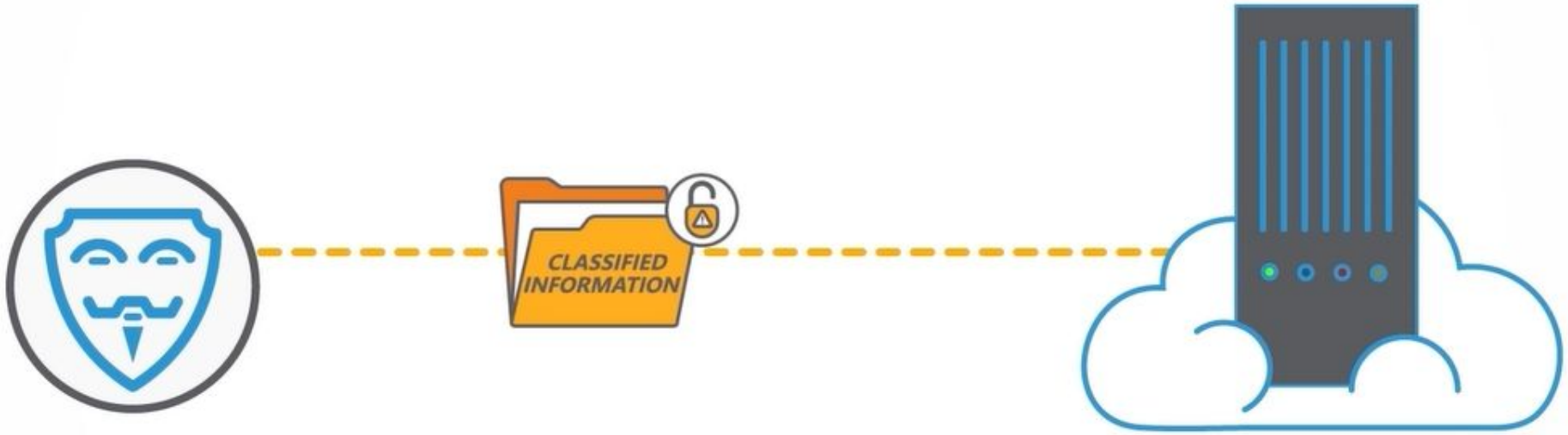
SECURE CODE WARRIOR

INSUFFICIENT VALIDATION

The Insufficient Validation of input parameters could let attackers send in data that allows them to bypass security procedures,

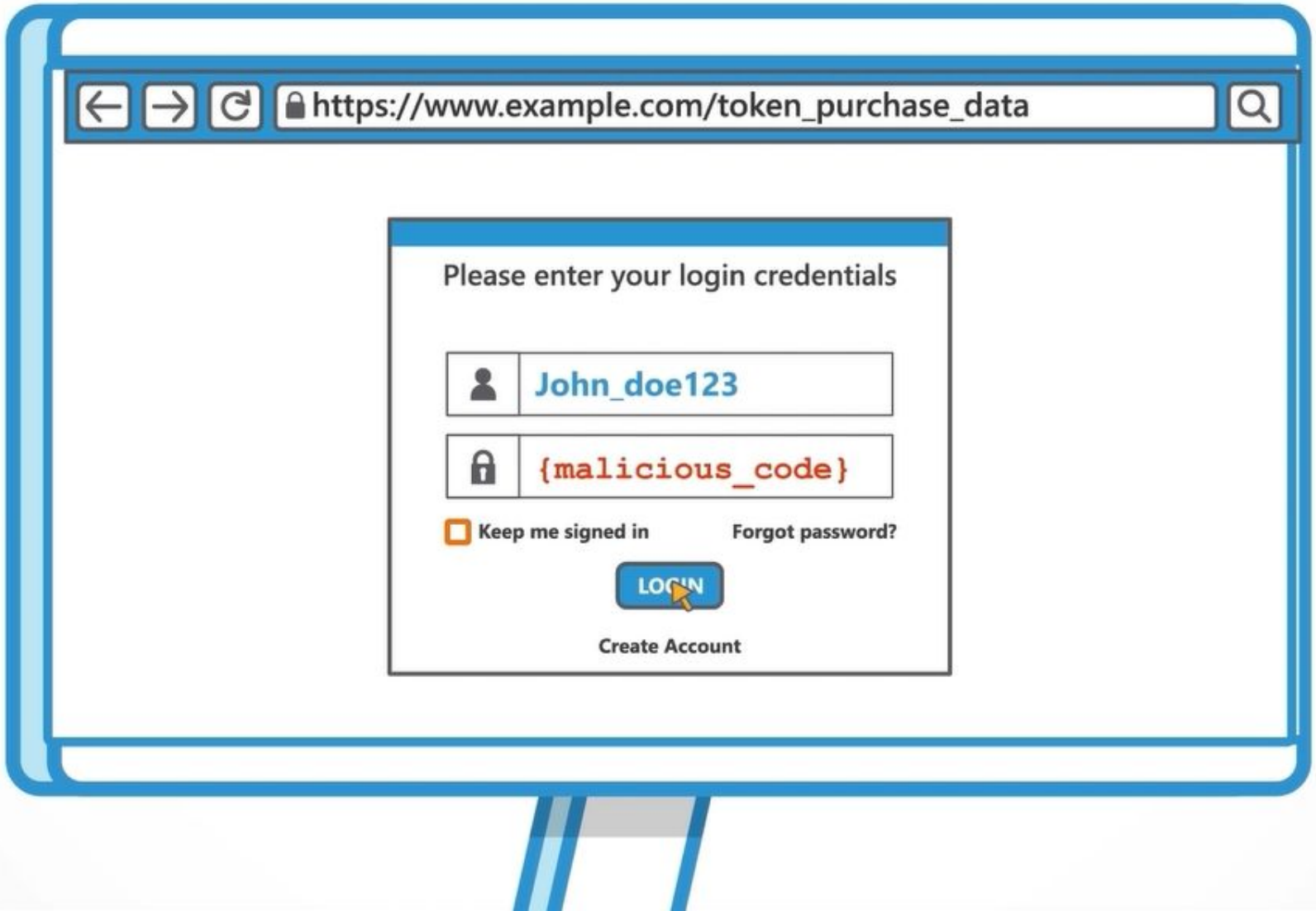
gain access to restricted information,



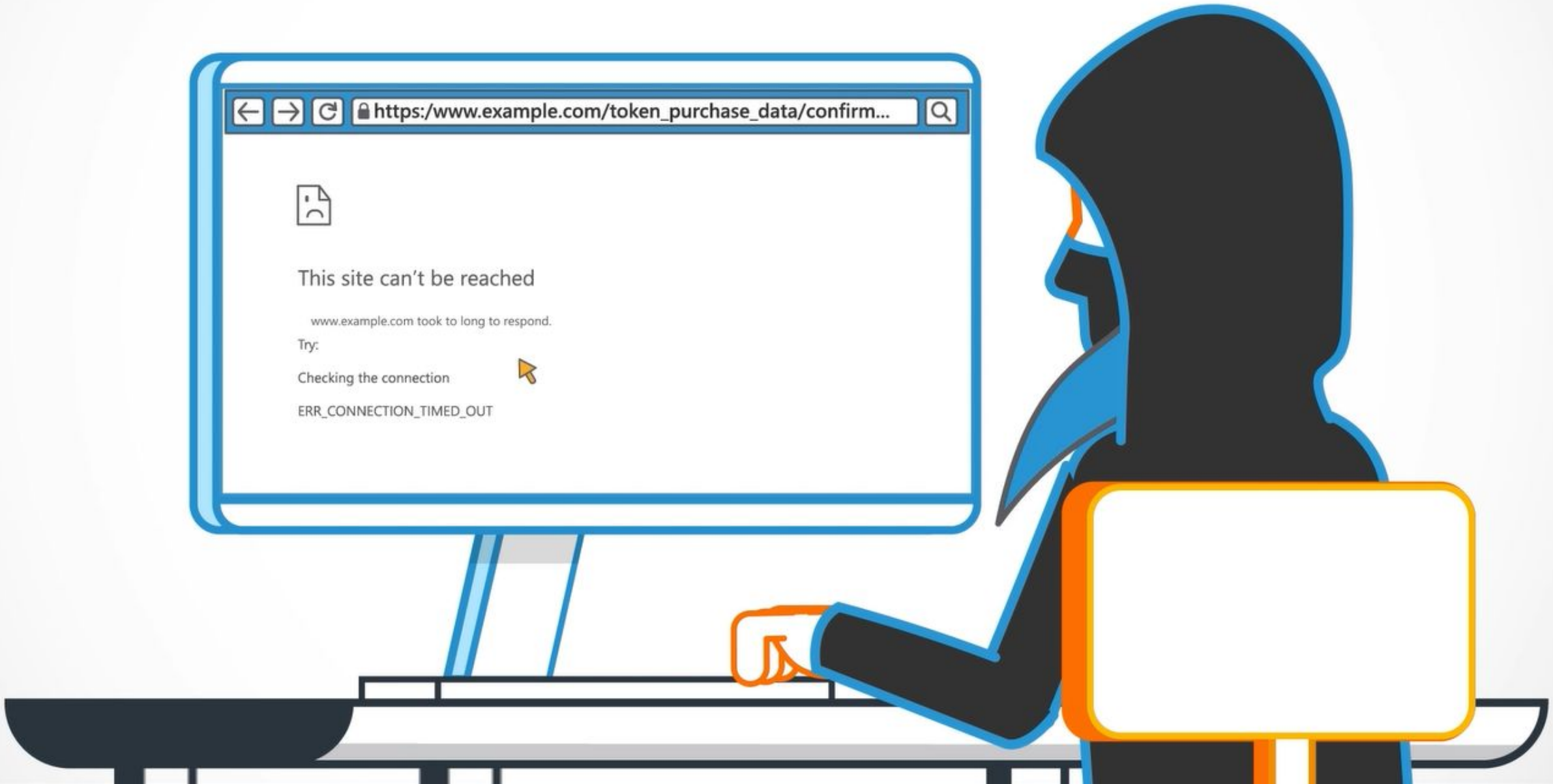
or cause services to crash.

WHERE DOES THIS VULNERABILITY OCCUR?

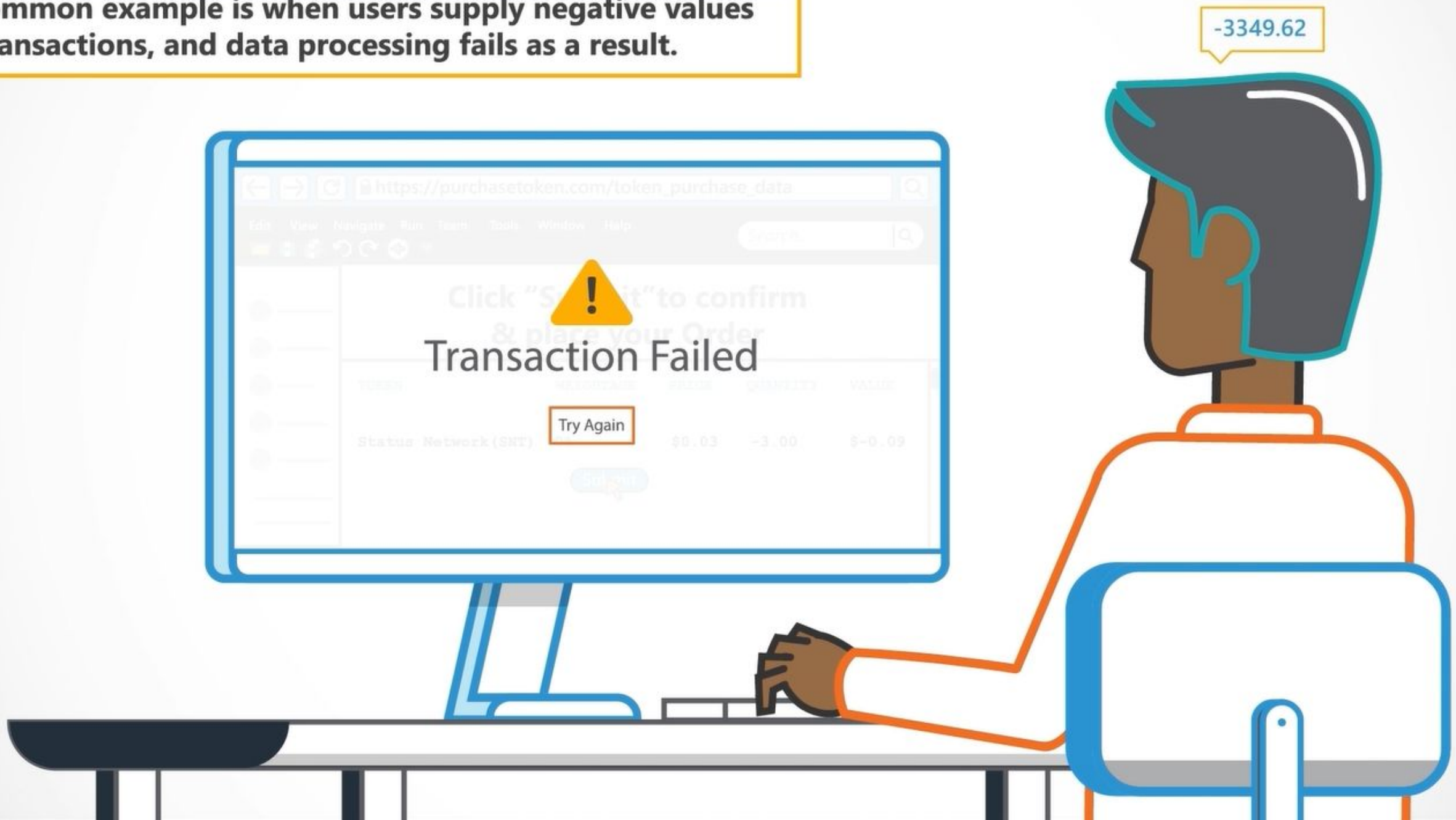
It can occur in any function that requires external inputs to complete its operation.



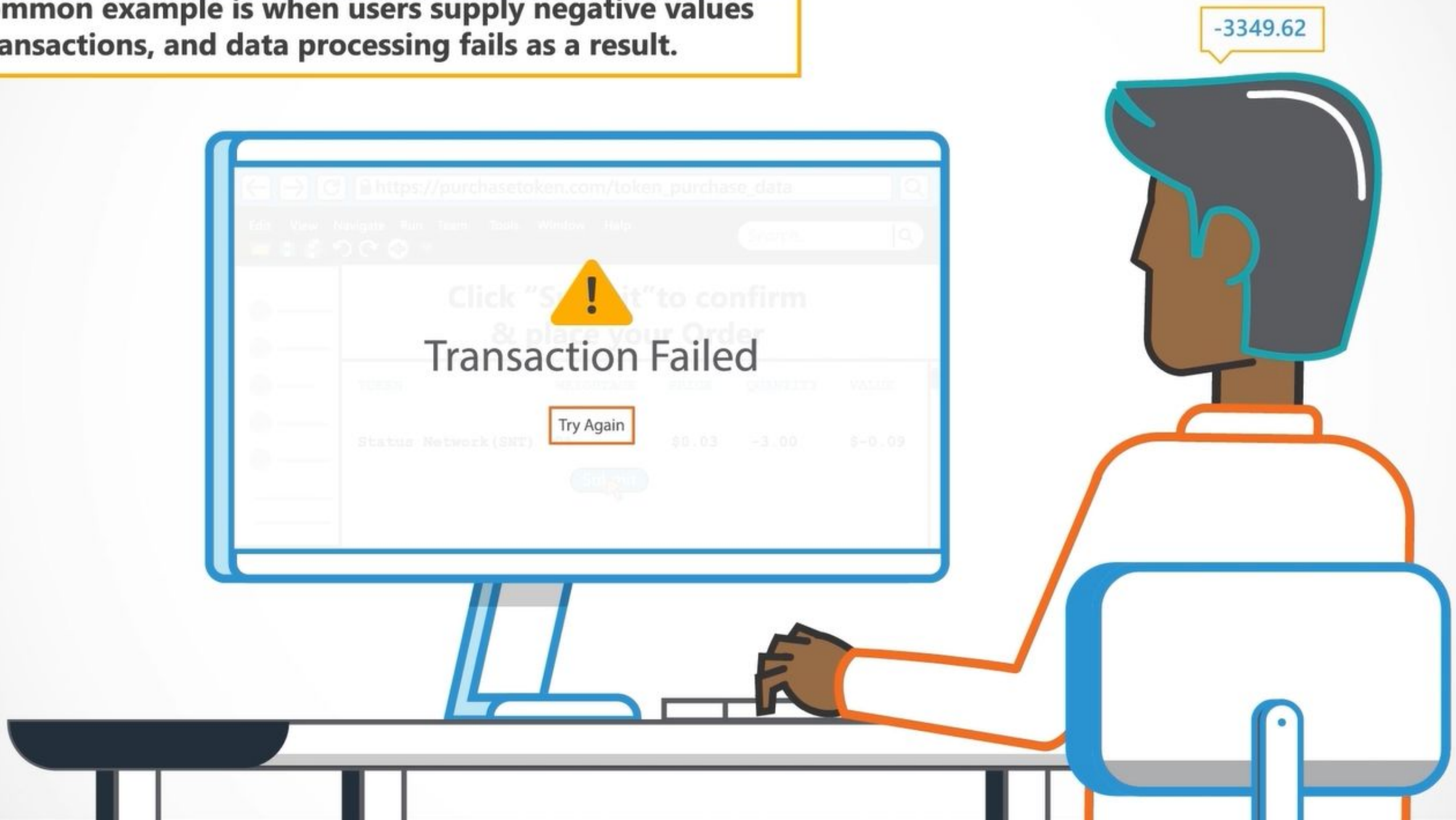
When attacked, these operations may fail in unexpected ways or throw exceptions.



A common example is when users supply negative values in transactions, and data processing fails as a result.

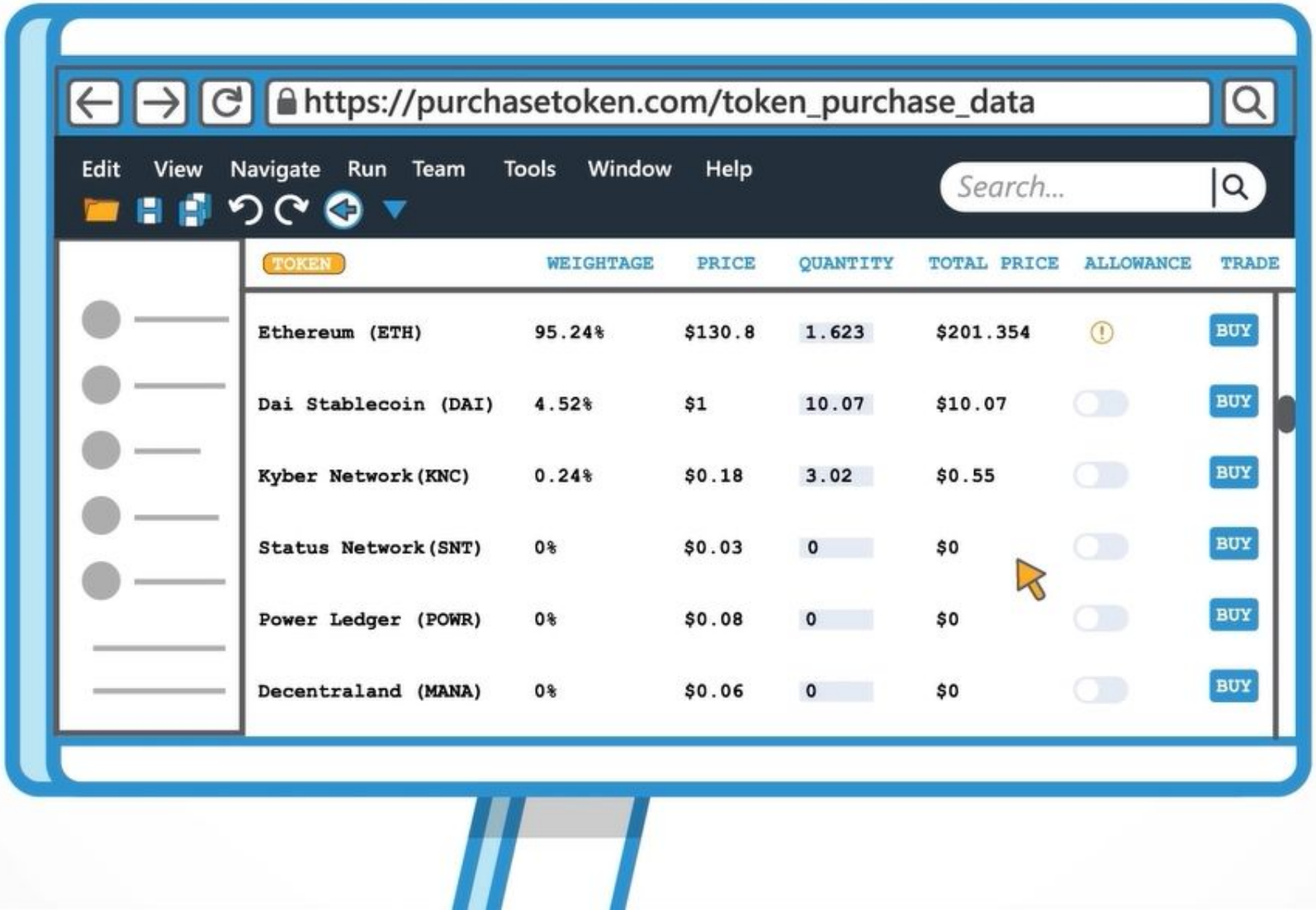


A common example is when users supply negative values in transactions, and data processing fails as a result.

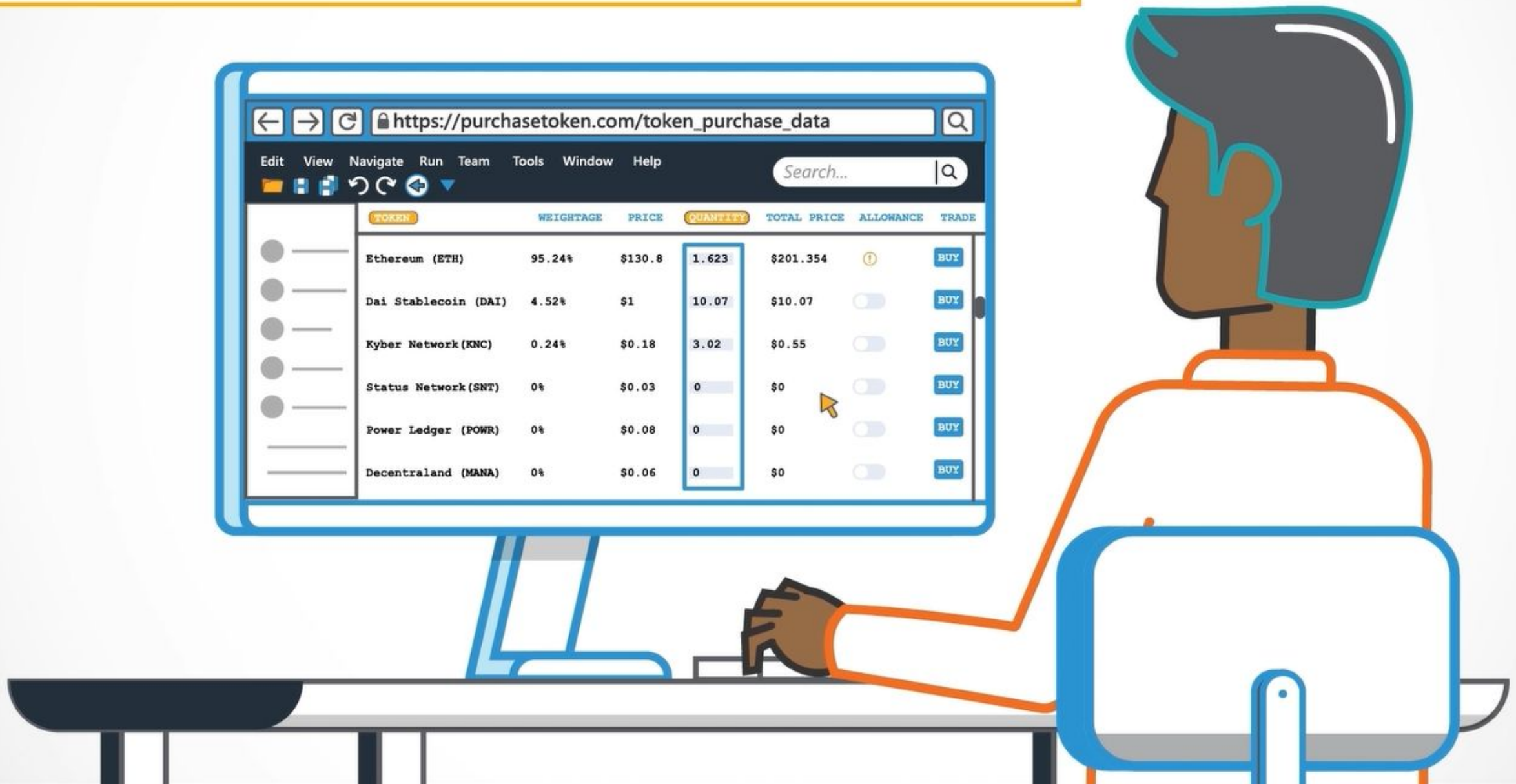


LET'S LOOK AT AN EXAMPLE

In this application, users can pre-purchase tokens to access functionality in the application.

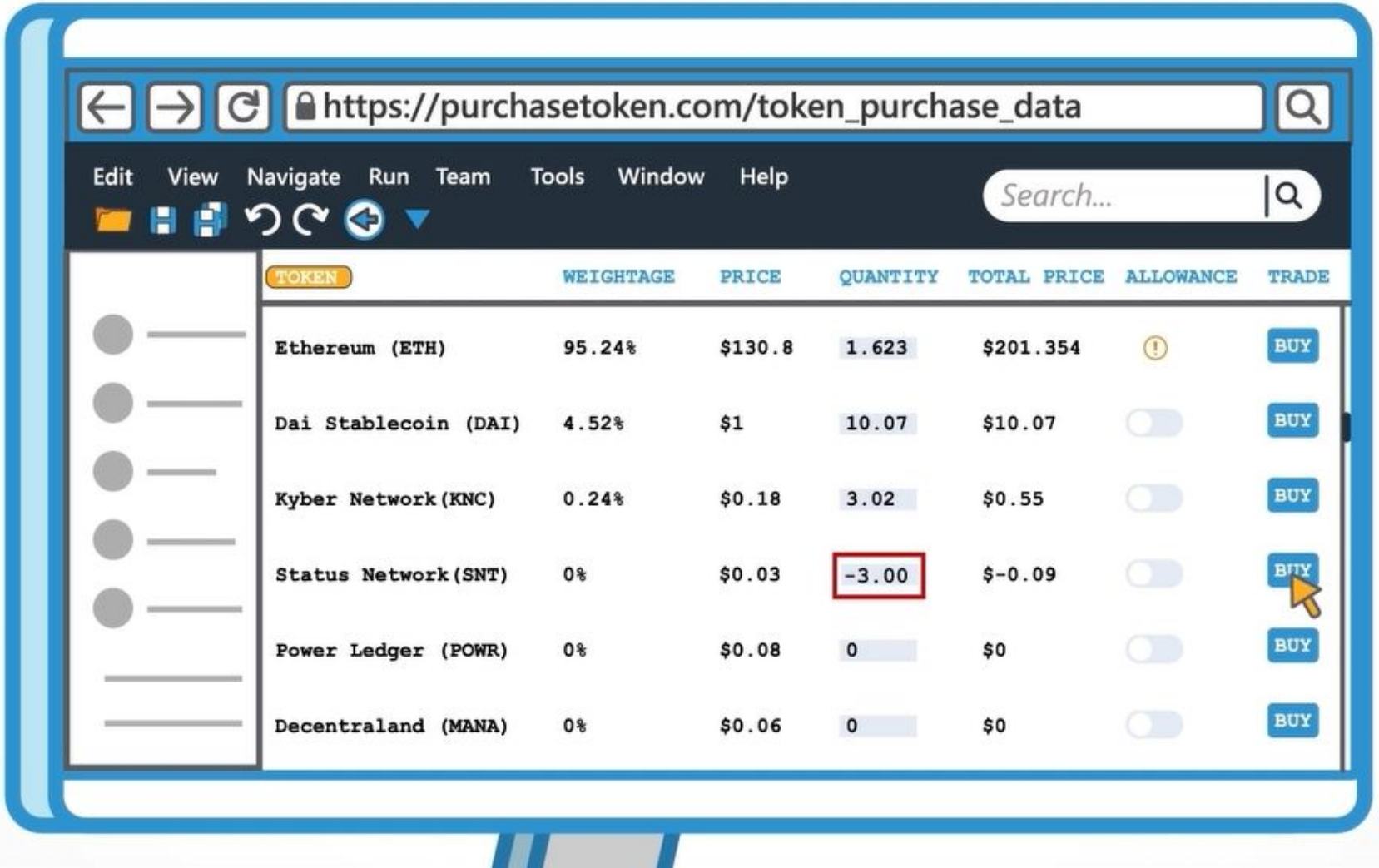


The application asks the user how many tokens they want to spend on this transaction in the platform, and provides a free text field for a response.

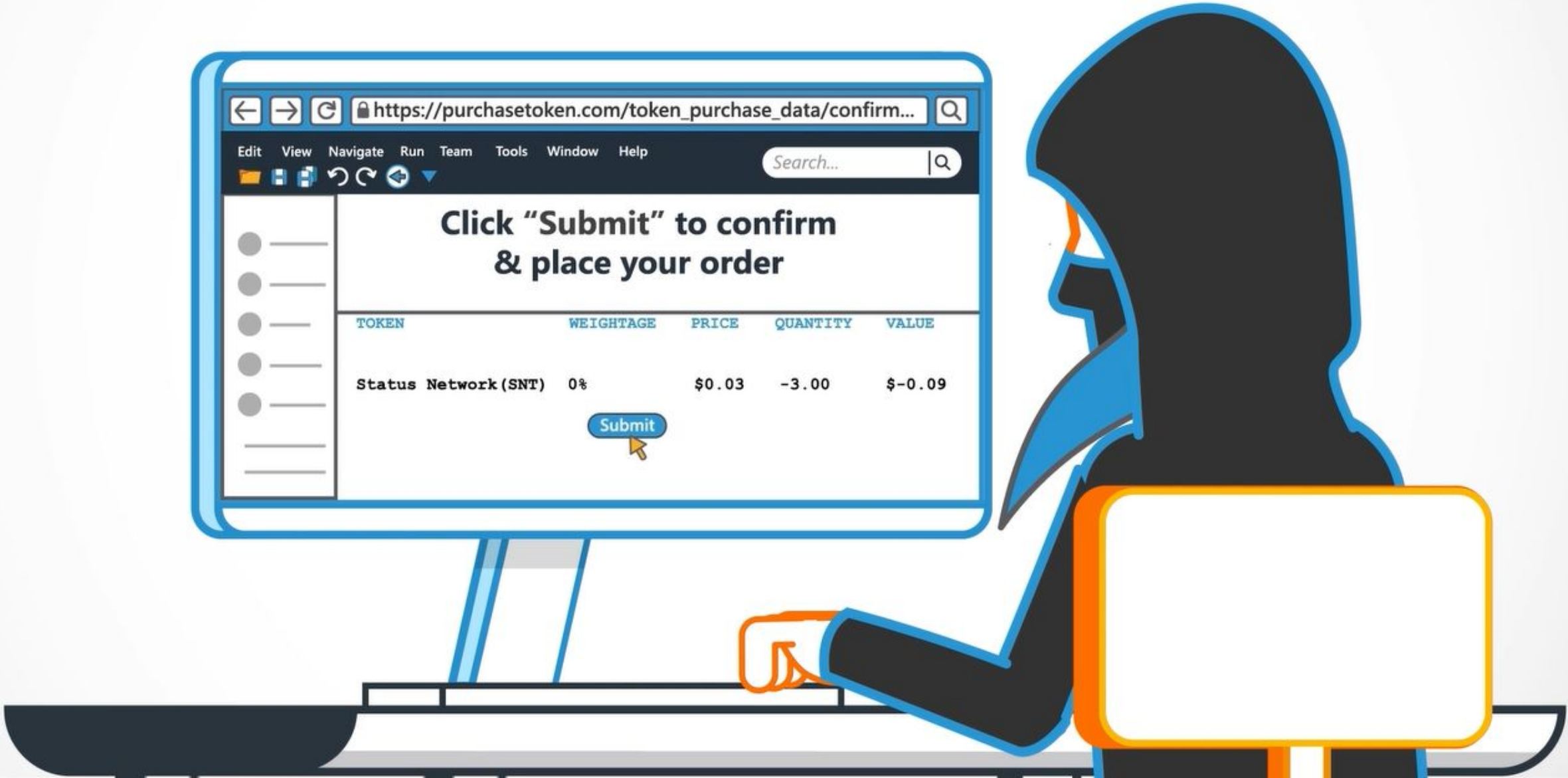


Unfortunately, the application does not validate the value received from the user.

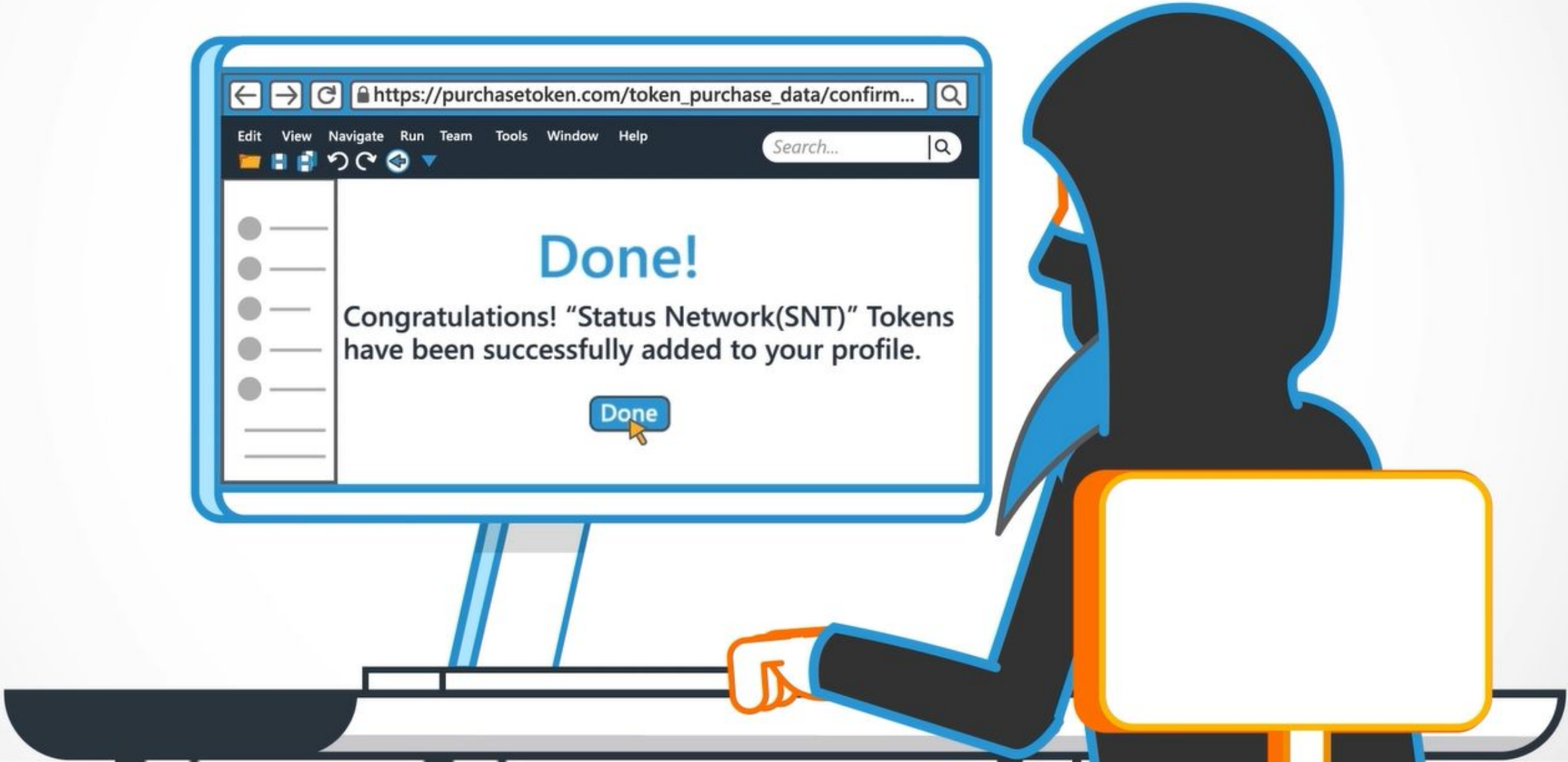
NO INPUT VALIDATION



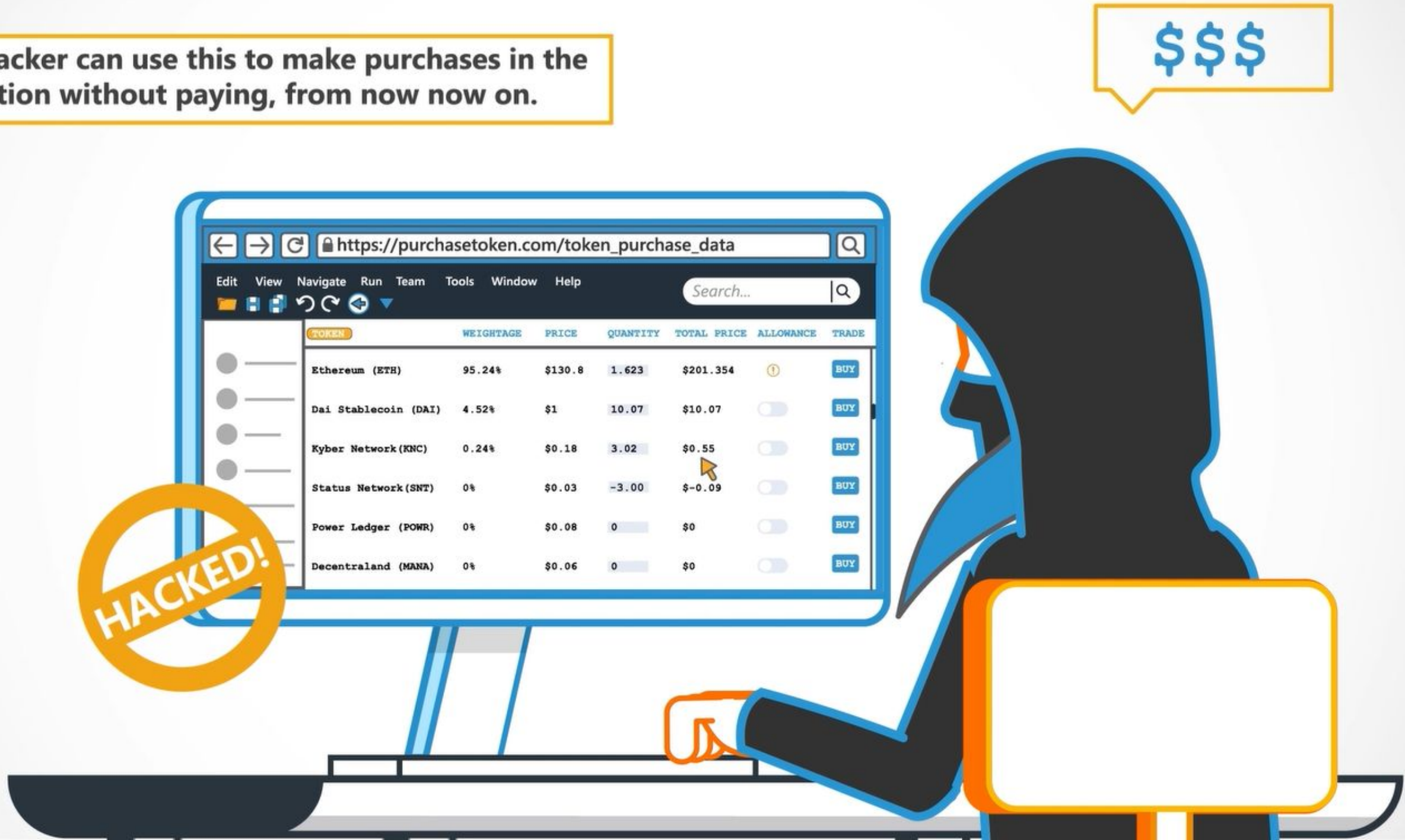
Realizing this, an attacker provides a negative value into the form and presses “Submit”.



Now, instead of removing the entered amount of tokens, the application adds the tokens to the attackers profile.



The attacker can use this to make purchases in the application without paying, from now now on.



To prevent Insufficient Validation, developers should :

- Consider all potential areas where inputs can enter the software and assume all input is malicious
- Consider using an allowlist with valid input parameters
- Ensure any security checks performed on the client side are duplicated on the server side
- Always convert inputs into the appropriate, expected data type

Congratulations, you have now completed this module!


SECURE
CODE
WARRIOR