CVE-2018-16341

Nuxeo

远程代码执行漏洞

目录

[1. 漏洞描述 3](#_Toc27475)

[2. 影响版本 3](#_Toc25949)

[3. 环境部署 3](#_Toc5232)

[4. 漏洞复现 7](#_Toc11219)

# 漏洞描述

Nuxeo平台是一个开源的可定制和可扩展的内容管理平台，用于构建业务应用程序。它为开发文档管理，数字资产管理，案例管理应用程序和知识管理奠定了基础。 您可以使用即用型插件轻松添加功能，也可以使用其扩展点系统扩展平台。nuxeo-jsf-ui组件处理facelet模板不当，当访问的facelet模板不存在时，相关的文件名会输出到错误页面上，而错误页面会当成模板被解析，文件名包含表达式也会被输出同时被解析执行，从而导致远程代码执行漏洞。攻击者可以远程对漏洞网站发起攻击,在网站操作系统上执行任意命令,获取网站控制权限。

# 影响版本

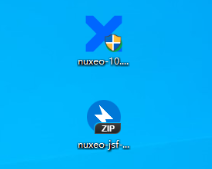
Nuxeo Server 版本 < 10.3

# 环境部署

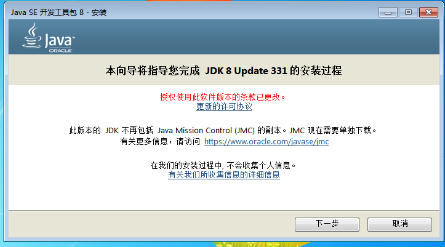
下载含有漏洞的软件

<https://cdn.nuxeo.com/nuxeo-10.2/nuxeo-10.2-setup.exe>

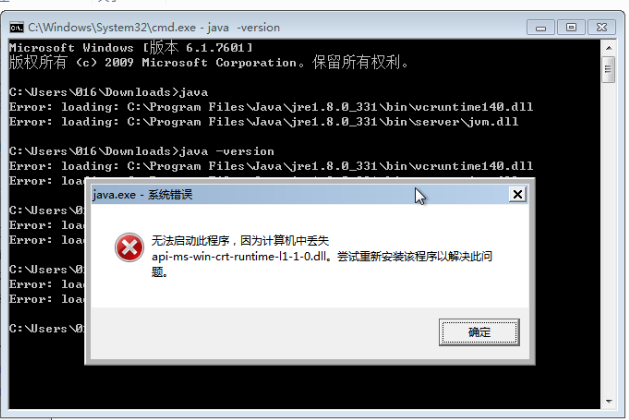
<https://connect.nuxeo.com/nuxeo/site/marketplace/package/nuxeo-jsf-ui?version=10.2.0>



配置Java8



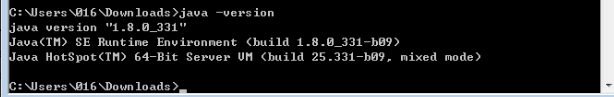




运行Java命令提示缺少运行库(dll)

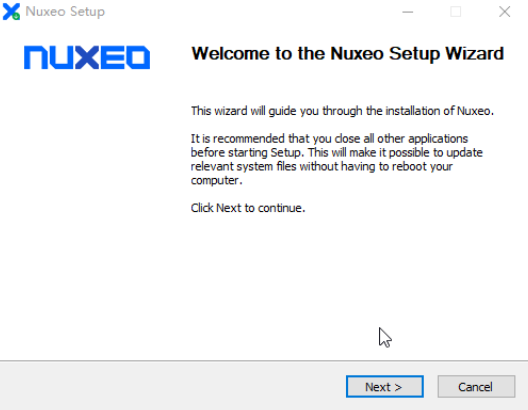


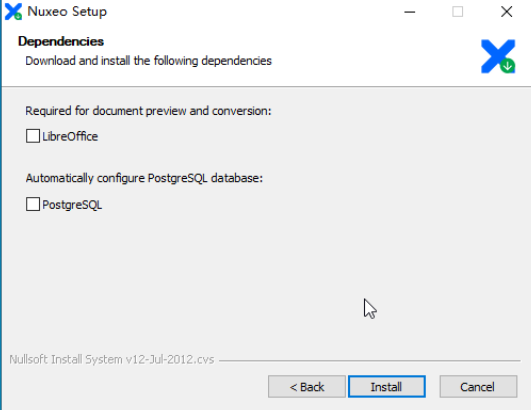
安装必备运行库

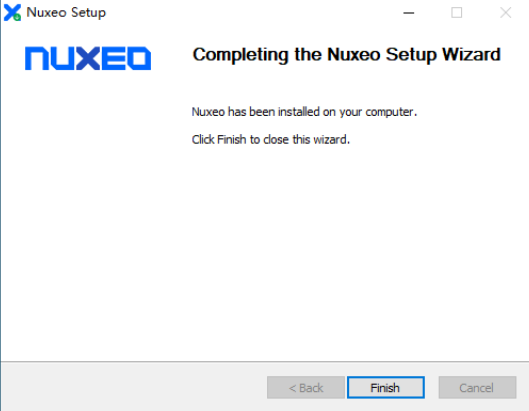


成功运行命令

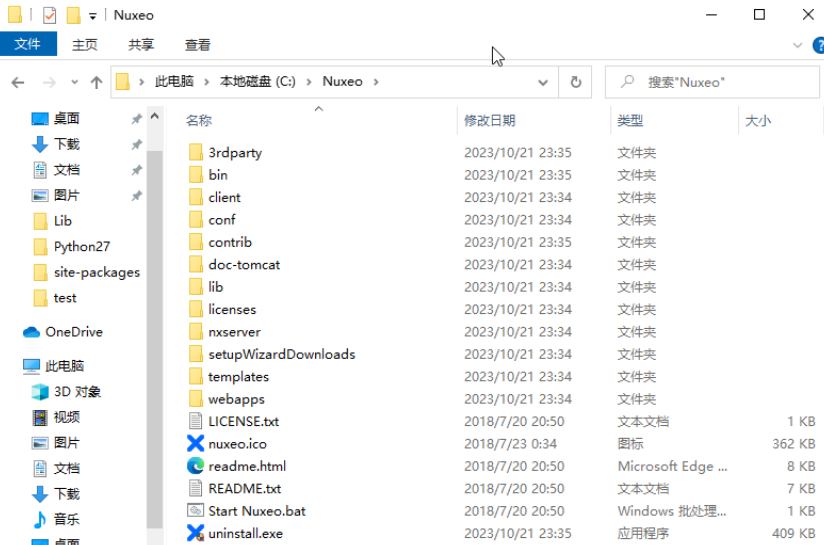
开始安装软件



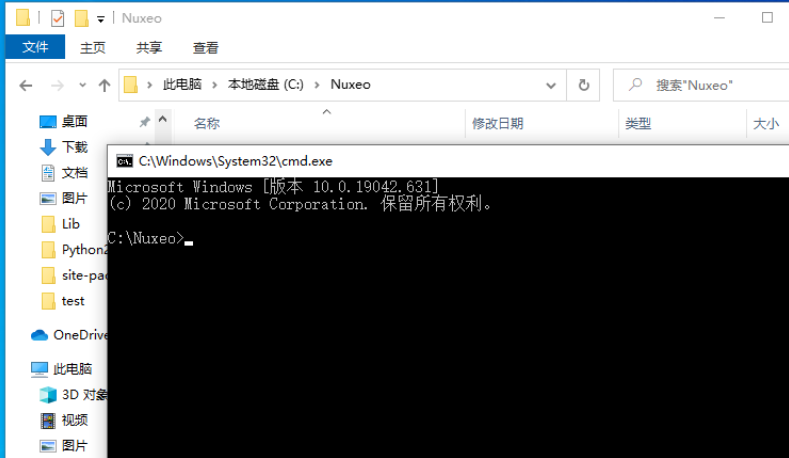




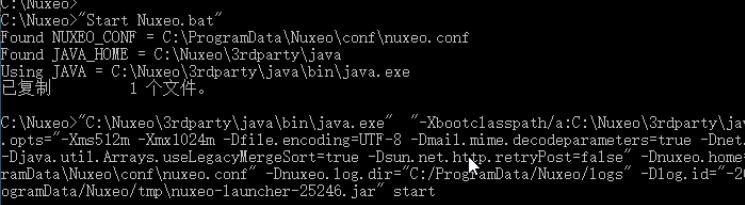
安装完成后打开软件根目录

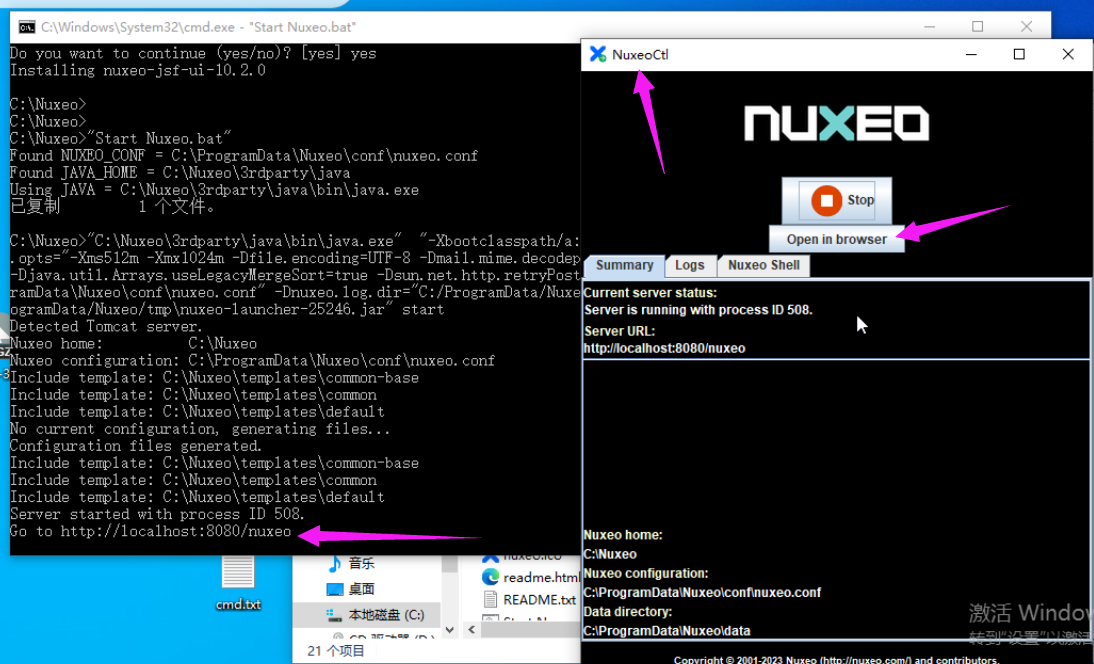


此处打开命令行



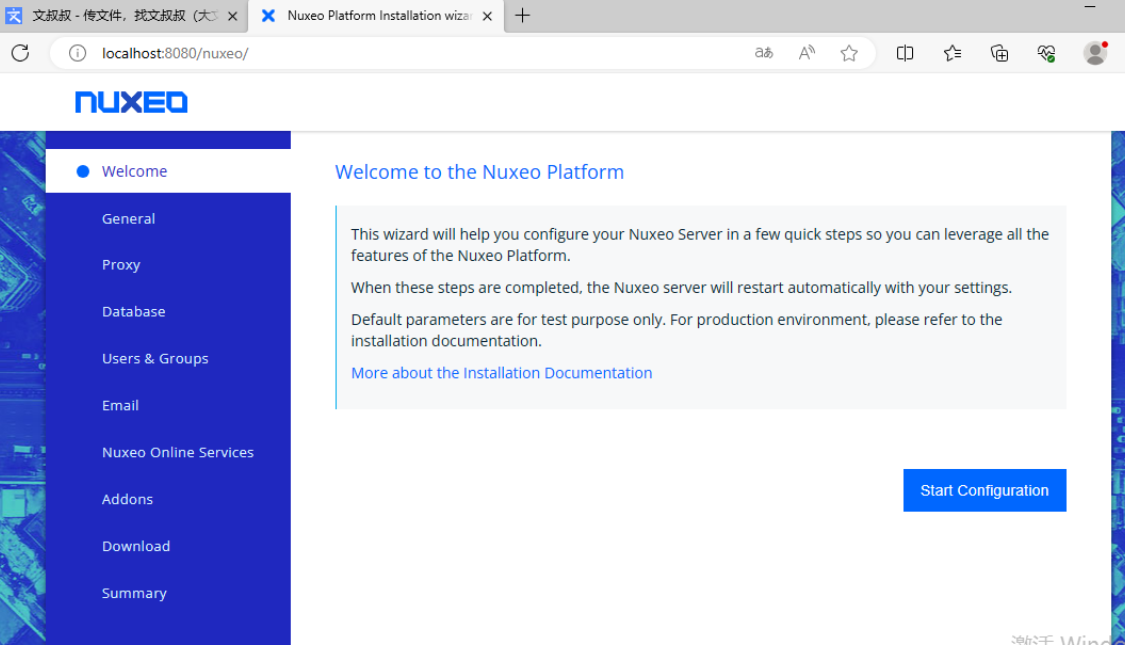
启动软件



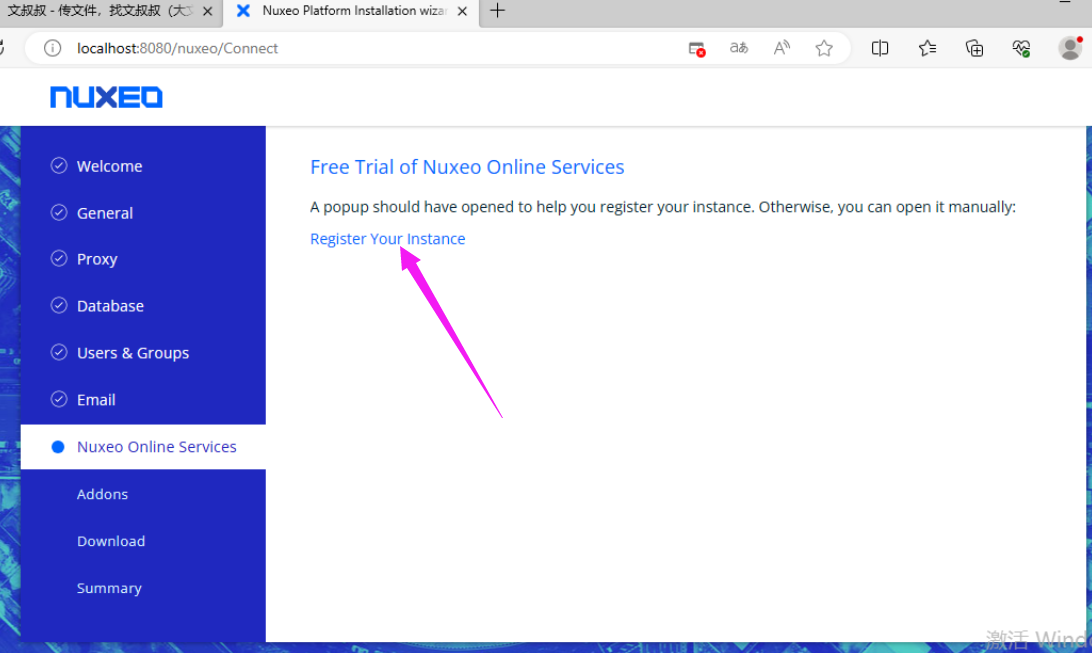


启动成功

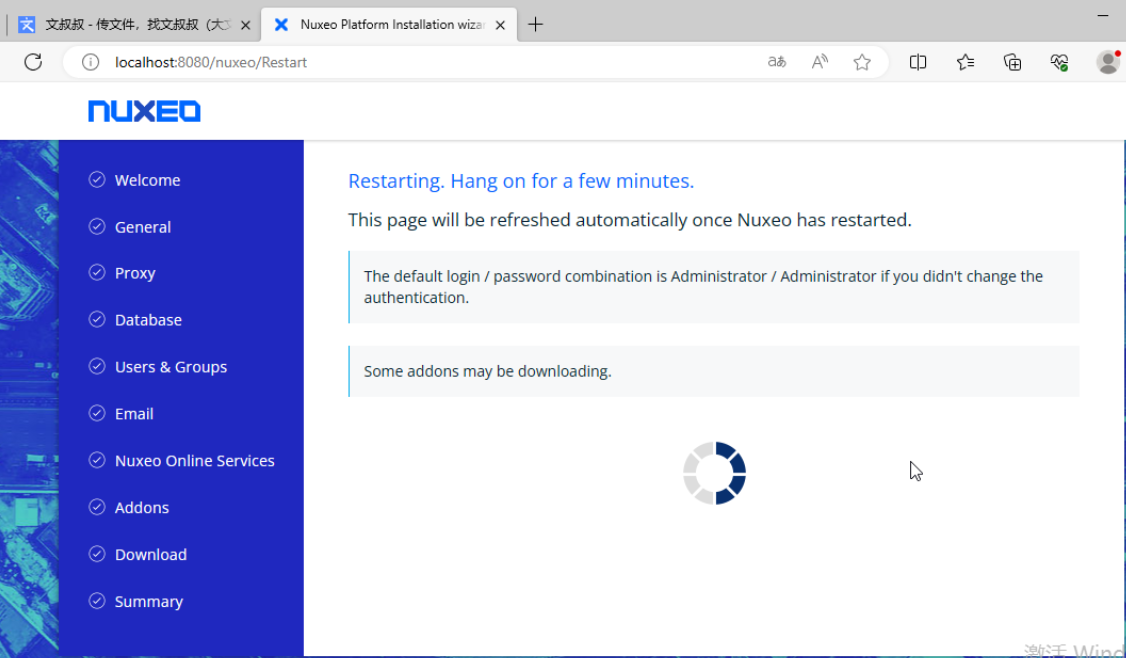
开始注册软件



一直点下一步



在线注册开始30天免费试用



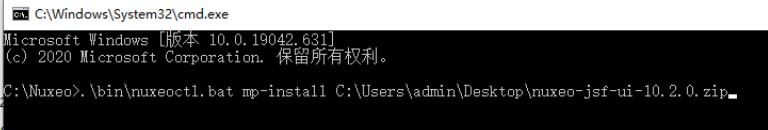
稍等后重启软件

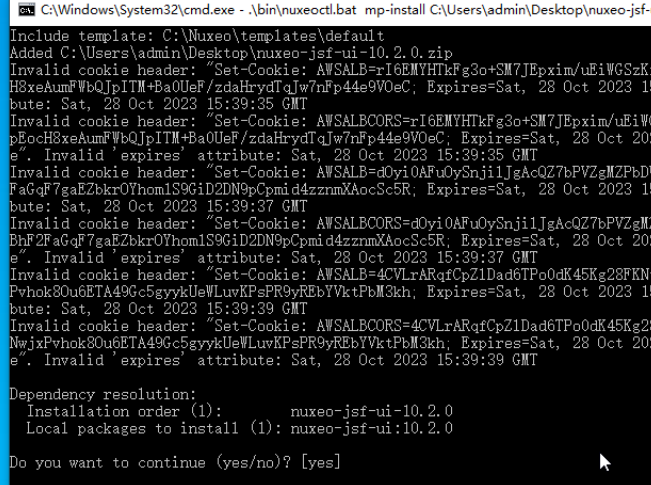
接下来我们要为软件安装插件



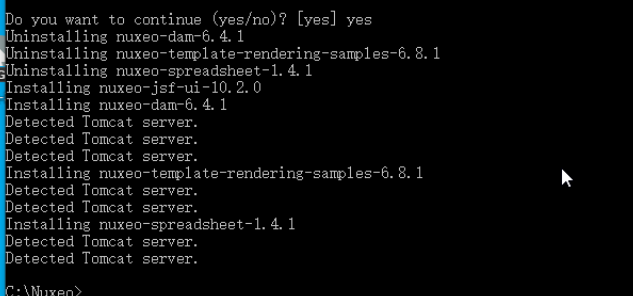
输入命令

.\bin\nuxeoctl.bat mp-install <nuxeo-jsf-ui路径>





输入yes

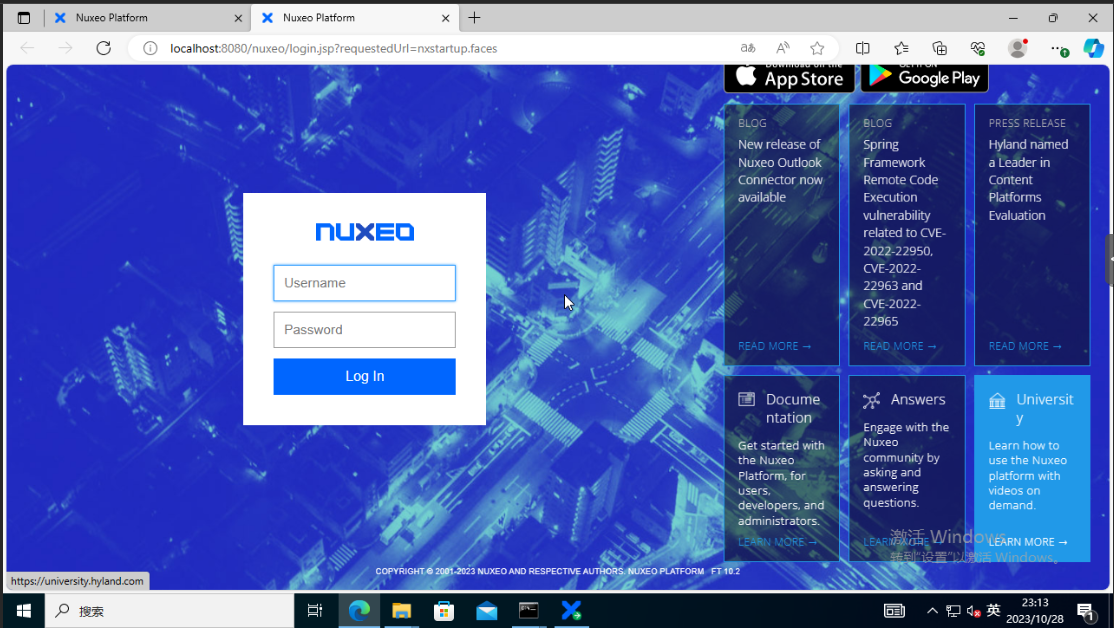


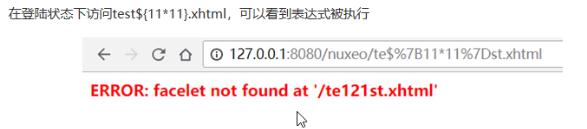
启动软件



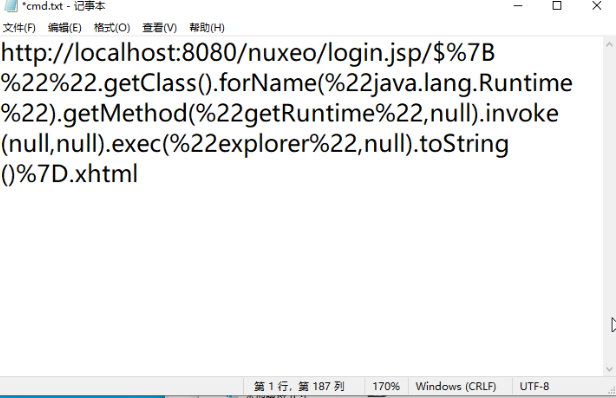
# 漏洞复现

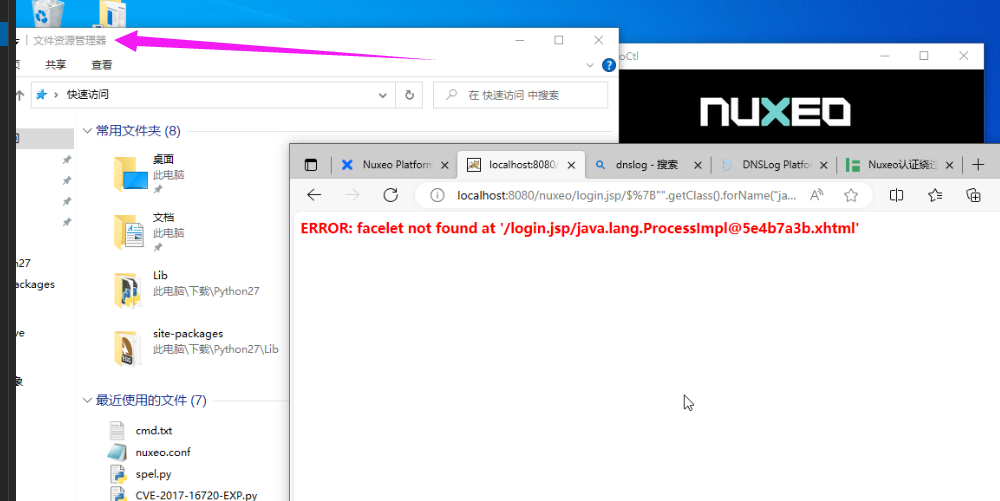
**访问首页**





**构造特殊的表达式运行**





**自动打开文件资源管理器**