

VUL-HOST195-RodrigoVilchez-03

Tipo de problema: ingreso de un precio negativo en un producto

Autor: Rodrigo Vilchez Ulloa

Localización del problema: sección de agregar un nuevo producto

Descripción del problema: al modificar el código HTML, se puede eliminar el *pattern* del input del precio, lo que permite a un posible atacante ingresar productos con precios negativos. La página no hace control sobre esto y permite al usuario agregar el producto con un precio erróneo.

Add a product

Product name:

Product price:

Product description:

Add product

```
<head></head>
<body>
  <nav class="navbar navbar-expand-lg navbar-light bg-light"></nav>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bo
otstrap.min.css">
  <style></style>
  <div class="container">
    <div class="text-center mt-5"></div>
    <div class="row">
      <div class="col-lg-7 mx-auto">
        <div class="card mt-2 mx-auto p-4 bg-light">
          <div class="card-body bg-light">
            <div class="container">
              <form action="sellPage" method="POST">
                <div class="controls">
                  <div class="row">
                    <div class="row">
                      <div class="col-md-6">
                        <div class="form-group">
                          <label for="price">Product price:</label>
                          <input id="price" type="text" name="price" class="form-control"
                            pattern="[0-9]*" title="only numbers are allowed." placeholder=
                            "Please enter the price" required="required" data-error="Price
                            is required.">
                        </div>
                      </div>
                    </div>
                  </div>
                </div>
              </form>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>
</body>
</html>
```

Our Market

Products currently in cart:

Buscar

| | |
|---|---|
| Rosa Usuario: Anonimo Rosa | € 12 <div>Add to carrito</div> |
| Prueba Usuario: prueba prueba | € 123 <div>Add to carrito</div> |
| Prueball Usuario: prueba es gratis | € -123456789 <div>Add to carrito</div> |

Nivel de gravedad: alto

Descripción del impacto: no permite el flujo íntegro del sistema, además puede ser aprovechado por un atacante para alterar los precios de los carritos y generar confusiones en los usuarios que visiten la página. Como es posible que no haya una verificación exhaustiva dentro del código, el formulario puede estar expuesto a ataques de inyección.

Tiempo dedicado: 10 minutos