老师好!我们是第五小组，下面开始我们的答辩。(翻页)

答辩主要由以下五部分构成。(翻页)

首先是项目任务概述。(翻页)

本组共完成一下11个漏洞的复现，在后面会一一介绍。(翻页)

然后是项目小组分工及安排。(翻页)

本组利用飞书共享文档，对项目进度进行管理与统计，并实时更新项目进度，下面是飞书文档的截图。(翻页)

上面是本组各成员的小组分工情况，PPT由所有人一起制作。以下是项目时间线总览，组内秩序良好，各司其职，很好的完成了各自的项内容。(翻页)

下面是项目完成情况的思考与复盘。(翻页)

接下来我要介绍的是**spring-messaging远程代码执行漏洞**，Spring Framework是一套开源的Java应用程序框架，它的spring-messaging模块存在远程代码执行漏洞。攻击者可利用漏洞向代理发送消息，导致远程代码执行攻击。下图是相应的Web页面。

复现过程主要分为三步。首先发送connect消息，建立与服务器的连接。然后发送订阅消息，并在selector字段中插入SpEL表达式。最后发送send消息，触发服务器向订阅地址发送消息、导致恶意代码执行。

把这三步编写成POC脚本并执行，进入容器中发现tmp目录下存在success文件，表明漏洞复现成功。这个漏洞可以通过升级版本、获取补丁和添加输入验证三个方法进行修复。