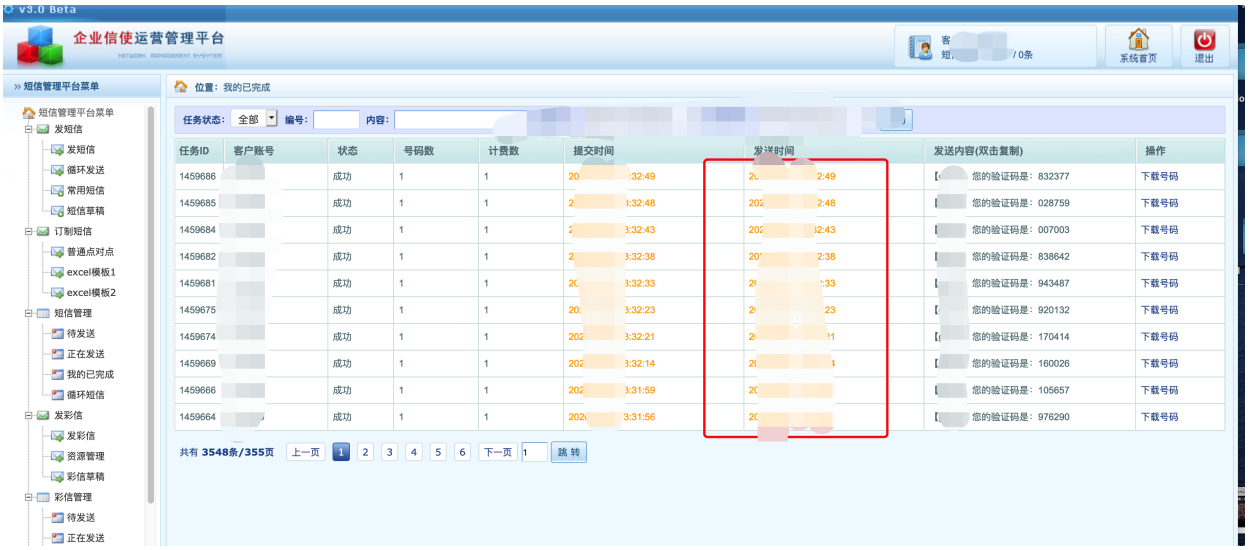


4、SMS发信配置信息

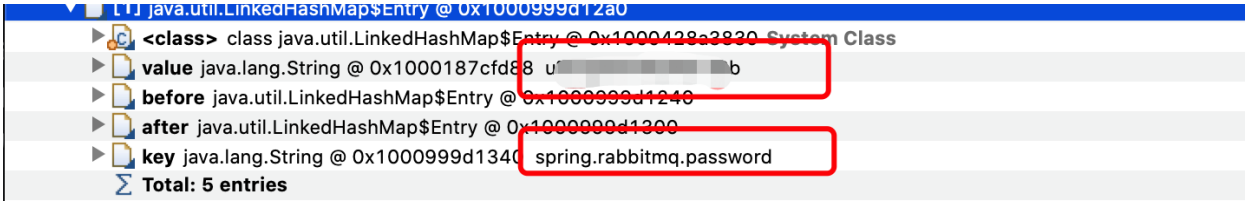




可以获取平台所有的sms发信记录



5.RabbitMQ密码



漏洞利用代码：

http://xxx.bxxxx.top/xx/x/actuator/heapdump

修复方案：

访问控制

漏洞总结

Actuator是Spring Boot提供的服务监控和管理中间件，使用默认配置的情况下可能会导致未授权访问漏洞，同时间Actuator的部分接口会泄露网站流量信息和内存信息等敏感内容。攻击者通过借助其他关联组件甚至可以获取到webserver的控制权限

开发人员可参考以下配置规避此漏洞

1. 禁用所有接口，将配置改成：endpoints.enabled = false
2. 引入spring-boot-starter-security依赖

```
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-security</artifactId>
</dependency>
```

3. 开启security功能，配置访问权限验证，类似配置如下：

```
management.port=8099
management.security.enabled=true
security.user.name=xxxxx
security.user.password=xxxxxx
```