PCI Compliance and YOU!

Rachel Makrucki
(m_rookie)

Disclaimer!!!!!!!!!!!!

I am not a QSA or a registered security expert
Presentation created based on our experience
Please consult with a qualified security assessor to make sure that your set up is indeed PCI Compliant

What is PCI Compliance

PCI stand for Payment Card Industry
PCI is a set of security standards jointly agreed upon by the major credit card vendors
(VISA, AMEX, MC, DSC)
These standards apply to any business that accepts credit cards in ANY FASHION

MORE on the standard go to :
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

PCI Compliance VS Security

PCI Compliance  Security

Good security measures ensure that you remain PCI Compliant.

Most Important

- Document Document Document
  - If a policy procedure or security setting is not on paper it never happened.

- Keep up on your network scans
  - Make sure that you are getting the results of the scans sent to you and that all vulnerabilities are documented and a plan to correct them is in place and DOCUMENTED

- NEVER SAVE FULL CREDIT CARD NUMBERS! EVER
  - While the PCI documentation has instructions for the storage of CC numbers after authorization; JUST SAY NO!

PCI vs PADSS and Drupal

- PADSS guidelines are placed on payment applications that are sold to consumers
- Good News -- Drupal does not have to be PADSS Certified because if fall under GPL
- Bad News -- You are responsible for the code as if you wrote it.

Treat it as if you wrote it

If you find security issues in any module (core or contributed)
You are responsible to fix it (according to PCI standards)
Document what you have found, attempt to fix the issue. Report it to the security team and supply a patch if you were successful in fixing the issue.

Subscribe to drupal security updates (required) -- http://drupal.org/security

You must update ever module that has a listed security patch as soon as possible.

Biggest Challenges

Creating required documentation

Implementing Developer requirements

Separate people to develop and deploy

Building security

Proving compliance to our payment processor

Total Project Time: 6.5 Months to Compliance
Daily Maintenance to remain compliant

Final Notes

Get the help of a Qualified Security Assessor

Compliance is a continuing process, you must be able to prove on any given day that you are compliant

These ARE NOT government regulations
... BUT
There are consequences for non-compliance

Know you merchant level
Majority in this room qualify as level 4 merchant.

Create a plan and DOCUMENT DOCUMENT DOCUMENT

Questions

twitter: http://www.twitter.com/m_rookie

drupal.org: m_rookie

IRC: m_rookie

Email: rachel.makrucki@gmail.com

If you have more specific questions please feel free to contact me, or stop me after the session

Thanks!