

VUL-HOST196-RodrigoVilchez-01

Tipo de problema: poco control en verificación del precio al agregar un artículo

Autor: Rodrigo Vilchez Ulloa

Localización del problema: se encuentra en la sección de agregar un artículo nuevo a la venta.

Descripción del problema: Con ayuda de un navegador, al agregar un artículo a la venta es posible modificar el código HTML para que el campo del precio no tenga un *pattern* ni un *maxlength*, esto permite que el precio pueda tener un valor muy alto e incluso números negativos, lo que afecta el carrito de compras del usuario al momento de pagar.


PONER ARTICULO

NOMBRE DEL ARTICULO

input.text 614.09 × 20

NUMERO DE EXISTENCIAS

```
<div class="login" style="background-color: rgb(248,248,255,0.8);">
  <h2 class="title"> Poner Articulo En Venta </h2>
  <form method="post" style="padding-top: 40px" action="product_page.cgi">
    <input type="text" class="text" name="productName" maxlength="51" required>
    <span>Nombre del articulo</span>
    <br>
    <br>
    <br>
    ...
    <input type="text" class="text" name="productCost" required title="Asegurese de digitar solo montos validos sin comas.">
    == $0
    <span>Precio</span>
    <br>
    <br>
    <br>
    <input type="text" class="text" name="existenceAmount" maxlength="9" required pattern="[0-9]+" title="Asegurese de digitar solo numeros.">
    <span>Numero de existencias</span>
    <br>
    <br>
    <br>
    <input hidden type="text" class="text" name="username" value="hola123" style="display:none;">
```



Perro

₡ -1e65

Existencias: 4

Agregar al carrito

CARRITO DE COMPRAS

| Producto | Cantidad | Precio | Actualizar | Eliminar |
|-----------------|----------|--------------|--|---|
| Perro | 1 | ₡ -1e+65 | <input type="text"/>  |  |
| Ayote | 2 | ₡800 | <input type="text"/>  |  |
| Chicles Trident | 10 | ₡12000 | <input type="text"/>  |  |
| Precio total | | ₡-2147470848 | | |

PROCESAR COMPRA

FACTURA

| Productos | Cantidad | Precio |
|-----------------|----------|--------------|
| Perro | 1 | €-1e+65 |
| Ayote | 2 | €800 |
| Chicles Trident | 10 | €12000 |
| Precio Total | | €-2147470848 |

Usuario:hola123
Correo:hola2@gmail.com
Gracias por su compra!

VOLVER

Nivel de gravedad: crítico

Descripción del impacto: puede producir errores por overflow. Al agregar un artículo con un valor negativo, se puede agregar al carrito y hacer que el total de la compra sea un número negativo e incluso se puede utilizar para bajar el precio al total del carrito, que contenga otros artículos con un precio válido, y así poder pagar menos del precio real y “camuflar” la transacción. El usuario podría hacer compras de productos sin tener que pagar por ello.

Tiempo dedicado: 30 minutos