**PHP安全事务：**

1.不要以普通文本形式保存和传送密码

2.不要把密码保存在脚本中，使用数据库保存

3.要保护多个页面

**加密技术：**

私有密钥加密：加密消息的人和解密消息的人有同样的密钥

共有密钥加密：依赖于两个不同的密钥，一个公有一个私有。任何有公有密钥人都可以发送一个秘密消息，但只有拥有密钥的人才可以解密

数字签名：一个数字证书可以将一个公有密钥与一个个人或者组织的细节以签名的数字格式结合起来

能够验证一条消息没有被篡改以及一组消息都是来自一个特定的用户或机器（防止否认）

**数据保存的地方：**

1. 数据库
2. 服务器（文件）
3. 用户的机器（cookies）

**密码的加密：**

PHP的sha1()函数和MySQl的SHA1()函数： 提供一个功能强的单向加密哈希函数，无法解密，他的输出是确定的，假设输入相同的字符串，sha1（）函数每次运行的结果是一样的。返回固定大小的数据，40个字符的字符串。

**保护多个页面：**

原因：HTTP是无状态的，对来自同一个人的连续请求不能识别

解决办法:

1. 添加在网页的每个超链接中（不安全，可以被浏览）
2. HTTP基本身份验证：

HTTP内置有身份验证功能，尽管Web服务器对每个用户的请求都要求新的身份验证详细信息，但Web浏览器不必在每页中都要求用户输入详细的信息，通常，浏览器可以保存这些详细信息，只要用户打开一个浏览器窗口，它就自动的将这些所需的详细信息重新发送到Web服务器。

使用HTTP基本身份验证时，不用自己编写HTML表单，用户浏览器负责显示对应的弹出框

加密套接字层（SSL）

实现的是Web服务器和Web浏览器之间的安全通信