VULNERABLE: SQL injection vulnerability exists in Victor Cms. An attacker can inject query in "admin/users.php?source=add_user" via the 'user_name, user_firstname, user_lastname, user_email' parameters.

Date: 01/21/2022

Author: KienNT

Contact:

Github: https://github.com/Nguyen-Trung-Kien

Gmail: nguyentrungkien.31120@gmail.com

Facebook: https://www.facebook.com/anhchangmutrang.auz1/

Twitter: https://twitter.com/kienan1100

Product: Victor Cms Version: 1.0

Description: The vulnerability is present in the "admin/users.php?source=add_user", and can be exploited throuth a POST request via the 'user_name, user_firstname, user_lastname, user_email' parameters.

Impact: Allow attacker inject query and access, disclosure of all data on the system.

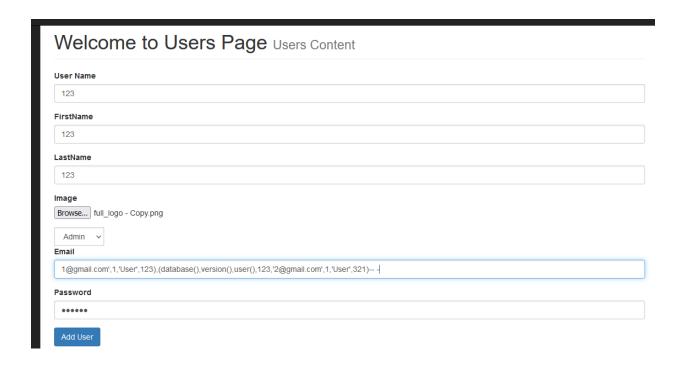
Suggestions: User input should be filter, Escaping and Parameterized Queries.

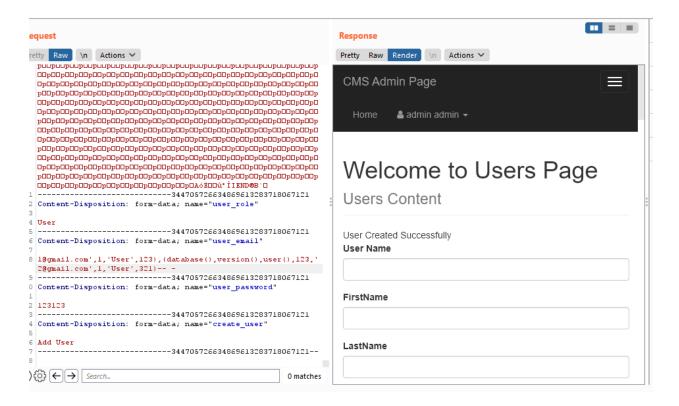
Payload:

1@gmail.com',1,'User',123),(database(),version(),user(),123,'2@gmail.com',1,'User',321)

Affect file: admin\includes\admin_add_user.php

POC





Result:

16	php_cms	10.4.21- MariaDB	root@localhost	2@gmail.com	123	user Im

Sqli success