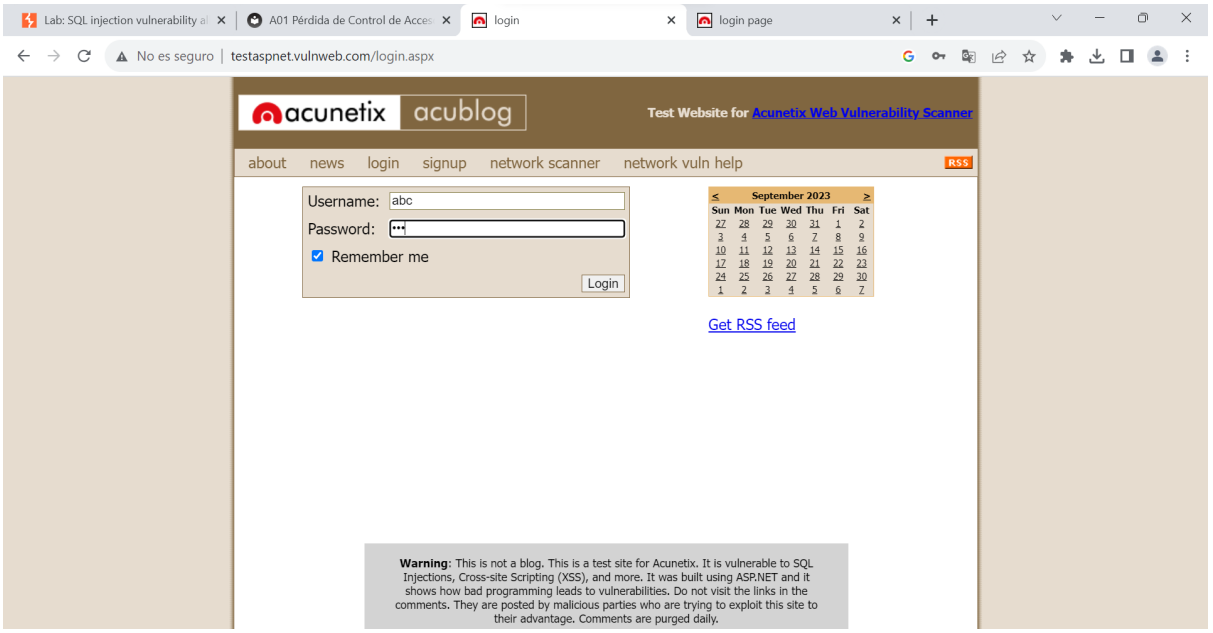
Reporte de informes de vulnerabilidad

Integrantes:
Ian Ricardo Garcia Delgado
Yutsent Rios Velazquez
Mario Eduardo Quiroga Bernal

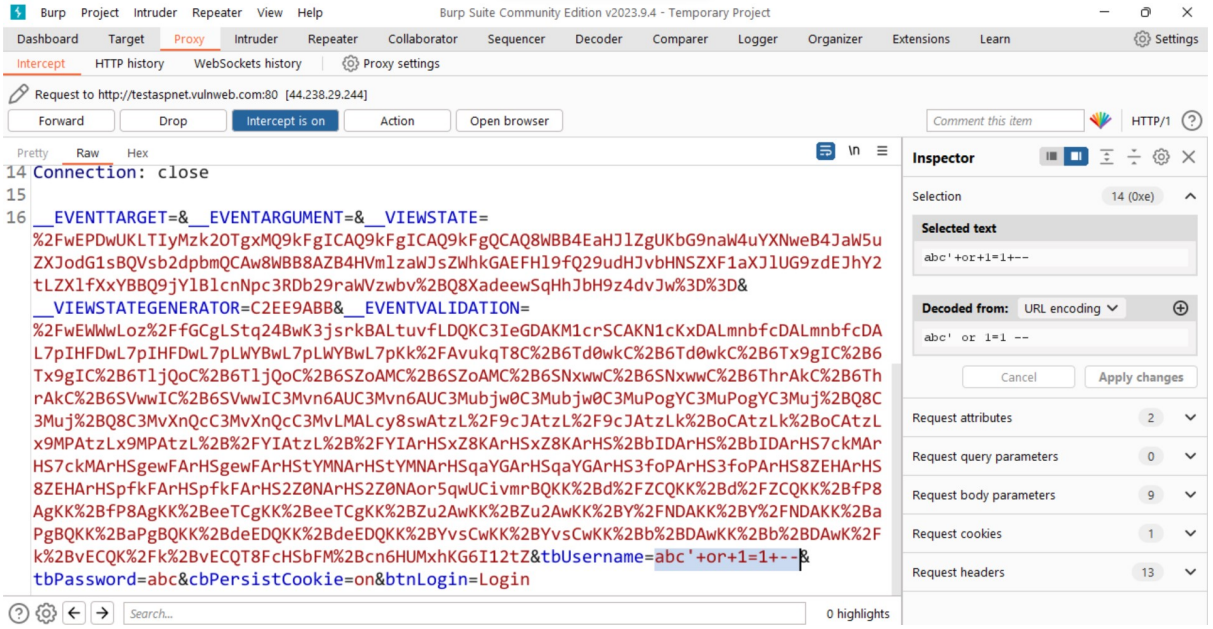
Se va vulneraron las páginas:
http://testphp.vulnweb.com/
http://testaspnet.vulnweb.com/

SQL Injection:

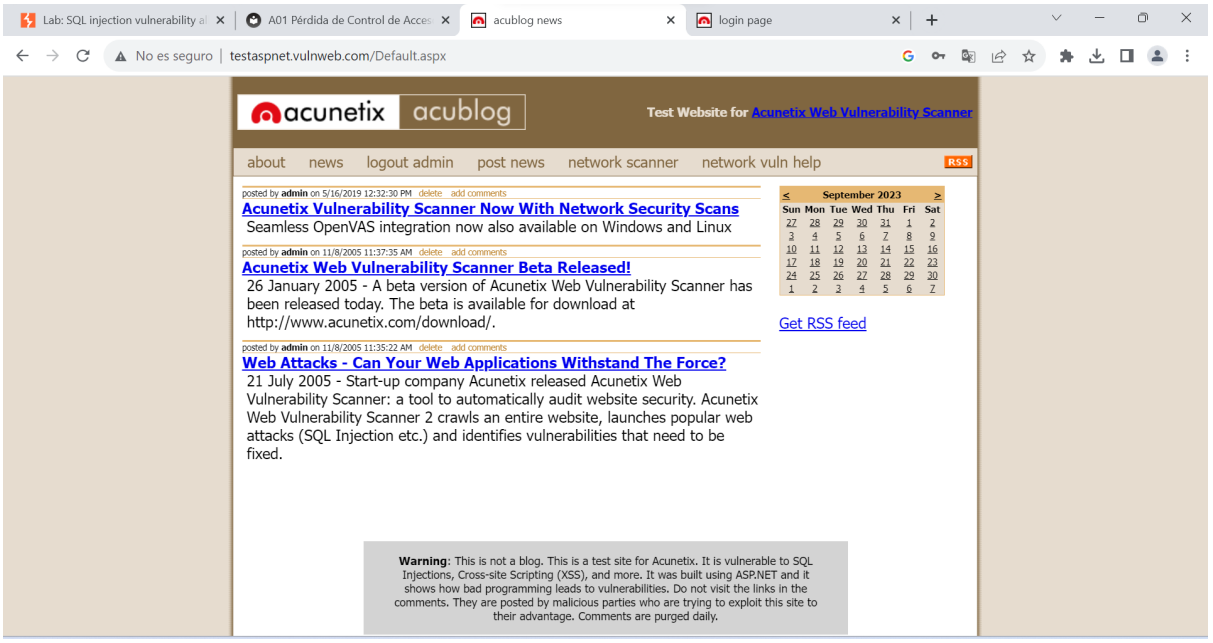
Primero se insertan datos random en el login, y se prepara Burp para interceptar la petición.



Se genera el script para entrar a la app con login, usando " abc' or 1=1 -- ", y se manda la petición.

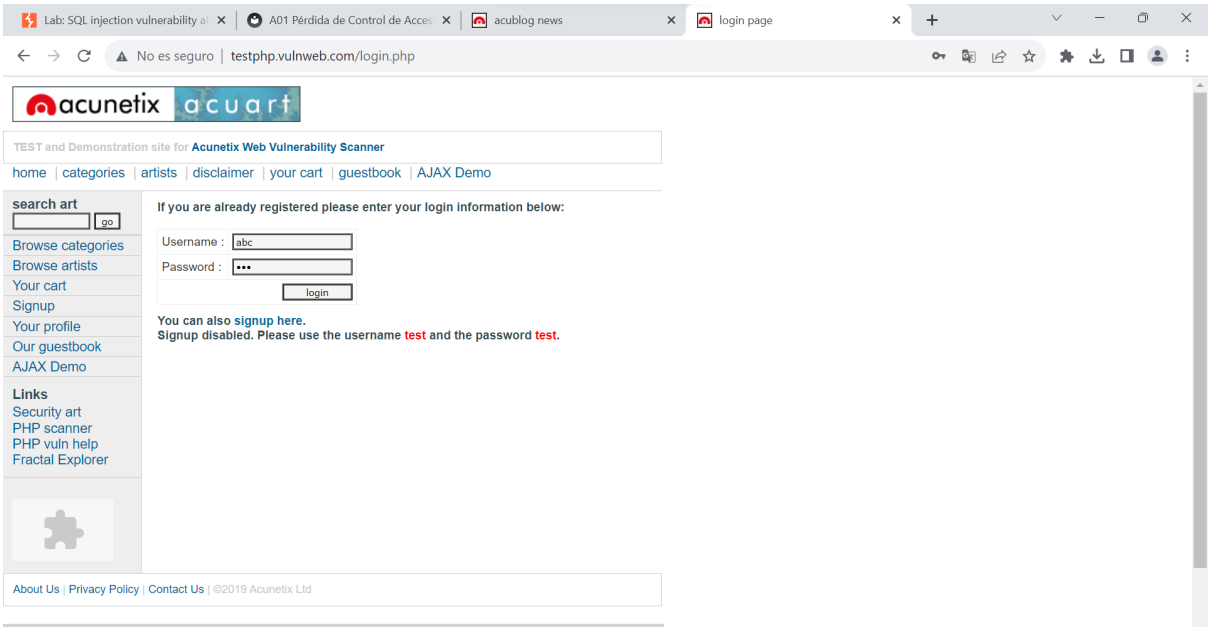


Se logró entrar como admin:

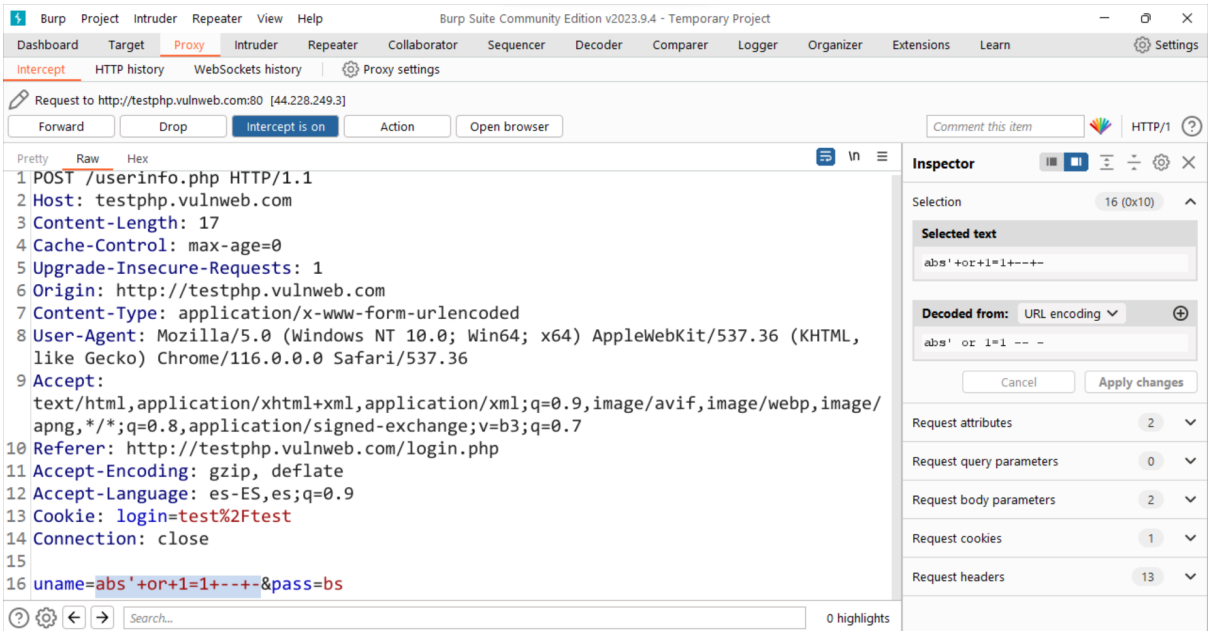


SQL Injection 2:

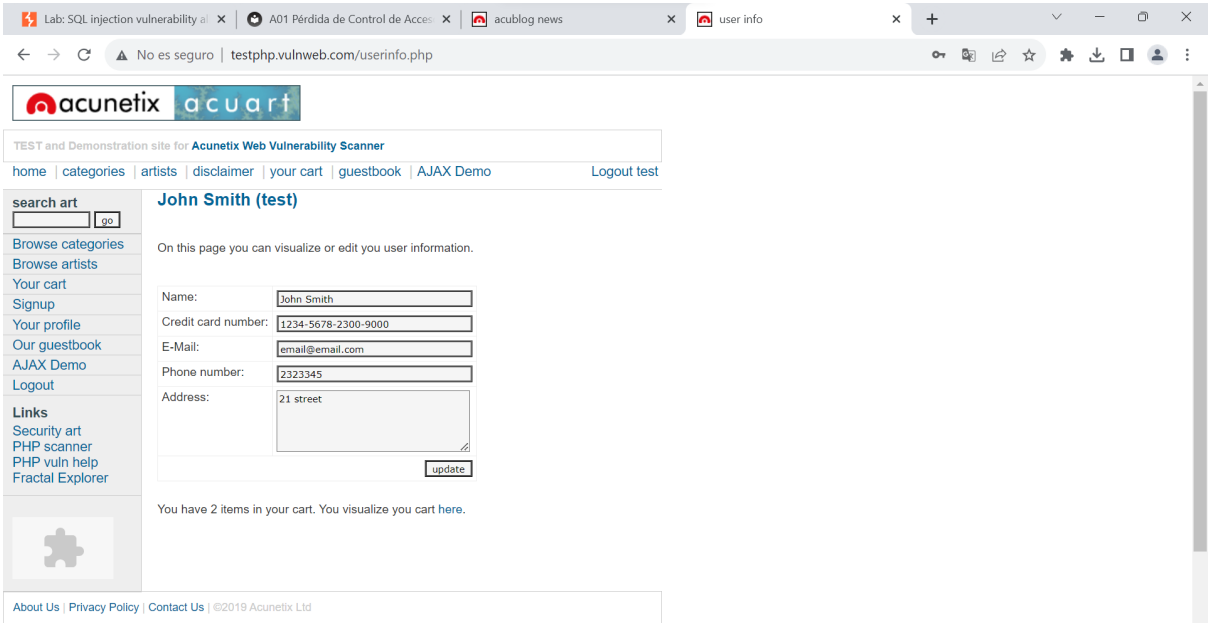
Se inserta cualquier dato en usuario y contraseña preparando el Burp para interceptar la petición.



Se prepara el SQL injection y se manda.



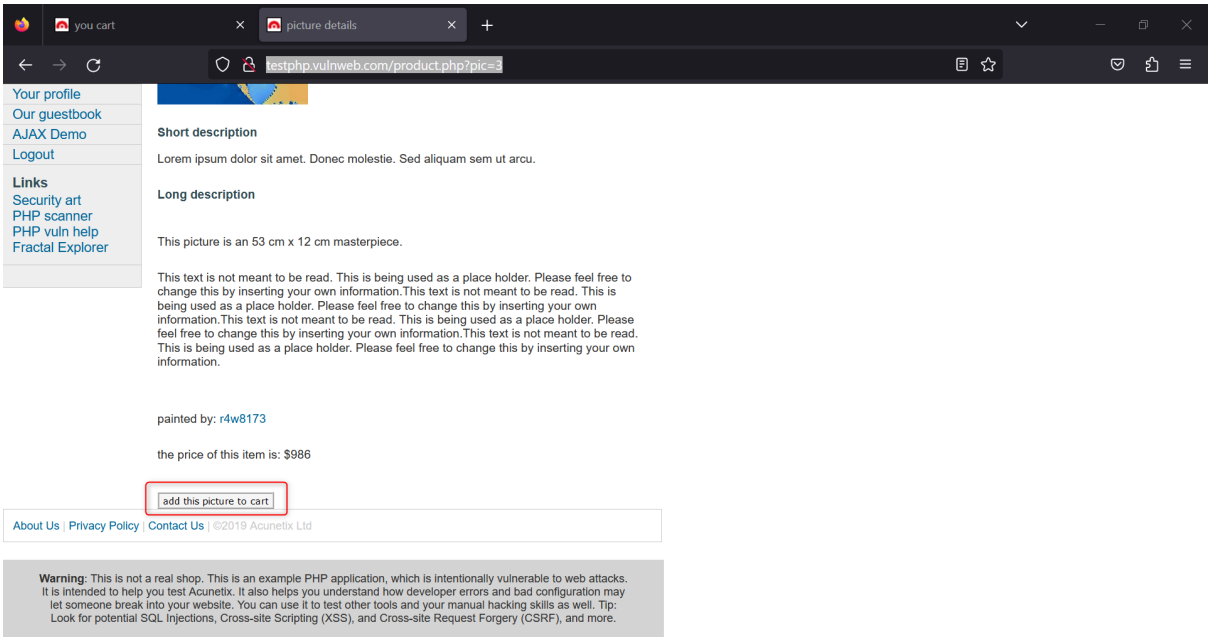
Se enteró a la app como John Smith.



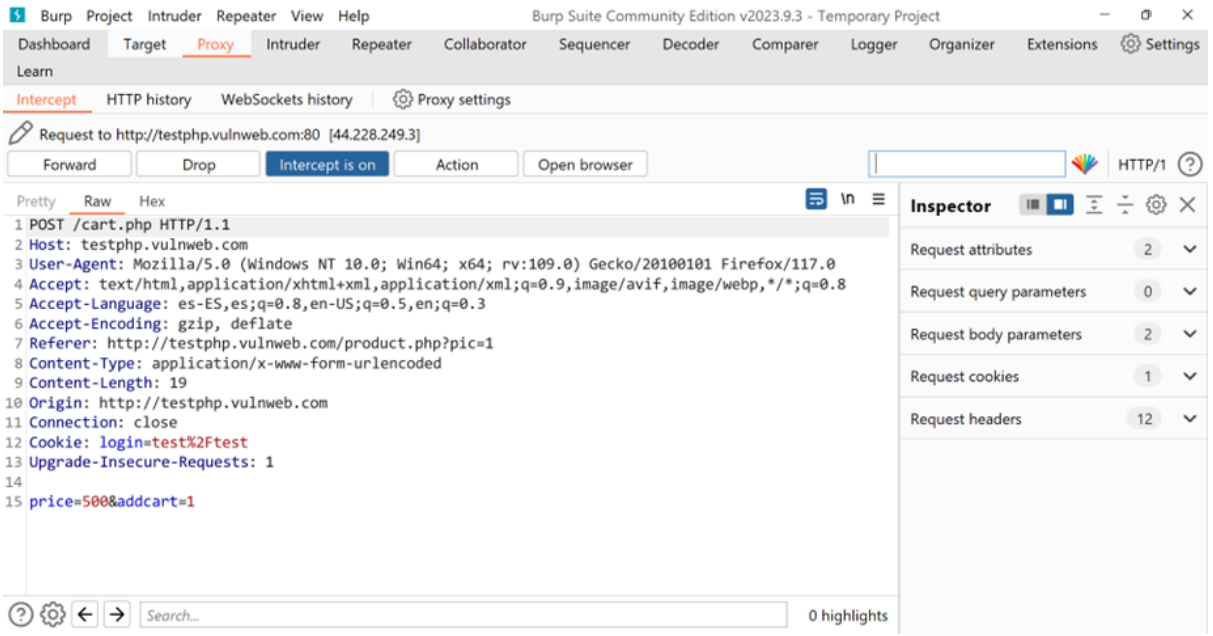
Vulnerabilidad IDOR (Cambio de precio en productos ingresados en carrito)

En primer lugar, se localiza la sección donde se añaden productos al carrito

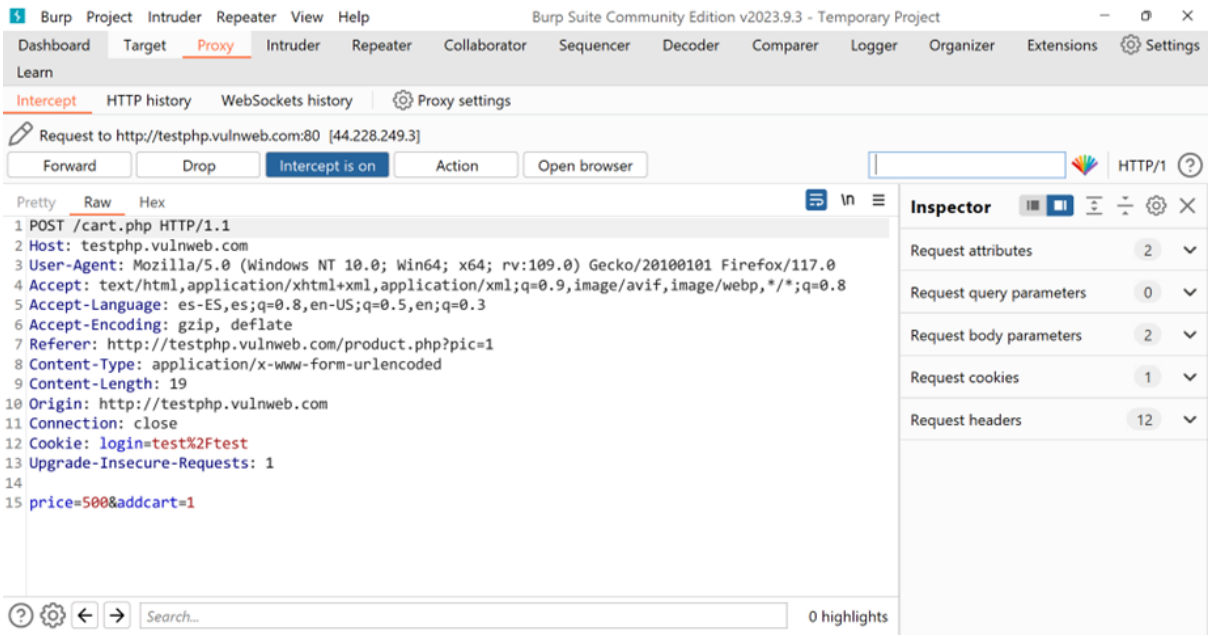
http://testphp.vulnweb.com/product.php?pic=3



Posteriormente se intercepta la request al presionar el botón “add this picture to cart”.



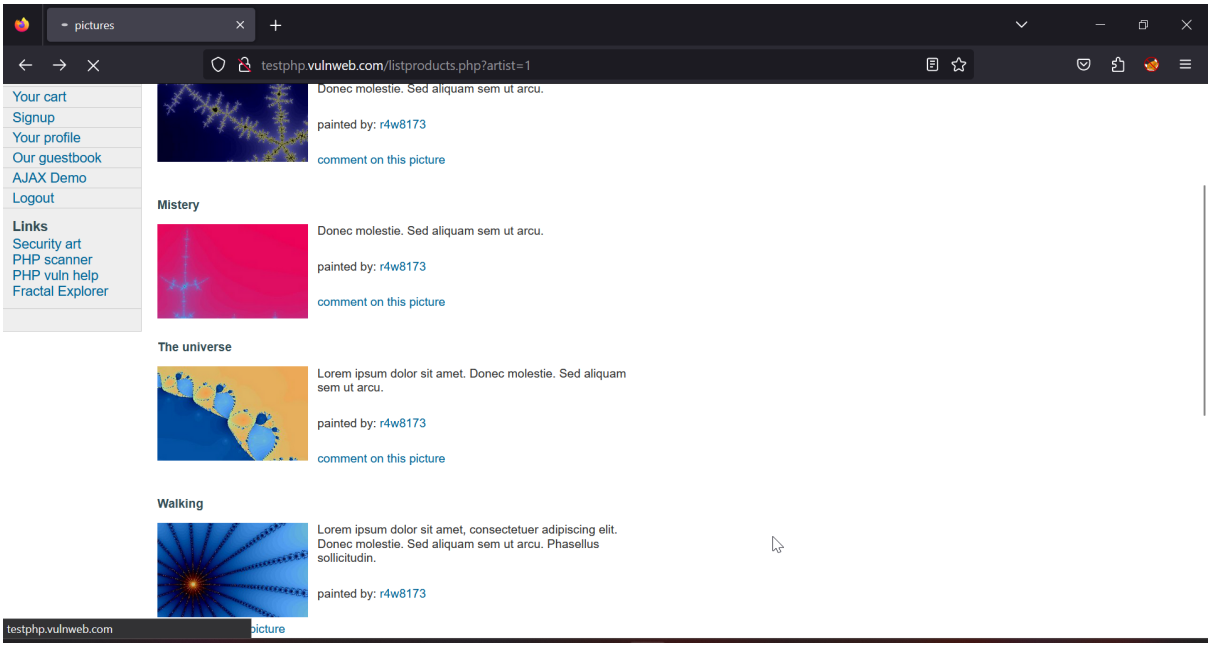
A continuación, es posible modificar tanto el precio como el ID del producto que queremos ingresar al carrito para cambiarle el precio al valor deseado. En este caso se ingresa el producto con ID=3, el cual corresponde a la pintura con título “The universe” y se le asigna el precio de 1$.



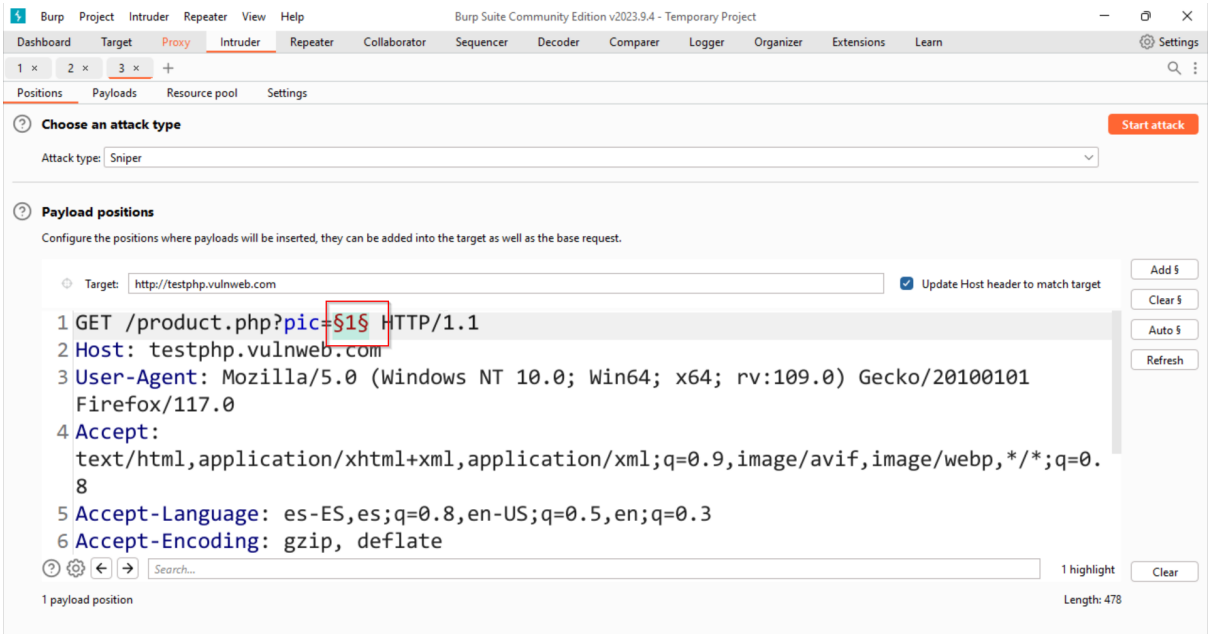
Con esto, al recargar la página del carrito, podremos observar que se ingresó el producto con el precio modificado.

Vulnerabilidad (IDOR) Cambio de Imágenes

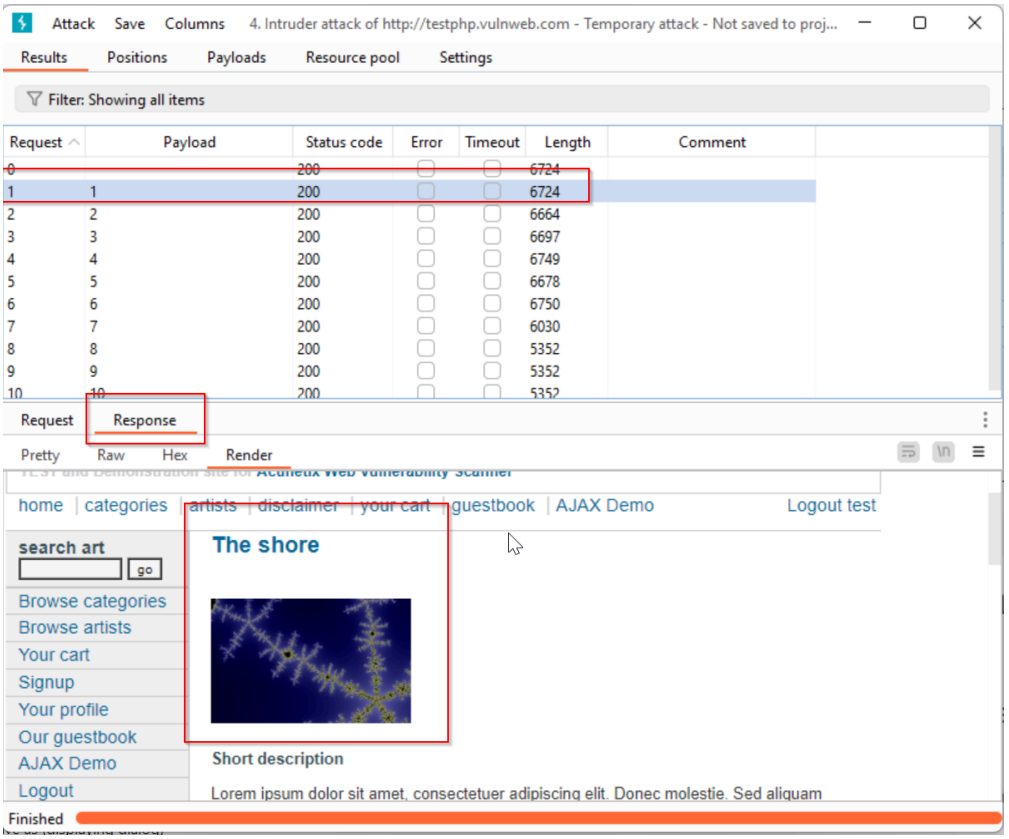
Se ingresó a la página siendo un usuario y al visitar el catálogo de productos



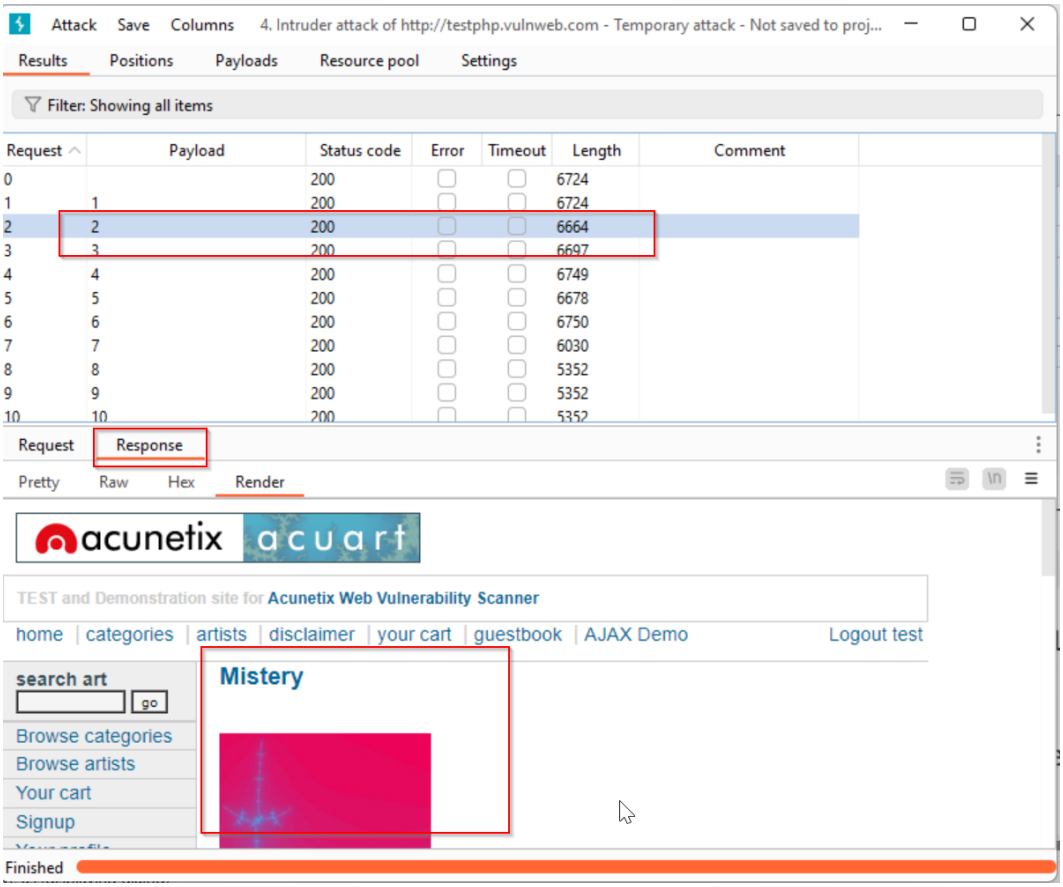
Al dar click en la imagen “The universe” nos redirige a otra página que nos desplegaba la imagen con una descripción. Al interceptar dicha petición se noto que se puede realizar un ataque tipo IDOR ya que se puede cambiar la imagen como se muestra en los pasos siguientes:



Primero se manda la petición al intruder y se selecciona el valor de “id” para ser atacado.



Aquí se muestra la imagen original



Y aquí se muestra la imagen cambiada.