SQL injection

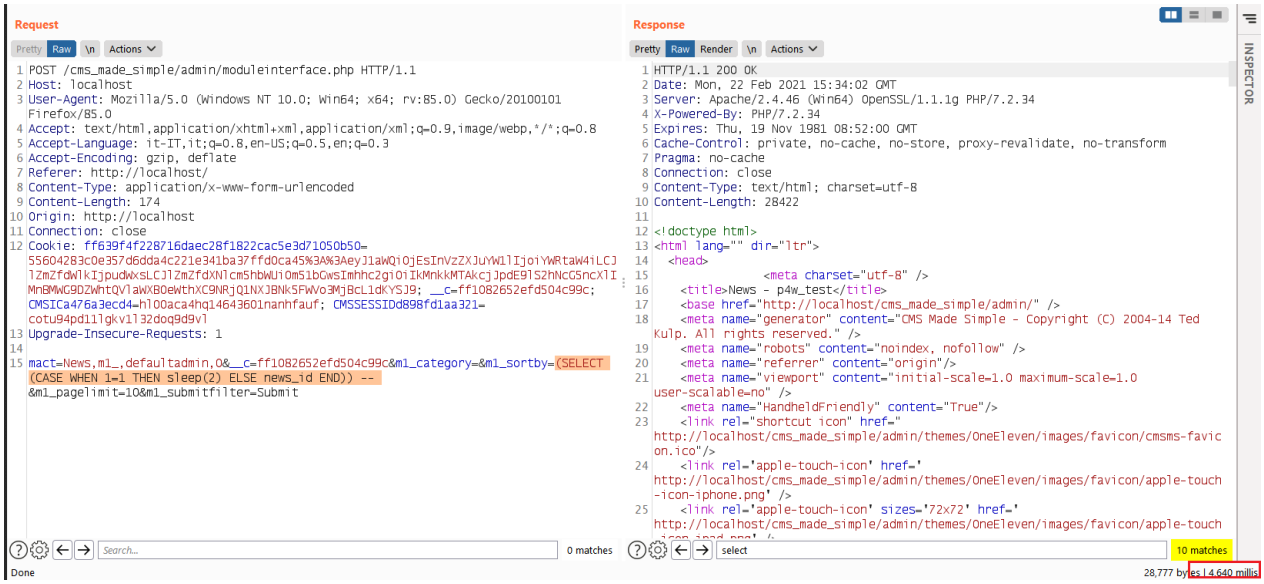
Author: Riccardo Krauter @ Soter IT Security

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_pagenumber']);
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_ne
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



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)) --`