PCI and WordPress

Barry Gould, BlogSec.net
Barry@blogsec.net

What is PCI / PCI DSS?

PCI = Payment Card Industry Security Standards Council

- Created by a consortium of Credit Card vendors: Visa, MC, Discover, AmEx, JCB (Japan)

PCI DSS = Data Security Standard

- attempt to reduce CC thefts/breaches (TJX)
- set of requirements for merchants

PCI DSS documents

- DSS is a 75-page document.
- Updated periodically (1.0, 1.1, 2.0 so far, as of 2010)
- Supplemental documents released to clarify requirements.
- Deadlines for compliance with new versions.

Who does it apply to?

- Any **merchant** who accepts credit/debit cards, **even if using 3rd-party gateway**.

- Any **service provider** "that stores, processes, or transmits cardholder data on behalf of another entity"

# of transactions determines 'level'

Type of system determines Assessment type.

Why should I comply?

Penalties:

- The payment brands may fine an acquiring bank $5,000 to $100,000 **per month** for compliance violations. The banks will likely pass this fine on to the merchant.
- The bank will also likely terminate your relationship or increase fees.

- Loss of business / reputation from loss of customer trust. Cleanup costs.

Levels and Assessment types

Levels: L4 - < 20k Visa, <1M total transactions

SAQ: Self-Assessment Questionnaire

A-D (**see p12, saq instr**)

- A - ecom only, 3rd-party payment gateway
- C - in-house dedicated terminal, **no storage**
- D - in-house systems, ecom w storage, **service providers**, …

A is easy (13q), C (41q) & D (225q) **extensive**

Storage of payment info

No problem (not sensitive): Cardholder Name, 1st 6 digits, last 4 digits, expiration, address, auth. Usually enough for refunds, renewals.

Sensitive (SAQ D): more digits than above.

- **Must encrypt DB, backups. PAIN.**

Prohibited: CVVC (3-digit code MC/Visa, 4-digit Amex front). MagStripe. PINs.

- **May never store**!

SAQs

- A - **discuss** pp 7-10 (parts 2b-3)
- C - adds network & physical security, ASV scans, extensive documentation of policies & procedures, ...
- D- adds Code Reviews, code security audits / WAF, more.

Compliance

- SAQ with statement of compliance (signed by Officer.) submitted to processor/bank.
- Schedule required if not compliant.
- "Compensating Controls" optional for non-compliant items. Must be documented.

Application Security Recommendations

Even if using 3rd-party gateway, someone could still redirect your payments.

1. Choose a **trusted, secure hosting provider** – preferably one which claims and promotes PCI compliance. Cheap, shared hosts are unlikely to comply.
2. Use security best practices when setting **passwords (WP, ssh/sftp, DB)** and **limit access** to your server.
3. **implement SSL** to help keep your checkout secure.
4. Keep installed plugins to a minimum; **compliance covers all installed software** incl WP, plugins, themes

Application Security Recommendations, cont.

5. Keep OS, Apache, WP, plugins, themes **up to date** to ensure latest security fixes are present.
6. (SAQ C) Use an ASV (approved scanning vendor) to scan your site and find issues – fixing any identified issues until passing the scan.
7. (recommended) scan yourself, using Web Application Vulnerability Scanner(s) - Acunetix, Nikto, et al.

Also run a network scanner (nmap) and make sure MySQL, Telnet, FTP, etc. are closed/firewalled.

Many of these should be done for any site, eCom or not.

WordPress Security

Choose your plugins carefully.

"7 out of top 10 most popular e-commerce plugins are vulnerable to common Web attacks

"20% of the 50 most popular WordPress plugins are vulnerable to common Web attacks"

- CheckMarx, June 2013

Many WP Themes have vulnerabilities as well.

Stuck?

- Hire a security professional or a QSA (Qualified Security Assessor).

- QSAs are formally recognized by PCI, and are insured.

  However, IME, they charge a fortune and aren't always very helpful.

- Ultimately, **you are responsible**, not the consultant/QSA.

Questions?

Questions?

Future Presentations?:

- bug in WP SQL generator
- more PCI
- WP security / lockdown

Contact me:

Barry@BlogSec.net

http://BlogSec.net

WP Security News

Ars Technica reports a BotNet with 90,000 IP addresses is trying to brute-force WordPress installs via password guessing.

Recommendations:

- disable or rename default admin accounts
- use strong passwords
- limit the number of admin / network admin accounts
- install a plugin such as Limit Login Attempts