New issue

Jump to bottom

There are a SQL inject at \admin\newpost.php #1

Open **wenfeiniubi** opened this issue on Aug 29, 2019 · 0 comments

wenfeiniubi commented on Aug 29, 2019

SQL inject start at line 6, `$_POST['title']` filtered by modify function `cleanTitle()` ,but the problem is : filter rules are too simple(cleanTitle function at CONF_mysql.php line51):

```
function cleanTitle($str) { $str = cleanUser($str); $str = strtolower(str_replace(' ', '-', $str)); return $str; }
```

you can see it's just replace space to '-' ,it's simple to bypass this filter with change space to comment

here is sql inject position code:

```
$title = $_POST['title']; $safe_title = cleanTitle($_POST['title']); mysql_query("INSERT INTO newpk (title, safe-title , author, date, text, open) VALUES ('$title', '$safe_title', '$user', '$newdate', '$text', '$open')") or die("Query failed with error: ".mysql_error()); mysql_query("UPDATE newpk_users SET posts=posts+1 WHERE name='" . getUser() . "'"); $comments = mysql_query("SELECT * FROM newpk WHERE title='$title'"); $row = mysql_fetch_array($comments);
```

fix advice:
add more filter rules
or use `addslashes()` to protect your variable

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant