

main

...

E-Commerce-Website / E-Commerce Website-xss.md



BigTiger2020 Update E-Commerce Website-xss.md

History

1 contributor

17 lines (9 sloc) 675 Bytes

...

- Exploit Title: E-Commerce Website 1.0 - Stored XSS
- Vendor Homepage: <https://www.sourcecodester.com/php/11024/ecommerce-fully-functioned-online-shopping-site.html>
- Software Link: <https://www.sourcecodester.com/download-code?nid=11024&title=eCommerce+Website+using+PHP%2FMySQLi+with+Source+Code+>
- Version: 1.0
- Vulnerable file: feedback\_process.php

```
<?php
include('config.php');

$sql="INSERT INTO contact (Name, Email, Phone, Subject)
VALUES ('$_POST[name]', '$_POST[email]', '$_POST[phone]', '$_POST[text]');

if (!mysqli_query($mysqli,$sql))
{
    die('Error: ' . mysqli_error($mysqli));
}
header("location: index.php");
echo "1 record added";

mysqli_close($mysqli);
?>
```

- Stored XSS

192.168.100.242/somstore/Admin/index.php

om  
tore.com  
Best Quality Best Merchandise

HOMEADD WAREHOUSEADD PRODUCTADD EMPLOYEECATEGORIES

ADMINISTRATION

STORE DATABASE BACKUP:

Backup Database

REPORTS:

Order ReportEmployee ReportCustomer ReportProduct Report

ADMINISTRATOR:

Add EmployeeAdd ProductAdd WarehouseAdd Category

ORDERS:

Order DetailCustomer Detail

ADMIN


Logout

Welcome To "SomStore" Admin Panel As: **Janan**

STATS



1

确定



TOTAL  
1,87  
2,11  
VIEW

Commands and Complain

| Check                    | ID | Name               | Email                     | TelliePhone   | Comment   |
|--------------------------|----|--------------------|---------------------------|---------------|---|
| <input type="checkbox"/> | 7  | A.rahman Osman     | Mucaad33@gmail.com        | 252634188000  | i like this Shopping site   |
| <input type="checkbox"/> | 8  | Abdrahman Ali Abdi | jananalibritish@gmail.com | 0252634138440 | What a nice shopping  |
| <input type="checkbox"/> | 9  | 123                | 123@qq.com                | 123           |  |
| <input type="checkbox"/> | 10 | adas               | 123@qq.com                | 123           |  |