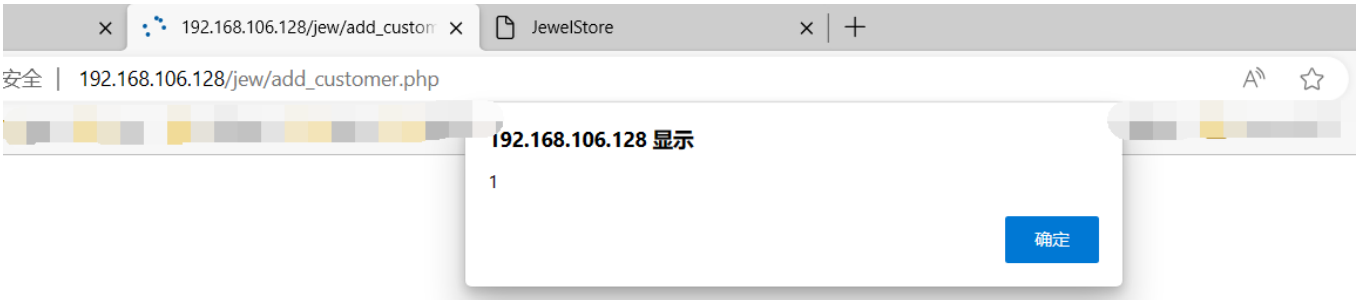
Jewelry Store System add_customer.php has Cross Site Scripting(Xss) vulnerability

Jewelry Store System add_customer.php has Cross Site Scripting(Xss) vulnerability
Attackers can execute their predefined malicious scripts in the browser, which can cause imagined harm, such as hijacking user sessions, inserting malicious content, redirecting users, using malware to hijack user browsers, propagating XSS worms, and even damaging websites, modifying router configuration information.




```php
if(isset($_POST["Cid"]) && isset($_POST["Cname"]) && isset($_POST["Caddress"]) && isset($_POST["Cphoneno"]) ){

$Cid=$_POST["Cid"];
$Cname=$_POST["Cname"];
$Caddress=$_POST["Caddress"];
$Cphoneno=$_POST["Cphoneno"];
// $Cdate=$_POST["Cdate"];

echo $Cid ;
echo $Cname;
echo $Caddress;
echo $Cphoneno;
// echo $Cdate ;

// $conn=mysqli_connect('localhost','root','','jewelleryshop');

   $sql1=" SELECT Cid FROM customerdetails WHERE Cid='$Cid'";
   $result = mysqli_query( $conn, $sql1 );
   $retval1=mysqli_fetch_assoc($result);
   echo $retval1;
   if( $retval1 > 0 ){
      echo "Customer already exist";
      // header ("Location: customer.php");
   }
   else
   {
   // $sql= "INSERT INTO `customerdetails` (`Cid`, `Cname`, `Caddress`, `Cphoneno`) VALUES (' $Cid ', ' $Cname', '$Caddress', '$Cphoneno');";
  $sql2 = "INSERT INTO `customerdetails` (`Cid`, `Cname`, `Caddress`, `Cphoneno`) VALUES ('$Cid', '$Cname', '$Caddress', '$Cphoneno')";
   $retval = mysqli_query( $conn, $sql2 );

   if(! $retval) {
      die('Could not enter data');
   }
   else {
```

```php
if(!$conn ) {
      die('Could not connect');
   }
   // $sql1=" SELECT  Cid,Cname,Caddress,Cphoneno FROM customerdetails WHERE Cid='12' ";
   $result = mysqli_query( $conn, " SELECT  Cid,Cname,Caddress,Cphoneno FROM customerdetails WHERE Cid='$Custid' ");
  if(!$result)
  {
    echo("Failed");
  }
   $retval1=mysqli_fetch_assoc($result);
   if( $retval1 < 1){
    echo "No item found ";
   }
  else{
     $Cid=$retval1['Cid'];
    $Cname=$retval1['Cname'];
    $Caddress=$retval1['Caddress'];
    $Cphoneno=$retval1['Cphoneno'];
    // $Cdate=$retval1['Cdate'];
  }
mysqli_close($conn);

}
```