VULNERABLE: SQL injection vulnerability exists in Victor Cms. An attacker can inject query in

"admin/posts.php?source=add_post" via the 'post_title' 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/posts.php?source=add_post", and can be exploited throuth a POST request via the 'post_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: 123',1,2,3,4,5,6),(1,database(),3,4,5,6,7,8)---

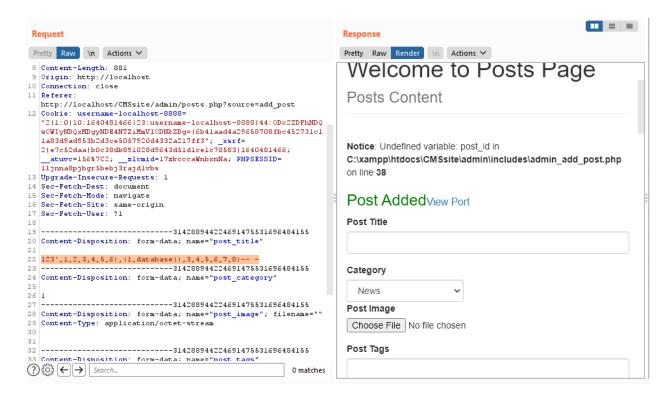
Affect file: admin\includes\admin_add_post.php

```
//</r>
//>
//------QUERY TO INSERT DATA INTO POST TABLE------
$post_query = "INSERT INTO posts(post_category_id,";
$post_query = "post_title,post_author.post_date,";
$post_query = "post_image,post_catent.post_tone,";
$post_query = "post_image,post_content,post_tone,";
$post_query = "post_istatus)";
$post_query = "Values('($post_category_id)','($post_title}','($post_author)',now(),'($post_image}','($post_content}','($post_tags}','($post_status)')";
$create_post_query = mysqli_query($con, $post_query);
echo "ch3 style='color:green;'>Post Added<small><a href=" ./post.php?post={$post_id}'>View Port</a></a></a>//small></a></a>
if (|$create_post_query) {
| die("Error in calling query" . mysqli_error($con));
}
}
```

POC

Welcome to Posts Page Posts Content





Result:



SQLinjection success