

延迟注入定义

延迟注入，是一种盲注的手法，提交对执行时间敏感的函数sql语句，通过执行时间的长短来判断是否执行成功，比如：正确的话会导致时间很长，错误的话会导致执行时间很短，这就是所谓的高级盲注。SQLMAP、穿山甲、胡萝卜等主流注入工具可能检测不出，只能手工检测，利用脚本程序跑出结果

sleep() //延迟函数

if(condition,true,false) //条件语句

ascii() //转换成ascii码

substring("string",start,length) //mid()也一样，取出字符串里的第几位开始，长度多少的字符

If表达式：IF(expr1,expr2,expr3)

如果 expr1 是TRUE (expr1 <> 0 and expr1 <> NULL)，则 IF()的返回值为expr2；否则返回值则为 expr3

Mid函数：MID(column_name,start[,length])

column_name	必需。要提取字符的字段。
start	必需。规定开始位置（起始值是 1）。
length	可选。要返回的字符数。如果省略，则 MID() 函数返回剩余文本。

延时注入的原理就是，所要爆的信息的ascii码正确时，产生延时，否则不延时

练习页面

🔍 PTE 漏洞练习平台 hack-hack-

🏠 系统介绍

🔒 暴力破解

🔗 Cross-Site Scripting

🔄 CSRF

➡️ SQL-Inject

概述

数字型注入(post)

字符型注入(get)

搜索型注入

xx型注入

"insert/update"注入

"delete"注入

"http header"注入

盲注(base on boolian)

盲注(base on time)

宽字节注入

🏠 sqlmap > 基于时间的盲注

what's your username?

查询

i don't care who you are!

输入: `kobe' and if((length(database()) > '1'), sleep(5), null)#`
结果: 页面5秒后才有返回信息, 说明sleep函数执行了。

依次尝试获得数据库名称长度

`kobe' and if((length(database()) > '1'), sleep(5), null)#`
数据库长度为7

变换语句 :

`kobe' and if((substr(database(), 1, 1))>'a', sleep(5), null)#`
依次尝试, 获得数据库名称为 pikachu

后面方法和11.盲注一致

获得数据库 pikachu的一个数据表的长度 num

获得数据库 pikachu的一个数据表的名称为 xx

获得数据库 pikachu 的一个数据表xx的长度第一列的长度

获得数据库 pikachu 的一个数据表xx的第一列的名称为yy

获得数据库 pikachu 的一个数据表xx度第一列的名称为yy的第一行数据长度zz

获得数据库 pikachu 的一个数据表xx度第一列的名称为yy的第一行数据名称kk

获得数据库 pikachu 的一个数据表xx度第一列的名称为yy的第一行数据名称kk的数据长度

获得数据库 pikachu 的一个数据表xx度第一列的名称为yy的第一行数据名称kk的数据