

VULNERABLE: SQL injection vulnerability exists in Victor Cms. An attacker can inject query in `"/admin/categories.php"` via the `'cat_title'` parameters.

Date: 21/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ Github: <https://github.com/truonghuuphuc>

+ Facebook: <https://www.facebook.com/DdosFulzac.auz1/>

+ Email: phuctruong2k@gmail.com

Product: Victor Cms Version: 1.0

Description: The vulnerability is present in the `"/admin/categories.php"`, and can be exploited through a POST request via the `'cat_title'` parameters.

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

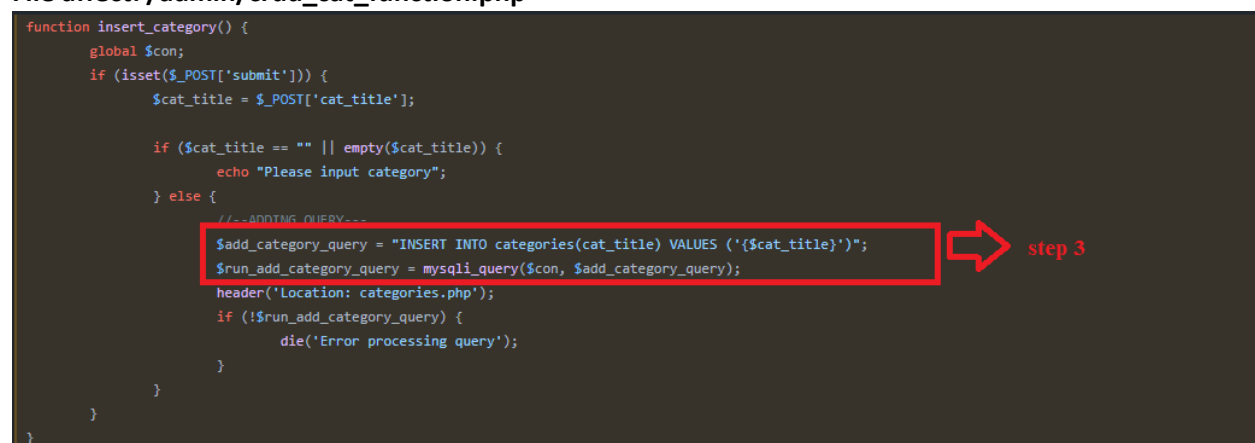
Suggestions: User input should be filter, Escaping and Parameterized Queries.

Payload exploit: `'),(query))-- -`

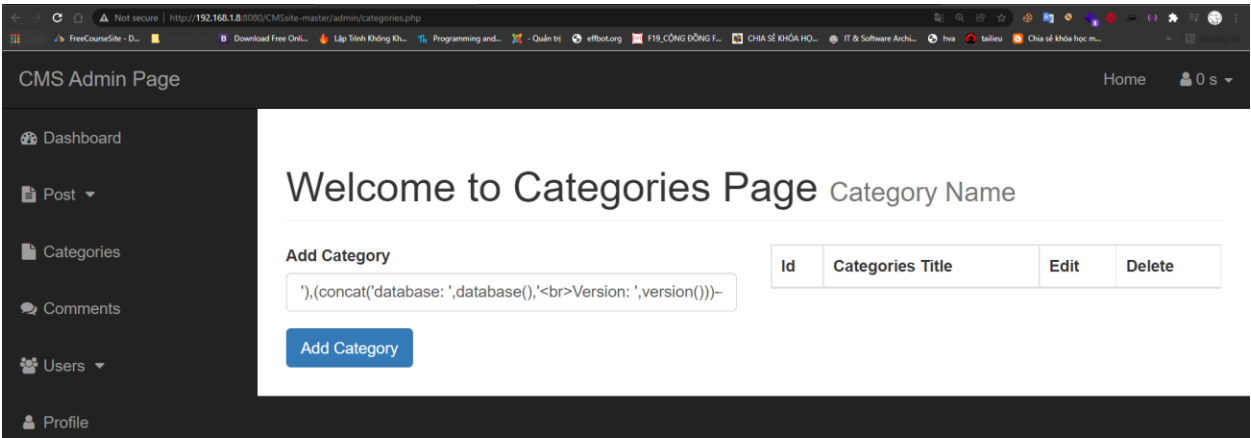
File affect: `/admin/categories.php`



File affect: `/admin/crud_cat_function.php`



Proof of concept (POC):
+ Injection query:



+ Injection query success

