# WB 2.11.0 - Security #39

## SQL injection vulnerabilities [reported by Marek Alaksa from citadelo]

2017-03-24 16:58 - admin

| | | | |
|---|---|---|---|
| **Status:** | Erledigt | **Start date:** | 2017-03-24 |
| **Priority:** | Sofort | **Due date:** | |
| **Assignee:** | Darkviper | **% Done:** | 100% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Operating System:** | Linux | | |

**Description**

Overview
WebsiteBaker 2.10.0 and lower versions are vulnerable to SQL injection vulnerabilities.
Details
It is possible for an unauthenticated user to inject SQL code into the variables "username" and "display_name" in the "account/signup.php" PHP script (signup form). The vulnerability exists due to insufficient filtration of user-supplied data. By exploiting this vulnerability, an attacker gains access to all records stored in the database with the privileges of the WebsiteBaker database user (e.g. administrator password MD5 hash).

http://www.citadelo.com/

### History

**#1 - 2017-03-24 17:00 - admin**

*- Status changed from Neu to Erledigt*