代码审计：

1. 存在SQL注入漏洞，$id 变量值来自 $_GET['id']，未经过任何过滤或转义就直接拼接在 SQL 语句中，攻击者可以构造恶意参数来执行任意 SQL 语句。
2. $result 变量只是一个结果集，没有对其进行是否为空的判断，如果查询的结果集为空，则 $row 变量就变成了一个空数组，不存在 'user' 和 'password' 属性，会造成程序崩溃。

修复后的代码：

```
<?php
$con=mysqli_connect("localhost","root","XFAICL1314","dvwa");
if(mysqli_connect_error())
{
die("连接失败:" .mysqli_connect_error());
}
$id=mysqli_real_escape_string($con, $_GET['id']); //对$id进行转义过滤
$result=mysqli_query($con,"select * from users where `user_id`=".$id);
if(mysqli_num_rows($result) > 0) //判断结果集是否为空
{
$row=mysqli_fetch_array($result);
echo $row['user'] . ":" . $row['password'];
echo "<br>";
}
else
{
echo "查询结果为空";
}
mysqli_close($con); //关闭数据库连接
?>
```