SQL Injection in category.php form #14

Open ztxyzwd opened this issue on Jul 7, 2020 · 2 comments

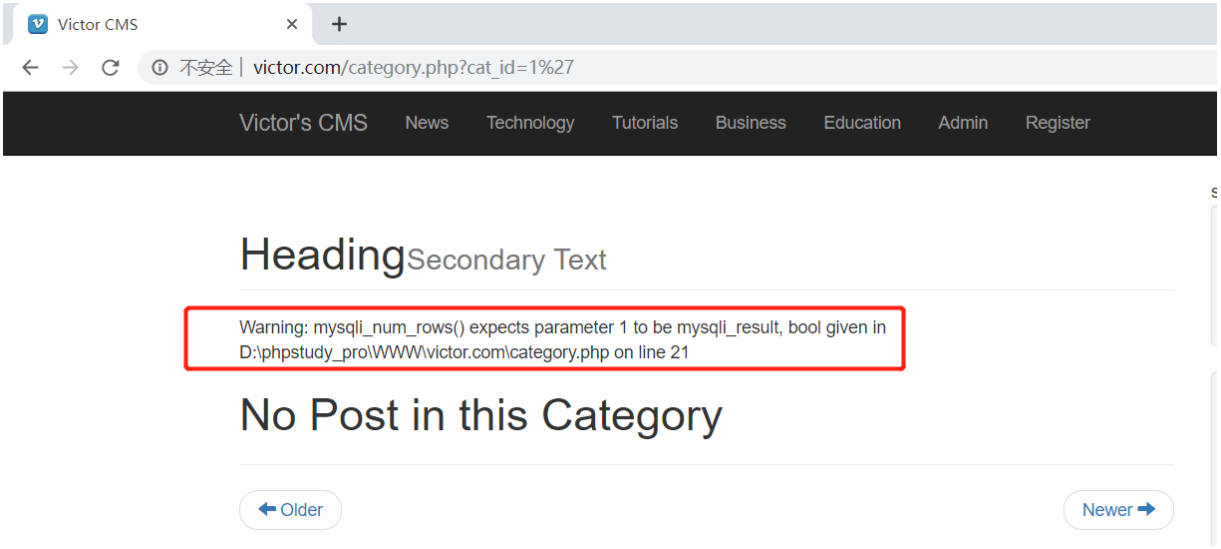
ztxyzwd commented on Jul 7, 2020 • edited

Hello, I found that there is a sql injection vulnerability in the cat_id parameter of the category.php file on the website. Entering single quotes in this parameter will cause the webpage to burst and the database statement to burst. And this parameter can be used by sqlmap to obtain data information in the database.

index.php | .htaccess | category.php | post.php | search.php | favicon.ico | index.php | Loca

```php
<!-- @author 'Victor Alagwu';
//   @project 'Simple Content Management System';
//   @date    '0ctober 2016'; -->
<?php include 'includes/header.php';?>
        <!-- Navigation Bar -->
    <?php include 'includes/navbar.php';?>
        <!-- Navigation Bar -->

    <div class="container">
        <div class="row">
            <!-- Page Content -->
            <div class="col-md-8">
            <h1 class="page-header">Heading<small>Secondary Text</small></h1>
            <?php
if (isset($_GET['cat_id'])) {
    $category = $_GET['cat_id'];
}
mysqli_real_escape_string($con,$category);
$query = "SELECT * FROM posts WHERE post_category_id=$category"
$run_query = mysqli_query($con, $query);
$count = mysqli_num_rows($run_query);
if ($count == 0) {
    echo "<h1>No Post in this Category</h1>";
} else {
    while ($row = mysqli_fetch_assoc($run_query)) {
        $post_title = $row['post_title'];
        $post_id = $row['post_id'];
        $post_category_id = $row['post_category_id'];
        $post_author = $row['post_author'];
        $post_date = $row['post_date'];
```



POC:

```
GET /category.php?cat_id=1%27 HTTP/1.1
Host: victor.com
Cache-Control: max-age=0
```

Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,/;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=ia9ksoo6lq6dticsuoddv0gh20
Connection: close

VictorAlagwu commented on Jul 7, 2020 • edited ▾ Owner

Hello **@ztxyzwd**, This is a project I worked on a few years back while learning PHP, so it's prone to have a lot of bugs, regardless of that if there is a fix or rather a PR that fix those issues, I would be glad to merge it.

ztxyzwd commented on Jul 7, 2020 • edited ▾ Author

Thank you. I will update the bugs found in the code in ISSUES.

👍 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants