Responsible Disclosure Report

Author: Krauter Riccardo || p4w || paw

Date: 7/07/2019

Affected software: Advanced Contact form 7 DB

email: 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:

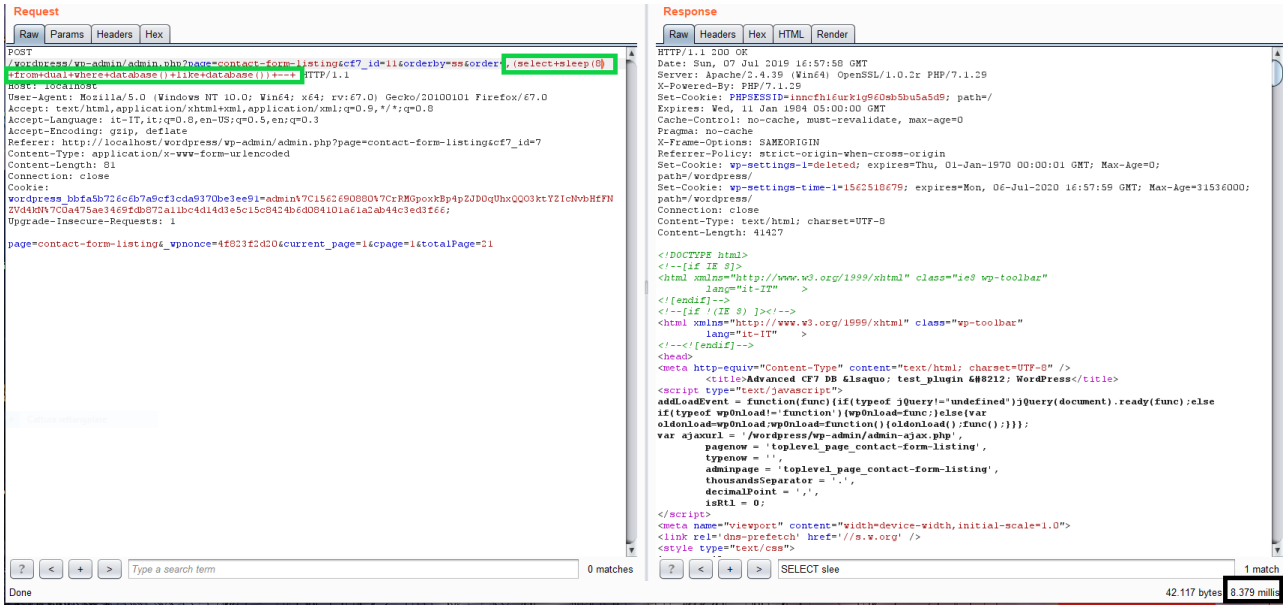

Figure 1 sqli poc payload

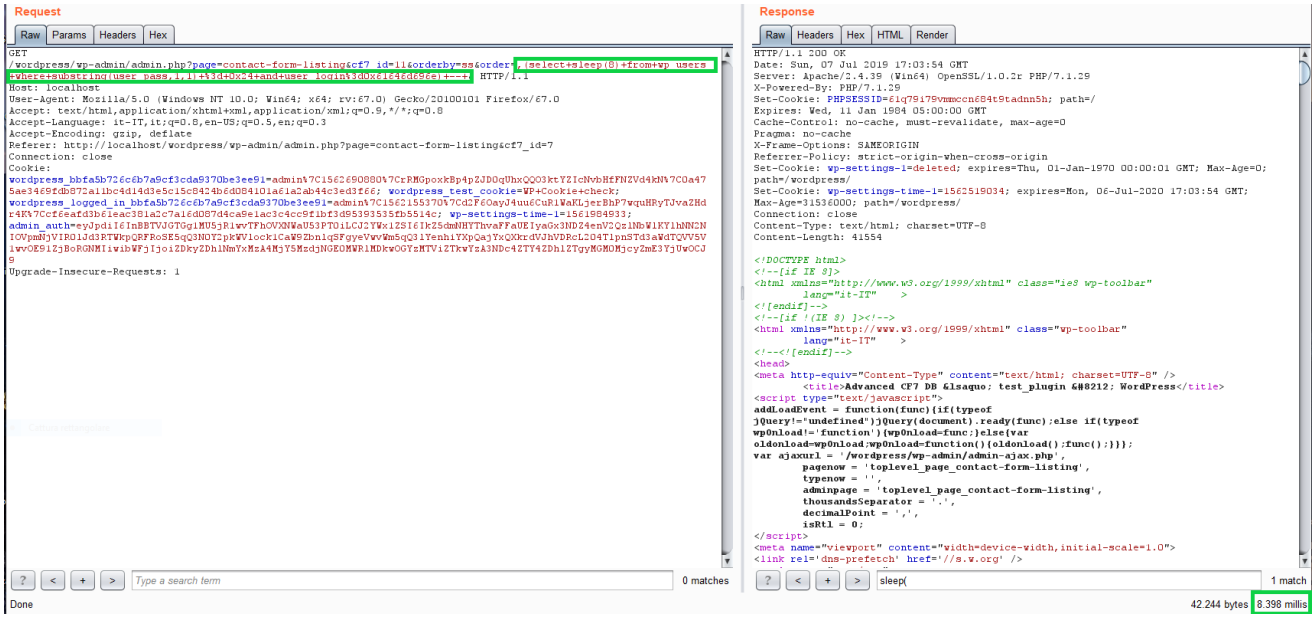

Figure 2 sqli extracting admin password

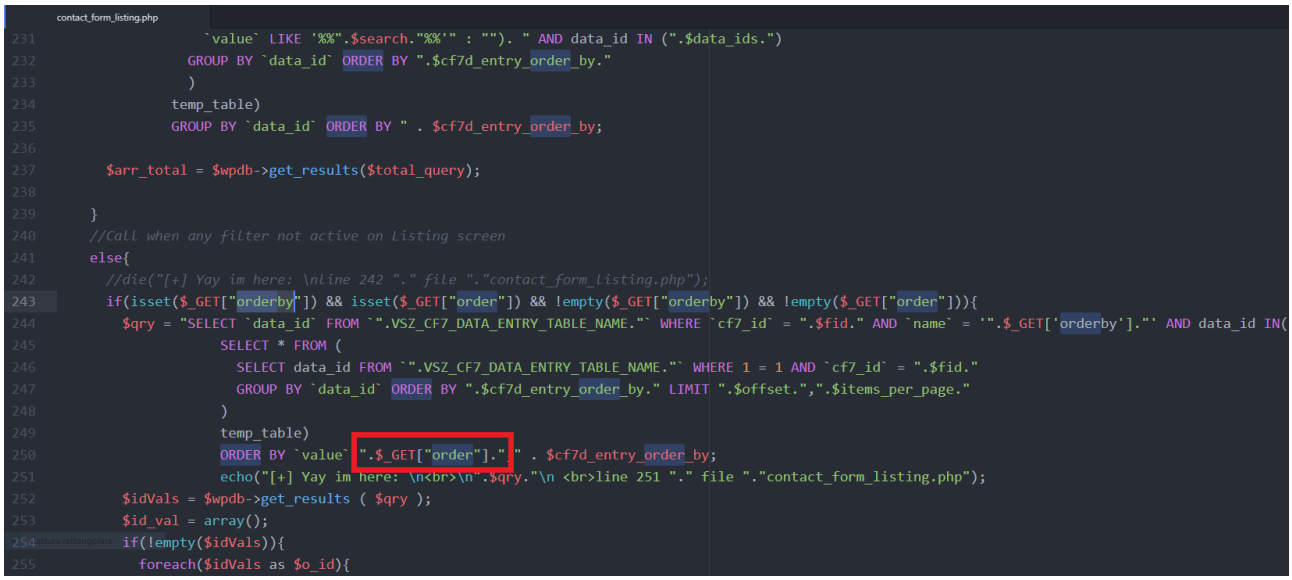

Figure 3 vulnerable code POC

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