Juice WebApp - Bug Report

ID number	#001
Name	Forget Password || Unable to Proceed with e2e Process
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	Forget Password user journey is breaking and the user is not able to proceed.
URL	https://juice-shop.herokuapp.com/#/forgot-password
Browser	Google Chrome Version 132.0.6834.84
Severity	Major
Priority	High

Description

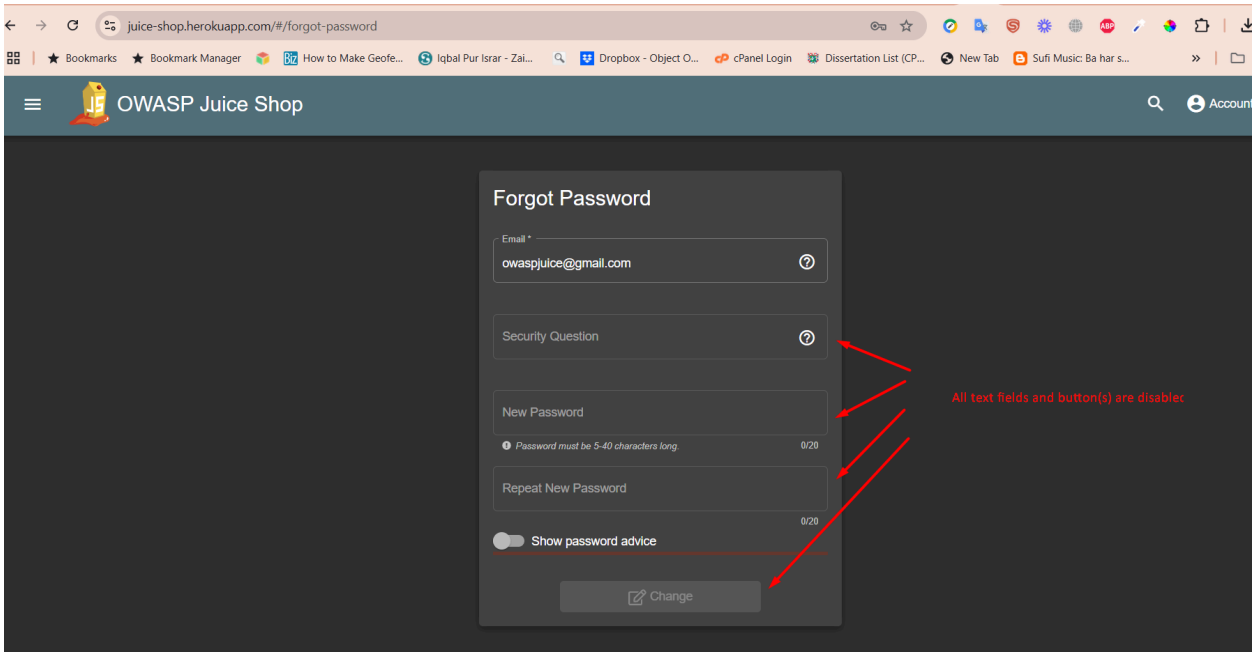
When the user lands on the Forget Password Screen all the input fields are disabled. And as a Result User is not able to change their Password.

Steps to reproduce

> Go to Juice App Login Screen.
> Click on “Forgot your password?”
> On the Forget Password screen enter an email.
> Security Question, New Password, Repeat New Password and Change Password button are disabled.

Note: It is important to note that this flow is only breaking on the Frontend and the Backend works fine. I tried changing the HTML for these fields and was able to change the password.

Attachments:



ID number	#002
Name	Important Data fields should be using UUID format
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	User ID, Product ID, Basket ID fields are using basic digits. These fields should be using UUID format so that these are not easily guessable.
URL	https://juice-shop.herokuapp.com/#/basket
Browser	Google Chrome Version 132.0.6834.84
Severity	Major
Priority	High

Description

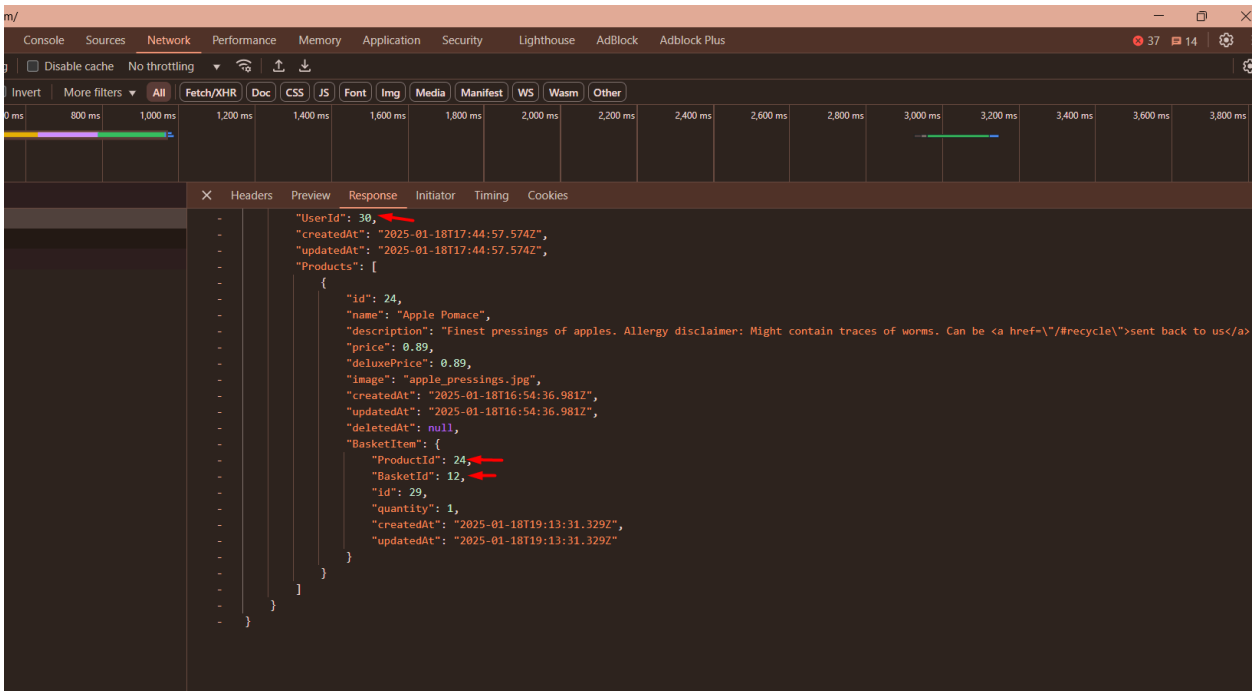
User ID is showing as 30 for my login. Which gives me information on predictability of other User IDs. i.e. 29, 28 etc. I can easily manipulate these using API Calls and getting private data of other Users.

Steps to reproduce

> Go to the Juice App Login Screen.

> Add a few items to the cart
> Open the Network tab of the browser
> Now go to the Cart
> Open the network call Response, it shows the Data IDs which are highly predictable.

Attachments:



ID number	#003
Name	Backend Checks missing on Wallet inputs
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	Negative field can be added to the wallet, which would affect the financial business logics
URL	https://juice-shop.herokuapp.com/#/wallet
Browser	Google Chrome Version 132.0.6834.84
Severity	Major
Priority	High

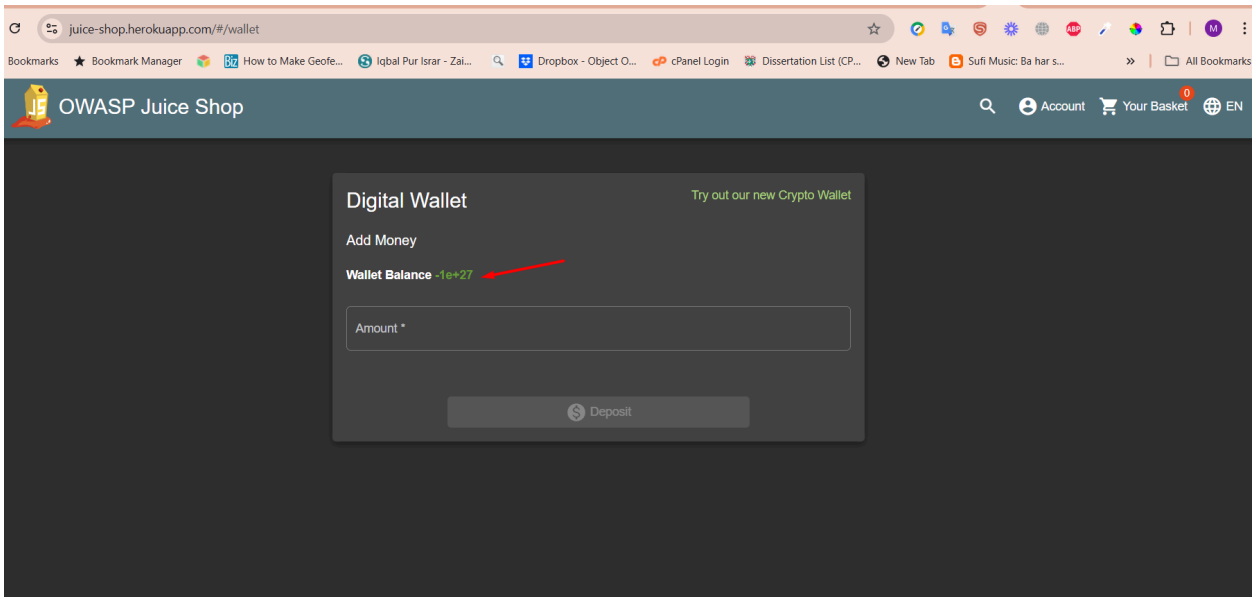
Description

Wallet's Frontend checks are not implemented on the BE. They can be bypassed easily.

Steps to reproduce

> Go to the Juice App Login Screen.
> Login with a valid User
> Go to Account -> Orders and Payments -> Digital Wallet
> Wallet is accessed, remove negative value checks using inspect element for the page HTML.
> Add a negative value to the wallet and it is added.

Attachments:



ID number	#004
Name	Backend Checks missing on Wallet inputs
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	FE checks i.e., 10-1000 range to be added to wallet is not implemented on the Backend.
URL	https://juice-shop.herokuapp.com/#/wallet
Browser	Google Chrome Version 132.0.6834.84
Severity	Major
Priority	High

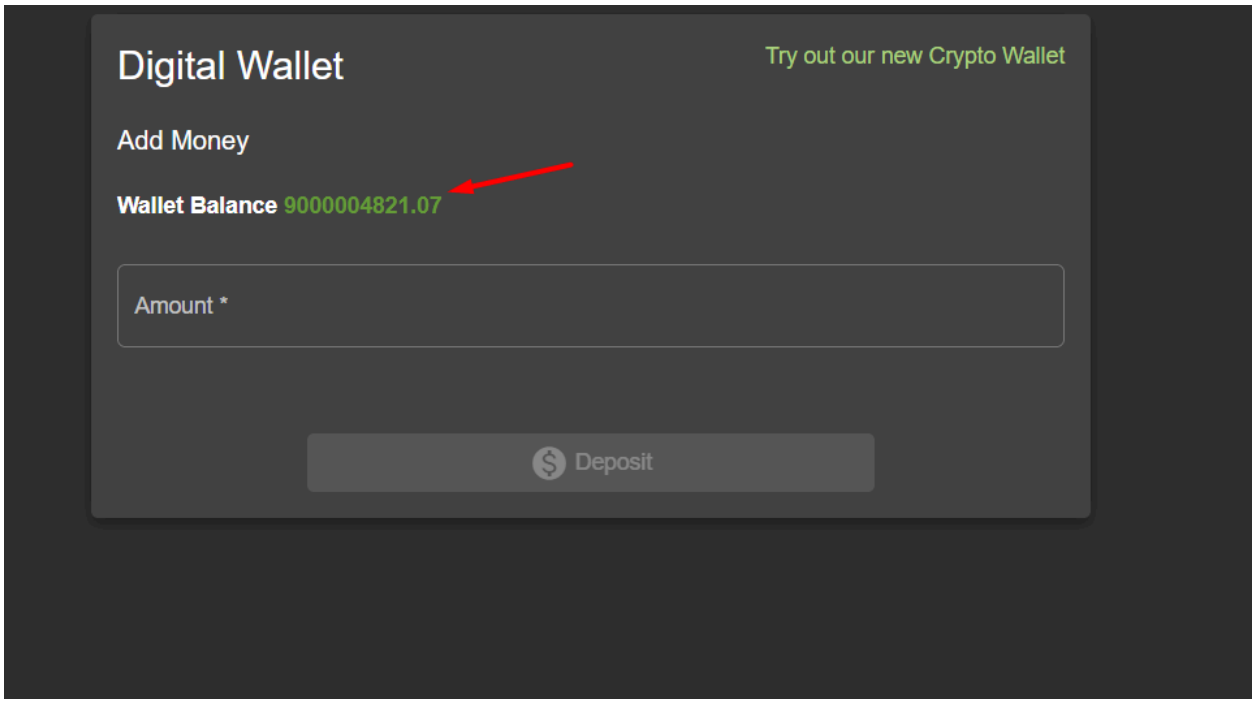
Description

Wallet's Frontend checks are not implemented on the BE. They can be bypassed easily.

Steps to reproduce

> Go to the Juice App Login Screen.
> Login with a valid User
> Go to Account -> Orders and Payments -> Digital Wallet
> Wallet is accessed, remove boundary value checks using inspect element for the page HTML.
> Add a very large number >1000 value to the wallet and it is added.

Attachments:



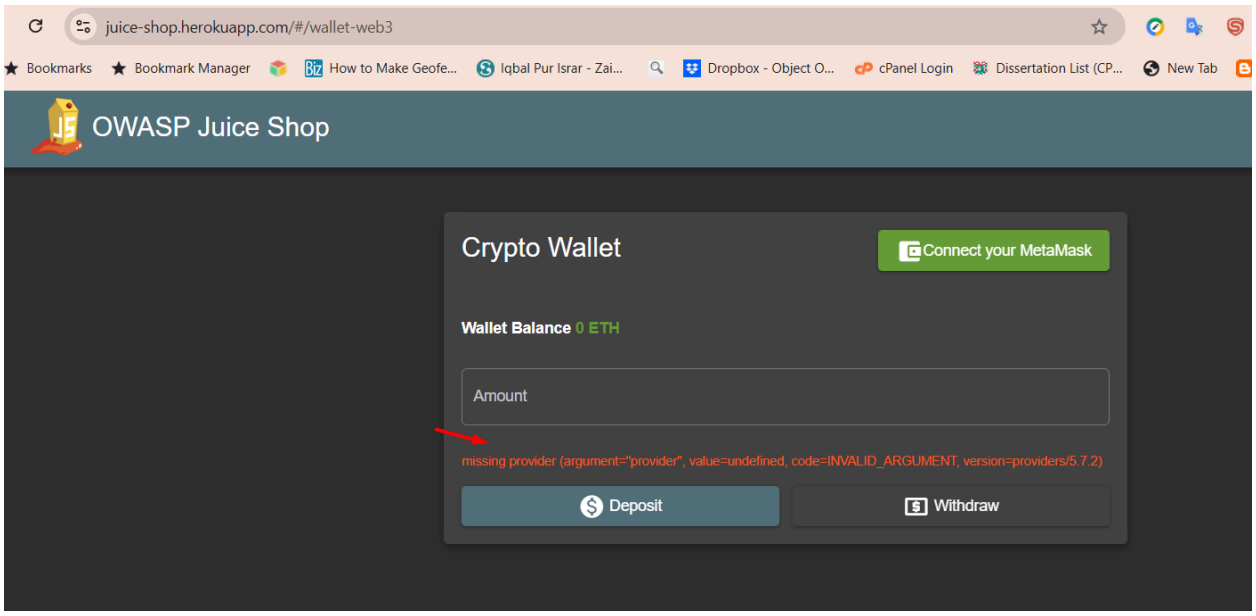
ID number	#005
Name	Web3 Wallet Withdraw throws an error stacktrace.
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	Error messages used on the FE should be in a readable format for the user.
URL	https://juice-shop.herokuapp.com/#/wallet-web3
Browser	Google Chrome Version 132.0.6834.84
Severity	Low
Priority	Low

Steps to reproduce

> Go to the Juice App Login Screen.

> Login with a valid User
> Go to Account -> Orders and Payments -> Digital Wallet
> Click on Try our new crypto wallet
> An Error message is thrown. Which shows BE error.

Attachments:

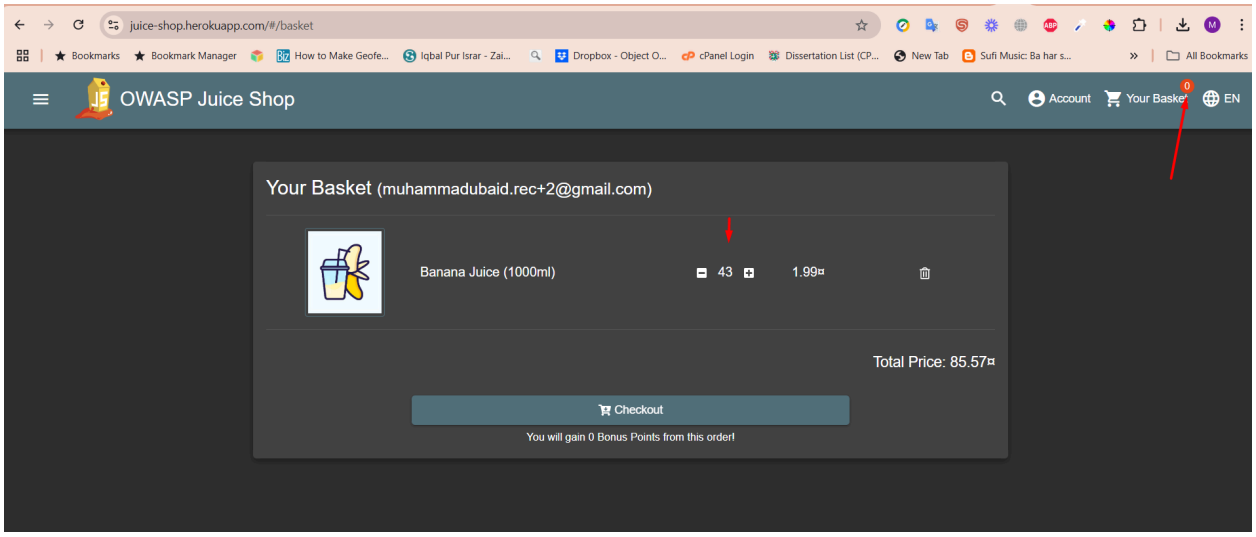


ID number	#006
Name	Basket counter resets to zero on refreshing URL.
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	Basket counter resets to zero when page is refreshed.
URL	https://juice-shop.herokuapp.com/#/basket
Browser	Google Chrome Version 132.0.6834.84
Severity	Medium
Priority	Medium

Steps to reproduce

> Go to the Juice App Login Screen.
> Login with a valid User
> Add a few items to cart
> Go to cart and refresh URL.
> Your basket shows zero count now.

Attachments:

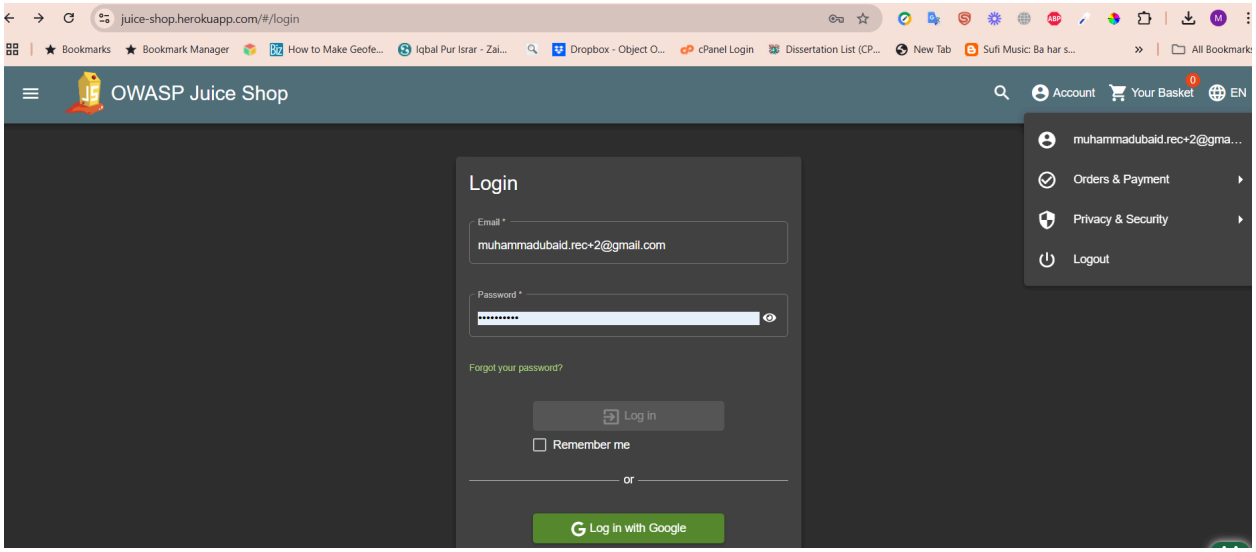


ID number	#007
Name	Login Page accessible while the User is logged In.
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	System allows the user to access the login screen when he is already logged In.
URL	https://juice-shop.herokuapp.com/#/login
Browser	Google Chrome Version 132.0.6834.84
Severity	Medium
Priority	Medium

Steps to reproduce

> Go to the Juice App Login Screen.
> Login with a valid User
> Click on Back button on browser.
> User lands on the Login Page again. While being in the context of login.
> Login should be a separate page outside this context.

Attachments:

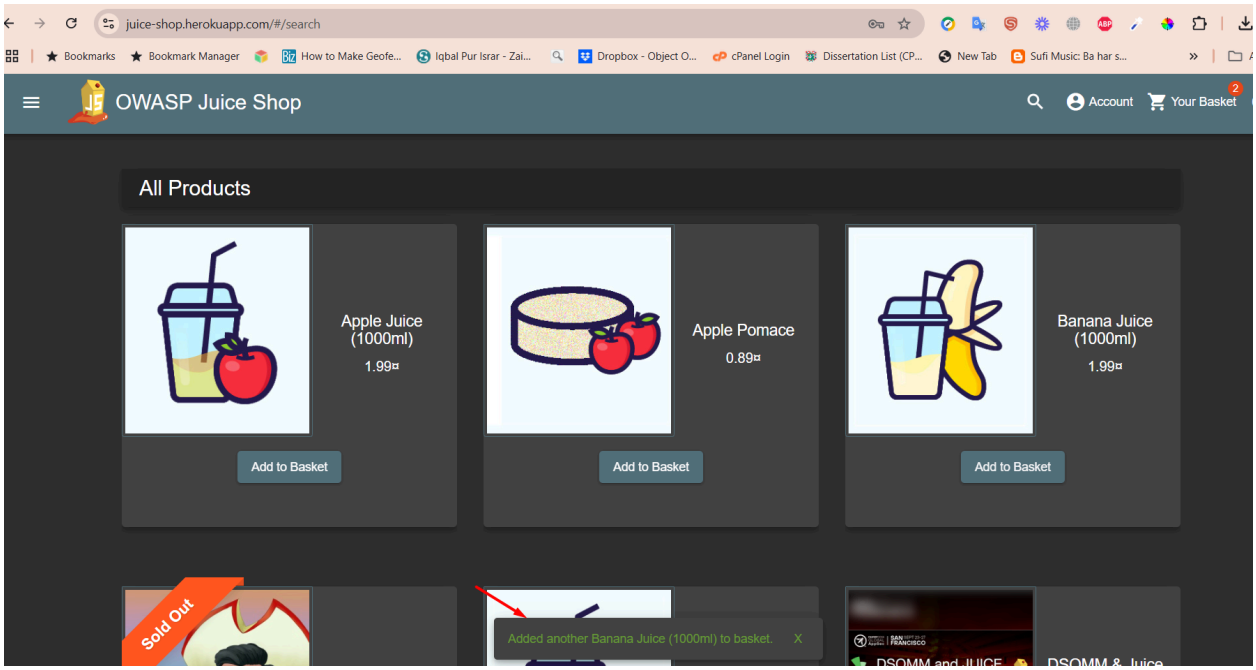


ID number	#008
Name	Added to basket notification showing on the middle of screen.
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	Add to Basket notification placement is not ideal.
URL	https://juice-shop.herokuapp.com/#/search
Browser	Google Chrome Version 132.0.6834.84
Severity	Medium
Priority	Medium

Steps to reproduce

> Go to the Juice App Login Screen.
> Login with a valid User
> Add a few items to cart
> Added to Basket success notification is not easily visible. It should be on the top right of the screen so that the User can easily navigate to the Basket.

Attachments:

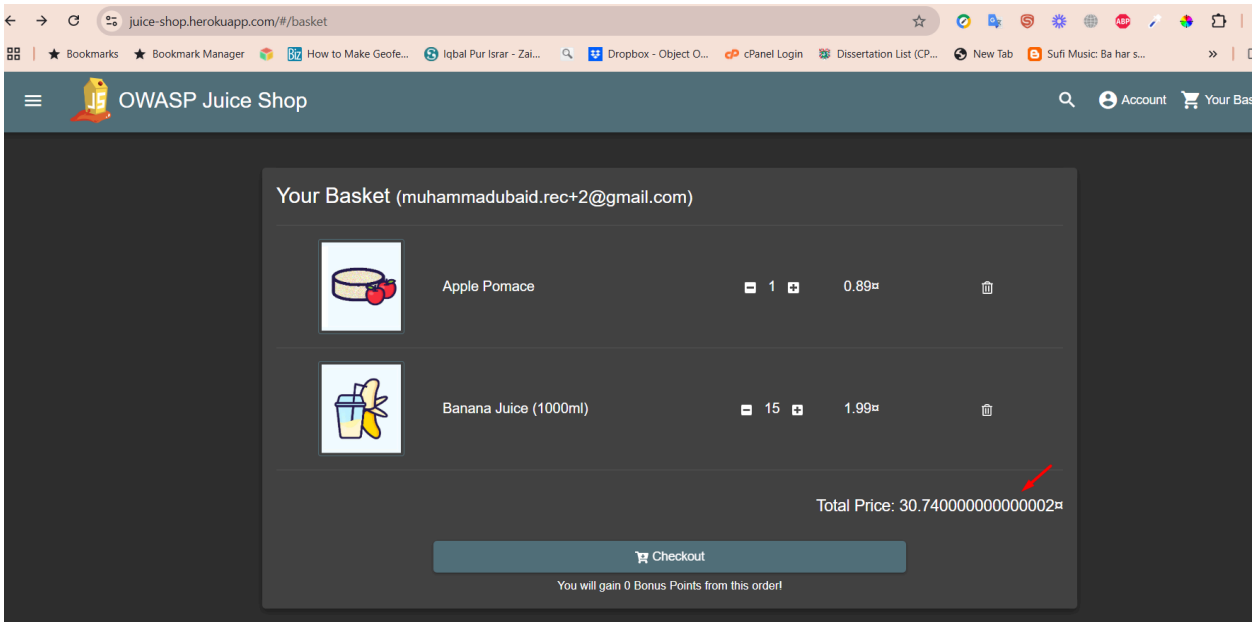


ID number	#009
Name	For some total calculations in cart items total value shows many decimal points
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
URL	https://juice-shop.herokuapp.com/#/basket
Browser	Google Chrome Version 132.0.6834.84
Severity	Medium
Priority	Low

Steps to reproduce

> Go to the Juice App Login Screen.
> Login with a valid User
> Add a few items to cart
> Increase count of items randomly and it shows a lot decimal points for some values.

Attachments:

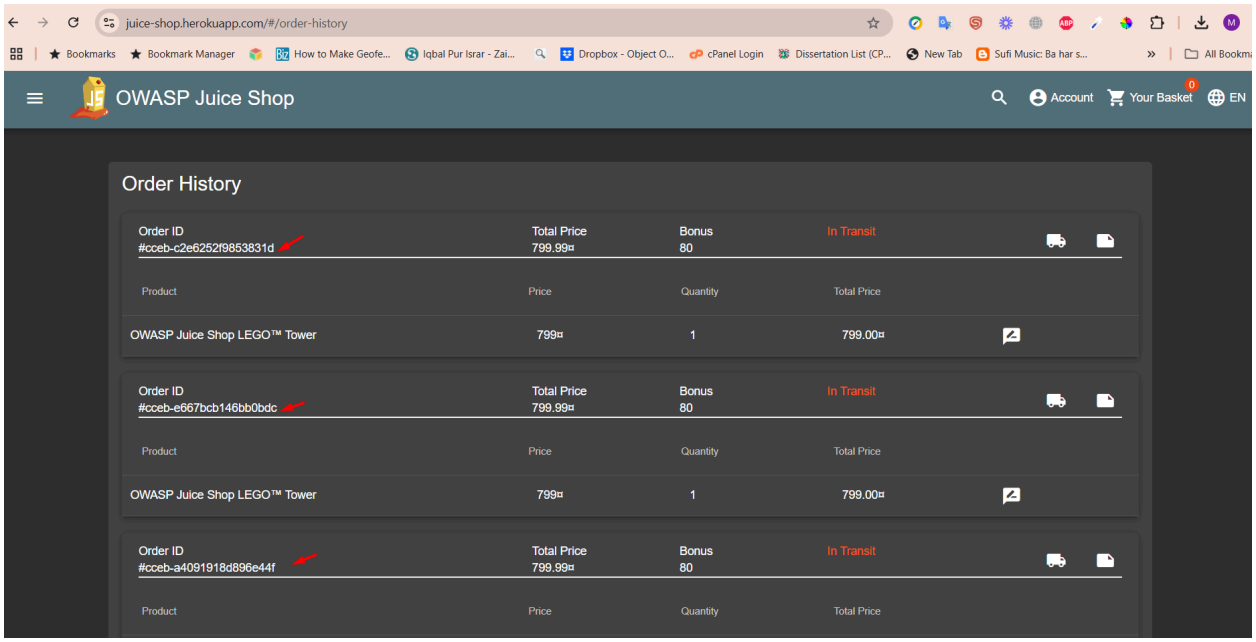


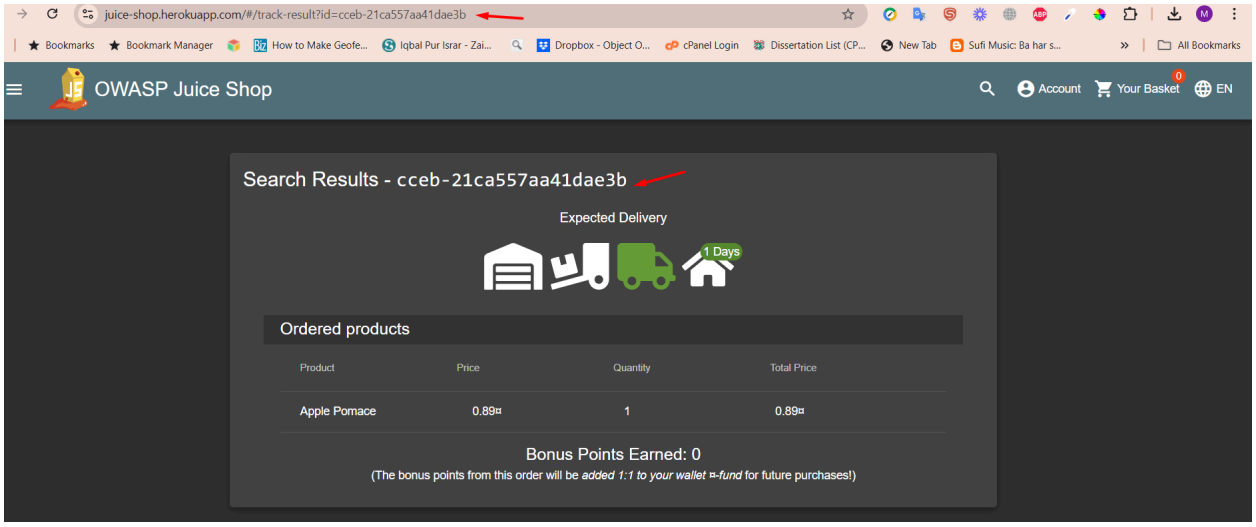
ID number	#010
Name	Databse IDs of Orders is visible to Customer
Reporter	Muhammad Ubaid
Submit Date	19 Jan, 2025
Summary	Order IDs should be human readable i.e. JU-01-238942 etc.
URL	https://juice-shop.herokuapp.com/#/orders
Browser	Google Chrome Version 132.0.6834.84
Severity	Medium
Priority	Medium

Steps to reproduce

> Go to the Juice App Login Screen.
> Login with a valid User
> Add a few items to cart
> Place Orders and goto Order tracking.
> Order IDs are shown as DB Values. Their should be a unique Order ID for DB, and a separate Order ID which is also Unique and is human readable.

Attachments:


juice-shop.herokuapp.com/#/order-history
OWASP Juice Shop
Account
Your Basket
EN
Order History
Order ID
#cceb-c2e6252f9853831d
Total Price
799.99¤
Bonus
80
In Transit
Product
Price
Quantity
Total Price
OWASP Juice Shop LEGO™ Tower
799¤
1
799.00¤
Order ID
#cceb-e667bcb146bb0bdc
Total Price
799.99¤
Bonus
80
In Transit
Product
Price
Quantity
Total Price
OWASP Juice Shop LEGO™ Tower
799¤
1
799.00¤
Order ID
#cceb-a4091918d896e44f
Total Price
799.99¤
Bonus
80
In Transit
Product
Price
Quantity
Total Price


juice-shop.herokuapp.com/#/track-result?id=cceb-21ca557aa41dae3b
OWASP Juice Shop
Account
Your Basket
EN
Search Results - cceb-21ca557aa41dae3b
Expected Delivery
1 Days
Ordered products
Product
Price
Quantity
Total Price
Apple Pomace
0.89¤
1
0.89¤
Bonus Points Earned: 0
(The bonus points from this order will be added 1:1 to your wallet ¤-fund for future purchases!)