New issue

Jump to bottom

SQL Injection Vulnerability on "order_by" parameter in Rukovoditel-3.2.1 #2

Open **Kubozz** opened this issue on Oct 15 · 0 comments

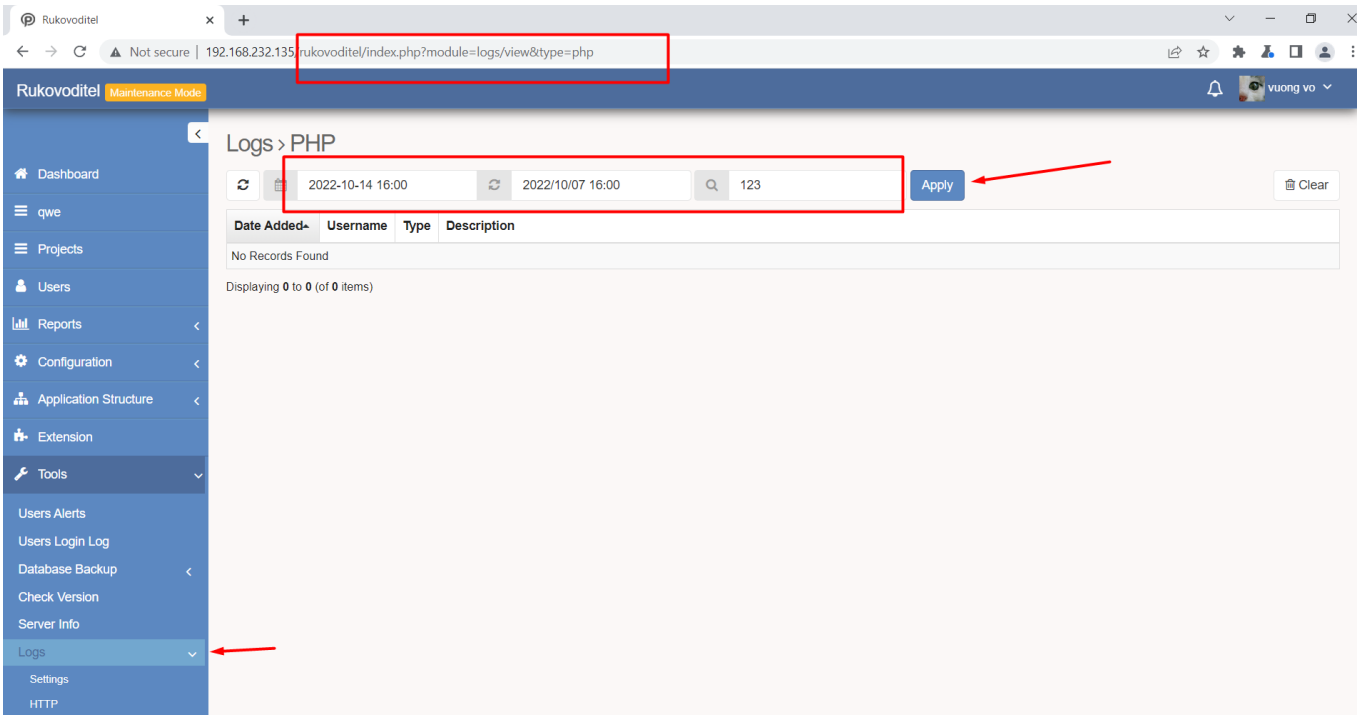
Kubozz commented on Oct 15 • edited Owner

Description:
I download Rukovoditel-3.2.1 from https://www.rukovoditel.net/download.php
The SQL Injection vulnerability can be exploited by injecting inside the field **order_by** parameter to generate error and get the query output.

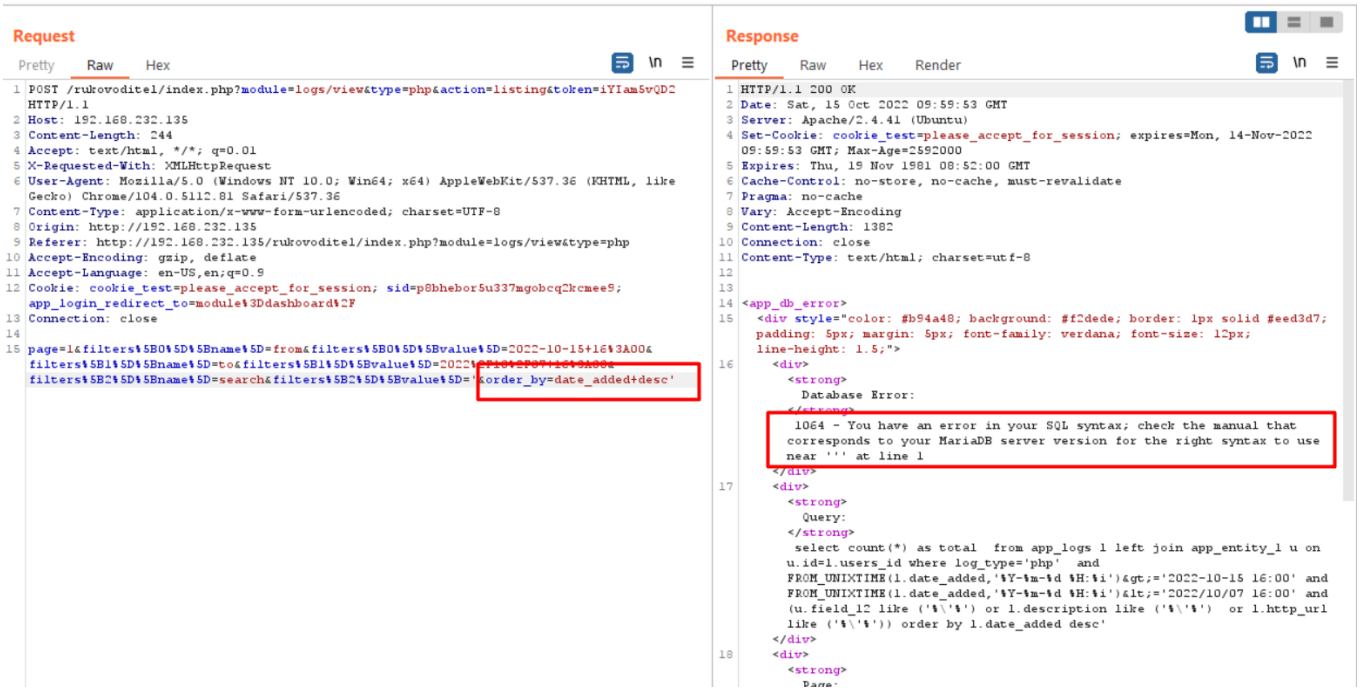
PoC:

1. Login account
2. Go to 'rukovoditel/index.php?module=logs/view&type=php'
3. Apply search query
4. Insert SQLi payload and I get presented with an error message dumping the output of SQL query

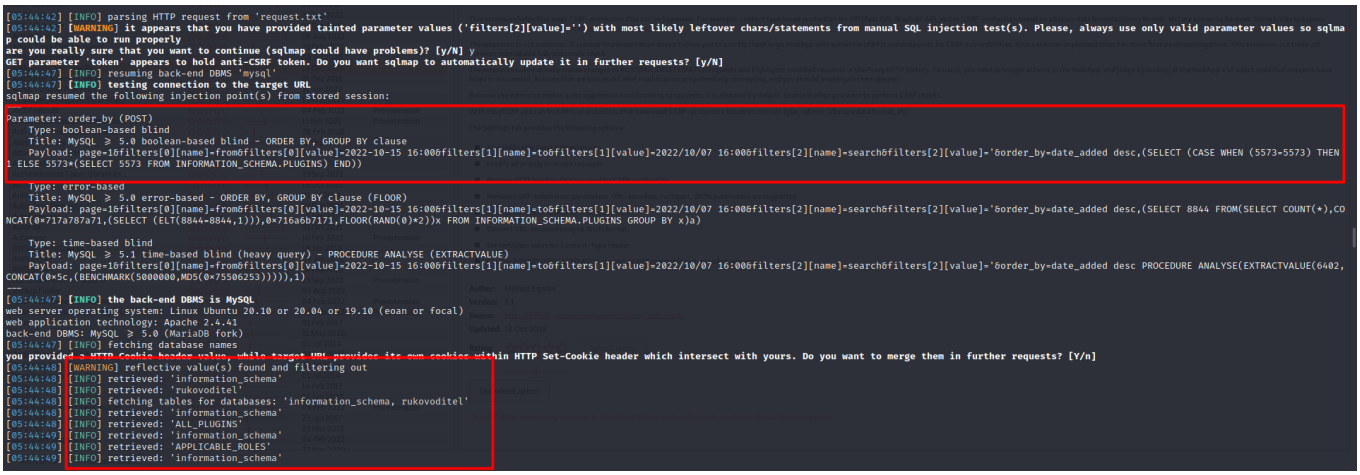
Screenshot:

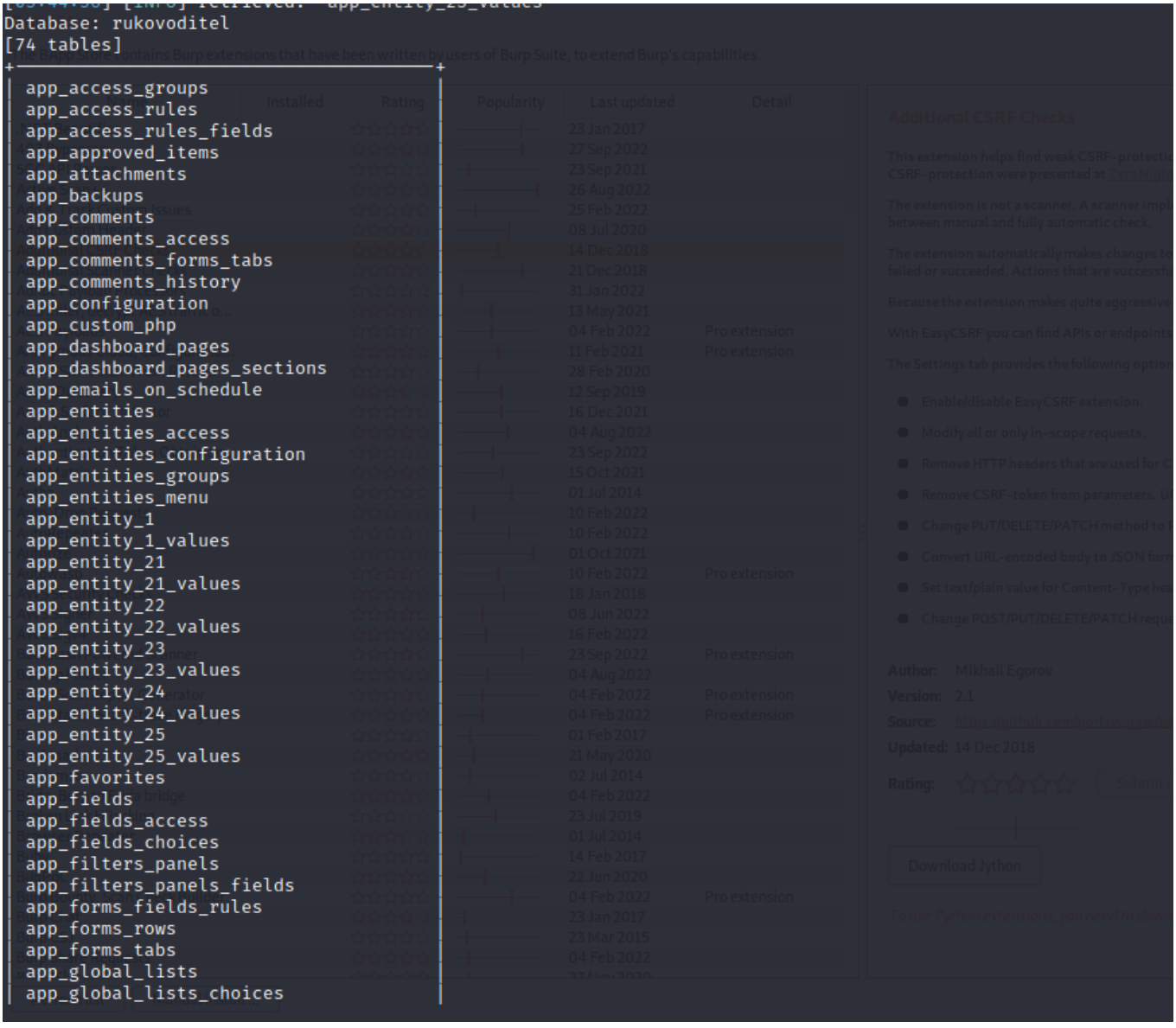


Request and response:



Retrieve the Database Tables:





Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant