X-Payments:PA-DSS implementation guide for X-Cart Payments 3

Contents

Introduction[edit]

The purpose of this PA-DSS Implementation Guide is to inform employees of organizations using the X-Cart Payments payment application by Qualiteam Software Limited about the methods and means of protection of account data in the X-Cart Payments software.

The methods include the need for compliance with the information security standards in the payment card industry developed by the international payment systems Visa and MasterCard - Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS). For additional information about PCI DSS, please visit the Official PCI Security Standards Council Site.

The document provides instructions on how to implement the application in a PCI DSS compliant manner.

Full product name - X-Cart Payments.
Product version - 3.1.x.

Any servers used to run the X-Cart Payments payment application must be configured according to this PA-DSS Implementation Guide.

This PA-DSS Implementation Guide should be updated:

◊ at least annually;
◊ after changes in the payment application (if required);
◊ after changes in the PCI DSS and PA-DSS standards.

The updated Version of the PA-DSS Implementation Guide has to be sent to all the merchants using X-Cart Payments.

The history of changes to the X-Cart Payments PA-DSS Implementation Guide is provided in the table below.

Table.1. X-Cart Payments PA-DSS Implementation Guide history of changes

Author	Date	Number	Change description
Alex Mulin	05/17/2016	01	The original version of the document, designed to meet the requirements of PCI DSS version 3.1 and PA DSS version 3.1
Alex Mulin	05/17/2017	02	The original version of the document, designed to meet the requirements of PCI DSS version 3.2 and PA DSS version 3.2
Alex Mulin	05/05/2018	03	Updated versions

Data protection[edit]

The PCI DSS and PA-DSS standards prohibit storage of sensitive authentication data (after authorization) or cardholder data in cleartext.

Cardholder data includes:

◊ Primary Account Number (PAN)
◊ Cardholder Name
◊ Expiration Date
◊ Service Code

Sensitive authentication data (SAD) includes:

◊ Full track data (magnetic-stripe data or equivalent on a chip)
◊ CAV2/CVC2/CVV2/CID
◊ PINs/PIN blocks

X-Cart Payments has the ability to store parts of cardholder data temporarily to perform 3D Secure verification and certain types of transactions for some of the integrated payment processors. During storage, cardholder data is encrypted using RSA 2048 algorithm and AES 256 for key encryption. When its storage period is over, the data is removed automatically via "cron" software that needs to be installed and configured to run X-Cart Payments periodic tasks.

X-Cart Payments may not be configured to store permanently in the database the following types of data:

◊ Full PAN
◊ Full track data (magnetic-stripe data or equivalent on a chip)
◊ CAV2/CVC2/CVV2/CID
◊ PINs/PIN blocks

Merchants and/or developers implementing X-Cart Payments should not attempt to customize this as a feature.

The payment application masks PAN on display (except for the moment when the user enters the card number). X-Cart Payments can display masked

PAN on the "Payment details" pages and in the "View details" pop-up windows for some of the integrated payment processors in the following format: 123456******1234 MM/YY or **********1234 MM/YY. The same data (partially masked with asterisks) may be passed via the API to the integrated software products. X-Cart Payments does not have the ability to display full PAN anywhere, and there are no settings that can change this behavior of the user interface.

Data Collected while Testing[edit]

Delete any sensitive authentication data (pre-authorization) gathered as a result of testing or troubleshooting your X-Cart Payments:

1. Sensitive authentication data (pre-authorization) must only be collected when needed to solve a specific problem. You should never use real credit card information when testing your store. Instead, contact your payment gateway and ask them for special credit card numbers that you can use while testing.
2. If you ever choose to collect credit card information to troubleshoot a problem that a customer of yours is having, then please note the following:
    - Such data must be stored only in specific, known locations with limited access.
    - Only collect a limited amount of data (no more than is needed to solve the problem).
    - Sensitive authentication data must be encrypted during storage. Make sure to encrypt it before storing it. There are many encryption software packages that you can install on your computer to do so.
3. Sensitive authentication data must be securely deleted immediately after use.

To prevent uncontrolled storage of cardholder data (for example, in case of operating system failure), it is recommended to disable the swap file or move it to a specially prepared encrypted partition.

Authentication and access[edit]

The X-Cart Payments payment application has an only user type. This type cannot get access to payment card numbers and does not have any administrative privileges that may affect PA-DSS compliance. There are no built-in/default user accounts in X-Cart Payments. You must carefully control access to X-Cart Payments. Follow these rules:

◊ Restrict the number of employees who have access to X-Cart Payments to only those who have a business need.
◊ Always provide unique usernames for each person who needs access.
◊ Do not use system-default usernames and/or passwords.
◊ Ensure that web server is run under a non-privileged user account and the application has access to the database from a limited privilege user account.

To set password lifetime:

1. Log in to X-Cart Payments.
2. Go to Settings -> General Settings.
3. In the "User account password lifetime" field, enter the number of days for which the user account password needs to be valid. The maximum allowed password lifetime is 90 days.

The following related rules apply:

◊ The minimum password length is 8 characters.
◊ A password must contain both numbers and lower- and uppercase characters.
◊ The last 4 passwords must be unique.
◊ A user account must be blocked for a specified period (30 minutes by default) after 6 unsuccessful attempts to enter a password.
◊ A user is logged off after an inactivity period of 15 minutes.

PCI compliance requires that you use unique user names and secure authentication to access any PCs, servers, and databases with payment applications and/or cardholder data. This means that you should use different user names/passwords:

◊ For your Web hosting account administration area (Web hosting account where your online store is hosted);
◊ For FTP access to the Web server;
◊ For Remote Desktop Connection to the Web server (if available);
◊ To connect to the MySQL server that contains your store data.

Linux authentication mechanism is used for login in the servers with running X-Cart Payments. Accounts for access to the operating system are managed by the Linux administrator. For Linux operating system accounts, you must configure the following attributes of the password policy:

◊ use personal accounts, do not use any group, shared, or generic accounts and passwords;
◊ changes to user passwords at least once every 90 days;
◊ require a minimum length of at least seven characters;
◊ contain both numeric and alphabetic characters;
◊ do not use last four passwords used previously;
◊ block account after six invalid logon attempts (minimum 30 minutes or until an administrator enables the user ID).

Two-factor authentication must be used for remote access to the operating system. The authentication methods, also known as factors, are:

◊ something you know, such as a password or a passphrase;
◊ something you have, such as a token device or a smart card;
◊ something you are, such as a biometric.

Logging[edit]

Audit trails are automatically enabled with the default installation of X-Cart Payments. Users do not have the ability to disable or change the logging parameters of X-Cart Payments. X-Cart Payments log journal does not contain cardholder data. It is implemented at the source code level. The setting of an event log journal does not require any additional action from users. The log files are created in the var/log/ directory. In X-Cart Payments 3.1, logs can be viewed via the X-Cart Payments admin back end.

Make sure you restrict access to the log files by business need-to-know. The following types of activity are logged:

◊ All actions taken by any individual with root or administrative privileges.
◊ Successes and failures of all individual accesses to application sections and functions.
◊ Initialization of the audit logs.
◊ User sign in and sign out.

Individual access to cardholder data is not logged, because cardholder data is not stored before and after authentication. Access to audit trails must be provided on the operating system level. Audit trails are written to the file system, to the files access.log and error.log. Each log event includes:

◊ Type of event;
◊ Date and time of event;
◊ Username and IP address;
◊ Success or failure indication;
◊ Action which led to the event;
◊ Component which led to the event.

There is also a meta-log which contains information about other log files being created. Make sure you have a system-level auditing software properly configured to monitor users' activity on the server. This software should:

◊ warn on a checksum change of any of X-Cart Payments source code files except for the log file and the database files;
◊ record any file writing operations related to X-Cart Payments files.

Communication[edit]

LAN channel or other available connection method can be used as a communication channel. X-Cart Payments payment application supports the following data formats:

Protocol	HTTP protocol (RFC 2616: HTTP/1.1) is used for data transfer between client and server
Data transmission method	Only encrypted cardholder data (RSA 2048 and AES 256) is transferred. RAW POST method is used for data transmission - (data stream is transmitted in the body of the request that is sent from client to server)
Data format	Data is transmitted in XML format (Extensible Markup Language (XML) 1.0) or in plain text using POST query via HTTPS
Port	X-Cart Payments payment application uses ports 80, 443

Network traffic encryption
X-Cart Payments uses encryption, such as TLS or IPSEC, for:

◊ transmission of cardholder data over public networks, per PCI DSS requirement 4.1.
◊ providing remote web-based access to the application.

If you use some tools to remotely access the application, you should encrypt all the communication using such technologies as TLS or IPSEC.
As per PCI DSS requirement, cardholder data must never be sent unencrypted by email, and X-Cart Payments does meet this requirement never sending cardholder data by email or by IMs. Merchants and/or developers implementing X-Cart Payments should not attempt to customize this as a feature unless an encryption solution is also implemented.

Enable TLS
TLS protects data that is transmitted between a browser and your web server. It is critical that you have TLS enabled on your web server, and one of the first steps you should take after the installation is to enable TLS.

◊ Your web server must be configured to use TLS v1.2 protocols with strong encryption (128-bit or longer key is required).
◊ You will need to have a certificate issued for your web domain. Read guidelines on installing Comodo's Instant TLS certificates.

If a web server does not have TLS enabled, X-Cart Payments will not function. X-Cart Payments does not support remote administrative access. Strong encryption must be used for remote access to the server. The connection of servers with X-Cart Payments payment application to the Internet must be protected by a firewall. In X-Cart Payments configurations involving more than one server, server connections should take place in network segments separated from the Internet via stateful inspection firewalls.

Wireless communications
If you use wireless networking to access X-Cart Payments, it is your responsibility to ensure your wireless security configuration follows the PCI DSS requirements.

◊ Personal firewall software should be installed on any mobile and employee-owned computers that have direct access to the internet and are also used to access your network.
◊ Change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.
◊ Encrypt wireless transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or TLS.
◊ Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:
    - Use with a minimum 104-bit encryption key and 24 bit-initialization value.
    - Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or TLS.
    - Rotate shared WEP keys quarterly (or automatically if the technology permits).
    - Rotate shared WEP keys whenever there are changes in personnel with access to keys.
    - Restrict access based on media access code (MAC) address.
    - Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless environment or to control any traffic if it is necessary for business purposes.

Remote access

X-Cart Payments provides web-based access using two-factor authentication based on one-time codes. Detailed information can be found on the X-Payments:Two-factor authentication page. If you enable remote access to your network and the cardholder data environment, you must implement two-factor authentication. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on TLS 1.2 or IPSEC) with individual certificates. You should make sure that any remote access software is securely configured by keeping in mind the following:

◊ Change the default settings in the remote access software (for example, change the default passwords and use unique passwords for each customer).
◊ Allow connections only from specific (known) IP/MAC addresses.
◊ Use strong authentication or complex passwords for logins.
◊ Enable encrypted data transmission.
◊ Enable account lockout after a certain number of failed login attempts.
◊ Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
◊ Enable any logging or auditing functions.
◊ Restrict access to customer passwords to authorized reseller/integrator personnel.
◊ Establish customer passwords according to PCI DSS requirements.

Qualiteam does not provide software updates via remote access on an automated basis.

Hardware and software[edit]

The following requirements must be met for X-Cart Payments payment application self-service terminals:
Operating System
Linux Ubuntu 16 or later, Linux Debian 6.0 or later, Linux CentOS 6 or later
DBMS
MySQL 5.6 or later
Software
PHP 7.1.x or PHP 7.2.x (For security reasons, the latest PHP version in the branch is required.)
Apache 2.4 or later

Product versioning methodology[edit]

Version number changes	Software changes	Description	PA-DSS changes
Version number does not change	Change of the software name Change of the vendor name	Changes not related to the software development process	Administrative
Increment of the minor version number to reflect a change not affecting the certification. For example, change of the version number from 1.0.5 to 1.0.6 (for the certification of 1.0.x)	- Changes to the user interface - Changes to the database schema - Changes to supported payment gateway integrations / Addition of new payment gateway integrations	Changes that have no impact on the PA-DSS requirements compliance or Payment Application security	No Impact
Increment of the second version number. For example, change of the version number from 1.1.* to 1.2.*	Software changes satisfy the following conditions: - Fewer than 4 sections of the standard (from 1 to 12) involved; - Fewer than a half of all the requirements of the standard (sections 1 to 12) involved; - Less than a half of the software functions (or code) modified; - Changes implemented for compatibility with the updated versions of previously tested OS, DBMS and third party software products. - Addition/removal of supported payment processors. - Recompilation of the source code using a new compiler or different compiler settings. - Changes of the software versioning policy. - Changes of the software not related to security.	- Changes in the software affecting payment card data mechanisms. - Changes addressing the identified vulnerabilities of the application. - Changes related to the completion of the annual cycle of development (if there are other changes).	Low Impact
Increment of the first version number. For example, change of the version number from 1.0.* to 2.0.*	Software changes satisfy the following conditions: - 4 or more sections of the standard (from 1 to 12) involved; - More than a half of all the requirements of the standard (sections 1 to 12) involved; - More than a half of the software functions (or code) modified; - Addition of new supported platforms/OS versions.	Major changes in the software architecture, global alterations of code	High Impact

The release of each new version is accompanied with a notification to all the application users (agents), which indicates the new application version number and a list of main changes in the new version.

New patches and updates delivery[edit]

New patches, updates, installation instructions and MD5 checksum files are delivered via secure HelpDesk system located at https://secure.x-cart.com using "File Area" section in users accounts there. We send newsletters about new patches and updates originating from x-cart.com domain name via verified and well-known email delivery system.

See also[edit]

- PCI FAQs
- PCI Security Standards Council website

This article can be **downloaded as a PDF file**