New issue

Jump to bottom

# [11.x, user manager] SQL injection #1410

Closed **plegall** opened this issue on May 13, 2021 · 0 comments

Assignees

Labels   Section: Security   Type: Bug

Milestone   11.5.0

**plegall** commented on May 13, 2021   Member

As reported by Harry Goodman from NCC Group:

> The 'order[0][dir]' parameter in admin/user_list_backend.php is vulnerable to SQL injection
>
> I believe this is because of the following pieces of code:

```
if ( $_REQUEST['columns'][$col]["searchable"] == "true" )
{
  $sOrder .= $aColumns[ $col ].' '.$_REQUEST["order"][0]["dir"].', ';
}
```

> I would suggest either using the check_inputs function that your application seems to rely on, or depending on how much functionality is needed, just do a check to ensure the parameter is either ASC or DESC.
>
> CVE-2021-32615

👍 2

**plegall** added Type: Bug Section: Security labels on May 13, 2021

**plegall** added this to the **11.5.0** milestone on May 13, 2021

**plegall** self-assigned this on May 13, 2021

**plegall** added a commit that referenced this issue on May 13, 2021

`fixes #1410 check on user input to prevent SQL injection`   2ce1e59

**plegall** closed this as completed on May 13, 2021

Assignees

plegall

Labels

Section: Security   Type: Bug

Projects

None yet

Milestone

11.5.0

Development

No branches or pull requests

1 participant