Keeping the Bank Happy - PCIDSS v4.0.1

Peter Jakowetz - PrivSec Consulting Ltd

OWASP Day 2024

Thank You to Our Sponsors and Hosts!

BASTION

SECURITY GROUP

DATACOM

84.

plexure

Without them, this Conference couldn't happen.

Whoami.txt

- Peter Jakowetz
- Managing Director - PrivSec Consulting
- Ex-QSA, now a PCIP
- CISSP, CISA, CISM, OSCP, CIPM, CRISC, BEng Elect ...
- Wellingtonian

What's this talk about?

- What is PCI-DSS
- Why is it important
- Does it affect us in NZ?
- What’s new in v4 of the standard
- What are the basics?
- What should I know?
- What's new in the new v4 standard
- What you have to do on a regular basis
- How do you benefit by meeting the standard
- Resources!

Anyone who stores, process or transmits credit card data must meet the Payment Card Industry Data Security Standard (PCI DSS). But what does that actually mean, and what do you have to do? This talk will run through the requirements of the PCI standard with a developer slant.

What is PCI-DSS?

- Payment Card Industry Data Security Standard
- A set of minimum requirements for those processing credit card payments
- There are other standards for those creating credit card processing hardware etc
- If you’re dealing with credit card details, you’re obligated to meet the standard by the card brands
- We’re up to version 4.0.1 of the standard

A little bit of history

- Been around since December 2004
- PCI Council:
  - American Express
  - Discover
  - JCB
  - Mastercard
  - Visa
  - (Now Union Pay as well)

Why is this important?

- Keeps you off the front page of the news
- Stops you from being fined by the banks
- Keeps you being able to process credit card transactions
- Allows your business to function, so you can stay working!
- Socially responsible thing to do

Why is this important?

Achieving PCI compliance gives your business the assurance that customer data is safe and secure from any malicious activity or potential breaches, while also helping you to meet an international standard of protection.

I.e. You have to care if you want to take credit card payments!

But I just use a payment processor

- It's still relevant to you if you take payments through any of the following forms:
  - Through your call centre
  - Website
  - Payment terminals
  - Mobile app.
- Or you might be a service provider to someone who does this (i.e. run a data centre, firewall service, call centre service)
- If you store, process or transmit cardholder data, you have a requirement to meet the Payment Card Industry Data Security Standard (PCI DSS).

Data security standards

4.6 (a) Unless otherwise advised by us, you must comply with the data security standards, which, among other things, means that you must successfully complete the protocols for the data security standards within the timeframe stipulated by us or the card schemes;

ix. where there is a data breach, then in order to continue processing card transactions, you may be required to undergo a full Payment Card Industry Data Security Standard (**PCI DSS**) accreditation by an approved Qualified Security Assessor (QSA). All reasonable costs of this accreditation exercise must be paid by you;

Data security standards

3.7 (a) Unless otherwise advised by us, you must comply with the data security standards, which, among other things, means that you must successfully complete the protocols for the data security standards within the time frame stipulated by us or the card schemes; and

(b) You acknowledge and agree that:

(i) you have processes and procedures in place that meet the data security standards and you follow those processes and procedures; and

(ii) we are obliged to report all data breach events to card schemes, law enforcement agencies and/or New Zealand regulators. You grant irrevocable and enduring consent for the release of details of any such data breach to the aforementioned bodies; and

(iii) if you use a third party who is involved in processing, transmission or storage of your transactions, then you must ensure that the third party confirms to you on an ongoing basis that it meets the data security standards; and

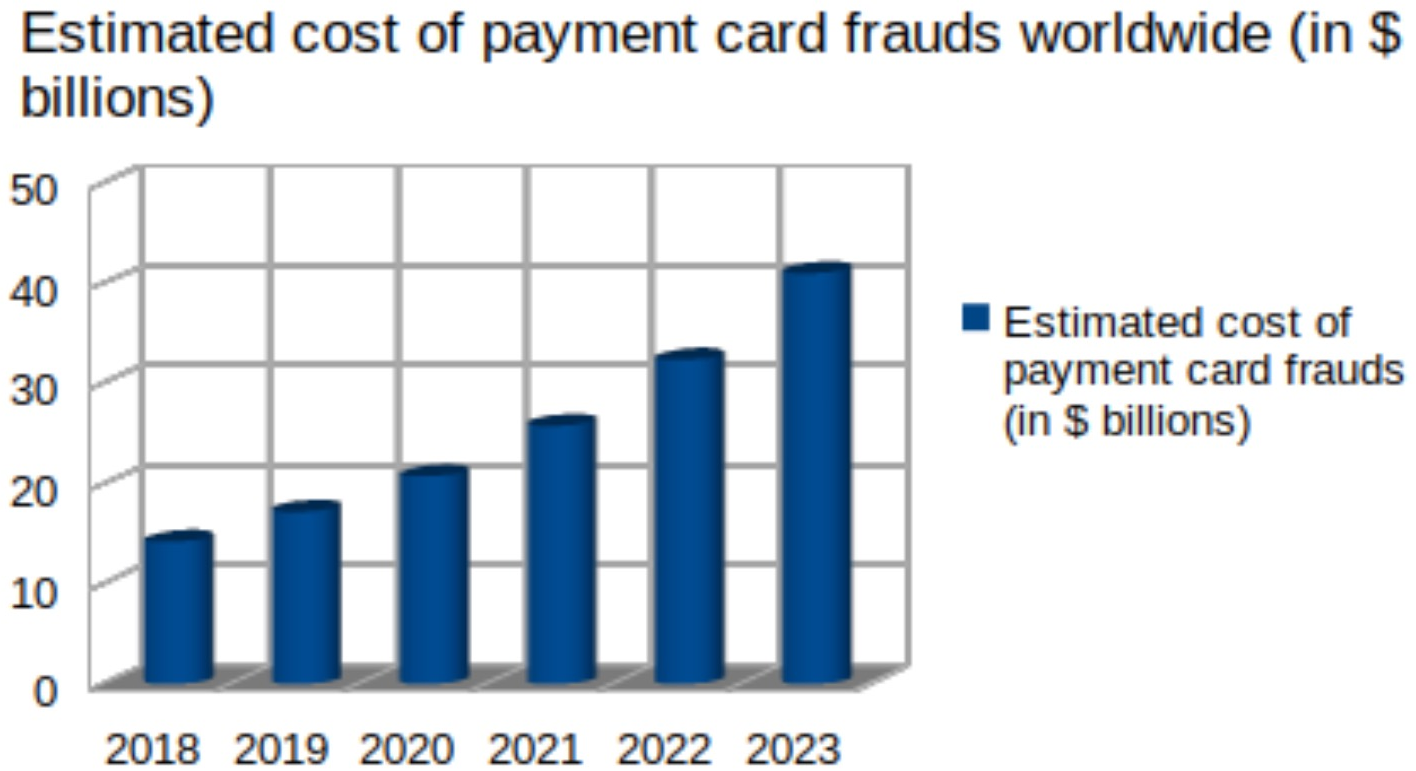
(iv) you will advise us immediately if you become aware of any data breach, whether suspected, potential, anticipated, attempted or actual relating to cardholder data held by you or on your behalf; and

How is This Weaponized?

- Steal data off credit card processing websites
- Sell it off at lower prices
- ~$45 a card – depends on quality of data
- Price depends on credit available, age, location etc

In 2018 – 444,602 cases of identity theft in US, 160’000 of those were credit card fraud.
Tripled in size between 2014 and 2018

Year	Estimated cost of payment card frauds (in $ billions)
2018	14.21
2019	17.18
2020	20.74
2021	25.75
2022	32.34
2023	40.95



Estimated cost of payment card frauds Continent wise (in $ billions)

Year	North America	South America	Europe	Asia	Africa	Australia
2018	9.74	0.96	1.83	1.22	0.35	0.09
2019	11.53	1.26	2.09	1.39	0.39	0.13
2020	13.88	1.57	2.48	1.61	0.44	0.17
2021	17.4	1.87	2.96	2.04	0.57	0.22
2022	22.62	2.22	3.52	2.44	0.7	0.26
2023	28.67	2.74	4.35	3	0.87	0.3

Examples of Breaches

Animates website forced offline after breach compromises customers' credit cards

21/09/2019 Katie Fitzgerald

Watch: Kiwis lost $33 million to scams in 2018. Credits: Image - Animates; Video - The AM Show

More fraudulent transactions reported following Kathmandu website data breach

By Aimee Shaw
Business Reporter · NZ Herald · 18 Mar, 2019 12:01 PM · 4 mins to read

Save Share

Kathmandu Holdings was hit by a data security breach on one of its websites. Photo / File

A hacker gained access to 100 million Capital One credit card applications and accounts

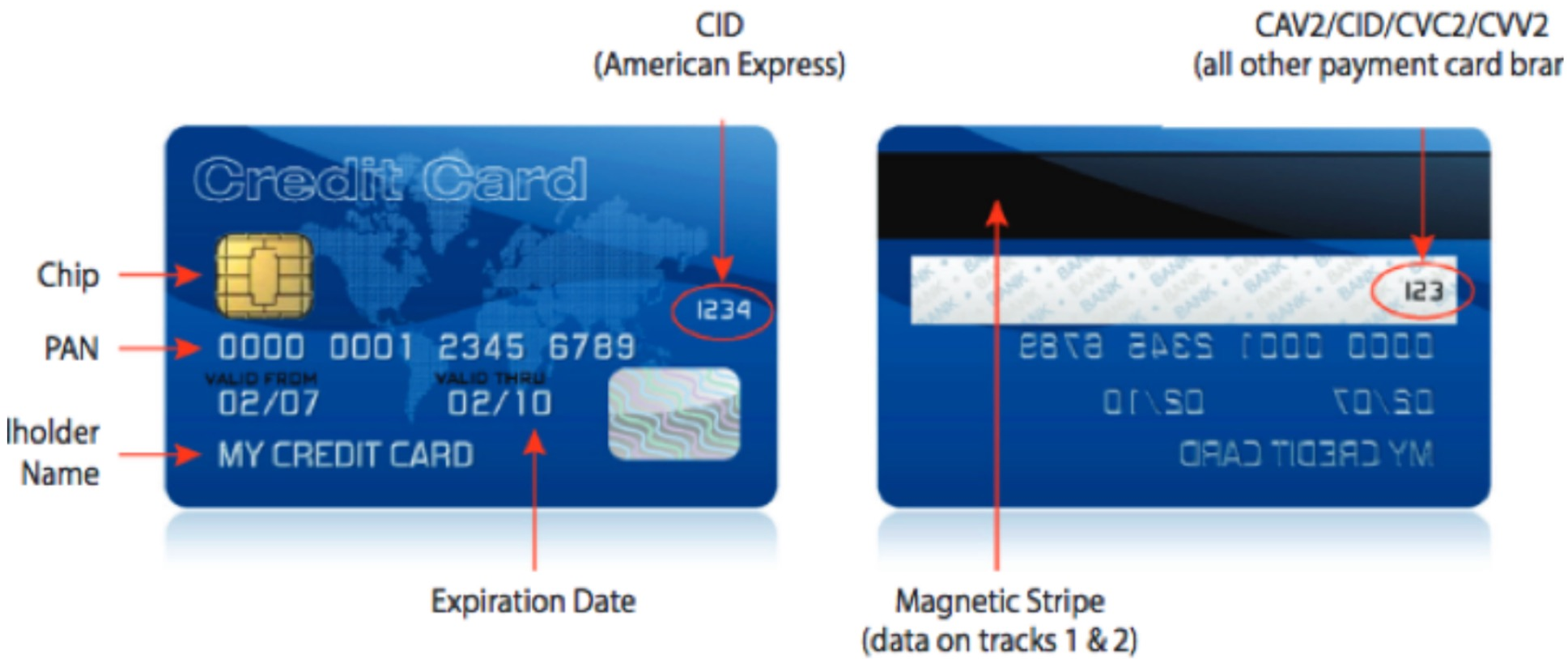
By Rob McLean, CNN Business

3 minute read · Updated 5:17 PM EDT, Tue July 30, 2019

BUT THE ACRONYMS!?!

- PCI – Payment card industry
- DSS – Data Security Standard
- QSA – Qualified Security Assessor & ISA - Internal Security Assessor
- ASV – Approved Scanning Vendor
- SAQ – Self Assessment Questionnaire
- AOC – Attestation of Compliance
- ROC – Report on Compliance
- CHD – Card holder data
- CDE – Card holder Data Environment

Types of Data on a Payment Card



Cardholder Data

- Primary Account Number (PAN)
- Cardholder Number
- Expiration Number
- Service Code

Sensitive Authentication Data

- Full magnetic stripe data or equivalent on a chip
- CAV2 / CVC2 / CVV2 / CID
- PINs/ PIN block

Terminology

- Acquiring bank (merchant bank) – maintains the merchants bank account
- Issuing bank – issues credit card to consumer on behalf of the card brands
- Card brands – Visa, Mastercard, AMEX etc
- Payment Gateway – card not present version of a POS terminal

Changes in the New Standard (v4)

- **Continue to meet the security needs of the payments industry** - Security practices must evolve as threats change.
- **Promote security as a continuous process** - Criminals never sleep. Ongoing security is crucial to protect payment data
- **Increase flexibility for organisations using different methods to achieve security objectives** - Increased flexibility allows more options to achieve a requirement's objective and supports payment technology innovation.
- **Enhance validation methods and procedures** - Clear validation and reporting options support transparency and granularity.

Defined Approach Requirements	Defined Approach Testing Procedures	Purpose
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).	**11.4.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed in accordance with all elements specified in this requirement.	Internal penetration testing serves two purposes. Firstly, just like an external penetration test, it discovers vulnerabilities and misconfigurations that could be used by an attacker that had managed to get some degree of access to the internal network, whether that is because the attacker is an authorized user conducting unauthorized activities, or an external attacker that had managed to penetrate the entity's perimeter. Secondly, internal penetration testing also helps entities to discover where their change control process failed by detecting previously unknown systems. Additionally, it verifies the status of many of the controls operating within the CDE. A penetration test is not truly a "test" because the outcome of a penetration test is not something that can be classified as a "pass" or a "fail." The best outcome of a test is a catalog of vulnerabilities and misconfigurations that an entity
Customized Approach Objective	**11.4.2.b** Interview personnel to verify that the internal penetration test was performed by a qualified internal resource or qualified external third-party and that organizational independence of the tester exists (not required to be a QSA or ASV).	
Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.		

Changes in the New Standard - Customised Approach

- Organisations can now choose how to implement technology to achieve compliance.
- Custom implementation means companies now have the freedom to innovate their custom control strategy to achieve their own custom complaint pathway.
- This new requirement offers greater flexibility in adhering to the strict cybersecurity standards of PCI DSS.
- The customised approach allows organisations to determine the security controls used to meet a stated objective in PCI DSS.

Changes in the New Standard - Vulnerability Management

- PCI DSS version 4.0 broadens the scope of security vulnerabilities that need to be remediated in version 3.2.1, which only requires critical and high-risk vulnerabilities to be addressed.
- Now, all vulnerabilities must be fixed, regardless of their severity level, with the most critical being prioritised.
- This is because every vulnerability if exploited, can potentially facilitate a data breach impacting cardholder data.

Change in the New Standard - Use EDR/ AV Scanning

- Use EDR!
- To mitigate the threat of ransomware attacks and other malware-related cyberattacks, overcoming isolation strategies like air gaps, PCI DSSv4.0 requires all removable media devices, such as USBs and external hard drives, to be scanned with malware detection software
- Either when the device is connected, or on a continuous system scanning level while the device is connected.
- Everyone does this already, so it shouldn't be a problem eh...

Change in the New Standard - Training

- Ensure staff are trained every 12 months
- Review training annually to ensure it reflects your threat landscape
- Ensure training covers social engineering and phishing, as these are common attack vectors for breaches.

Change in the New Standard - Authentication

- Use more secure authentication methods
- MFA must be used to access the CDE
- MFA & Zero trust are among the most effective measures for protecting payment data

How is the Standard Built

- 300+ Controls
- 12 key areas

What are the Principles

Goal: Build and Maintain a Secure Network and Systems

- Install and Maintain Network Security Controls
- Apply Secure Configurations to All System Components

Goal: Protect Account Data

- Protect Stored Account Data
- Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Goal: Maintain a Vulnerability Management Programme

- Protect All Systems and Networks from Malicious Software
- Develop and Maintain Secure Systems and Software

Goal: Implement Strong Access Control Mechanisms

- Restrict Access to System Components and Cardholder Data by Business Need to Know
- Identify Users and Authenticate Access to System Components
- Restrict Physical Access to Cardholder Data

Goal: Regularly Monitor and Test Networks

- Log and Monitor all Access to System Components and Cardholder Data
- Test Security of Systems and Networks Regularly

Goal: Maintain an Information Security Policy

- Support Information Security with Organisational Policies and Programs

What Do *I* Need To Care About?

- That's great
- But what does that *actually* mean??
- What should I be focussing on in my dev/ devops job?


1

Document all the things (and assign ownership)

- Define your CDE
- Policies
- Designs
- Delegations
- Decisions
- Processes (and follow them)
- Strong information security policy & training

Harden all the things

- Restrict access
- Firewalls/ Network access control
- Implement MFA
- Put on change detection
- Log on them
- Alert on them
- Change default passwords and parameters
- Run AV/ EDR
- Patch

Avoid holding cardholder data (but when you do..)

- Encrypt all the things (at rest and in transit)
- Store your keys securely
- Segregate where you’re storing them
- Encrypt/ hash/ mask or trunk data

Secure Coding

- Internal penetration testing
- Internal vulnerability scanning
- Vulnerability Scanning (ASV scans)
- External penetration testing
- Code review
- Separate dev, test and prod environments
- Scan for card data in your network

Security Testing Types

The PCI DSS v4 standard requires the following testing types to be conducted:

- Internal Penetration Testing
- External Penetration Testing
- Segmentation Testing

This relates to the following requirements within the PCI DSS v4 standard:

- 11.4 - External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.
    - 11.4.2 - Internal penetration testing is performed:
    - 11.4.3 External penetration testing is performed:
    - 11.4.5 - If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

Coding Tips

- Address common coding vulns in software dev processes
  - Train developers annually in coding techniques
  - Develop apps based on secure coding guidelines [read: OWASP]
- Follow a change control process/ CI CD process & document changes
- Test after major changes
- Don’t leave test accounts in prod
- Peer review code – don’t mark your own homework

What are We Avoiding? (Section 6.2.4)

- Injection flaws (SQL etc)
- Attacks on data and data structures (i.e. buffer overflows)
- Attacks on cryptography usage
  Attacks on business logic
- XSS
- CSRF
- Attacks on access control mechanisms
- Attacks via. any 'high-risk' vulnerabilities

Restrict Access

- Limit access between test and prod
- Use strong passwords
- Use MFA
- Log access
- Restrict access
- Use unique IDs

Consider the other bits you touch (& document and record them!)

- Data center providers
- Firewall providers
- Payment processors
- Physical destruction companies

Regular Activities

Hod do I Report This?

PCI DSS MERCHANT LEVEL	NUMBER OF CARD SCHEME CARD TRANSACTIONS	PCI TOOLS REQUIRED TO BE COMPLETED
Level 1	More than 6 million card transactions per annum (any type of transaction)	• On-site review by a qualified security assessor **(annually)** • Network vulnerability scans by an approved scanning vendor **(quarterly)**
Level 2	More than 1 million but < 6 million transactions per annum (any type of transaction)	• On-site review by a qualified security assessor (QSA) or self-assessment by a qualified internal security assessor (ISA) **(annually)** • Network vulnerability scans by an approved scanning vendor **(quarterly)**
Level 3	More than 20,000 but < 1 million **e-commerce** transactions per annum	• Self-assessment questionnaire **(annually)** • Network vulnerability scans by an approved scanning vendor **(quarterly)**
Level 4	All other merchants	• Self-assessment questionnaire **(annually)** • Network vulnerability scans by an approved scanning vendor **(quarterly)**

But What SAQ?

SAQ DOCUMENT	DESCRIPTION OF PROCESSING
A	Card-not-present merchants (e-commerce or mail/telephone order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels*.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on a merchant's systems or premises.
B	Merchants using only standalone, dial-out terminals with no electronic storage and/or imprint machines with no electronic cardholder data storage.
B-IP	Merchants using only standalone, PTS-approved payments terminals with an IP connection to the payment processor, with no electronic cardholder data storage.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.
C	Merchants with payment application systems connected to the internet, no electronic cardholder data storage.
D	All merchants not included in descriptions for the above SAQ types.

Continuous Monitoring

- Can make life *much* easier
- What do you rely on a lot?
    - Network security controls
    - IDS/ IPS
    - Change detection mechanisms
    - Anti-malware solutions
    - Access Control
- If you can automate monitoring of these - then it's much easier to prove to your auditor you do all the good things
- Continuous log review will be a requirement from next year (2025)

Things to Consider

Don’t think of PCI as aspirational… think of it as the basics of what you need to do

- Limit the data you touch
- When you do touch cardholder data, keep it segregated and touching as few components as possible
- Don’t fall for: “AWS is PCI compliant so I’m sweet” – what about the bits you’ve developed that touch credit card data
- Be careful about saying “I’m ISO27001 compliant so I’ll be sweet for PCI” – they’re looking at 2 different things and the scopes aren’t often the same

How to Sell This to Your Boss

- They have to if they want to keep selling their services
- You'll likely get fined and you'll no longer be able to accept payment cards if you're not compliant with PCI DSS regulations

How Do *you* Benefit From the Standard?

- More training
- Budget to fix issues
- Budget to do things rights
- Warm fuzzies of doing things the right way!

What Tools Can I Leverage

You don’t have to pay a fortune to make this stuff happen

- Scan your own code using OpenVAS first to make sure it looks clean
- Check your https headers using sslscan
- Put ZAP into your CI CD pipeline for automated testing
- Search databases for cardholder data using regex searches

Resources

- https://www.owasp.org/images/5/5c/Pci-dss.pdf
- https://www.owasp.org/images/3/38/MeucciPciMilan09.pdf
- https://owasp.org/www-pdf-archive/OWASPNightFaspay.pdf
- https://owasp.org/ProjectReviews/review/pci_toolkit/index.html
- https://owasp.org/www-pdf-archive/Dallas_OWASP_9-11-2013.pdf

PCI Council Resource

- https://www.pcisecuritystandards.org/document_library
- https://docs-prv.pcisecuritystandards.org/Guidance Document/Penetration Testing/Penetration-Testing-Guidance-v1_1.pdf
- https://docs-prv.pcisecuritystandards.org/PCI DSS/Supporting Document/PCI-DSS-v4-0-At-A-Glance.pdf
- https://docs-prv.pcisecuritystandards.org/PCI DSS/Supporting Document/PCI_DSS-QRG-v4_0.pdf
- https://docs-prv.pcisecuritystandards.org/PCI DSS/Standard/PCI-DSS-v4-0-to-v4-0-1-Summary-of-Changes.pdf
- https://docs-prv.pcisecuritystandards.org/Guidance Document/Intro to PCI/PCI Data Storage Dos and Donts.pdf
- https://docs-prv.pcisecuritystandards.org/PCI DSS/Standard/PCI-DSS-v4_0_1.pdf

Useful Resources

- https://www.upguard.com/blog/pci-compliance
- https://www.bnz.co.nz/business-banking/support/merchant-services/pci-dss/guide-to-pci-dss-compliance

Thanks!