SpringBoot应用监控Actuator使用的安全隐患

cryin / 2018-03-30 13:53:17 / 浏览数 49255 安全技术 WEB安全 顶(0) 踩(0)

SpringBoot应用监控Actuator使用的安全隐患

概述

微服务作为一项在云中部署应用和服务的新技术是当下比较热门话题，而微服务的特点决定了功能模块的部署是分布式的，运行在不同的机器上相互通过服务调用进行交互，

而Actuator正是Spring Boot提供的对应用系统的监控和管理的集成功能，可以查看应用配置的详细信息，例如自动化配置信息、创建的Spring beans信息、系统环境变量的配置信以及Web请求的详细信息等。如果使用不当或者一些不经意的疏忽，可能造成信息泄露等严重的安全隐患。

Actuator使用

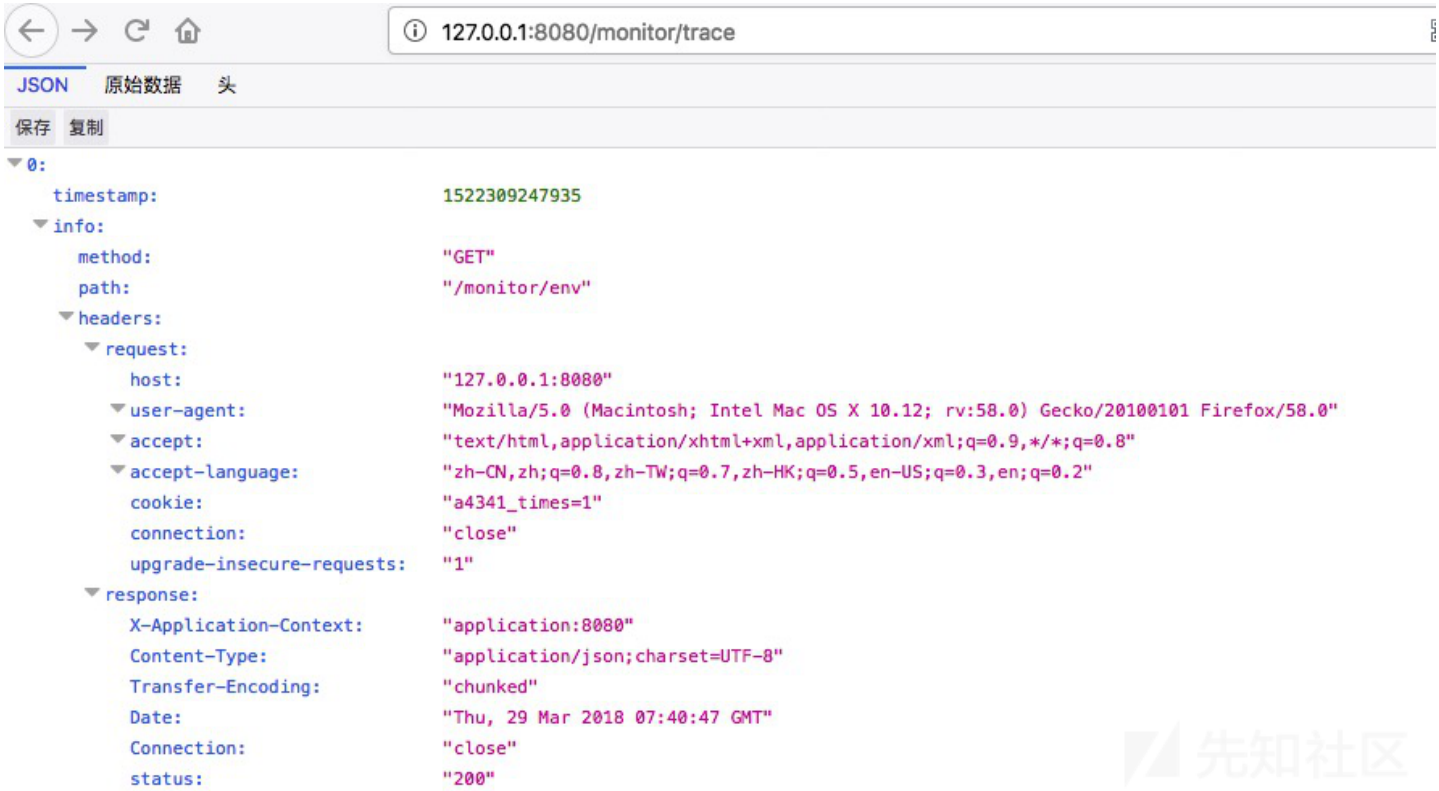
Actuator应用监控使用只需要添加spring-boot-starter-actuator依赖即可，如下：

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

可以在application.properties中指定actuator的访问路径，如指定路径为/monitor：

```
management.context-path=/monitor
```

此时，运行示例,访问/monitor/env即可查看系统环境变量的配置信息，之后再访问/monitor/trace即可查看所有Web请求的详细信息，包括请求方法、路径、时间戳以及请



Actuator监控分成两类：原生端点和用户自定义扩展端点，原生的主要有：

路径	描述
/autoconfig	提供了一份自动配置报告，记录哪些自动配置条件通过了，哪些没通过
/beans	描述应用程序上下文里全部的Bean，以及它们的关系
/env	获取全部环境属性
/configprops	描述配置属性(包含默认值)如何注入Bean
/dump	获取线程活动的快照
/health	报告应用程序的健康指标，这些值由HealthIndicator的实现类提供
/info	获取应用程序的定制信息，这些信息由info打头的属性提供
/mappings	描述全部的URI路径，以及它们和控制器(包含Actuator端点)的映射关系
/metrics	报告各种应用程序度量信息，比如内存用量和HTTP请求计数
/shutdown	关闭应用程序，要求endpoints.shutdown.enabled设置为true

/trace 提供基本的HTTP请求跟踪信息(时间戳、HTTP头等)

安全措施

如果上述请求接口不做任何安全限制，安全隐患显而易见。实际上Spring Boot也提供了安全限制功能。比如要禁用/env接口，则可设置如下：

```
endpoints.env.enabled= false
```

如果只想打开一两个接口，那就先禁用全部接口，然后启用需要的接口：

```
endpoints.enabled = false
endpoints.metrics.enabled = true
```

另外也可以引入spring-boot-starter-security依赖

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

在application.properties中指定actuator的端口以及开启security功能，配置访问权限验证，这时再访问actuator功能时就会弹出登录窗口，需要输入账号密码验证后才允

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

安全建议

在使用Actuator时，不正确的使用或者一些不经意的疏忽，就会造成严重的信息泄露等安全隐患。在代码审计时如果是springboot项目并且遇到actuator依赖，则有必要对
安全的做法是一定要引入security依赖，打开安全限制并进行身份验证。同时设置单独的Actuator管理端口并配置不对外网开放。

参考

- http://www.csecgroup.com/blog/springboot_actuator_security_tips/
- https://docs.spring.io/spring-boot/docs/current/reference/htmlsingle/#production-ready

上一篇：如何用不同的数值构建一样的MD5 ... 下一篇：Dedecms V5.7 后台文件...

1. 4 条回复

71428****@qq.com 2018-09-28 16:48:56

类似的情况也要考量druid、hystrix.stream之类的组件依赖和监控，可以排查gradle和pom文件里的配置。es搜索为命令为
"query": {
"bool": {
"must": [

```
#{"term": {"extension": "xml"}},
              # {"match_phrase":{"contents": "mybatis-3-mapper.dtd"}},
               #{"match": {"contents": ""}},
               {"match": {"contents": "org.springframework.boot:spring-boot-starter-actuator"}},
               {"match":{"refs": "master"}}
          ]
       }
    }
```

0 回复Ta


寇明明 2019-02-13 17:26:47

您好，配置security后，登陆页面怎么弹出，需要配置自定义登陆页面吗

0 回复Ta


完整的镜子 2019-06-13 15:11:01

感谢分享，我也挖到了这样的洞，这篇文章帮了我很多。

0 回复Ta


cryin 2019-10-15 14:34:33

@寇明明 在application.properties中开启security功能，配置访问账号密码，重启应用即可弹出。不需要自己写登录页面。配置示例如下：
management.security.enabled=true
security.user.name=admin

security.user.password=adminxxx

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板