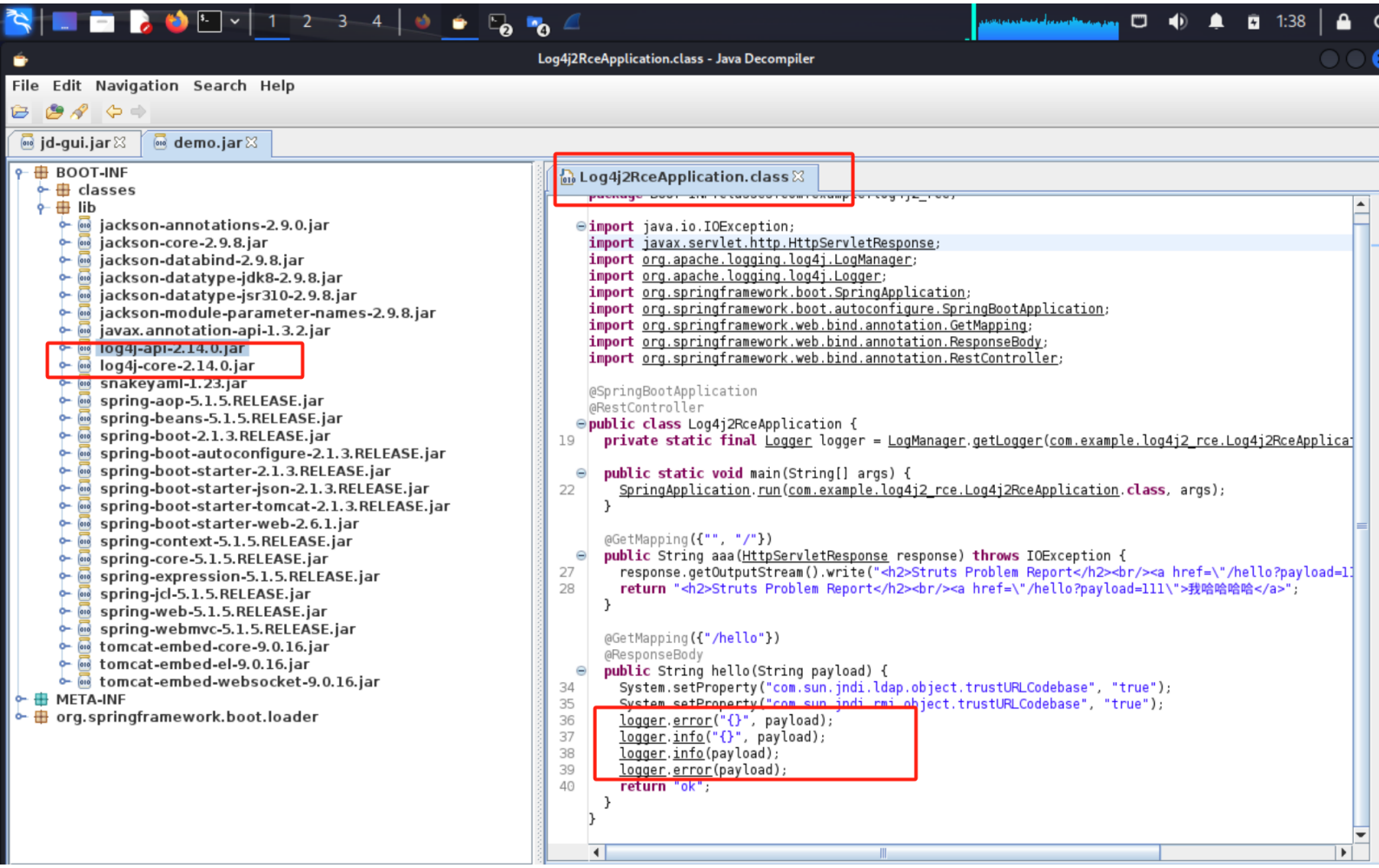
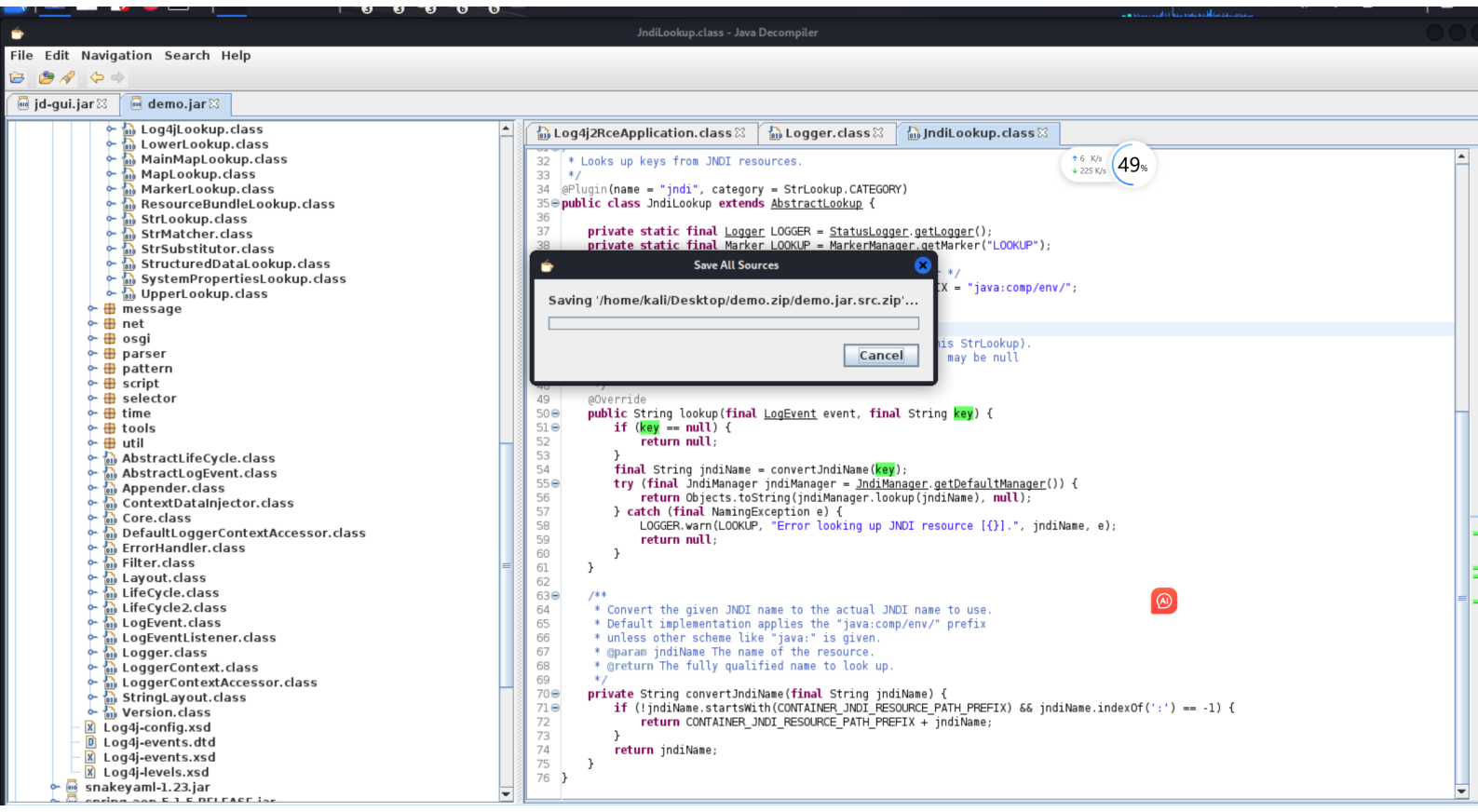
log4j修复.md /* https://github.com/microsoft/vscode/blob/master/extensions/markdown-language-features/media/markdown.css */ /*---------- * Copyright (c) Microsoft Corporation. All rights reserved. * Licensed under the MIT License. See License.txt in the project root for license information. *----------*/ body { font-family: var(--vscode-markdown-font-family, -apple-system, BlinkMacSystemFont, "Segoe WPC", "Segoe UI", "Ubuntu", "Droid Sans", sans-serif); font-size: var(--vscode-markdown-font-size, 14px); padding: 0 26px; line-height: var(--vscode-markdown-line-height, 22px); word-wrap: break-word; } #code-csp-warning { position: fixed; top: 0; right: 0; color: white; margin: 16px; text-align: center; font-size: 12px; font-family: sans-serif; background-color:#444444; cursor: pointer; padding: 6px; box-shadow: 1px 1px 1px rgba(0,0,0,.25); } #code-csp-warning:hover { text-decoration: none; background-color:#007acc; box-shadow: 2px 2px 2px rgba(0,0,0,.25); } body.scrollBeyondLastLine { margin-bottom: calc(100vh - 22px); } body.showEditorSelection .code-line { position: relative; } body.showEditorSelection .code-active-line:before, body.showEditorSelection .code-line:hover:before { content: ""; display: block; position: absolute; top: 0; left: -12px; height: 100%; } body.showEditorSelection li.code-active-line:before, body.showEditorSelection li.code-line:hover:before { left: -30px; } .vscode-light.showEditorSelection .code-active-line:before { border-left: 3px solid rgba(0, 0, 0, 0.15); } .vscode-light.showEditorSelection .code-line:hover:before { border-left: 3px solid rgba(0, 0, 0, 0.40); } .vscode-light.showEditorSelection .code-line .code-line:hover:before { border-left: none; } .vscode-dark.showEditorSelection .code-active-line:before { border-left: 3px solid rgba(255, 255, 255, 0.4); } .vscode-dark.showEditorSelection .code-line:hover:before { border-left: 3px solid rgba(255, 255, 255, 0.60); } .vscode-dark.showEditorSelection .code-line .code-line:hover:before { border-left: none; } .vscode-high-contrast.showEditorSelection .code-active-line:before { border-left: 3px solid rgba(255, 160, 0, 0.7); } .vscode-high-contrast.showEditorSelection .code-line:hover:before { border-left: 3px solid rgba(255, 160, 0, 1); } .vscode-high-contrast.showEditorSelection .code-line .code-line:hover:before { border-left: none; } img { max-width: 100%; max-height: 100%; } a { text-decoration: none; } a:hover { text-decoration: underline; } a:focus, input:focus, select:focus, textarea:focus { outline: 1px solid -webkit-focus-ring-color; outline-offset: -1px; } hr { border: 0; height: 2px; border-bottom: 2px solid; } h1 { padding-bottom: 0.3em; line-height: 1.2; border-bottom-width: 1px; border-bottom-style: solid; } h1, h2, h3 { font-weight: normal; } table { border-collapse: collapse; } table > thead > tr > th { text-align: left; border-bottom: 1px solid; } table > thead > tr > th, table > thead > tr > td, table > tbody > tr > th, table > tbody > tr > td { padding: 5px 10px; } table > tbody > tr + tr > td { border-top: 1px solid; } blockquote { margin: 0 7px 0 5px; padding: 0 16px 0 10px; border-left-width: 5px; border-left-style: solid; } code { font-family: Menlo, Monaco, Consolas, "Droid Sans Mono", "Courier New", monospace, "Droid Sans Fallback"; font-size: 1em; line-height: 1.357em; } body.wordWrap pre { white-space: pre-wrap; } pre:not(.hljs), pre.hljs code > div { padding: 16px; border-radius: 3px; overflow: auto; } pre code { color: var(--vscode-editor-foreground); tab-size: 4; } /** Theming */ .vscode-light pre { background-color: rgba(220, 220, 220, 0.4); } .vscode-dark pre { background-color: rgba(10, 10, 10, 0.4); } .vscode-high-contrast pre { background-color: rgb(0, 0, 0); } .vscode-high-contrast h1 { border-color: rgb(0, 0, 0); } .vscode-light table > thead > tr > th { border-color: rgba(0, 0, 0, 0.69); } .vscode-dark table > thead > tr > th { border-color: rgba(255, 255, 255, 0.69); } .vscode-light h1, .vscode-light hr, .vscode-light table > tbody > tr + tr > td { border-color: rgba(0, 0, 0, 0.18); } .vscode-dark h1, .vscode-dark hr, .vscode-dark table > tbody > tr + tr > td { border-color: rgba(255, 255, 255, 0.18); } /* Tomorrow Theme */ /* http://jmblog.github.com/color-themes-for-google-code-highlightjs */ /* Original theme - https://github.com/chriskempson/tomorrow-theme */ /* Tomorrow Comment */ .hljs-comment, .hljs-quote { color: #8e908c; } /* Tomorrow Red */ .hljs-variable, .hljs-template-variable, .hljs-tag, .hljs-name, .hljs-selector-id, .hljs-selector-class, .hljs-regexp, .hljs-deletion { color: #c82829; } /* Tomorrow Orange */ .hljs-number, .hljs-built_in, .hljs-builtin-name, .hljs-literal, .hljs-type, .hljs-params, .hljs-meta, .hljs-link { color: #f5871f; } /* Tomorrow Yellow */ .hljs-attribute { color: #eab700; } /* Tomorrow Green */ .hljs-string, .hljs-symbol, .hljs-bullet, .hljs-addition { color: #718c00; } /* Tomorrow Blue */ .hljs-title, .hljs-section { color: #4271ae; } /* Tomorrow Purple */ .hljs-keyword, .hljs-selector-tag { color: #8959a8; } .hljs { display: block; overflow-x: auto; color: #4d4d4c; padding: 0.5em; } .hljs-emphasis { font-style: italic; } .hljs-strong { font-weight: bold; } /* * Markdown PDF CSS */ body { font-family: -apple-system, BlinkMacSystemFont, "Segoe WPC", "Segoe UI", "Ubuntu", "Droid Sans", sans-serif, "Meiryo"; padding: 0 12px; } pre { background-color: #f8f8f8; border: 1px solid #cccccc; border-radius: 3px; overflow-x: auto; white-space: pre-wrap; overflow-wrap: break-word; } pre:not(.hljs) { padding: 23px; line-height: 19px; } blockquote { background: rgba(127, 127, 127, 0.1); border-color: rgba(0, 122, 204, 0.5); } .emoji { height: 1.4em; } code { font-size: 14px; line-height: 19px; } /* for inline code */ :not(pre):not(.hljs) > code { color: #C9AE75; /* Change the old color so it seems less like an error */ font-size: inherit; } /* Page Break : use to insert page break ---------- */ .page { page-break-after: always; } mermaid.initialize({ startOnLoad: true, theme: document.body.classList.contains('vscode-dark') || document.body.classList.contains('vscode-high-contrast') ? 'dark' : 'default' }); log4j 漏洞原理 Log4j 是一款通用日志记录工具，其原理如下：开发人员可利用它记录当前程序状态，除直接记录文本外，还能使用简单表达式记录动态内容。表达式用 ${} 包裹，通过不同解析器解析，如 sys 解析器可在系统环境变量中查找指定内容进行替换。

Log4j 中的 jndi 解析器通过 JDK 获取 jndi 对象来替换原有文本打印。JDK 会从指定 url 路径下载字节流并反序列化为 Java 对象作为 jndi 返回，反序列化过程会执行字节流中的程序。若攻击者能控制日志打印内容，就可让目标服务器从其指定的 url 下载代码

字节流，使附带代码在目标服务器上执行。 漏洞修改原理： log4j2中通过JndiLookup类进行jndi查找，造成漏洞。禁用JndiLookup一种方式是找到应用程序中打包的 log4j-core.jar，将其中的JndiLookup.class 文件删除后重新打包成新的 log4j-core.jar 即可。 漏洞修改过程： 获取源码





修改代码:直接修改 JndiLookup 类，让其 lookup 方法不进行实际的 JNDI 查找，而是直接返回一个安全的默认值。

```java
package org.apache.logging.log4j.core.lookup;

import org.apache.logging.log4j.core.LogEvent;

/**
 * Looks up keys from JNDI resources.
 */
public class JndiLookup extends AbstractLookup {

    /**
     * Looks up the value of the JNDI resource.
     * @param event The current LogEvent (is ignored by this StrLookup).
     * @param key  the JNDI resource name to be looked up, may be null
     * @return A safe default value instead of performing JNDI lookup.
     */
    @Override
    public String lookup(final LogEvent event, final String key) {
        return "JNDI lookup is disabled for security reasons.";
    }
}
```

编译打包：重新编译项目并打包成新的 log4j-core.jar 文件。