New issue

Jump to bottom

SQL Injection Vulerable. #259

Open T3qui1a opened this issue on Oct 31, 2019 · 0 comments

T3qui1a commented on Oct 31, 2019

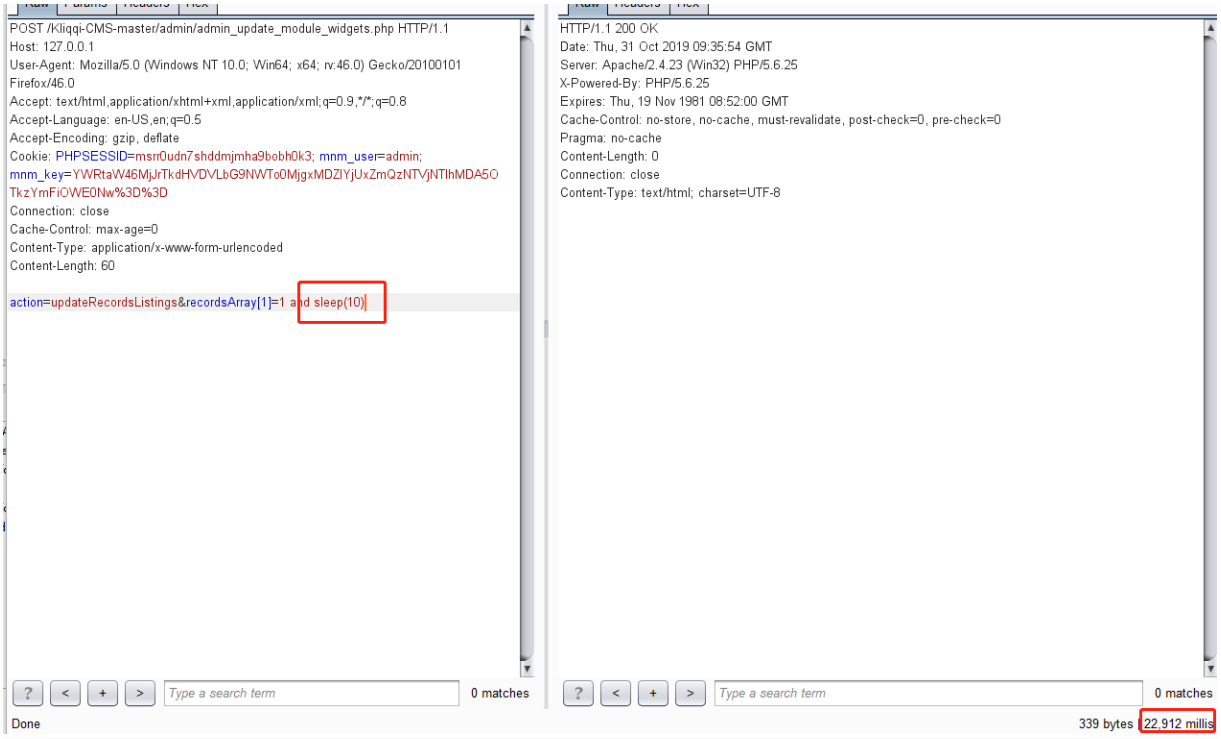
This is a SQL Injection vulerable in "admin_update_module_widgets.php" file.

At line 47, "$recordIDValue" Parameters are not wrapped in single quotes. And the parameters also are not safely processed.

```
if($canIhaveAccess == 1){
    $action                 = mysql_real_escape_string($_POST['action']);
    $updateRecordsArray     = $_POST['recordsArray'];
    if ($action == "updateRecordsListings"){
        $listingCounter = 1;
        foreach ($updateRecordsArray as $recordIDValue) {
            $query = "UPDATE " .table_modules. " SET weight = " . $listingCounter . " WHERE id = " . $recordIDValue;
            mysql_query($query) or die('Error, insert query failed');
            $listingCounter = $listingCounter + 1;
        }
    }

}
```

When you have installed modules. There is a time-based sql injection.(If the tables didn't exists datas, time-based didn't work)



Go Cancel

Target: http://127.0.0.1

Request

Raw Params Headers Hex

```
POST /Kliqqi-CMS-master/admin/admin_update_module_widgets.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:46.0) Gecko/20100101
Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=msrr0udn7shddmjmha9bobh0k3; mnm_user=admin;
mnm_key=YWRtaW46MjJrTkdHVDVLbG9NWTo0MjgxMDZlYjUxZmQzNTVjNTlhMDA5O
TkzYmFiOWE0Nw%3D%3D
Connection: close
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 46

action=updateRecordsListings&recordsArray[1]=1
```

Type a search term 0 matches

Response

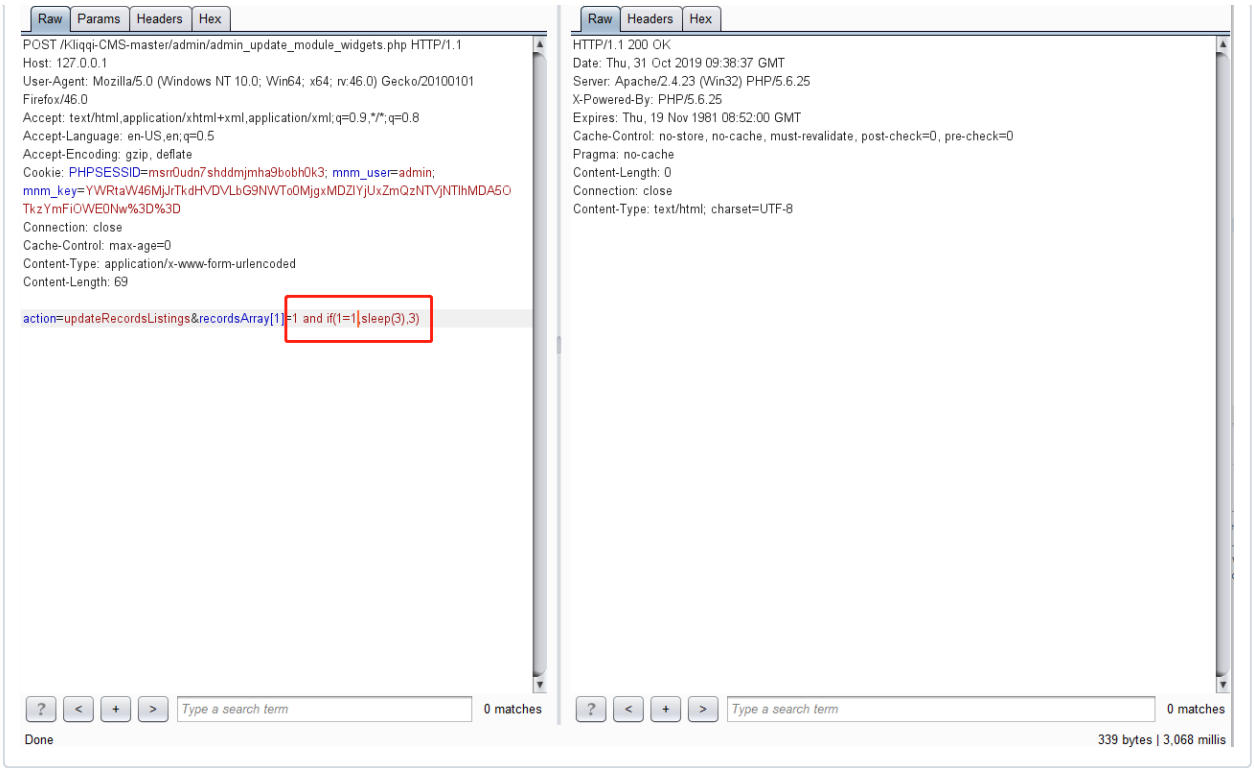
Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Thu, 31 Oct 2019 09:37:32 GMT
Server: Apache/2.4.23 (Win32) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

Type a search term 0 matches

Done

339 bytes | 48 millis



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant