加密存储模型

SSL/SSH 能保护客户端和服务器端交换的数据，但 SSL/SSH 并不能保护数据库中已有的数据。SSL 只是一个加密网络数据流的协议。

如果攻击者取得了直接访问数据库的许可（绕过 web 服务器），敏感数据就可能暴露或者被滥用，除非数据库自己保护了这些信息。对数据库内的数据加密是减少这类风险的有效途径，但是只有很少的数据库提供这些加密功能。

解决这个问题最简单的方法是创建自己的加密包，然后在 PHP 脚本中使用它。PHP 可以通过一些扩展来帮助你解决这个问题，比如 [OpenSSL](https://www.php.net/manual/zh/book.openssl.php) 和 [Sodium](https://www.php.net/manual/zh/book.sodium.php)，涵盖了多种加密算法。脚本在将数据插入数据库之前对其进行加密，并在检索时对其进行解密。更多关于加密工作的例子请参见参考文献。