

# Write-up DBS401: Group 5

👋 Welcome to my write-up!

🔧 Tools: Burp Suite

## 📁 Flags' Completion Table

Flag Number	Vulnerability's Name	Done	Flag
1	Information disclosure	yes	<b>flag{c8f6201b79cc995679499beb78c88f1b}</b>
2	Improper Input Validation	yes	<b>flag{nhom5dbs}</b>
3	IDOR	yes	<b>Flag{uelcom_T0_th\$_Ric\$!eID}</b>



## Description

- A website that selling phones 📱

The screenshot shows a web browser displaying the ICT SHOP website. The header includes the shop name, a search bar, and navigation links for Điện thoại, TÌM KIẾM SẢN PHẨM, ĐIỆN THOẠI, LAPTOP, PHỤ KIỆN, LIÊN HỆ, and ĐƠN HÀNG. A prominent banner on the right side features three Samsung A50 phones with the text "Đặt trước A50" and "A50". Below the banner, there are two large promotional boxes: one for "SỐ 1 VỀ BẢO HÀNH & DỊCH VỤ" featuring an iPhone X, and another for "1 ĐỔI 1 LỐI LÀ ĐỔI" featuring an iPhone XS MAX. At the bottom, there is a section titled "SẢN PHẨM NỔI BẬT" showing three more phones: an iPhone X, an iPhone XS MAX, and a HTC U11+.

## ✓ Solution

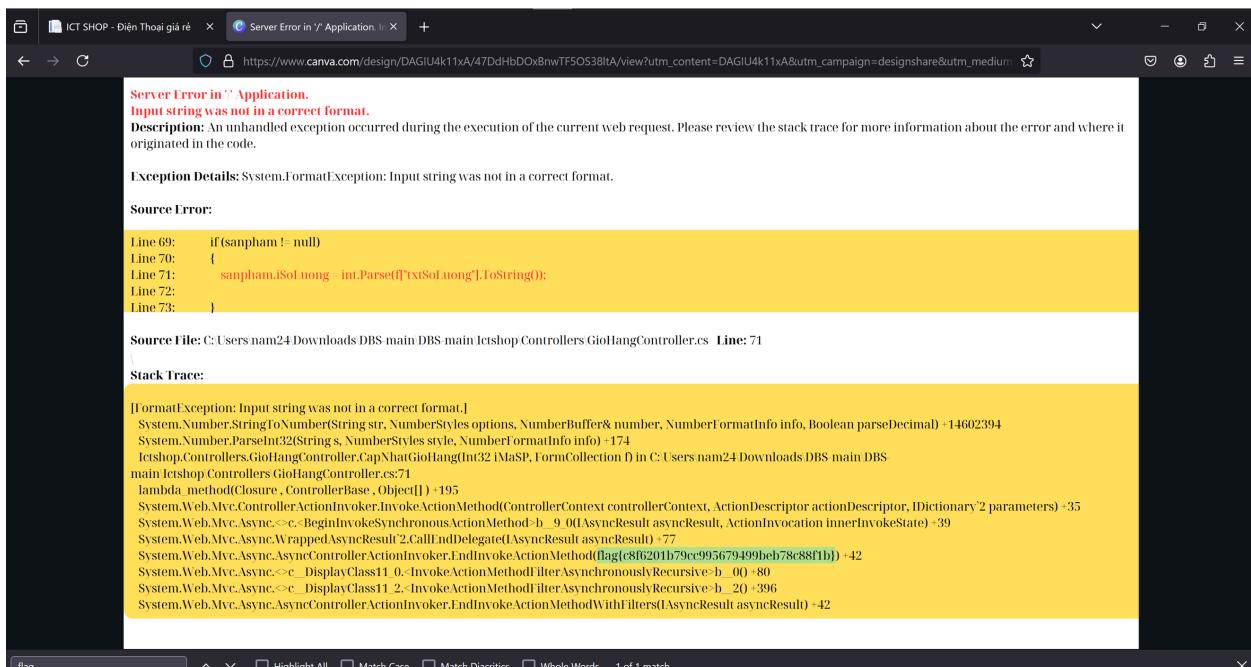
## Flag 1: Information Disclosure

**Description:** This vulnerability involves revealing sensitive information in the HTML source code.

- Ctrl+U to view HTML source code

```
1 </u1v>
2 </div>
3 <br>
4 <div class="container body-content">
5
6
7
8
9 <br />
10 <div class="row">
11 <div class="col-md-8">
12 
13 </div>
14 <div class="col-md-4">
15 
16 <p class="hidden"><a href="https://www.canva.com/design/DAGIU4k11xA/47DdHbDOxBnwTF50S38ltA/view?utm_content=DAGIU4k11xA&utm_source=canva.com&utm_medium=design" class="btn btn-default" style="color: #000000; background-color: #e6f2ff; border-color: #000000; border-radius: 4px; padding: 10px 20px; font-size: 16px; font-weight: bold; text-decoration: none; transition: all 0.3s ease; text-align: center; width: 100%; height: 100%; display: flex; align-items: center; justify-content: center; gap: 10px; margin-bottom: 10px;">Tải lên</a></p>
17 </div>
18 </div>
19 <div>
20 
21 </div>
22 <br />
23 <div class="spnoibat">
24 <div class="row">
25
26 <h3> SẢN PHẨM NỔI BẬT</h3>
27 <div class="col-md-4">
28 
29 </div>
30 <div class="col-md-4">
31 
32 </div>
33 <div class="col-md-4">
34 
35 </div>
36 </div>
```

- We can see a suspicious link at line 86



- Open the link and we get the first flag!

► Flag: flag{c8f6201b79cc995679499beb78c88f1b}

## Flag 2: Improper Input Validation

**Description:** The "edit cart" function does not properly validate the input for the "quantity" field, leading to unintended behaviour.

The screenshot shows a web browser window with the URL [103.249.200.71/GioHang/SuaGioHang](http://103.249.200.71/GioHang/SuaGioHang). The page title is "Giỏ hàng (1)". The user is logged in as "Xin chào : abe@gmail.com ĐĂNG XUẤT". The navigation menu includes "ĐIỆN THOẠI", "LAPTOP", "PHỤ KIỆN", "LIÊN HỆ", and "ĐƠN HÀNG". Below the menu is a search bar with placeholder "Tim kiem san pham...". The main content area is titled "GIỎ HÀNG" and displays a table with one item:

Mã SP	Tên SP	Ảnh bìa	Đơn giá	Số lượng	Thành tiền
2	Apple Iphone 3		2,000,000 VND	a	2,000,000 VND

Buttons for "Cập nhật" (Update) and "Xóa" (Delete) are visible. The URL in the address bar is [103.249.200.71/GioHang/GioHang](http://103.249.200.71/GioHang/GioHang).

- Try to input anything that is not number then this web will return a flag.

The screenshot shows a web browser window with the URL [103.249.200.71/GioHang/GioHang](http://103.249.200.71/GioHang/GioHang). The page title is "Giỏ hàng (1)". The user is logged in as "Xin chào : abe@gmail.com ĐĂNG XUẤT". The navigation menu includes "ĐIỆN THOẠI", "LAPTOP", "PHỤ KIỆN", "LIÊN HỆ", and "ĐƠN HÀNG". Below the menu is a search bar with placeholder "Tim kiem san pham...". The main content area is titled "GIỎ HÀNG" and displays a table with one item:

Mã SP	Tên SP	Ảnh bìa	Đơn giá	Số lượng	Thành tiền
2	Apple Iphone 3		2,000,000 VND	1	2,000,000 VND

Buttons for "Chỉnh sửa giỏ hàng" (Edit cart) and "Đặt hàng" (Place order) are visible. The URL in the address bar is [103.249.200.71/GioHang/GioHang](http://103.249.200.71/GioHang/GioHang).

► Flag: flag{nhom5dbs}

## Flag 3: IDOR

**Description:** The "view user profile" function handles user IDs in a predictable manner, allowing unauthorized access to user credentials.

Hồ sơ cá nhân

Họ tên	abcd
Email	abcd@gmail.com
Điện thoại	123456789
Mật khẩu	abcd1234
Địa chỉ	abcd

Chỉnh sửa hồ sơ

- Using intruder of Burp Suite to find admin's account

5. Intruder attack of http://103.249.200.71 - Temporary attack - Not saved to project file

Request	Payload	Status co...	Error	Timeout	Length	Comment
0	14	200	<input type="checkbox"/>	<input type="checkbox"/>	6495	
15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	6540	
16	16	200	<input type="checkbox"/>	<input type="checkbox"/>	6512	
17	16	200	<input type="checkbox"/>	<input type="checkbox"/>	6543	
37	36	200	<input type="checkbox"/>	<input type="checkbox"/>	6500	
40	39	200	<input type="checkbox"/>	<input type="checkbox"/>	6504	
42	41	200	<input type="checkbox"/>	<input type="checkbox"/>	6504	
43	42	200	<input type="checkbox"/>	<input type="checkbox"/>	6504	
45	44	200	<input type="checkbox"/>	<input type="checkbox"/>	6495	
46	45	200	<input type="checkbox"/>	<input type="checkbox"/>	6493	
47	46	200	<input type="checkbox"/>	<input type="checkbox"/>	6490	

Hồ sơ cá nhân

Ảnh đại diện	
Họ tên	Man tran admin
Email	Admin@gmail.com
Điện thoại	0812883636
Mật khẩu	12345678
Địa chỉ	Bình dương

- Use this credential to login as admin and get the last flag

Dashboard - SB Admin

103.249.200.71/Admin/Nguoidungs

ICT SHOP

Search for...

MENU

- Sản phẩm
- Hàng sản xuất
- Hệ điều hành
- Người dùng
- Phân quyền
- Đơn hàng
- Thống kê

Logged in as:  
IctShop

Flag(uelcom\_T0\_th\$\_Ric\$f!eID)

Privacy Policy · Terms & Conditions

Họ tên	Email	Phone	Address	Role	Actions
mantran	mantran@gmail.com	0812883637	12345678	Member	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
Nguyễn Văn A	testa@gmail.com	0812883636	12345678	Member	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
Nguyễn Văn B	tetsb@gmail.com	0812883636	12345678	Member	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
Nguyễn Văn C	testc@gmail.com	0812883636	12345678	Member	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
abcd	abcd@gmail.com	123456789	abcd1234	abcd	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
test	test@gmail.com	123456789	abcd1234	ab	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
abe	abe@gmail.com	009090909	abe@12345	a	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
group4	group4@gmail.com	123412341	abcd1234	ab	<a href="#">Chi tiết</a> <a href="#">Xóa</a>
trong	vt@gmail.com	0865581213	hieu9911	dfsdfv	<a href="#">Chi tiết</a> <a href="#">Xóa</a>

▶ Flag: Flag{uelcom\_T0\_th\$\_Ric\$f!eID}