X-Payments:PCI DSS implementation guide for X-Payments 2.2

Contents

Introduction

This guide covers **X-Cart Payments** 1.0, 2.0, 2.1, 2.2 and is intended for merchants and integrators who wish to implement the application in accordance with guidelines set by the PCI Data Security Standard (PCI DSS).

X-Cart Payments versioning policy

X-Cart Payments version number must look like "X.Y.z" (e.g. 1.0.6, 2.0.1, 2.2.1, 3.0.0), where

- X - major release version number that gets incremented when high impact changes are introduced and certified under PA-DSS requirements;
- Y - minor release version number that gets incremented when low impact changes are added to X-Cart Payments package;
- Z - maintenance/bug-fix release version number that gets incremented when no impact and administrative changes are done to X-Cart Payments package.

See samples of changes below:

- High-impact - major update of core X-Cart Payments functions such as login routine, credit card processing inside X-Cart Payments.
- Low-impact - update of integration with newer versions of DBMS, OS and middleware whose older versions have been already verified, adding or removing payment processor integrations, re-compiling source code using new code compiler or new compiler settings, change to X-Cart Payments versioning policy, other changes not related to security of the application.
- No impact - UI changes, changes to DB schemes, report module updates, update or adding of new payment gateway.
- Administrative change - change of application name, change of software vendor name.

PCI DSS

PCI DSS specifies 12 requirements broken into 6 groups for compliance that apply both to hardware and software parts of the system that is used to collect, store, transmit and process valuable credit card data as well as the human factor.

Build and Maintain a Secure Network	• Requirement 1: Install and maintain a firewall configuration to protect cardholder data • Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	• Requirement 3: Protect stored cardholder data • Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	• Requirement 5: Use and regularly update anti-virus software • Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	• Requirement 7: Restrict access to cardholder data by business need-to-know • Requirement 8: Assign a unique ID to each person with computer access • Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	• Requirement 10: Track and monitor all access to network resources and cardholder data • Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy	• Requirement 12: Maintain a policy that addresses information security

Specifically, relevant elements to an e-commerce business' PCI compliance status include:

- Properly using your payment application. For this purpose, carefully review the section below for information on how to use **X-Cart Payments** in a way that ensures PCI compliance.
- Using a PCI compliant Web hosting environment
- Using a PCI compliant payment provider

You can find and review the complete specification by visiting https://www.pcisecuritystandards.org/

This guide is intended to help merchants implement the **X-Cart Payments** application in a way that is compliant with version 2.0 of the PCI DSS.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard is a worldwide information security standard assembled by the major credit card vendors, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. The standard was designed to help organizations involved in processing credit card payments online make their payment systems secure from cardholder data fraud.

X-Cart Payments has been designed and certified to meet all of the requirements of the **PA-DSS** version 2.0. This does not automatically make you, the merchant, PCI DSS compliant. To ensure PCI DSS compliance, it is necessary that you follow the recommendations and instructions provided in this guide.

For additional information about **PCI DSS** please visit the Official PCI Security Standards Council Site.

Cardholder data storage

X-Cart Payments has the ability to store parts of cardholder data temporarily for performing 3D Secure verification and certain types of transactions for some of the integrated payment processors. While stored cardholder data is encrypted using special cryptographic algorithm. The data is removed automatically when its storing period is over using "cron" software that needs to be installed and configured to run X-Cart Payments periodic tasks.

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

- unmasked PAN
- PIN
- CVV
- magnetic stripe (track data)

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

X-Cart Payments can display masked PAN on "Payment details" pages and in "View details" pop-up windows for some of the integrated payment processors in the following format: 123456******1234 MM/YY or **********1234 MM/YY. **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.

Configuring and using X-Cart Payments in PCI compliant manner

Installation

Follow the standard procedure for deployment of X-Cart Payments files to the web server.

Once installed, X-Cart Payments WILL NEVER:

- store unmasked credit card numbers (PANs)
- send credit card data or any other information to Qualiteam for debug purposes

Access control

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
- Web server must be run under a non-privileged user account. Application must access the database from a limited privilege user account.
- All default user accounts use secure authentication mechanisms and password policy settings that comply with all the standard requirements:
  - ♦ user accounts inactive for more than 3 days are blocked
  - ♦ password lifetime is set to 30 days

    To set password lifetime:

    1. Login to **X-Cart Payments**
    2. Go to Settings -> General Settings
    3. Enter the number of days the user account password will be valid for in the "User account password lifetime" field. The maximum allowed password lifetime is 90 days.

  - ◊ minimum password length is 8 characters
  - ◊ password must contain both lower and upper case characters and numbers
  - ◊ the last 4 passwords must be unique
  - ◊ user account must be blocked for a specified period (30 minutes by default) after 6 unsuccessful attempts to enter a password
  - ◊ user is logged off after inactivity period of 10 minutes

Please note that changing default password policy settings will lead to breaking PCI DSS standard requirements.

Enabling SSL (Secure Socket Layer)

SSL protects data that is transmitted between a browser and your web server. It is critical that you have SSL enabled on your web server, and this should be among the first steps taken after installation.

- 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 SSL certificates.

If a web server does not have SSL enabled **X-Cart Payments** will not function or will be notifying users depending on **allow_insecure_protocol** parameter set in config.ini.php file (disabled by default).

Data Collected while Testing

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 collect credit card information to troubleshoot a problem that one of your customers 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 such data as needed to solve a specific problem
   - ♦ Sensitive authentication data must be encrypted while stored. 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. Such data must be securely deleted immediately after use.

Encryption Key Management

As part of your PA DSS v3.1 requirements, encryption key must be changed annually (changing every 90 days is recommended). You should also change the key any time an employee with access to the key leaves your company. Always replace the key if you know or suspect it has been compromised by any means.

To change the encryption keys:

1. Log in to **X-Cart Payments**
2. Go to Maintenance -> Encryption keys
3. Click "Generate new keys"

Use unique user IDs and secure authentication to access PCs, servers and databases

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:

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

The passwords for the accounts mentioned above must also meet the following requirements:

- be at least 8 characters in length
- contain both numbers and letters in lower and upper case
- not coincide with any part of your email address
- not coincide with any of the last four passwords you have used
- have a lifetime of less than 90 days
- account lockout threshold must be set to 6.
- account lockout duration must be set to 30 minutes (or until unblocked by the administrator).
- user must be logged off after 15 minutes of inactivity

Audit trails

Audit trails are automatically enabled with the default installation of X-Cart Payments. There is no option to disable audit logging. The log files are created in the var/log/ directory. 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 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.

OS-level audit trails

Make sure you have a system-level auditing software properly configured to monitor users' activity on server. This software should:

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

Encrypting network traffic

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 tools to remotely access the application, you should encrypt all communication using technologies such as TLS or IPSEC.

As per PCI DSS requirement 4.2, cardholder data should never be sent unencrypted by e-mail, and X-Cart Payments does meet this requirement **never** sending cardholder data by e-mail 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.

Wireless communications

If you use wireless networking to access **X-Cart Payments**, it is your responsibility to ensure your wireless security con figuration 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 cod e (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 PIN codes. Detailed information can be found at Managing PIN codes 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 default settings in the remote access software (for example, change 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 8.1, 8.2, 8.4, 8.5

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

See also

- PCI FAQs
- PCI Security Standards Council website

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