Write-up DBS401: Group 5

👋 Welcome to my write-up!

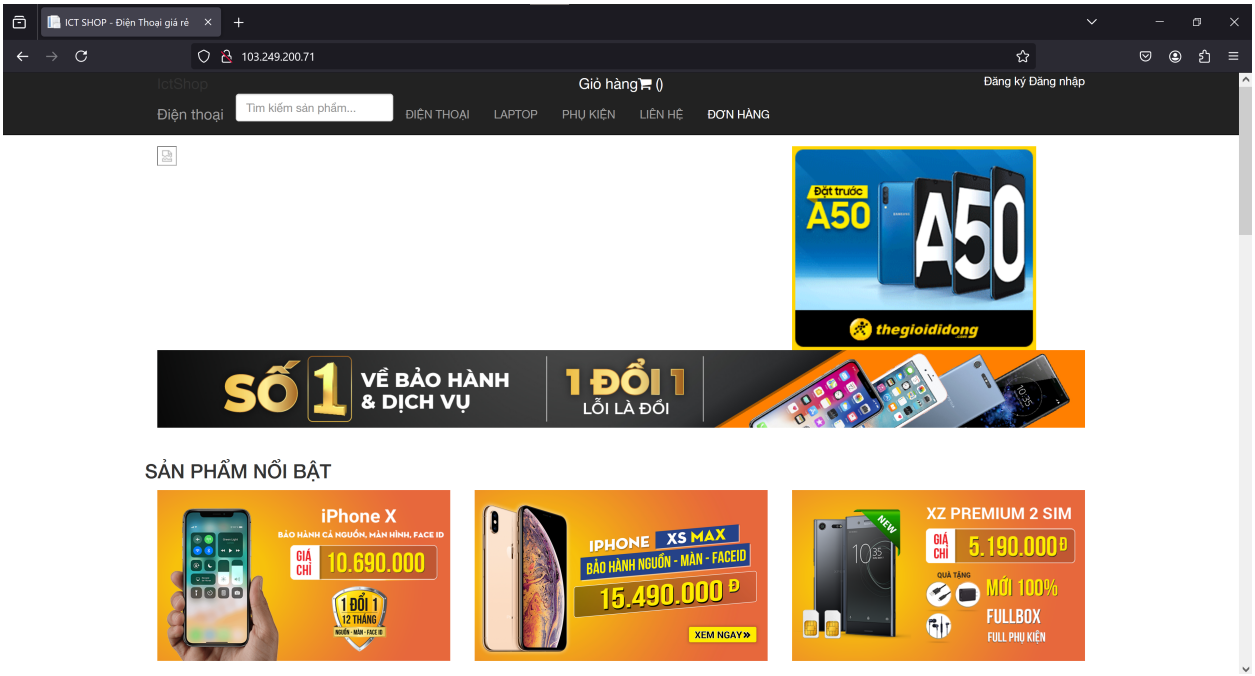
🔧 Tools: Burp Suite

🗂️ Flags' Completion Table

Flag Number	Vulnerability's Name	Done	Flag
1	Information disclosure	yes	**flag{c8f6201b79cc995679499beb78c88f1b}**
2	Improper Input Validation	yes	**flag{nhom5dbs}**
3	IDOR	yes	**Flag{ưelcom_T0_th$_Ric$f!elD}**

📝 Description

- A website that selling phones 📱

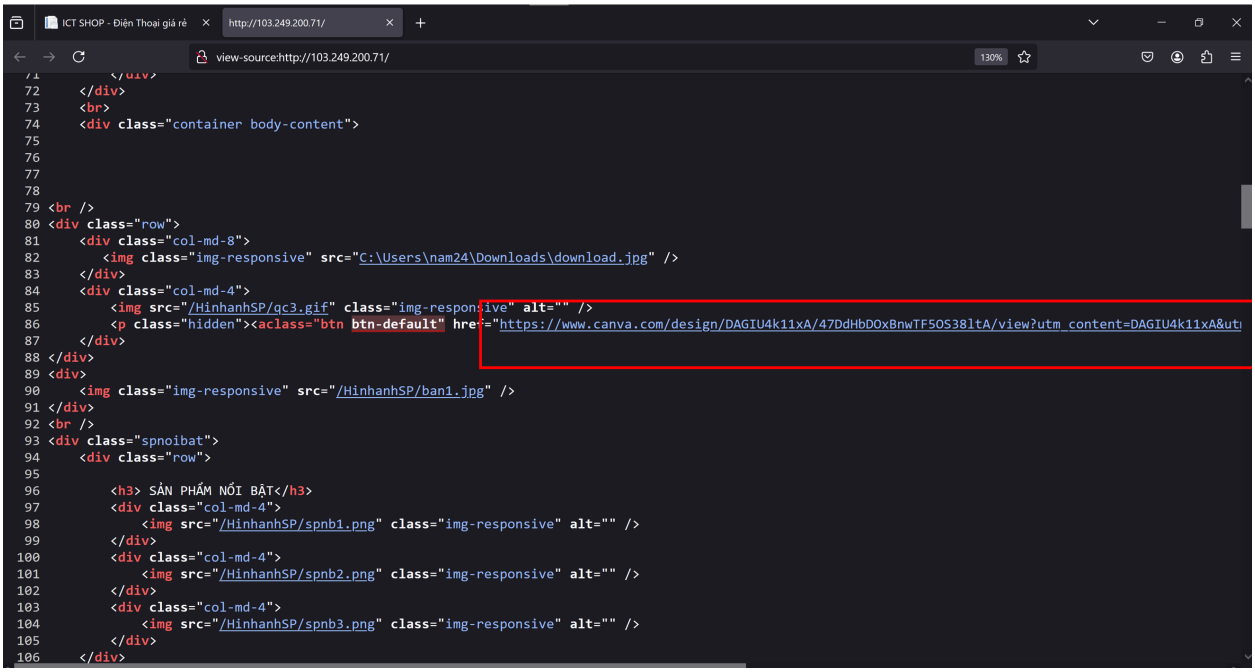


✅ Solution

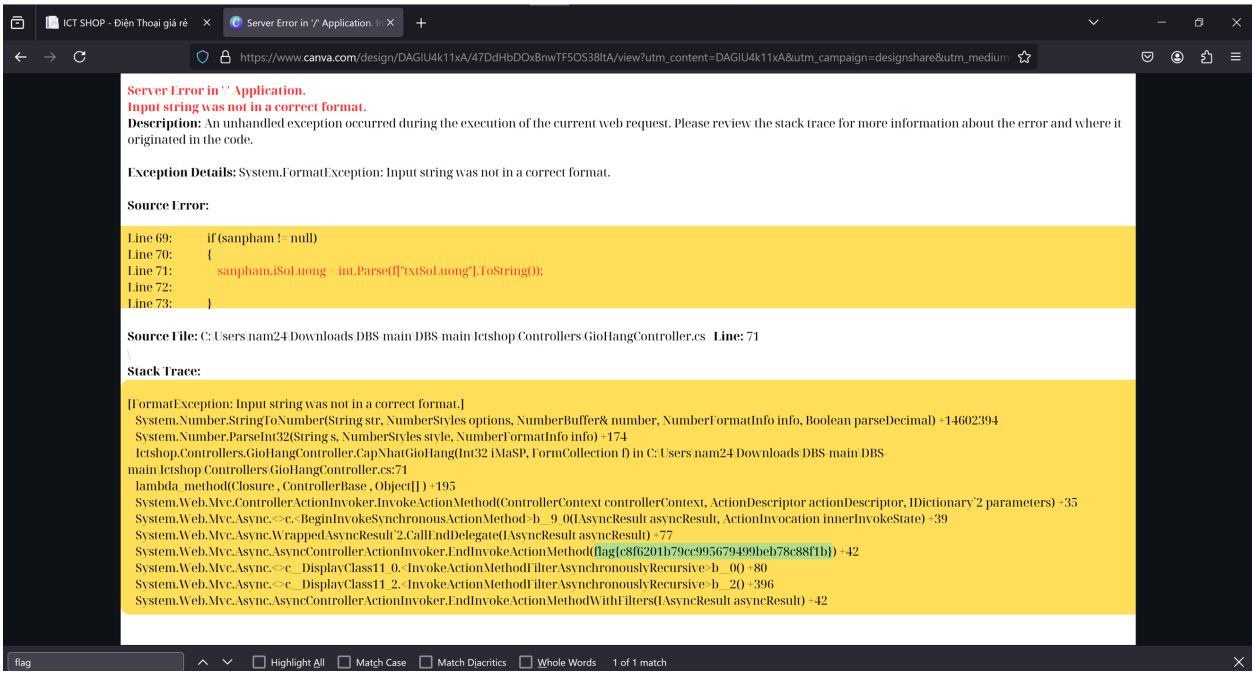
Flag 1: Information Disclosure

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

- Ctrl+U to view HTML source code



- We can see a suspicious link at line 86

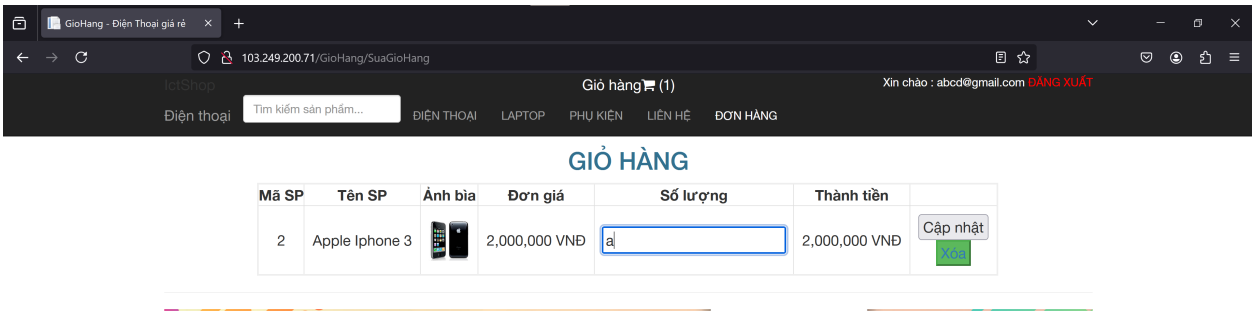


- Open the link and we get the first flag!

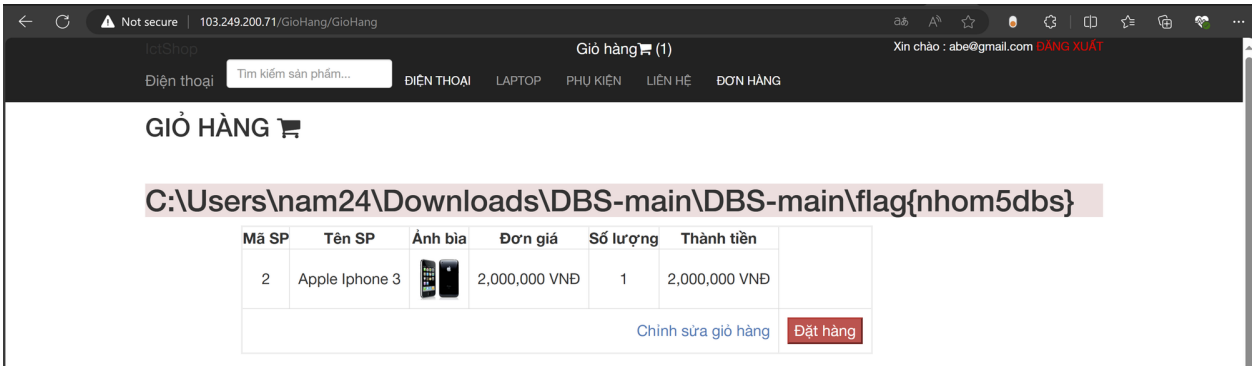
Flag: flag{c8f6201b79cc995679499beb78c88f1b}

Flag 2: Improper Input Validation

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



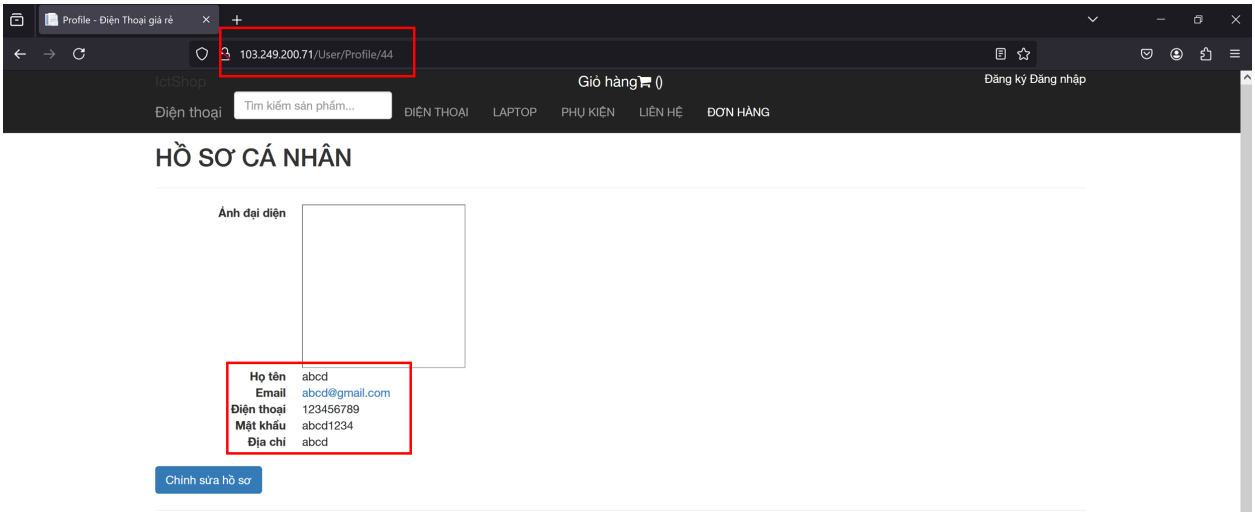
- Try to input anything that is not number then this web will return a flag.



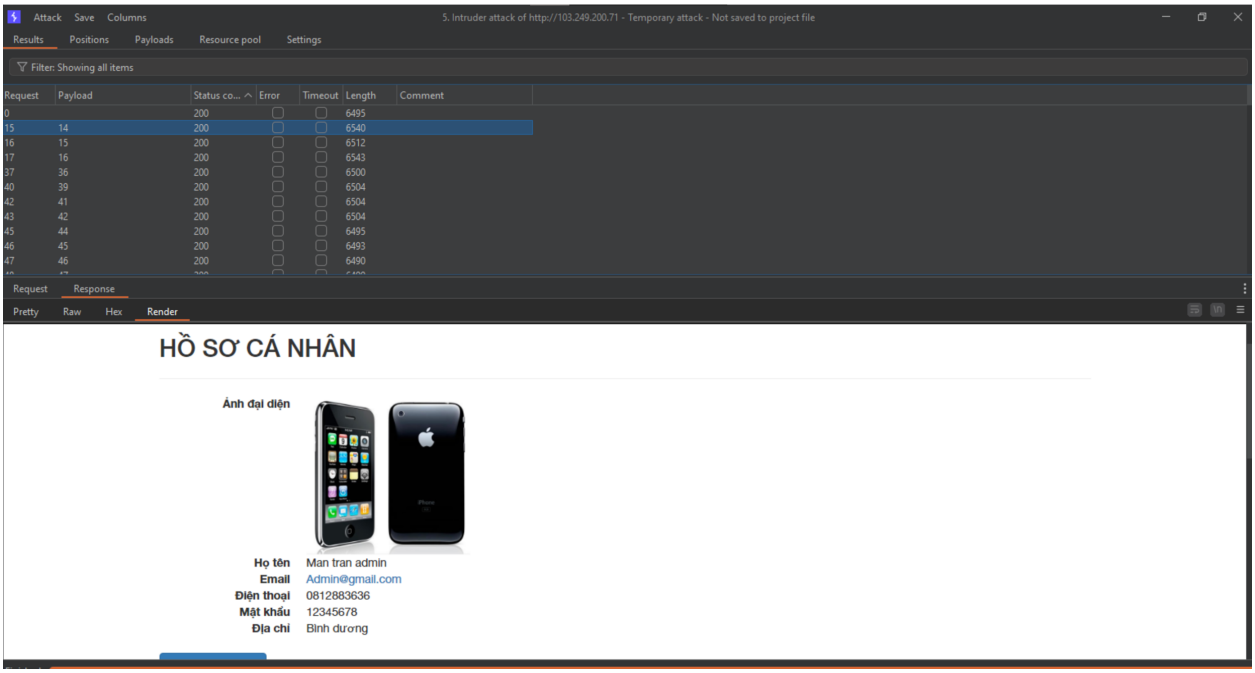
Flag: flag{nhom5dbs}

Flag 3: IDOR

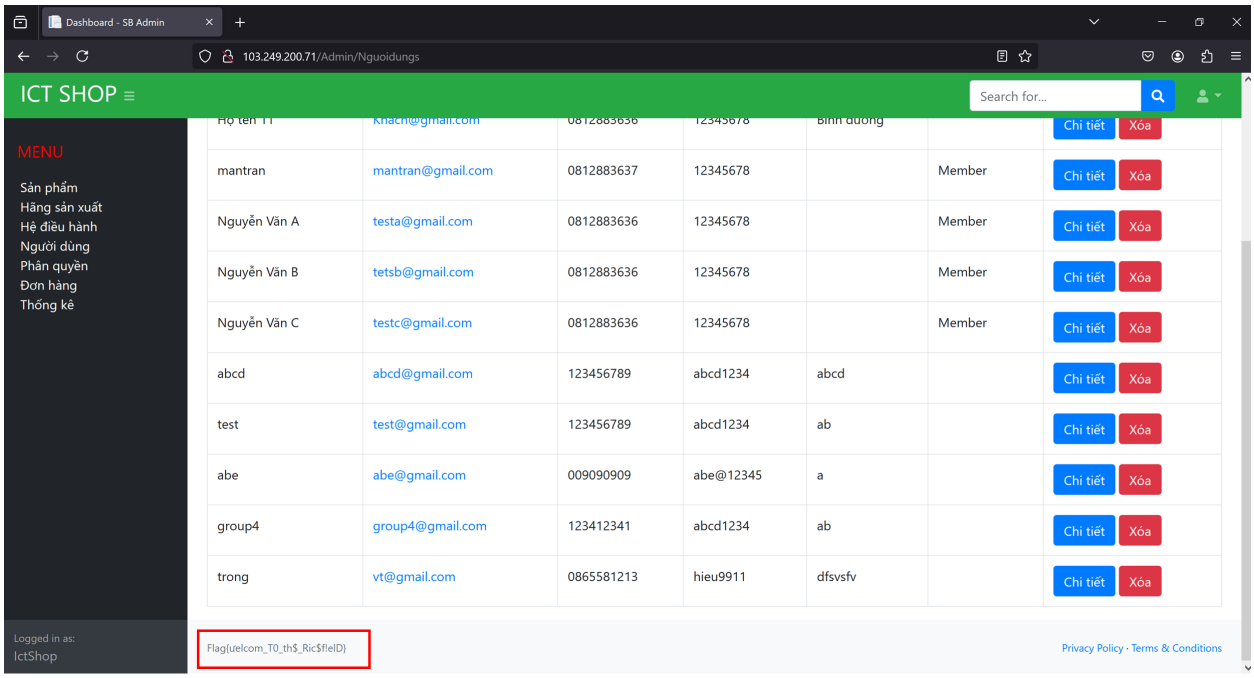
Description: The "view user profile" function handles user IDs in a predictable manner, allowing unauthorized access to user credentials.



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



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



Flag: Flag{ưelcom_T0_th$_Ric$f!elD}