

**# Description:** Subrion CMS v4.2.1 allows XSS via the panel/phrases/

**# Affected Version:** Subrion CMS v 4.2.1

**# About Subrion:** Subrion is a Content Management System (CMS) which allows you to build websites for any purpose. Yes, from blog to corporate mega portal. It is a powerful web application which requires a server with PHP / MySQL to run. Subrion is a free and open source software distributed under the GPL v3.

**# Type of Vulnerability:** Stored XSS

**# Discovered By:** Nitin Goplani

**# CVE ID:** 2019-7356

**Vulnerability Description:** Cross site scripting, better known as XSS, occur whenever an application takes data that originated from a user and sends it to a web browser without first validating or encoding that content.

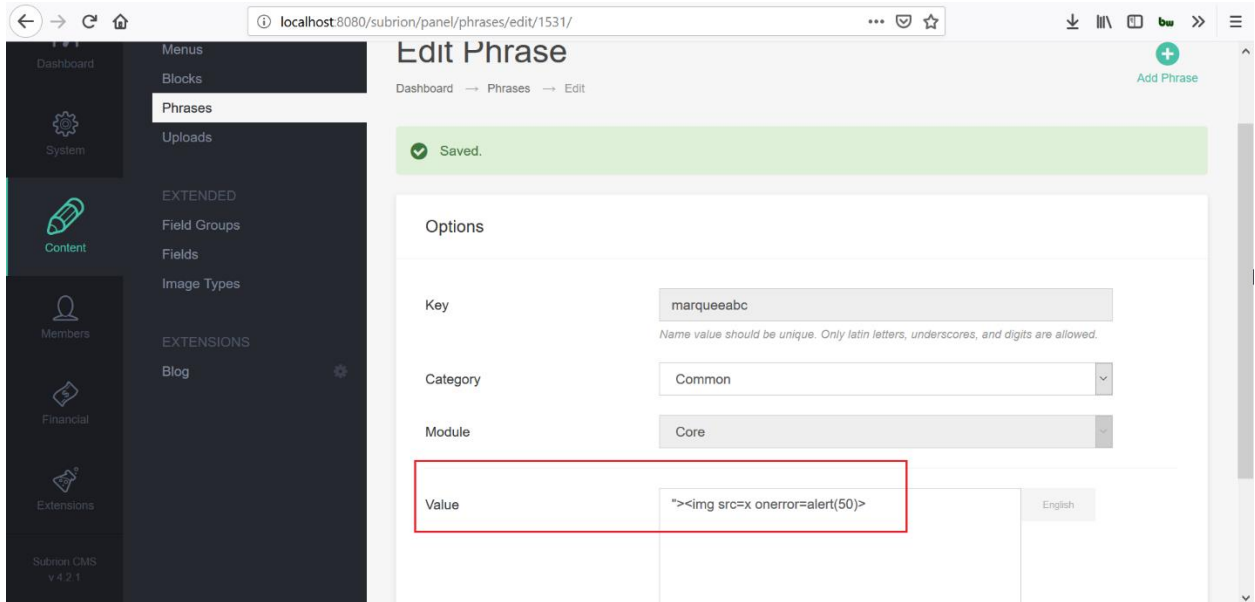
**Severity:** Medium

**Vector:** CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

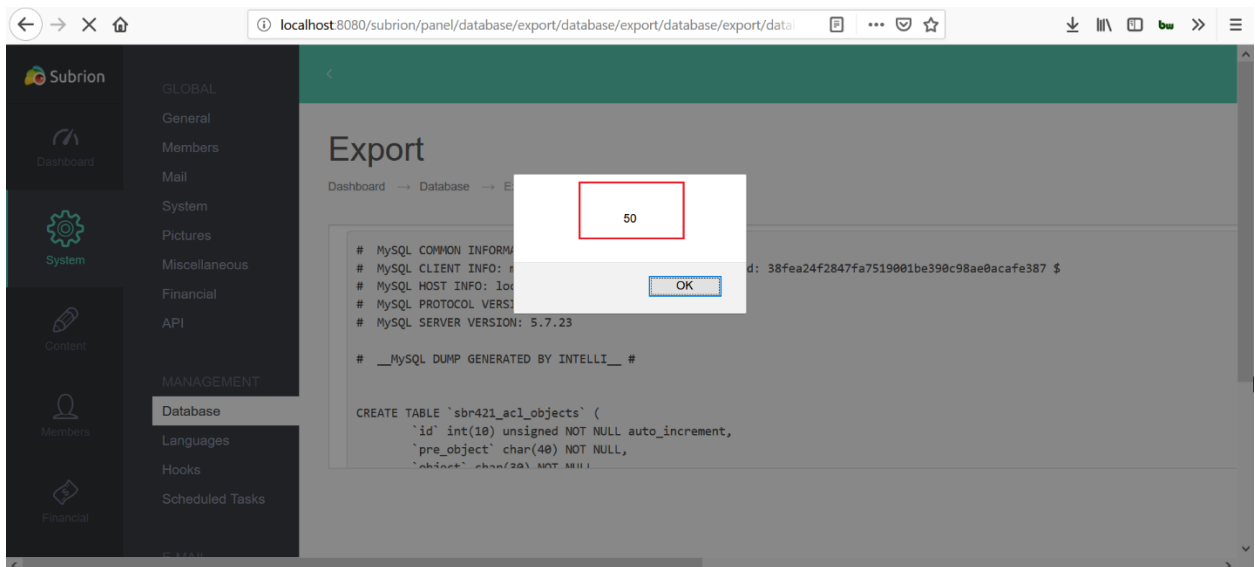
**Vulnerable URL:** http://<your server>/subrion/panel/database/export/

**Steps to Reproduce:**

- 1- Log into the Subrion CMS
- 2- Now go to panel/phrases/
- 3- Click on Add Phrase
- 4- Inject the script "><img src=x onerror=alert(7)>" under the value [Value Parameter is Vulnerable]



5- Now go to System/Database/Export and observe the script executed successfully



**Fix:** Download the latest version of Subrion