



— DRUPALCON —

DENVER

MARCH 19-23, 2012

Collaborative Publishing for Every Device

**PCI:
A Four-Letter
Word of
E-Commerce**

Presented by Matt Kleve (vordude)



ALL

CREDIT

CARDS GOOD

WHERE

Who is this guy?



- 5 years of Drupal
- Been in the PCI 'trenches'
- Drupal Security Team
- Senior Developer, Lullabot



Consulting | Development | Training



FASTCOMPANY



Sony Music



O'REILLY®

The Economist



The Washington Post



Warning, this guy is **not**:



- A PCI Qualified Security Assessor (QSA)
- A lawyer
- Willing to provide references or suggestions for web hosting, scanning vendors, consultants, etc.



Once upon a time...





DANGER
EYE PROTECTION
REQUIRED
BEYOND THIS POINT

WARNING
PERSONNEL HAZARD
KEEP MOVING



Payment Card Industry (PCI) Data Security Standard



Requirements and Security Assessment Procedures

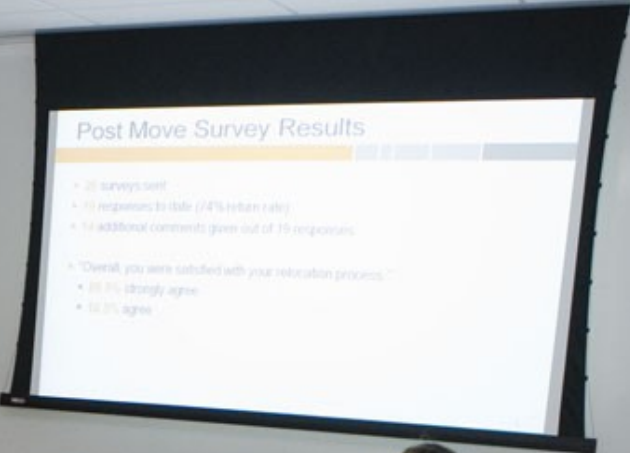
Version 2.0

October 2010









What is this PCI Thing?



- **P**ayment **C**ard **I**ndustry
- **D**ata **S**ecurity **S**tandard

(PCI-DSS)
(Not the PA-DSS)

What is this PCI Thing?



**Are you Transmitting, Processing,
or Storing Credit Card Data?**

It applies to you.

Heartland data breach damages still mounting

Visa removes processor from PCI-compliant list

By Seamus McAfee

More than two months after the first announcement of the Heartland Payment Systems security breach, the processor has continued to draw fire from merchants and issuers. Damages from what may be the largest PCI data breach in history continue to snowball into public relations disputes, lawsuits and government probes aimed at the company.

Card processing giant Visa on March 23 delivered a public slap to Heartland, a leading processor of credit and debit payments, by temporarily removing it from Visa's list of service providers that comply with Payment Card Industry Data Security Standards (PCI DSS). PCI compliant service providers adhere to a strict set of data security standards to protect consumers' card information and fight identity theft and fraud.

Visa has questioned Heartland's [security compliance](#), especially at the time the processor was breached in 2008, saying no merchant that has been PCI compliant has been compromised. Heartland has countered that it was validated for PCI a month before the breach is thought to have begun, and critics have [said](#) Visa may be simply trying to dodge questioning of itself and its favored security standard. Visa indicated that it would re-place Heartland on its list of PCI compliant processors as soon as the company meets the standards, which Heartland CEO Robert O. Carr [said](#) his company could achieve in weeks.

The breach

Visa's move is one in a long string of events since Jan. 20, 2009, when, after being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, Heartland announced that malicious software had compromised its data in 2008. The data potentially exposed through this breach includes card numbers, expiration dates and other data from the card's magnetic stripe, and in some cases, the names of customers who used



Heartland data breach damages still mounting

Visa removes processor from PCI-compliant list

By Seamus McAfee

More than two months after the first announcement of the Heartland Payment Systems security breach, the processor has continued to draw fire from merchants and issuers.

◆ Heartland faces dozens of [lawsuits](#) in federal and district courts,

removed a public slap to Heartland, a leading processor of credit and debit payments, by temporarily removing it from Visa's list of service providers that comply with Payment Card Industry Data Security Standards (PCI DSS). PCI compliant service providers adhere to a strict set of data security standards to protect consumers' card information and fight identity theft and fraud.

Visa has questioned Heartland's [security compliance](#), especially at the time the processor was breached in 2008, saying no merchant that has been PCI compliant has been compromised. Heartland has countered that it was validated for PCI a month before the breach is thought to have begun, and critics have [said](#) Visa may be simply trying to dodge questioning of itself and its favored security standard. Visa indicated that it would re-place Heartland on its list of PCI compliant processors as soon as the company meets the standards, which Heartland CEO Robert O. Carr [said](#) his company could achieve in weeks.

The breach

Visa's move is one in a long string of events since Jan. 20, 2009, when, after being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, Heartland announced that malicious software had compromised its data in 2008. The data potentially exposed through this breach includes card numbers, expiration dates and other data from the card's magnetic stripe, and in some cases, the names of customers who used



Heartland data breach damages still mounting

Visa removes processor from PCI-compliant list

By Seamus McAfee

More than two months after the first announcement of the Heartland Payment Systems security breach, the processor has continued to draw fire from merchants and issuers.

- Heartland faces dozens of [lawsuits](#) in federal and district courts,

...announced a public slap to Heartland, a leading processor of credit and debit payments, by temporarily removing it from Visa's list of service providers that comply with Payment Card Industry Data Security Standards (PCI DSS). PCI compliant service providers adhere to a strict set of data security standards to protect consumers' card information and fight identity theft and fraud.



Heartland announced it has fallen subject to **formal inquiries** by the Securities and Exchange Commission, the Federal Trade Commission, the U.S. Department of the Treasury's Office of the Comptroller of the Currency, as well as an investigation by the U.S. Department of Justice.

...critics have [said](#) Visa may be simply trying to dodge questioning of itself and its favored security standard. Visa indicated that it would re-place Heartland on its list of PCI compliant processors as soon as the company meets the standards, which Heartland CEO Robert O. Carr [said](#) his company could achieve in weeks.



The breach

Visa's move is one in a long string of events since Jan. 20, 2009, when, after being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, Heartland announced that malicious software had compromised its data in 2008. The data potentially exposed through this breach includes card numbers, expiration dates and other data from the card's magnetic stripe, and in some cases, the names of customers who used

debit or credit cards at Heartland's network of 250,000 businesses.

Heartland data breach damages still mounting

Visa removes processor from PCI-compliant list

By Seamus McAfee

More than two months after the first announcement of the Heartland Payment Systems security breach, the processor has continued to draw fire from merchants and issuers.

- Heartland faces dozens of [lawsuits](#) in federal and district courts,

delivered a public slap to Heartland, a leading processor of credit and debit payments, by temporarily removing it from Visa's list of service providers that comply with Payment Card Industry Data Security Standards (PCI DSS). PCI compliant service providers adhere to a strict set of data security standards to protect consumers' card information and fight identity theft and fraud.



Heartland announced it has fallen subject to **formal inquiries** by the Securities and Exchange Commission, the Federal Trade Commission, the U.S. Department of the Treasury's Office of the Comptroller of the Currency, as well as an investigation by the U.S. Department of Justice.

critics have [said](#) Visa may be simply trying to dodge questioning of itself and its favored security standard. Visa indicated that it would re-place Heartland on its list of PCI compliant processors as soon as the company meets the standards, which Heartland CEO Robert O. Carr [said](#) his company could achieve in weeks.



Heartland's [stock value](#) has plunged since the announcement of the breach,

Heartland announced that malicious software had compromised its data in 2008. The data potentially exposed through this breach includes card numbers, expiration dates and other data from the card's magnetic stripe, and in some cases, the names of customers who used

debit or credit cards at Heartland's network of 250,000 businesses.

What is this PCI Thing?



“But I don't handle 5% of the payments the big guys do”

What is this PCI Thing?



- > 80% of the instances of unauthorized access to card data have involved small merchants
- These businesses account for 85% of the total number of merchants

What is this PCI Thing?



- Malicious attacks were the root cause of 31% of the data breaches
- Average cost is \$214 per compromised record

What is this PCI Thing?




“The credit card provider is generally liable only if the retailer was PCI-compliant at the time the security breach occurred.”

Protecting Credit Card Data:
How to Achieve PCI Compliance
Motorola White Paper

Sony PlayStation suffers massive data breach

 Recommend

 3,171 people recommend this. Be the first of your friends.



By [Liana B. Baker](#) and [Jim Finkle](#)

NEW YORK/BOSTON | Tue Apr 26, 2011 7:36pm EDT

(Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

Sony learned that user information had been stolen from its PlayStation Network seven days ago, prompting it to shut down the network immediately. But Sony did not tell the public until Tuesday.

 Tweet 228

 Share 77

 Share this

 +1 0

 Email

 Print

Factbox

[Sony breach latest in string of cyber attacks](#)

Tue, Apr 26 2011

Analysis & Opinion

[Facebook scam warning pages under fire](#)

[Need a loan? 4 tips to improve your debt health](#)


Related Topics

[Tech »](#)

[Media »](#)

Sony PlayStation suffers massive data breach

 Recommend

 3,171 people recommend this. Be the first of your friends.



Shaun Sullivan

@LiquidSullivan

 Follow



If you have a Playstation 3, change all your passwords on all your Internet services. I already detected access from an IP in China on mine

1

RETWEET



7:16 AM - 28 Apr 11 via web · Embed this Tweet 

 Reply  Retweet  Favorite

Sony learned that user information had been stolen from its PlayStation Network seven days ago, prompting it to shut down the network immediately. But Sony did not tell the public until Tuesday.

[Tech »](#)
[Media »](#)

What is this PCI Thing?



Financial Risk

Reputation Risk

What is this PCI Thing?



12 Requirements

“The Dirty Dozen”

What is this PCI Thing?



Requirement 1:

Install and maintain a firewall configuration to protect cardholder data

What is this PCI Thing?



Requirement 2:

Do not use vendor-supplied defaults for system passwords and other security parameters

What is this PCI Thing?



Requirement 3:

Protect stored cardholder data

What is this PCI Thing?



Requirement 4:

Encrypt transmission of
cardholder data across
open, public networks

What is this PCI Thing?



Requirement 5:

Use and regularly update anti-virus software or programs

What is this PCI Thing?



Requirement 6:

Develop and maintain secure systems and applications

What is this PCI Thing?



Requirement 7:

Restrict access to cardholder data
by business need to know

What is this PCI Thing?



Requirement 8:

Assign a unique ID to each person with computer access

What is this PCI Thing?



Requirement 9:

Restrict physical access to cardholder data

What is this PCI Thing?



Requirement 10:

Track and monitor all access to network resources and cardholder data

What is this PCI Thing?



Requirement 11:

Regularly test security systems and processes.

What is this PCI Thing?



Requirement 12:

Maintain a policy that addresses information security for all personnel

Basic PCI DSS Principles



- Do not store cardholder data unless it's absolutely necessary
- Never store "Verification Code," "Full Track," or "PIN"
- The first six and last four digits are the maximum number of digits to be displayed.

Basic PCI DSS Principles



Document everything

Basic PCI DSS Principles



Get it in writing from your vendors or service providers.

Basic PCI DSS Principles



You are never done

Assess → Remediate → Report



its sum.

21

of its nth term as $n \rightarrow \infty$.

. Actually I don't know
to do this

s sum.

$$\frac{8}{5/6} = \frac{48}{1} \rightarrow 48$$

tes the statement or answers the question.

Merchant, Know Thyself



Which SAQ?

- SAQ-A
- SAQ-B
- SAQ-C
- SAQ-C-VT
- SAQ-D

Merchant, Know Thyself



Which SAQ?

- SAQ-A – All sensitive data handling offloaded
- SAQ-B – Manual Paper Pushing, no Internet
- SAQ-C – “Standard” e-commerce setup
- SAQ-C-VT – “Virtual Terminal”
- SAQ-D – “Other”

Merchant, Know Thyself



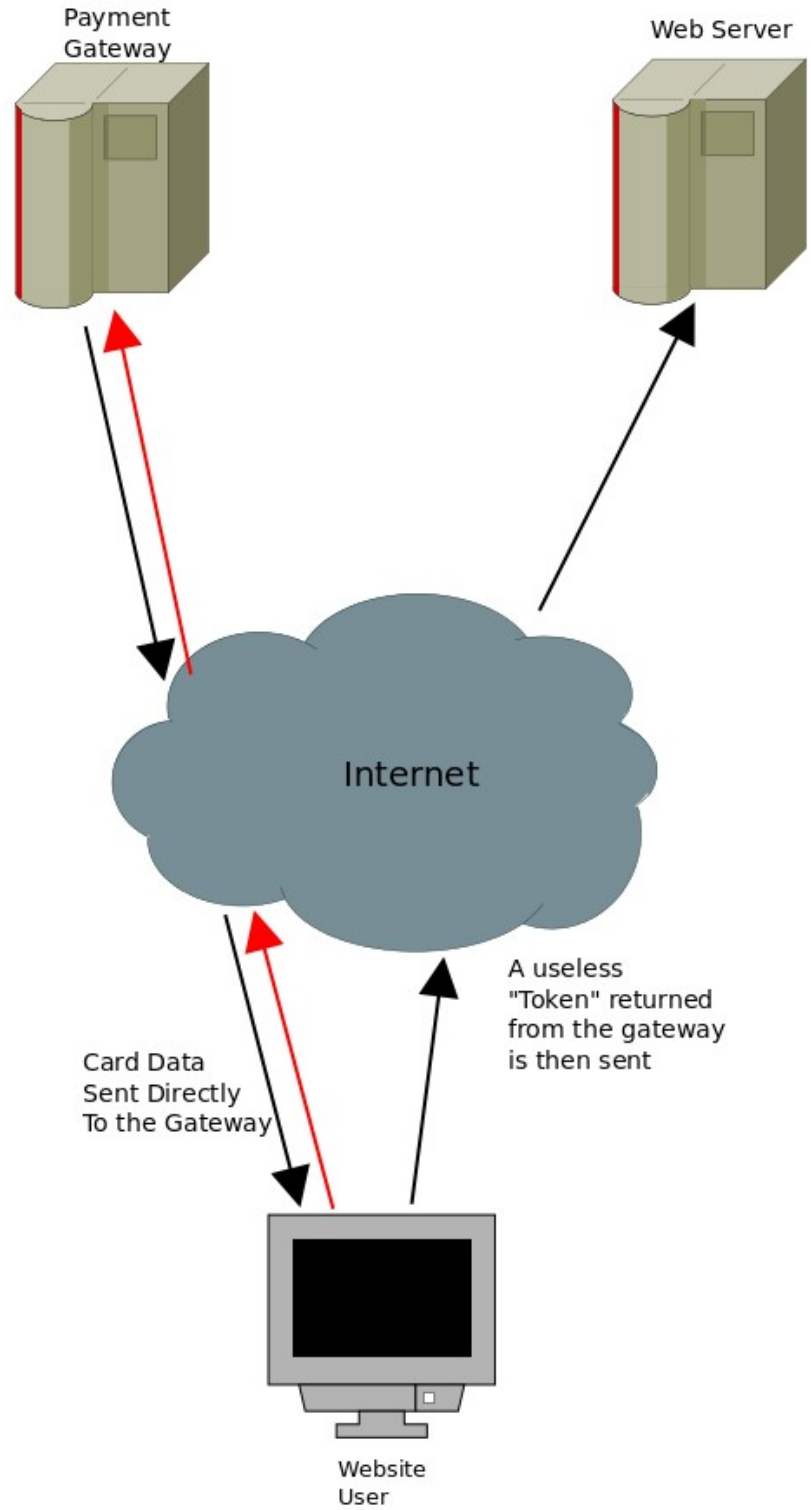
Which SAQ?

- SAQ-A – All sensitive data handling offloaded
- SAQ-C – “Standard” e-commerce setup
- SAQ-D – “Other”

SAQ-A



- **14 Questions (2 of the 12 Requirements)**
- **Physical Security**
- **Information Security Policy**



Payment Gateway

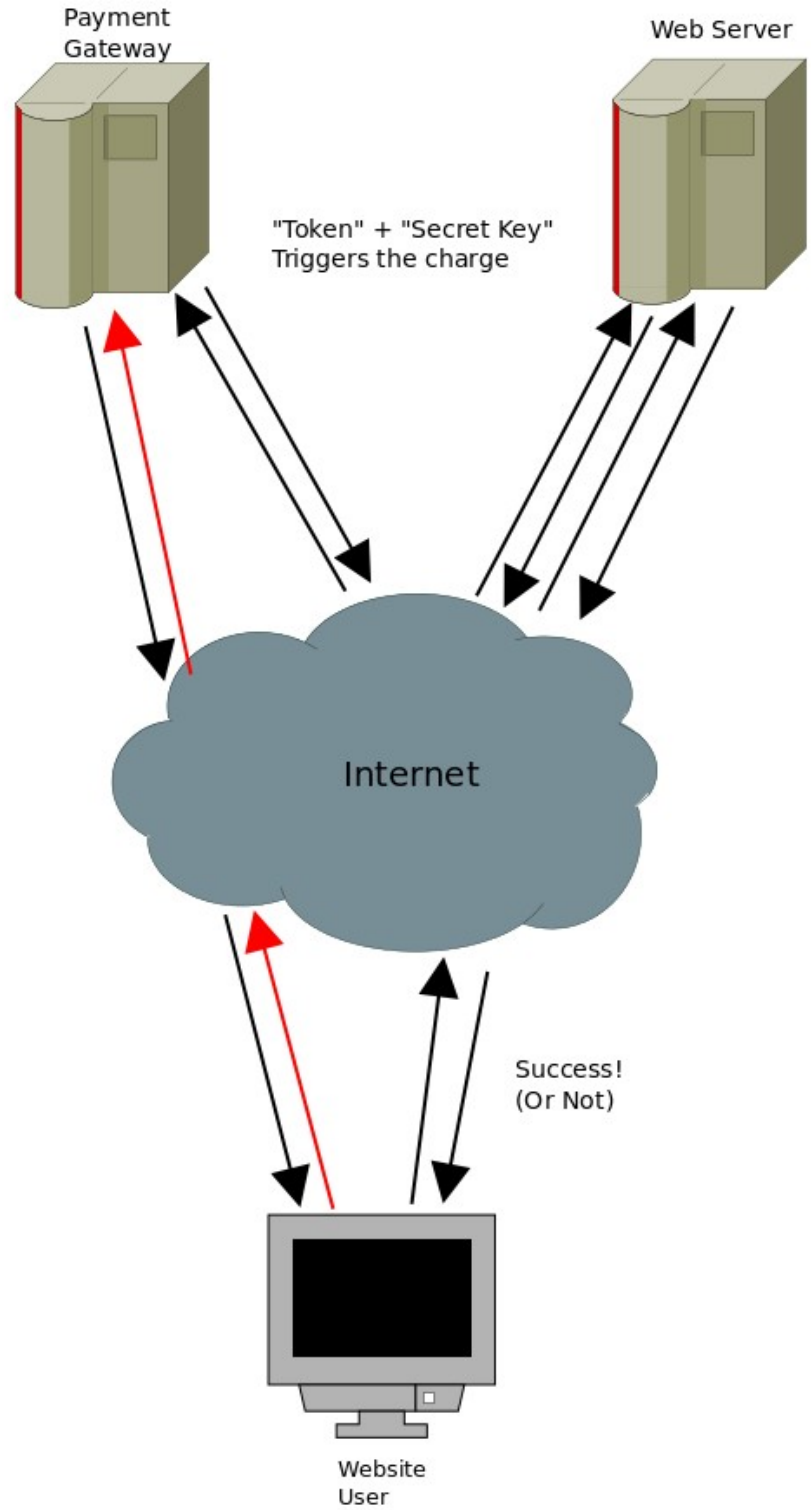
Web Server

Internet

Card Data Sent Directly To the Gateway

A useless "Token" returned from the gateway is then sent

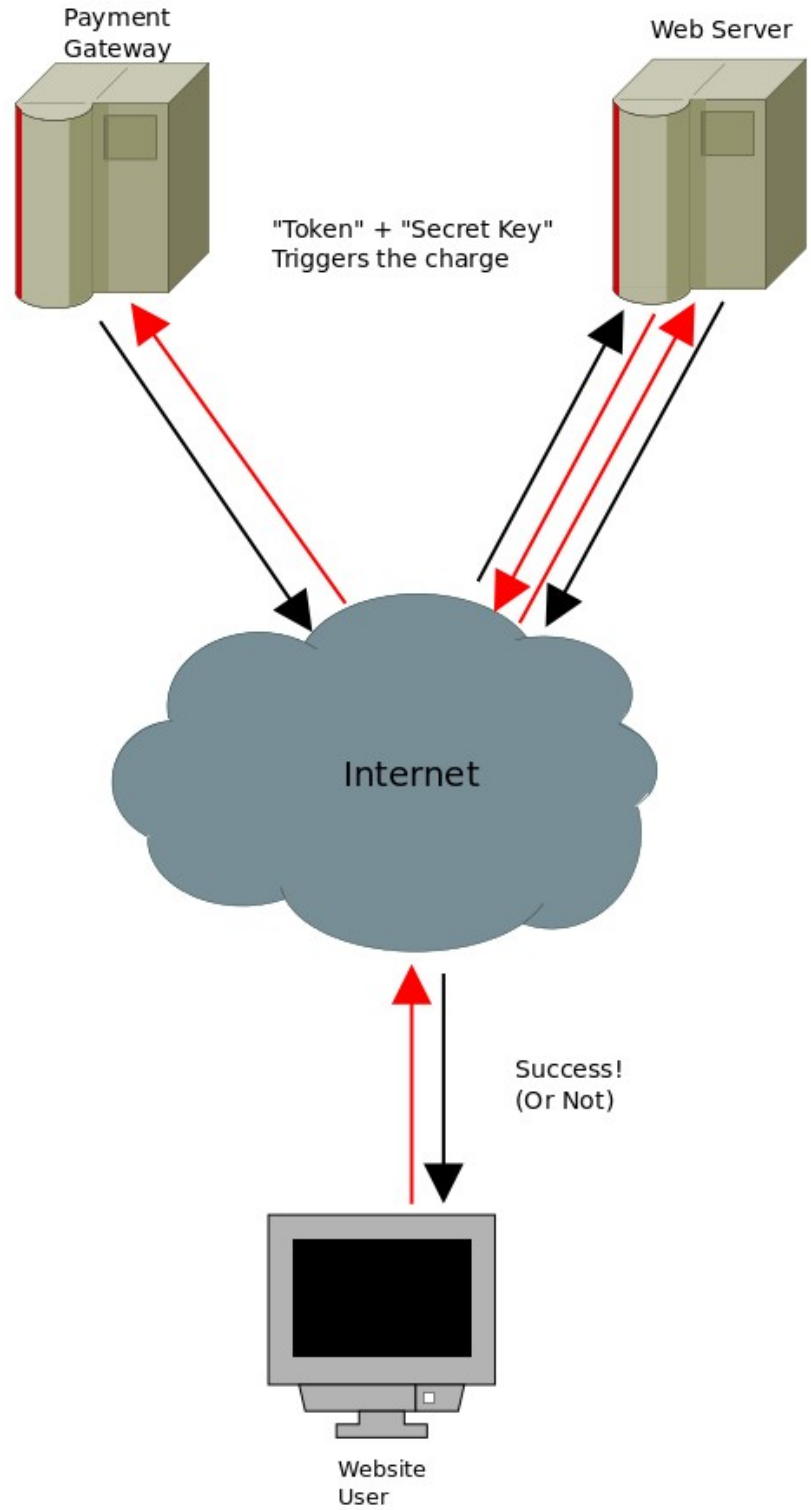
Website User



SAQ-C



- **85 Questions (11 of the 12 Requirements)**
- **Securing Sensitive Data**
- **Monitoring and Testing**



SAQ-D



- **~225 Questions (12 of the 12 requirements)**
- **Intense review of everything**
- **Sensitive data storage**

Merchant, Know Thyself



Merchant “Levels”

- “Level” 1-4
- Each card brand sets its own rules
- “Level Reciprocity” among the brands
(Highest common denominator)

Merchant, Know Thyself



Level / Tier	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region ²	<ul style="list-style-type: none">• Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or internal auditor if signed by officer of the company• Quarterly network scan by Approved Scan Vendor ("ASV")• Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	<ul style="list-style-type: none">• Annual Self-Assessment Questionnaire ("SAQ")• Quarterly network scan by ASV• Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	<ul style="list-style-type: none">• Annual SAQ• Quarterly network scan by ASV• Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	<ul style="list-style-type: none">• Annual SAQ recommended• Quarterly network scan by ASV if applicable• Compliance validation requirements set by acquirer

Merchant, Know Thyself



Level 1

- Annual Report on Compliance (by a QSA)
- Full security assessment of procedures
- > 6 million transactions (per type)
- Previous data breach

Merchant, Know Thyself



Level 2

- 1-6 Million transactions (per type)
- June 30, 2012 deadline. (Mastercard)
SAQ must be done by a QSA or a certified ISA

Merchant, Know Thyself



Level 3-4

- Quarterly Security Scans
- Complete **S**elf **A**ssessment **Q**uestionnaire



Merchant, Know Thyself



The Bottom Line:

Your payment processor
(acquirer)
has the final say.



Yes, but what about Drupal?



- It's open source.
- You've customized it.
- You need to treat it like it's 100% your code.
- Get very familiar with Requirement #6.

```
function commerce_payment_method_instance_load($instance_id) {
    // Return FALSE if there is no pipe delimiter in the instance ID.
    if (strpos($instance_id, '|') === FALSE) {
        return FALSE;
    }

    // Explode the method key into its component parts.
    list($method_id, $rule_name) = explode('|', $instance_id);

    // Return FALSE if we didn't receive a proper instance ID.
    if (empty($method_id) || empty($rule_name)) {
        return FALSE;
    }

    // First load the payment method and add the instance ID.
    $payment_method = commerce_payment_method_load($method_id);
    $payment_method['instance_id'] = $instance_id;

    // Then load the Rule configuration that enables the method.
    $rule = rules_config_load($rule_name);

    // Iterate over its actions to find one with the matching element ID and pull
    // its settings into the payment method object.
    $payment_method['settings'] = array();

    foreach ($rule->actions() as $action) {
        if ($action->getElementName() == 'commerce_payment_enable_' . $method_id) {
            if (is_array($action->settings['payment method']) && !empty(
```




Yes, but what about Drupal?



cache_form

```
mysql> describe cache_form;
+-----+-----+-----+-----+-----+-----+
| Field          | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| cid            | varchar(255)  | NO   | PRI |          |       |
| data           | longblob      | YES  |     | NULL     |       |
| expire         | int(11)       | NO   | MUL | 0        |       |
| created        | int(11)       | NO   |     | 0        |       |
| serialized     | smallint(6)  | NO   |     | 0        |       |
+-----+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

mysql>
```

Yes, but what about Drupal?



Doing It Wrong



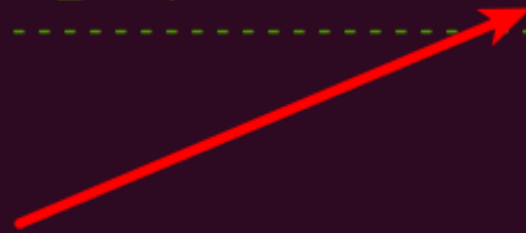
Yes, but what about Drupal?



\$_SESSION

ssid	hostname	timestamp	cache	session
PDNDrWI	127.0.0.1	1332307185	0	cc_num s:16:"4111111111111111";

ಠ_ಠ



Yes, but what about Drupal?



Session Hijack (mixed HTTP / HTTPS)



Download & Extend

[Download & Extend Home](#)[Drupal Core](#)[Modules](#)[Themes](#)[Translations](#)[Installation Profiles](#)

PCI Update

[View](#)[Version control](#)[Edit](#)[Outline](#)[Revisions](#)[Automated Testing](#)

Posted by [bendodd](#) on *September 27, 2011 at 12:14pm*

A simple module to encompass updates to Drupal to satisfy vulnerabilities reported by Approved Scan Vendors (ASV), often as a result of the PCI DSS compliance processes.

Currently this module only affects the login form, but will be a home for updates as they are identified in the future

Downloads

Recommended releases

Version	Downloads	Date	Links
7.x-1.0	tar.gz (7.34 KB) zip (7.76 KB)	2011-Oct-11	Notes Edit
6.x-1.1	tar.gz (7.34 KB) zip (7.76 KB)	2011-Oct-11	Notes Edit

Development releases

Version	Downloads	Date	Links
7.x-1.x-dev	tar.gz (7.34 KB) zip (7.77 KB)	2011-Oct-12	Notes Edit
6.x-1.x-dev	tar.gz (7.34 KB) zip (7.77 KB)	2011-Oct-12	Notes Edit

Project Information

Maintainers for PCI Update

[bendodd](#) - 5 commits

last: 23 weeks ago, first: 25 weeks ago

[View all committers](#)

[View commits](#)

Issues for PCI Update

To avoid duplicates, please search before submitting a new issue.

[Advanced search](#)

All issues

0 open, 2 total

Bug reports

0 open, 1 total

[Subscribe via e-mail](#)

[Issue statistics](#)

Yes, but what about Drupal?



XSS, SQL Injection, CSRF
and other vulnerabilities



Security advisories

[Drupal core](#)[Contributed projects](#)[Public service announcements](#)

These posts by the Drupal security team are also sent to the security announcements e-mail list.

SA-CORE-2012-001 - Drupal core multiple vulnerabilities

Posted by [Drupal Security Team](#) on February 1, 2012 at 10:06pm

- Advisory ID: DRUPAL-SA-CORE-2012-001
- Project: [Drupal core](#)
- Version: 6.x, 7.x
- Date: 2012-February-01
- Security risk: [Moderately critical](#)
- Exploitable from: Remote
- Vulnerability: Access bypass, Cross Site Request Forgery, Multiple vulnerabilities

[Read more](#)

Categories: [Drupal 6.x](#), [Drupal 7.x](#)

SA-CORE-2011-003 - Drupal core - Access bypass

Posted by [Drupal Security Team](#) on July 27, 2011 at 7:32pm

- Advisory ID: DRUPAL-SA-CORE-2011-003
- Project: [Drupal core](#)
- Version: 7.x
- Date: 2011-july-27
- Security risk: [Less critical](#)

Security announcements

All security announcements are posted to an email list as well. Once logged in, go to [your user profile page](#) and subscribe to the security newsletter on the *Edit » My newsletters* tab.

You can also get rss feeds for [core](#), [contrib](#), or [public service announcements](#) or follow [@drupalsecurity](#) on twitter.

Contacting the Security Team

In order to report a security issue, or to learn more about the security team, please see the [Security team handbook](#) page.

Writing Secure Code

If you are a Drupal developer, please read the handbook section on [Writing](#)

FEAR IS
NEVER A
GOOD REASON
TO DO
NOTHING

Your new TODO list:



- <https://www.pcisecuritystandards.org/>
- Download and read the standard
- Also Read “Navigating PCI DSS”
- Keep the “Glossary of Terms Abbreviations and Acronyms” close by.

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Response:	Yes	No	Special*
9.6	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Do controls include the following:		<input type="checkbox"/>		<input type="checkbox"/>
9.7.1	Is media classified so the sensitivity of the data can be determined?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7.2	Is media sent by secured courier or other delivery method that can be accurately tracked?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8	Are logs maintained to track all media that is moved from a secured area, and is management approval obtained prior to moving the media (especially when media is distributed to individuals)?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9	Is strict control maintained over the storage and accessibility of media?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.10	Is all media destroyed when it is no longer needed for business or legal reasons?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Is destruction performed as follows:		<input type="checkbox"/>		<input type="checkbox"/>
9.10.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Are containers that store information to be destroyed secured to prevent access to the contents? (For example,		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The Prioritized Approach to Pursue PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) provides a detailed, 12 requirements structure for securing cardholder data that is stored, processed and/or transmitted by merchants and other organizations. By its comprehensive nature, the standard provides a large amount of information about security – so much that some people who are responsible for cardholder data security may wonder where to start the continuous journey of compliance. Toward this end, the PCI Security Standards Council provides the following Prioritized Approach to help stakeholders understand where they can act to reduce risk earlier in the compliance process. No single milestone in the Prioritized Approach will provide comprehensive security or PCI DSS compliance, but following its guidelines will help stakeholders to expedite the process of securing cardholder data.





Questions?



What did you think?

Locate this session on the
DrupalCon Denver website

<http://denver2012.drupal.org/program>

Click the "Take the Survey" link.

THANK YOU!