CVE-2022-26138_Confluence_Server 硬编码漏洞分析

漏洞描述

7 月 21 日，Atlassian 官方发布了 2022 年 7 月的安全更新，其中涉及到 Confluence Server 的多个漏洞，其中 CVE-2022-26138 为一个硬编码漏洞。

当 Confluence Server 或 Data Center 上的 Questions for Confluence app 启用时，它会创建一个名为 disabledsystemuser 的 Confluence 用户帐户。此帐户旨在帮助将数据从应用程序迁移到 Confluence Cloud 的管理员账号中。该帐户通过使用硬编码密码创建并添加到 confluence-users 组中，在默认情况下允许查看和编辑 Confluence 中的所有非受限页面。未经身份验证攻击者可以利用所知的硬编码密码登录 Confluence 并访问该组有权限访问的所有页面。

Update: This advisory has been updated since its original publication.

22 Jul 2022 9:30 AM PDT (Pacific Time, -7 hours)

- Updated the *Fixes* section to explain only option 2 can be used for Confluence Server and Data Center instances configured to use a read-only external directory

22 Jul 2022 9:00 AM PDT (Pacific Time, -7 hours)

- Added a link to a page of frequently asked questions about CVE-2022-26138

21 Jul 2022 8:30 AM PDT (Pacific Time, -7 hours)

- An external party has discovered and publicly disclosed the hardcoded password on Twitter. **It is important to remediate this vulnerability on affected systems immediately.**
- The *Summary of Vulnerability* and *Severity* sections have been updated to include this new information

Summary	Confluence account with hardcoded credentials created by Questions for Confluence
Advisory Release Date	20 Jul 2022 10:00 AM PDT (Pacific Time, -7 hours)
Affected Products	Questions For Confluence app for: • Confluence Server • Confluence Data Center The Questions for Confluence app for Confluence Cloud is not affected.
CVE ID(s)	CVE-2022-26138

相关介绍

Atlassian Confluence Server 是澳大利亚 Atlassian 公司的一套具有企业知识管理功能，并支持用于构建企业 WiKi 的协同软件的服务器版本。

利用范围

Questions for Confluence app == 2.7.34

Questions for Confluence app == 2.7.35

Questions for Confluence app == 3.0.2

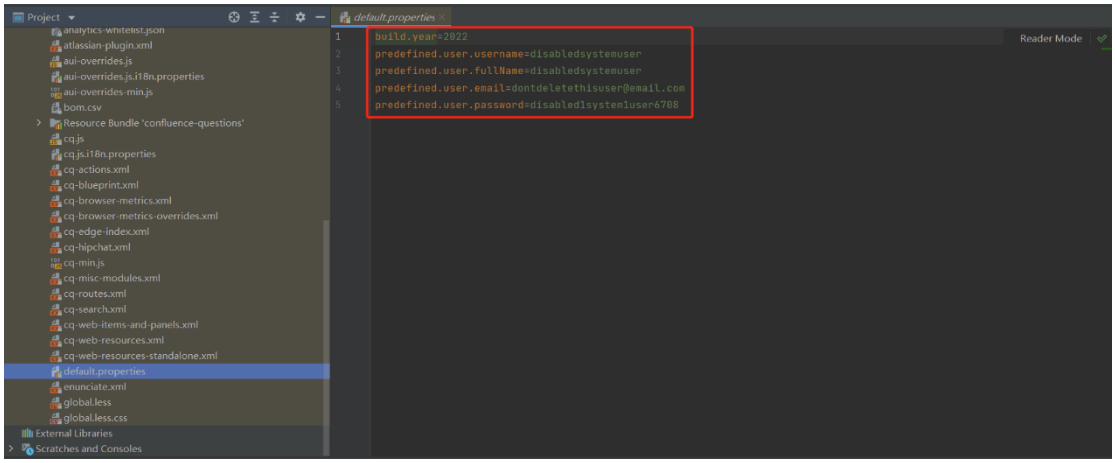
漏洞分析

环境搭建

此次漏洞分析环境可参考 CVE-2022-26134 Confluence OGNL RCE 漏洞分析 进行搭建。分析源码为 confluence-questions-3.0.2.jar 或者另外两个版本。

代码分析

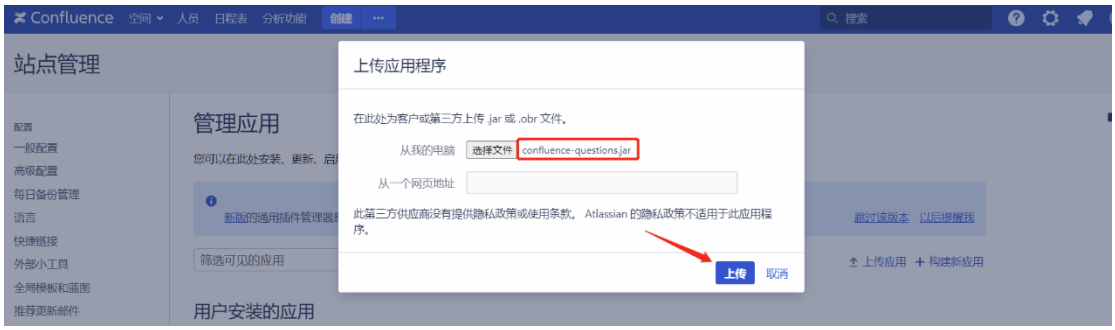
动态调试之前，在配置文件 default.properties 中可以找到所创建用户的相关信息，其中的 username 和 password 都是固定的。



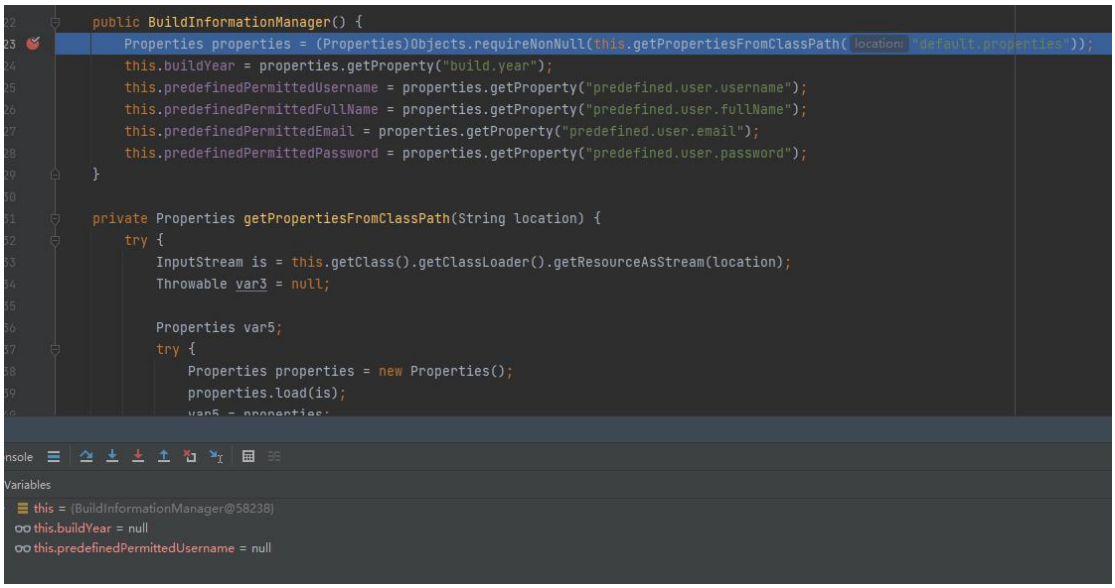
紧接着在 com.atlassian.confluence.plugins.questions.util#BuildInformationManager 处打下断点。

```java
package com.atlassian.confluence.plugins.questions.util;

import ...

public class BuildInformationManager {
    private static final String PROPERTIES_LOCATION = "default.properties";
    private final String buildYear;
    private final String predefinedPermittedUsername;
    private final String predefinedPermittedFullName;
    private final String predefinedPermittedEmail;
    private final String predefinedPermittedPassword;

    public BuildInformationManager() {
        Properties properties = (Properties)Objects.requireNonNull(this.getPropertiesFromClassPath( location: "default.properties"));
        this.buildYear = properties.getProperty("build.year");
        this.predefinedPermittedUsername = properties.getProperty("predefined.user.username");
        this.predefinedPermittedFullName = properties.getProperty("predefined.user.fullName");
        this.predefinedPermittedEmail = properties.getProperty("predefined.user.email");
        this.predefinedPermittedPassword = properties.getProperty("predefined.user.password");
    }

    private Properties getPropertiesFromClassPath(String location) {
        try {
            InputStream is = this.getClass().getClassLoader().getResourceAsStream(location);
            Throwable var3 = null;

            Properties var5;
            try {
                Properties properties = new Properties();
                properties.load(is);
                var5 = properties;
            } catch (Throwable var15) {
                var3 = var15;
                throw var15;
            } finally {
                if (is != null) {
```

开启 debug 模式，随后在 confluence 中上传 confluence-questions.jar 应用。



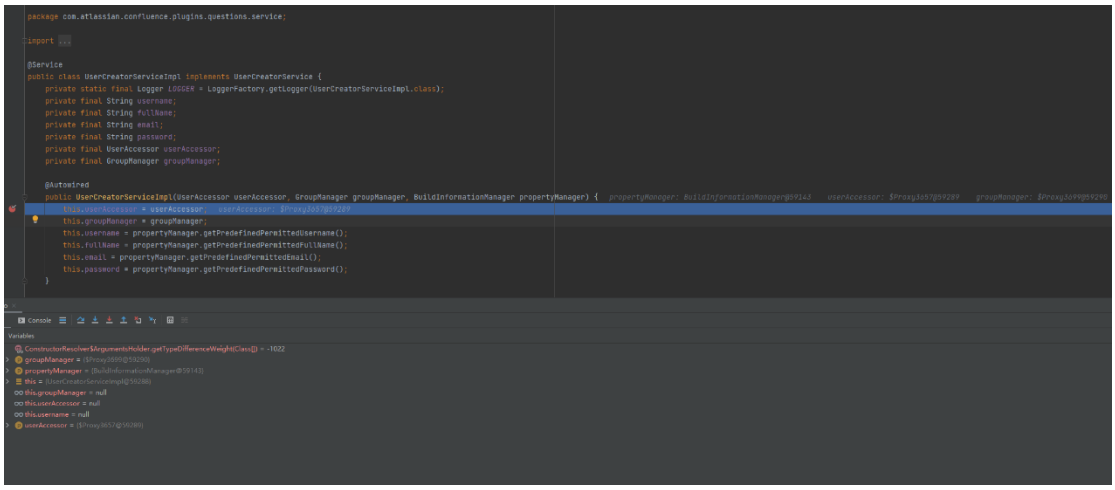
在安装应用的过程中，会从配置文件中获取到固定的账号信息。



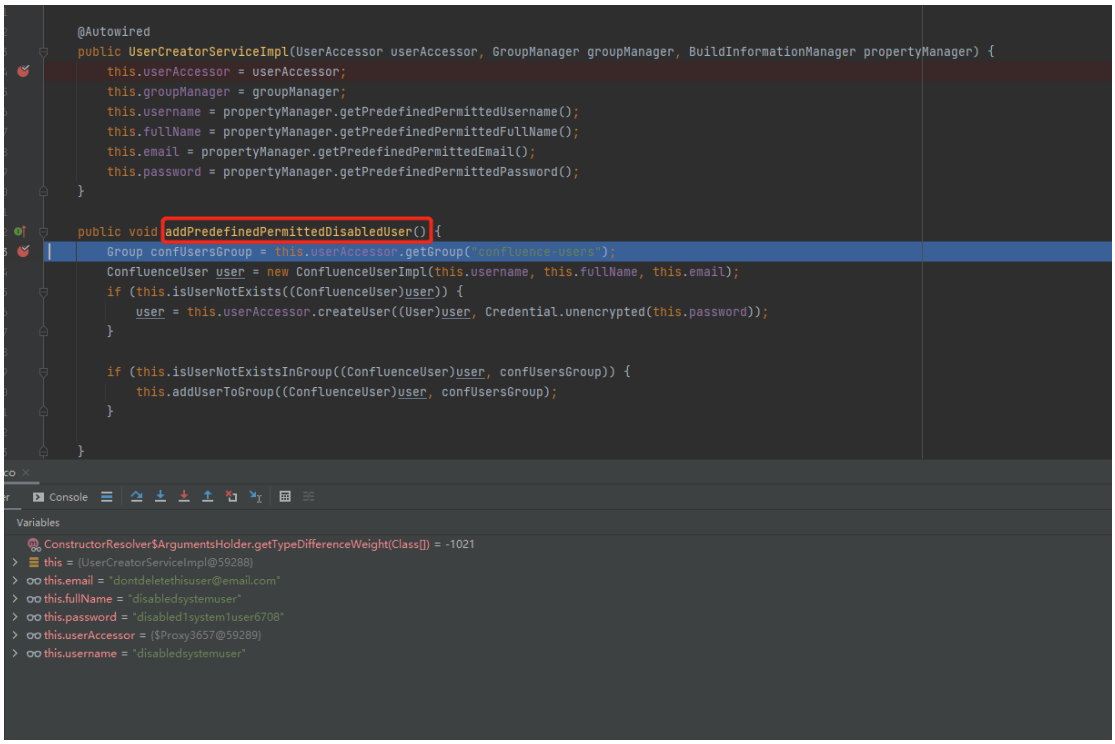
随后进入

com.atlassian.confluence.plugins.questions.service.UserCreatorServiceImpl

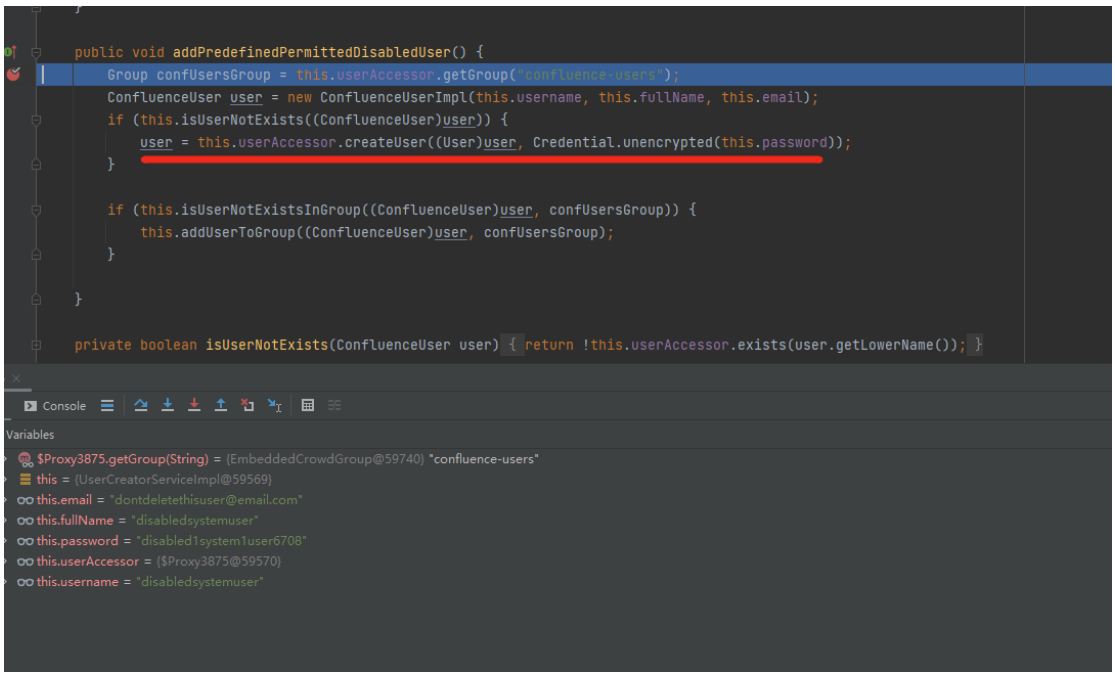
实例化 UserCreatorServiceImpl 对象



继续跟进，会进入下面的 addPredefinedPermittedDisabledUser 方法



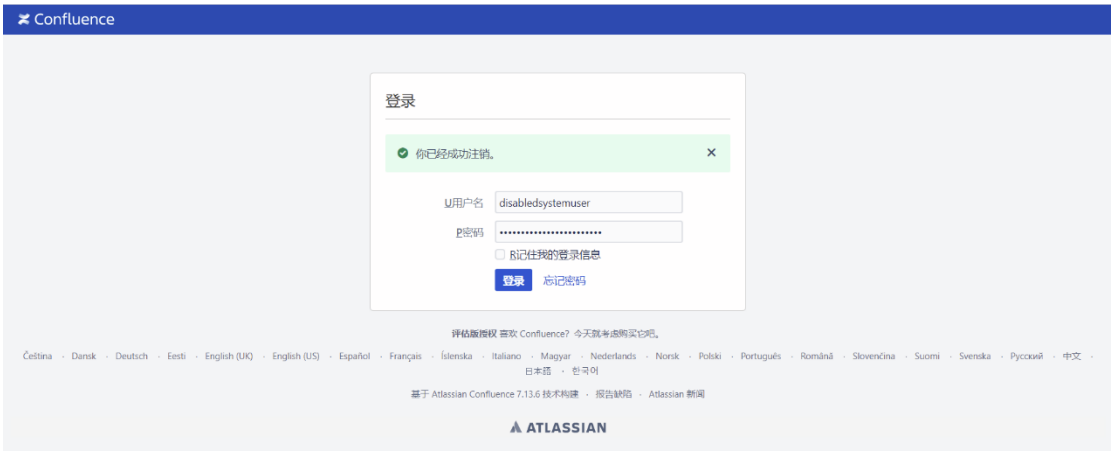
在此，固定 disabledsystemuser 用户完成创建并将其添加到 confluence-users 组



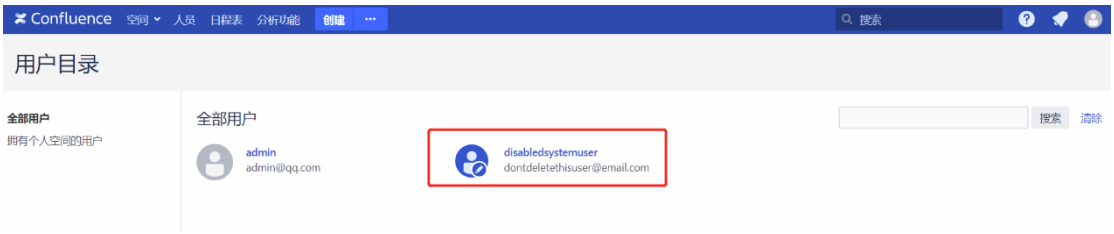
漏洞复现

成功上传 Questions for Confluence 应用程序

使用硬编码密码创建的账号进行登陆



成功登陆，且该用户拥有管理员权限



修复建议

参考官方公告中的修复建议：

更新 Questions for Confluence 扩展至以下安全版本:

2.7.x >= 2.7.38 (Confluence 6.13.18 到 7.16.2)

Versions >= 3.0.5 (Confluence 7.16.3 之后的版本)