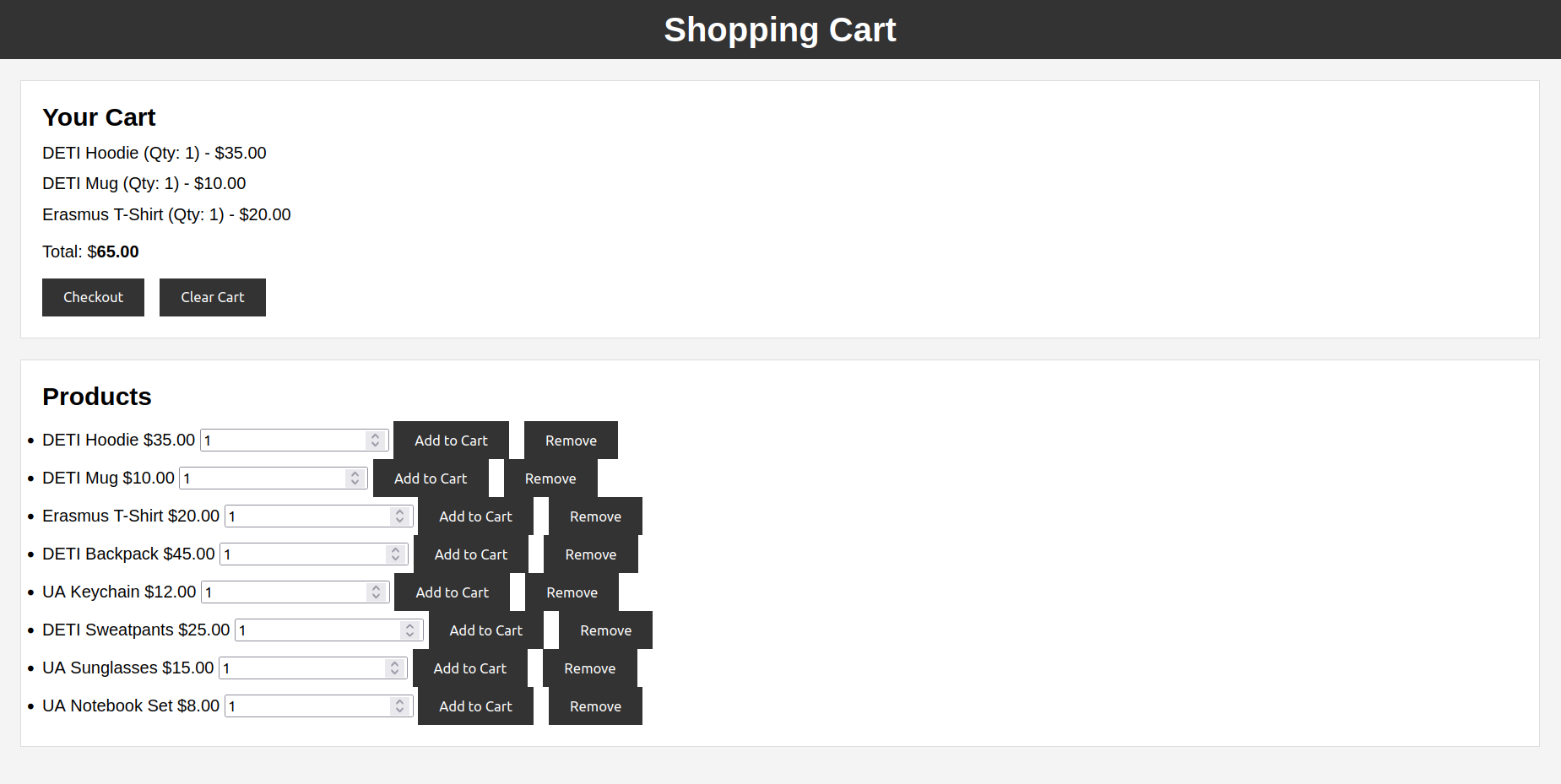
**CWE-20: Improper Input Validation**

The vulnerability at hand is found in the page that simulates a shopping cart and its associated javascript. It is basically a lack of input filtering that could possibly allow otherwise impossible purchases.

**Demonstration of the vulnerability:**

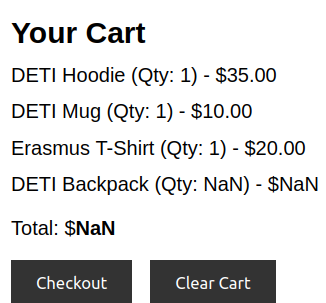
In the cart page, a selection of items is added.

****

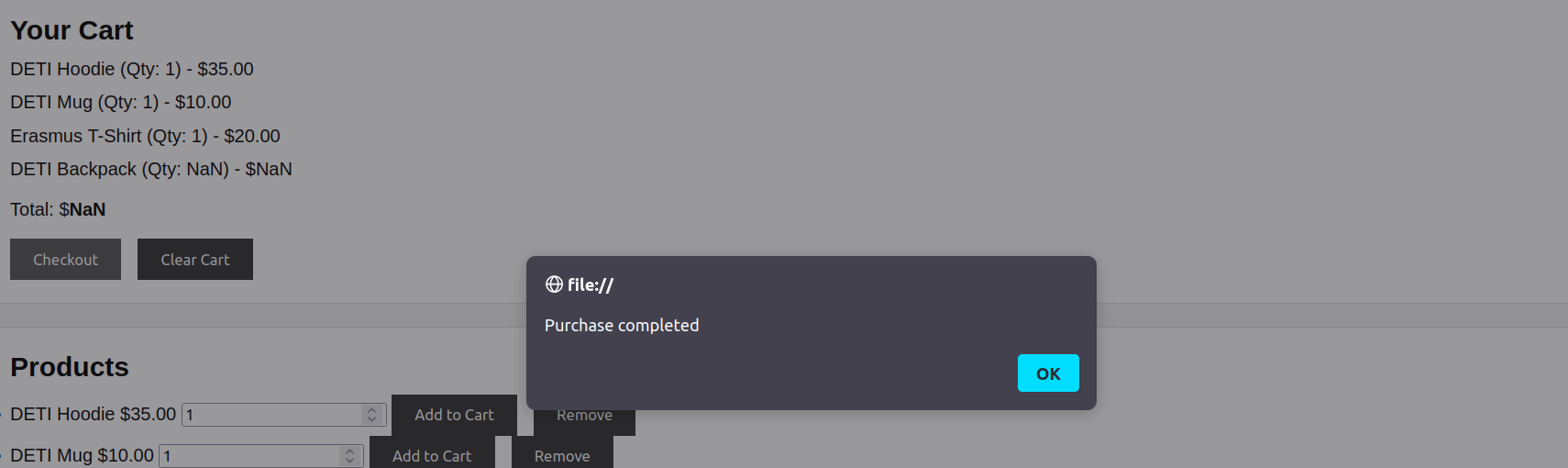
Afterwards, a malicious user adds an item in an amount that should not be possible.

****

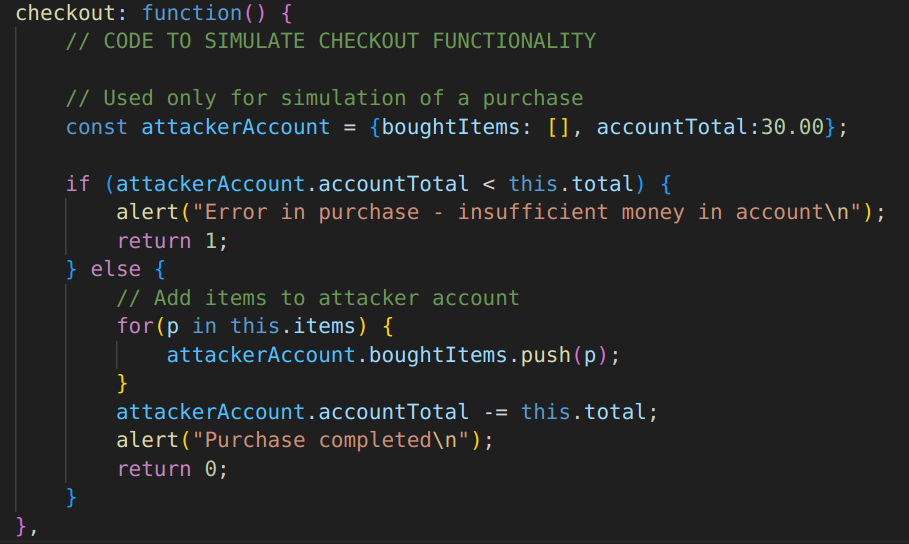
The item, however, is succesfully added. This also changes the cart total in an unintended way.



After clicking ‘Checkout’, the user is allowed to complete the purchase.

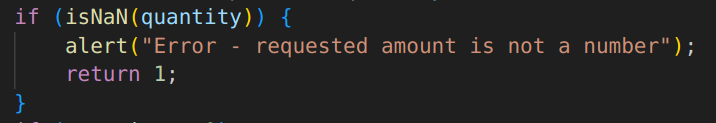


The following snippet shows that the user should not have enough money to complete this transaction.

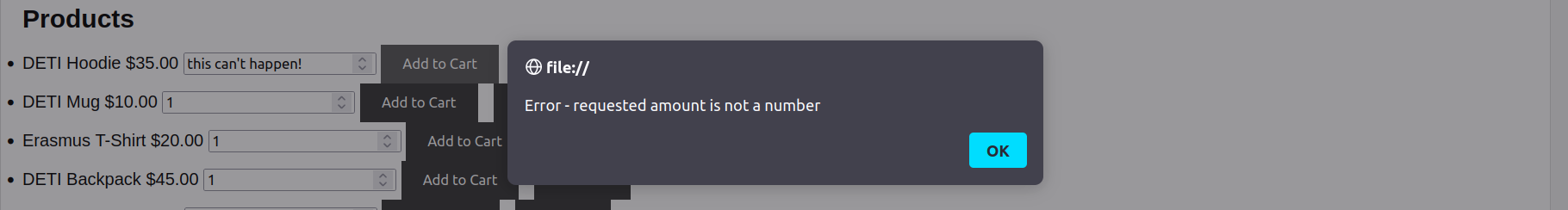


**Fixing the vulnerability:**

This vulnerability can only be exploited because the function addToCart, which is called every time a user tries to insert an item, does not check for the possibility of the quantity provided not being a number. Therefore, this issue can easily be solved by adding the following code to the javascript file of the cart page:



Now, if a user tries to abuse the vulnerability:



The operation is blocked. The cart also remains in the same state as before.

