spring-boot-actuator-logview 文件包含(CVE-2021-21234)漏洞分析

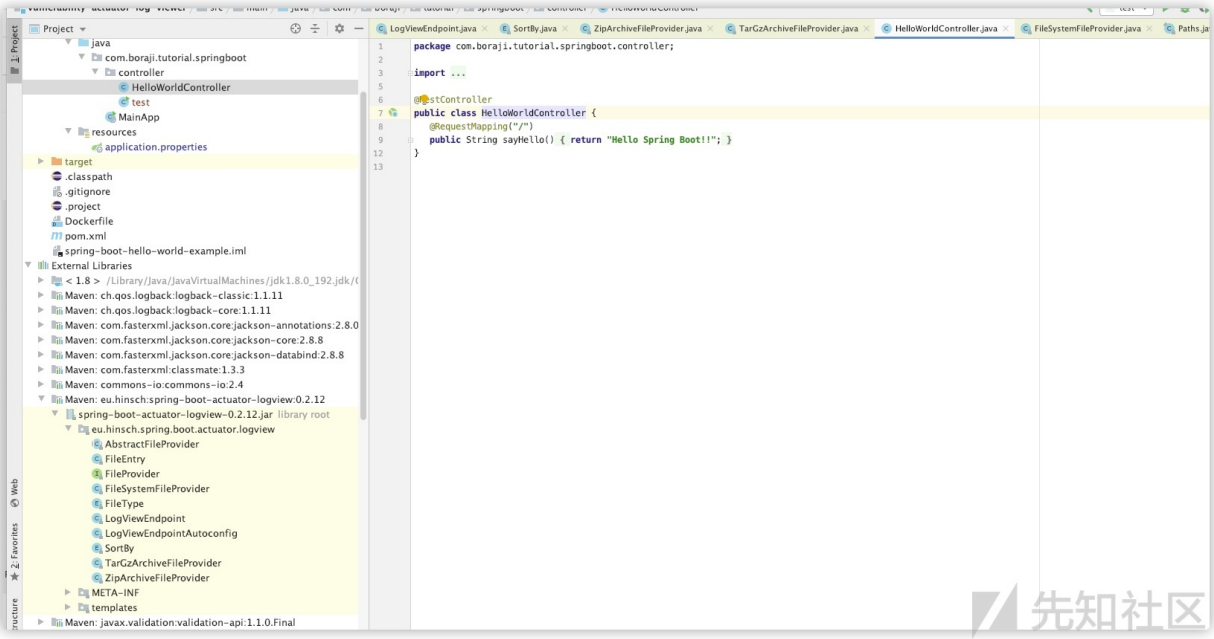
t4mo / 2021-07-28 23:50:00 / 浏览数 2684

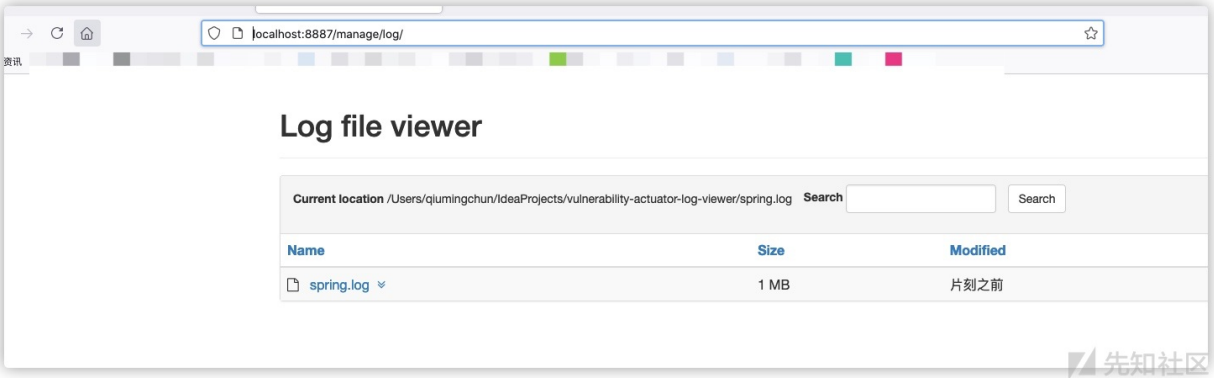
前言

日常搬砖过程中在github发现的一个CVE，https://github.com/ARPSyndicate/kenzer-templates/blob/1f1dd550ddbde72cbe378452973b93b3e62003f5/jaeles/cvescan/medium/CVE-2021-21234.yam 看着带了springboot就分析了下

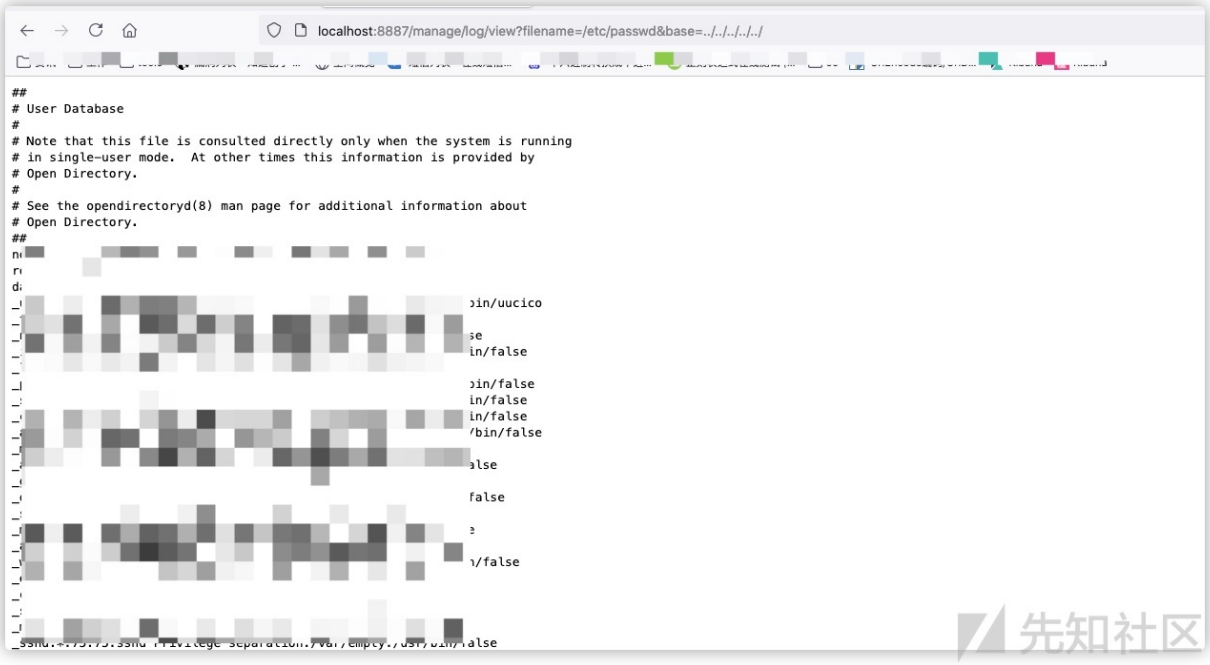
环境搭建

git clone https://github.com/cristianeph/vulnerability-actuator-log-viewer
启动之后访问 http://localhost:8887/manage/log/

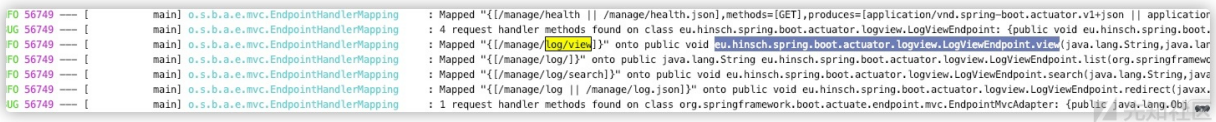




漏洞复现分析



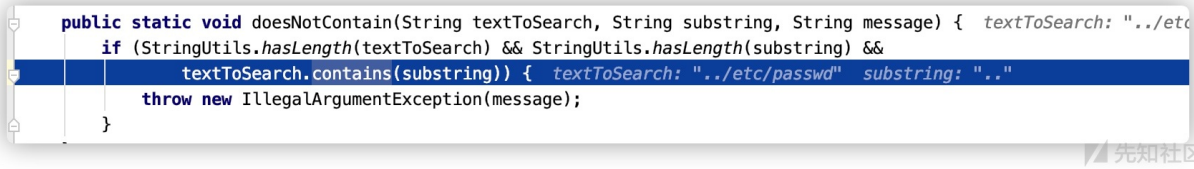
根据springboot启动日志发现/log/view 对应的方法为eu.hinsch.spring.boot.actuator.logview.LogViewEndpoint.view



对应代码

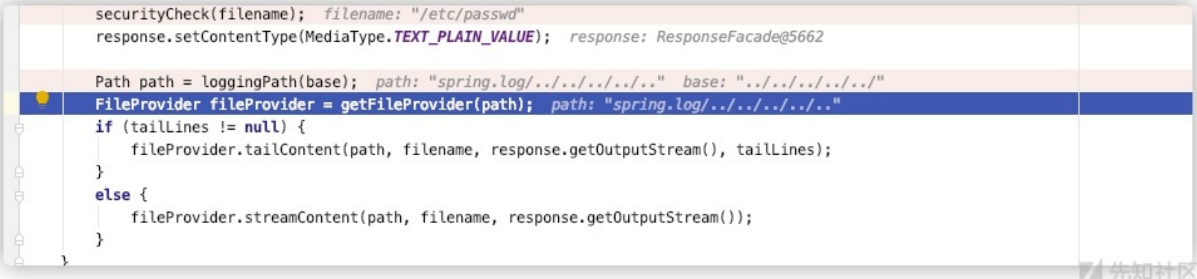
```
@RequestMapping("/view")
    public void view(@RequestParam String filename,
                     @RequestParam(required = false) String base,
                     @RequestParam(required = false) Integer tailLines,
                     HttpServletResponse response) throws IOException {
        securityCheck(filename);
        response.setContentType(MediaType.TEXT_PLAIN_VALUE);

        Path path = loggingPath(base);
        FileProvider fileProvider = getFileProvider(path);
        if (tailLines != null) {
            fileProvider.tailContent(path, filename, response.getOutputStream(), tailLines);
        }
        else {
            fileProvider.streamContent(path, filename, response.getOutputStream());
        }
    }
```

先从RequestParam获取filename参数，然后调用securityCheck进行检查，判断filename是否包含..

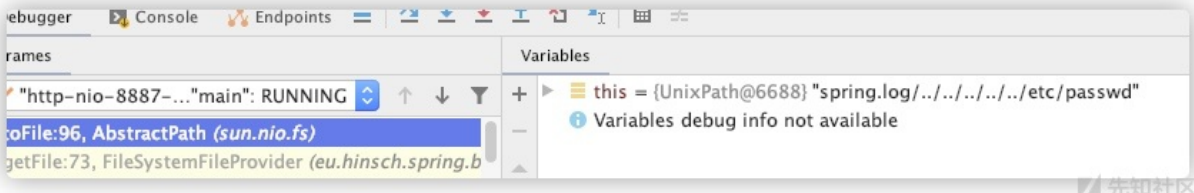


安全检查通过之后，将application.properties中logging.path和base拼接，返回path，base从RequestParam获取，并未经过securityCheck

然后生成fileProvider 在调用 streamContent



将path和base拼接，然后用fileinputstream打开，造成任意文件读取



上一篇： 记一次实战渗透(上)
下一篇： Java内存马：一种Tomcat全...

2 条回复

bluedo****

2021-07-29 10:18:48

第一个链接挂了

0 回复Ta

b1gd0d

2021-07-29 15:59:09

太强了

0 回复Ta

登录 后跟帖