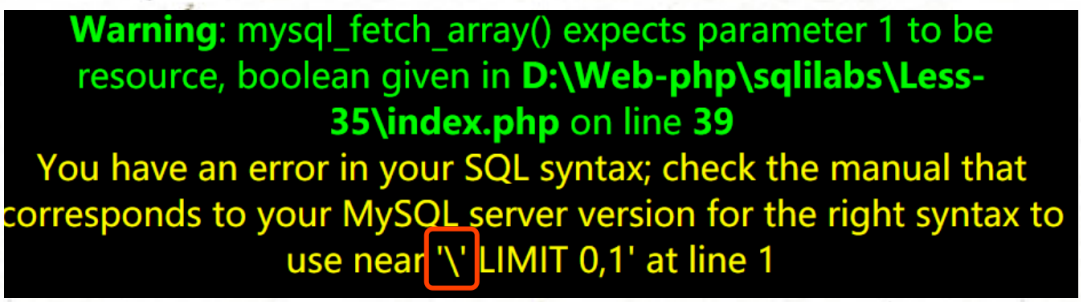
这个题虽然加了Addslashes()函数，但是id是数字型注入

```
mysql_query("SET NAMES gbk");
$sql="SELECT * FROM users WHERE id=$id LIMIT 0,1";
$result=mysqli_query($con, $sql);
$row = mysqli_fetch_array($result, MYSQLI_BOTH);
```

看了源码也证实了这一点

不看源码如何发现呢

尝试?id=1 不报错，id=1' 报错



注意这里\'都在错误中，说明'没有被使用，尝试"也没有被使用，则说明是数字型

因此直接联合查询即可

?id=-1 union select 1,version(),database()--+

而没有错误回显时，我们又应该怎么判断是数字型注入还是引号被过滤呢?

在能分辨出正确回显和错误回显（有固定字符串）时，id=1正确回显，尝试id=1'和id=1"：

- 若两者都正确回显：很可能是被过滤引号
- 若两者无正确回显：很可能是数字型查询
- 若一有一无：基本可确定是字符型查询