



# PCI 自我评估问卷表

1.0 版本

2004 年 12 月

**VISA PAYMENT SECURITY SERVICES**  
ASIA PACIFIC



## 免责声明

本支付卡产业 (PCI) 自我评估问卷表用作“检查清单”，以保证所有储存、处理及传输 Visa 卡持卡人数据的公司符合 PCI 数据安全标准。然而，无论是否执行所推荐的本问卷，Visa 亚太公司不保证，也并未声称完成或符合本问卷就能防止安全危害或损失，并对发生的任何安全破坏或丢失，不承担任何责任或义务。

## 重要提示

此 PCI 自我评估问卷表是 Visa 亚太公司全套账户信息安全 (AIS) 文件的一部分。所有会员及其代理（商户及服务提供者）应确保其处理、储存和传输持卡人信息时，必须符合 PCI 数据安全标准（该标准取代 2000 年 3 月 Visa AIS 标准 1.4 版本）。

更多 Visa 亚太公司 AIS 详细资料，请访问 <http://www.visa-asia.com/secured>。

## 如何完成问卷表？

---

本问卷表分为六部分。基于 PCI 数据安全标准包含的要求，各部分注重特定的安全范围。任何标有“不适用”字样的问题，必须附上简单说明。

## 问卷表报告

---

自我评估问卷表和系统周界扫描结果必须包括以下内容：

### 组织信息

公司名称：

数据库管理员：

联系人姓名：

职位：

联系电话：

电子邮件：

大约每年处理的交易 / 账户数：

---

### 请简述公司的业务

支付过程中贵公司业务所处的角色？如何储存、处理和 / 或传输的持卡人数据, 以及容量大小？

---

### 列出所有第三方服务提供者

处理方：

网关：

网站主机：

购物车：

公司位置：

其他：

---

列出所使用的销售终端机(POS)软/硬件：



### 评估鉴定

完成各部分评估后，用户应填写以下鉴定框：

各部分如是下列情况时：	则该部分等级则为：
所有问题用“是”或“不适用”回答时	<b>绿色：</b> 商户或服务提供者与 PCI 数据安全标准的自我评估的部分一致。 备注：标有“不适用”字样时，应附简要说明。
任何问题用“否”回答时	<b>红色：</b> 商户或服务提供者不符合要求。如要符合，须解除风险，同时重填自我评估表，证明已符合要求。

第 1 部分	绿色 红色	第 4 部分	绿色 红色
第 2 部分	绿色 红色	第 5 部分	绿色 红色
第 3 部分	绿色 红色	第 6 部分	绿色 红色

整体级别：                      绿色      红色

## 建立和维护安全网络

### 要求一：安装和维护防火墙设置来保护数据

	说 明	回 答		
1.1	所有路由器、交换机、无线接入点以及防火墙设置是否有保护，并符合文档化的安全标准？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.2	使用无线技术时，是否仅限于通过验证设备访问网络？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
1.3	更换防火墙是否需要授权，有更换记录日志吗？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.4	是否使用防火墙保护网络并对商务往来业务设置限制？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.5	为防止虚假 IP 地址的通过，是否在所有边界路由器上安装流出和流入过滤器？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.6	支付卡账户信息是否存储到数据库，且该数据库位于内部网络（非 DMZ），并用防火墙加以保护？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.7	使用无线技术时，周界防火墙是否存在于无线网络和支付卡环境之间？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
1.8	直接连接到网络的每台移动电脑上，是否已安装个人防火墙和防病毒软件？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
1.9	是否将位于公众可到达的网络段的网络服务器与内部网络用防火墙（DMZ）隔开？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
1.10	使用网络地址转换软件，是否可将已设置的防火墙转换（隐藏的）内部 IP 地址？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	

## 建立和维护安全网络

### 要求二: 不要使用厂商提供的默认的系统密码或其他安全参数

	说 明	回 答		
2.1	系统投入生产前, 是否在生产系统过程中更换厂商默认的安全设置?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
2.2	系统投入生产前, 是否在生产系统过程中使厂商默认的账户或密码失效或更改?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
2.3	使用无线技术, 供应商默认设置是否改变(例如, WEP 密钥, SSID, 密码, SNMP 简单网络管理协议团体口令, 使服务区标志符 SSID 广播失效)?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
2.4	使用无线技术, 当 WPA 可用时, 是否使用 Wi-Fi 保护访问技术进行编码和验证?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
2.5	是否删除不需要的通过默认配置安装的程序和协议, 使所有产品系统(服务器和网络配件)变得坚强?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
2.6	是否对产品系统和应用的远程管理使用安全的加密通信?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用



## 维持防范弱点攻击的管理程序

### 要求三: 保护储存的数据

	说 明	回 答	
3.1	不再需要使用机密持卡人数据时, 是否已安全销毁?	<input type="checkbox"/> 是	<input type="checkbox"/> 否
3.2	是否禁止在数据库、日志文件或销售终端机产品中储存磁条上 (在卡片背面, 芯片等) 的任何磁轨的全部内容?	<input type="checkbox"/> 是	<input type="checkbox"/> 否
3.3	是否禁止在数据库、日志文件或销售终端机产品中储存卡片验证值 (印在卡上签名栏处的 3 位数码)?	<input type="checkbox"/> 是	<input type="checkbox"/> 否
3.4	显示持卡人数据时, 除了账号的最后 4 位外, 是否均不能看到其他所有的数字?	<input type="checkbox"/> 是	<input type="checkbox"/> 否
3.5	是否通过例如加密或截断的方式安全储存(在数据库、日志文件, 媒体备份等的)账号?	<input type="checkbox"/> 是	<input type="checkbox"/> 否
3.6	登陆查帐记录前是否已清理账号?	<input type="checkbox"/> 是	<input type="checkbox"/> 否

### 要求四: 通过公众网络传输持卡人数据和敏感信息必须加密

	说 明	回 答		
4.1	当通过公众网络传输敏感的持卡人数据时, 是否使用 SSL 或其他行业可接受的方法进行加密?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
4.2	当用 SSL 进行敏感的持卡人数据传输时, 是否使用 3.0 版的 128 Bit 编码?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
4.3	使用无线技术时, 是否使用 WPA, VPN, 128-bit 的 SSL 或 WEP 进行通信加密?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
4.4	使用无线技术时, 是否使用 128-bit 的 WEP 和附加的加密技术, 且可每季旋转共享的 WEP 密钥?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
4.5	通过电子邮件传输账号时, 是否进行加密?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用

## 维持防范弱点攻击的管理程序

### 要求五: 使用和定期更新防病毒软件

	说 明	回 答	
5.1	所有服务器和工作站上是否安装有定期更新的病毒扫描器?	<input type="checkbox"/> 是	<input type="checkbox"/> 否

### 要求六: 开发和维护安全系统和应用程序

	说 明	回 答		
6.1	是否用厂商发布的最新安全补丁, 来更新开发、测试及产品系 统?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
6.2	软件及应用开发程序是否建立在工业最佳模式基础上; 是否整个 软件开发生命周期 (SDLC) 过程包括了信息安全?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
6.3	使用生产数据用于测试和开发目的之前, 敏感持卡人数据是否已 清除?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
6.4	是否所有生产环境和应用的变更在使用前经正式授权、计划或记 录过?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
6.5	开发网络应用, 是否考虑过经安全社区 (例如OWASP组织, <a href="http://www.owasp.org">www.owasp.org</a> ) 认可的每月指导建议?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
6.6	鉴定网络真实性时, 是否将应用程序设计成可防止恶意使用者企图 攻击已存在的使用者的账户?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
6.7	敏感的持卡人数据是否保存在安全或已加密的收藏夹?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
6.8	服务器端的控制装置能否防止 SQL 指令植入式攻击或其他客户端 控制的绕过攻击?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用

## 实施有力的访问控制检测程序

### 要求七: 限制访问数据,因业务需要也应知道

	说 明	回 答	
7.1	是否根据因业务需要访问也应知道的原则,对用户支付卡账号的访问设限?	<input type="checkbox"/> 是	<input type="checkbox"/> 否

### 要求八: 分配给每个人独特的 ID 来进入计算机

	说 明	回 答		
8.1	是否要求验证所有用户的使用,至少使用惟一用户名和口令?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.2	当雇员、管理员或第三方可远程访问网络时,是否可用惟一用户名和口令的方式,并用编码及其他开启的安全功能来配置远程访问软件(例如 PCAnywhere, dial-in 拨入,或 VPN)	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
8.3	是否所有网络设备和系统的密码口令均要加密?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.4	雇员离开公司时,是否该雇员的用户账号和密码立即无效?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.5	是否定期检查使用者账户以保证不会产生有恶意、过期或不知名的账户?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.6	当预确定的时限后,系统内的长时间不使用的非消费账户是否自动失效?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.7	供应商使用的用于远程维护的所有账户是否只在必要的时间内才有效?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
8.8	是否禁止非消费用户使用群、共享或普通账户和口令?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.9	是否要求非消费用户在预确定的周期上更换其口令?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.10	对非消费用户而言,是否有口令策略可以强行使用强口令,并防止再次提交已用过的口令?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
8.11	是否有账号封锁机制,能阻止恶意使用者用多种口令重试或强制的方式获得访问一个账户?	<input type="checkbox"/> 是	<input type="checkbox"/> 否	

## 实施有力的访问控制检测程序

### 要求九： 限制物理访问持卡人数据

	说 明	回 答		
9.1	是否在获得进入设备的地方，设置多重物理安全控制（例如标记、保卫或陷阱），来防止未授权的个人	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.2	使用无线技术时，是否限制访问无线接入点、无线网关和无线手持装置？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
9.3	为防止未经授权访问的情况发生，设备（如服务器、工作站、笔记本电脑和硬盘驱动）和含有持卡人数据的媒质是否已受物理保护？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.4	为防止未经授权访问的情况发生，已打印在纸上或通过传真接收的所有持卡人数据是否已受保护？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.5	是否对备份和其他含有敏感的持卡人数据媒质有安全处理分发和处置的程序？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.6	是否所有储存持卡人数据的媒介装置均已正确清点并安全储存？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
9.7	物理配置持卡人数据前是否已被删除或破坏（例如，使用碎纸机或消磁备份媒介）？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	

## 术语

### 要求十: 跟踪并监控所有对网络资源和持卡人数据的访问

说 明		回 答	
10.1	是否对所有对持卡人数据（包括根目录/管理）的访问进行记录？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.2	访问控制记录是否包含成功或失败登陆企图和对审核记录的访问？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.3	所有重要系统时钟和时间是否同步，记录是否包括日期和时间标志？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.4	为防范未经授权交易发生，是否定期检查防火墙、路由器、无线接入点和验证服务器的日志？	<input type="checkbox"/> 是	<input type="checkbox"/> 否
10.5	是否对审核记录做定期备份、保护，并对所有重要系统至少保留在线三个月,离线一年？	<input type="checkbox"/> 是	<input type="checkbox"/> 否

### 要求十一: 定期测试系统的安全和处理过程

说 明		回 答		
11.1	使用无线技术时，无线分析器是否定期运行来识别所有无线装置？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不适用
11.2	所有互联网界面的应用程序和系统在投产前，是否进行弱点扫描和渗透测试？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
11.3	网络中是否使用入侵防护或阻止系统？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	
11.4	是否定期监控入侵侦测或入侵防范系统（IDS / IPS）的安全警报，并安装最新 IDS / IPS 信号？	<input type="checkbox"/> 是	<input type="checkbox"/> 否	

## 术语

### 要求十二: 保持涉及到信息安全的策略

	说 明	回 答
12.1	是否能提供正式的记录访问控制, 应用和系统开发、操作、网络和物理安全等信息安全策略方面的文件?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.2	是否向所有系统用户(包括供应商, 合同商和商业伙伴)发布信息安全策略和其他相关安全信息?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.3	是否至少每年一次检查信息安全策略, 并在需要时进行更新?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.4	信息安全的任务和责任在公司范围内是否已被明确定义?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.5	是否所有系统用户具有最新的信息安全意识和培训课程?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.6	是否所有雇员需要签订证明他们已经阅读并理解安全策略和程序的协议?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.7	是否对所有雇员访问账号进行背景调查(例如当地法律允许范围内的信用和犯罪前科记录)?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.8	是否访问敏感持卡人数据的第三方公司都有合约明确其有责任与卡组织安全标准相符合?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.9	是否有正式的安全突发事件响应计划的证明文件, 并对适当责任方发布?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.10	是否安全突发事件有向负责安全调查的个人汇报?	<input type="checkbox"/> 是 <input type="checkbox"/> 否
12.11	危及持卡人数据时, 是否有突发事件响应小组随时准备开展工作?	<input type="checkbox"/> 是 <input type="checkbox"/> 否

## 术语

术语	定义
<b>Access control</b> 访问控制	限制授权人或应用程序访问信息或信息处理资源的措施。
<b>Account harvesting</b> 账户获得	基于反复试验的方法，确定现有的用户账户。用错误消息方式发出很多信息可以泄露信息，使进攻者更易穿透或危及系统。
<b>Account number</b> 账号	证明发行人和特定持卡人账户的支付卡数据（信用或借记）。
<b>Acquirer</b> 收单行	指银行卡协会会员，可用作发起和维护受理 VISA 卡和 MASTER 卡的商户间关系。
<b>Asset</b> 资产	组织的信息或信息处理资源。
<b>Audit log</b> 审查日志	按时间顺序针对系统活动的一份记录，可按顺序对环境及活动进行重组、回顾和检查，伴随或导向一项操作、过程或事件记录在交易过程中自始至终的结果。特殊情况下，有时用作安全审查追踪。
<b>Authentication</b> 鉴定	检验某个项目或过程的身份的程序。
<b>Authorization</b> 授权	针对用户、程序或过程的准许访问或其他权利。
<b>Backup</b> 备份	一种数据复制，用以存档或保护以防破坏或丢失。
<b>Card-validation code</b> 卡片验证值	在支付卡签名栏上印有的三位数值用以确定卡片不出现的交易。MASTER 支付卡上叫做 CVC2，VISA 支付卡上为 CVV2。
<b>Cardholder</b> 持卡人	持有已发行的卡或授权使用该卡的客户。
<b>Cardholder data</b> 持卡人数据	关于持卡人和会员(例如账号、有效日期、会员提供的数据、其他商户/代理收集的电子数据，等等)关系的所有个人识别数据。该术语解释了其他集合了关于持卡人的地址、电话号码等方面的个人信息。
<b>Compromise</b> 泄露	入侵计算机系统，即发生未经授权情况下泄露、修改或破坏持卡人数据的情况。

## 术语

---

术语	定义
<b>Console</b> 控制台	某个屏幕或键盘,可允许在网络环境下, 访问或控制服务器/主机。
<b>Consumer</b> 消费者	购买产品和/或服务的个体。
<b>Cookies</b> 记录资料夹	在网络服务器和网络浏览器之间转换数据字符串以维持某个进程。记录资料夹包括用户性能和个人信息。
<b>Database</b> 数据库	一种结构格式, 使得容易重新找回组织和维持的信息。比如一个简单的数据库就是一份表格或一份电子数据表。
<b>DBA</b> 象做业务	建立在 DBA 或连锁店(不是拥有一些连锁的公司)的交易量上的符合确认级别。
<b>Default accounts</b> 默认账户	指已在生产系统中预定义的系统登陆账户, 可在系统初次使用时允许初始登陆。
<b>Default password</b> 默认口令	当系统从生产商运出时的系统管理或服务账户的口令, 并通常与默认账户相关联。默认账户和口令是公开的和广而告之的。
<b>Dual control</b> 双重控制	特定交易完成前, 通过要求多个各自独立的个人采取措施, 来保存过程完整性的方法。
<b>DMZ (de-militarized zone)</b> 隔离区	在秘密网络和公众网络之间增加的网络, 目的是提供一个附加的安全层。
<b>Egress</b> 流出	离开网络的流量。
<b>Encryption</b> 加密	将信息转化为除特定密匙持有者外, 对其他任何人都无法破解的格式的过程。使用加密, 可以保证在加密和解密(加密的反过程)过程中的信息, 在未授权情况下不会泄露。
<b>Firewall</b> 防火墙	保护来自其他网络用户的网络资源的硬件和 / 或软件。典型的情况是, 拥有企业内部互联网的企业允许自己的员工访问宽带互联网必须使用防火墙, 来防止外来者用其私人数据资源进行访问。
<b>Host</b> 主机	承载软件的主要硬件。

## 术语

术语	定义
<b>Information security</b> 信息安全	保护信息的机密性、完整性和可用性。
<b>Ingress</b> 流入	进入网络的流量。
<b>Intrusion detection systems</b> 入侵侦测系统	入侵侦测系统 IDS 可以检查所有网络进出活动，并验证所怀疑的模式，是否是某人意图攻击闯入或危及某系统的网络或系统。
<b>IP address</b> IP 地址	一个 IP 地址就是一个数字代码，可以唯一确定互联网上的某台特定的计算机。
<b>IP Spoofing</b> 虚假 IP	入侵者通过发送消息给某台计算机，其 IP 地址表明其来自可信赖的主机，在未授权情况下获得访问计算机的技术。
<b>ISO 8583</b> 国际标准 8583	用在金融系统之间，作为通信使用所制定的一套标准。
<b>Key</b> 密钥	加密过程中，一个密钥可当一个数值来用；使用某个运算法则从一个未加密的文本产生一个加密文本。在得到的消息解密出文本的难度，通常由密钥长度决定。
<b>Magnetic Stripe Data (Track Data)</b> 磁条数据（轨道数据）	在磁条中编码的数据，用以卡片出现的交易进行授权。公司在交易授权后不可保留全部的磁条数据。特别情况下，授权后必须清除服务代码、任意数据 / CVV，以及 VISA 保留的数值,但可以提取保留帐号、有效期和姓名。
<b>Monitoring</b> 监控	查看网络活动。
<b>Network</b> 网络	网络是两台或更多计算机相互连接，并可以共享资源。
<b>Network Address Translation (NAT)</b> 网络地址转化	指互联网协议地址（即 IP 地址）的转化，是将一个网络使用的 IP 地址转化为另一个网络可识别的不同的 IP 地址。
<b>Non consumer users</b> 非消费者用户	Any user, excluding consumer customers, that accesses systems, including but not limited to, employees, administrators, and third parties.指任何访问系统的，包括但不限于，雇员、管理员和第三方的所有用户，消费者用户外除外。

## 术语

术语	定义
<b>Password</b> 密码	一系列字符串，用于用户认证。
<b>Patch</b> 补丁	一组程序的快速修补工作。产品正式发布后，软件产品的贝塔测试分布或试用期间，经常会出现各种问题。一个补丁就是可提供给用户的紧急解决方案。
<b>Penetration</b> 渗透	穿过系统安全机制的成功行为。
<b>Penetration Test</b> 渗透测试	指为了安全，而查探计算机或网络的弱点和攻击者可能利用的安全漏洞。这种测试包括找出所有的存在问题的安全特征。测试完毕后，渗透测试者提交一份系统弱点的报告以及如何提高系统安全性的建议。
<b>System Perimeter Scan</b> 系统周界扫描	包括检查外部周围系统及外部网络的服务（例如接入互联网的服务）报告的一种非侵入式的测试方法。
<b>Policy</b> 策略	在使用计算机资源、安全行为和操作过程的指引开发上可接受的组织级别的管理规则。
<b>Procedure</b> 程序	程序提供有关策略如何应用的描述性方式，即策略如何实施。程序告诉公司一个政策怎么执行。
<b>Protocol</b> 协议	一种网络通讯的相互认可方式。描述在一个网络中进行活动而应当遵从的规则及程序的一种规范。
<b>Risk analysis</b> 风险分析	同样也称为风险评估，系统地判断资源价值及其所受的威胁、损失暴露量（例如潜在的损失风险）及发生的频率和成本费用的一个方法，有时也会推荐应对措施来指导如何分配资源，将全部的损失降到最低。
<b>Router</b> 路由器	路由器是用于连接两个或更多网络的硬件或软件部分。路由器作为分类器和解释器，查明地址及信息比特，传递到正确的目标位置。软件型路由器有时称作网关。
<b>Sanitization</b> 清除	删除文件、设备或系统中的机密数据，或修改数据，以致攻击数据无效。
<b>Security officer</b> 安全员	组织中对安全相关事务负主要责任的人员。
<b>Security policy</b> 安全策略	组织所采取的一系列法规、规则和手段来管理、保护和分发机密信息。
<b>Sensitive cardholder data</b> 敏感持卡人数据	未授权的泄密数据会被用于欺诈交易中。敏感数据包括：账号、磁条数据、CVC2 / CVV2 和有效日期。

## 术语

术语	定义
<b>Separation of duties</b> 职责分离	将某一系统功能分成几个步骤让不同人员参与的一种手段，以防止过程遭受单个人员破坏。
<b>Server</b> 服务器	提供类似通讯处理、文件储存或打印工具等服务给其它计算机的计算机。
<b>SQL injection</b> SQL 入侵	一种针对数据库驱动的网站而采取的攻击方法，攻击者通过利用连接到互联网的系统存在的不安全代码来执行非法的 SQL 命令。SQL 入侵攻击被用于从一般来说不被访问到的数据库中盗窃信息，并且 / 或者通过数据库所在计算机访问到组织的主计算机。
<b>SSL</b> 加密套接字协议层	SSL 作为已经建立的工业标准，对网页浏览器和网站服务器之间的通道进行信息加密，确保通过此通道传递的数据的保密性及可靠性。
<b>Tamper-resistance</b> 抗破坏性	一个抗破坏性的系统是难以被修改或破坏，即便在攻击者进行物理层访问情况下。
<b>Threat</b> 威胁	一种可能引起信息或信息处理资源出现故意或意外的丢失、修改、暴露、不能访问或对组织造成损失的状况称为威胁。
<b>Token</b> 个人持证	执行动态验证的一种设备。
<b>Transaction data</b> 交易数据	涉及电子支付系统的数据。
<b>Truncation</b> 截断	删除数据段的一种方法。一般来说，在账号被截断时，前 12 位数字被删除，仅保留最末 4 位数。
<b>Two-factor authentication</b> 双因子验证	一种要求用户出示两种证明措施的验证方法：一是用户持有（例如智能卡或个人持证），二是用户知道（例如密码）。为了访问系统，用户必须持有两者。
<b>User ID</b> 用户 ID	用作区分系统中每个用户的唯一标识字符串。
<b>Virus</b> 病毒	能修改或破坏软件或数据的一种程序、代码串，并能够自我复制。
<b>Vulnerability</b> 弱点	系统的安全程序、系统设计、系统执行或内部控制上存在的弱点，攻击者可利用这些弱点进行侵犯系统安全策略的行为。

## 术语

---

术语	定义
<b>Vulnerability scan</b> 弱点扫描	用于自动检测商户或服务供应商系统漏洞的工具，基于外部界面的互联网协议地址，可对使用公网 IP 地址的网络和网站应用程序进行远程检测。操作系统、服务及设备的漏洞（可被黑客用来攻击公司局域网）可用扫描工具识别。