ACHIEVE PCI-DSS COMPLIANCE USING OWASP GUIDELINES

JOHANNA CURIEL

PAYMENT CARD INDUSTRY PROFESSIONAL (PCIP)

AGENDA

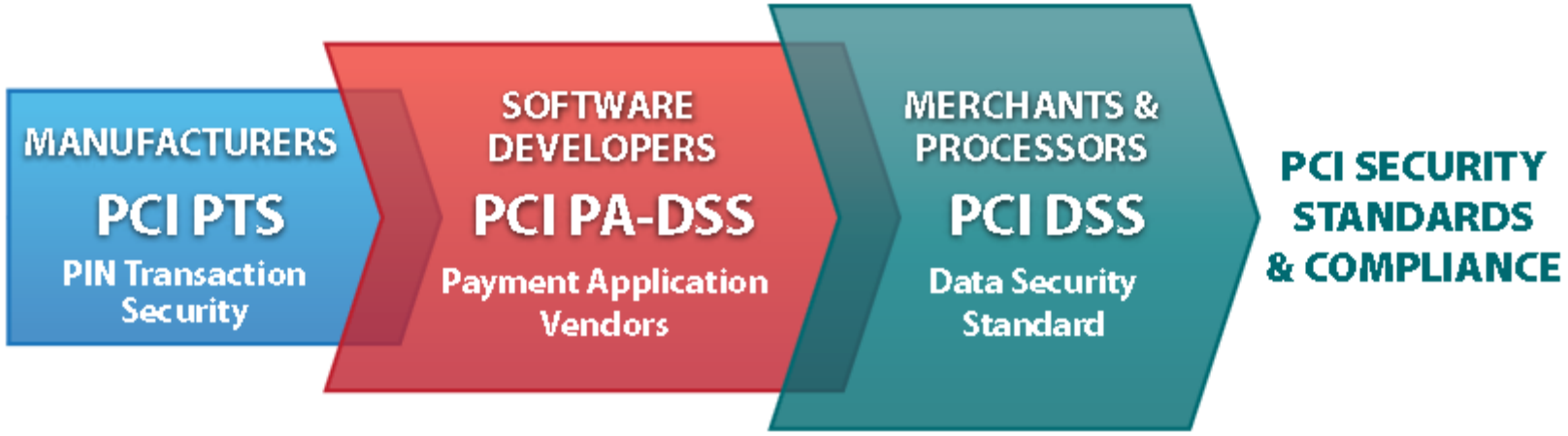
- Introduction to PCI-DSS requirements
- OWASP guidelines
- Wait: did you Scope?
- Case one: Bank ACME must be PCI-DSS compliant by 2014 : help me!
- To action : Requirement 6: Develop and maintain secure systems and application: HOW?
- Applying OWASP guidelines to PCI compliance and understanding the requirements
- Conclusions
- Questions

WHO? ME?

- Johanna Curiel
- Msc. In Security Engineer and OWASP evangelist for 2 years
- Contributions to XSS cheat sheets, Code Review, Google Summer of Code 2013 -2014
- Obtained Payment Card Industry Professional certificate in December 2013
- Helping organizations to implement and properly use OWASP guidelines to achieve PCI compliance

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

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

PCI-DSS REQUIREMENTS

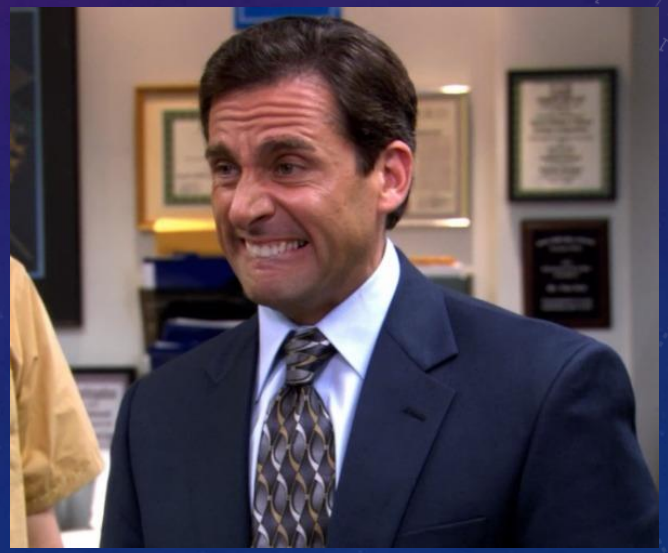
- 12 main requirements, more than 200 sub detail requirements
- You fail one: no compliance
- It’s all about the scope
- Understanding the scope process: most organizations fail at this
- Implementing changes : the painful part
- OWASP guidelines: Focusing on Requirement 6

GOAL: MAINTAIN A VULNERABILITY PROGRAM

- Requirement 6: Develop and maintain secure applications that applies to OWASP
- Case : Bank Acme
- Must achieve appliance and management is clueless on how to begin
- Different web applications

CASE BANK ACME: CISO TOM HAS A CHALLENGE

- CISO Tom has been assigned by the Board of directors to implement PCI-DSS
- Deadline from VISA : December 2016
- No idea where to begin.
- Has assigned his bright IT manager to work on it: John McGiver



AFTER 1 YEAR...2015

- John hasn’t been able to implement the any PCI-DSS requirement properly.
- Operations issues , daily troubleshooting and no resources has left him empty handed
- Approach: Secure everything
- ACME ‘s IT Developer team doesn't understand what is XSS, CSFR or SQL injections
- PCI-QSA auditor asks: Do you use OWASP? ANSWER: Did you said WASP, we kill them!
- CISO Tom will have a meeting with the board and must report the latest progress which are…

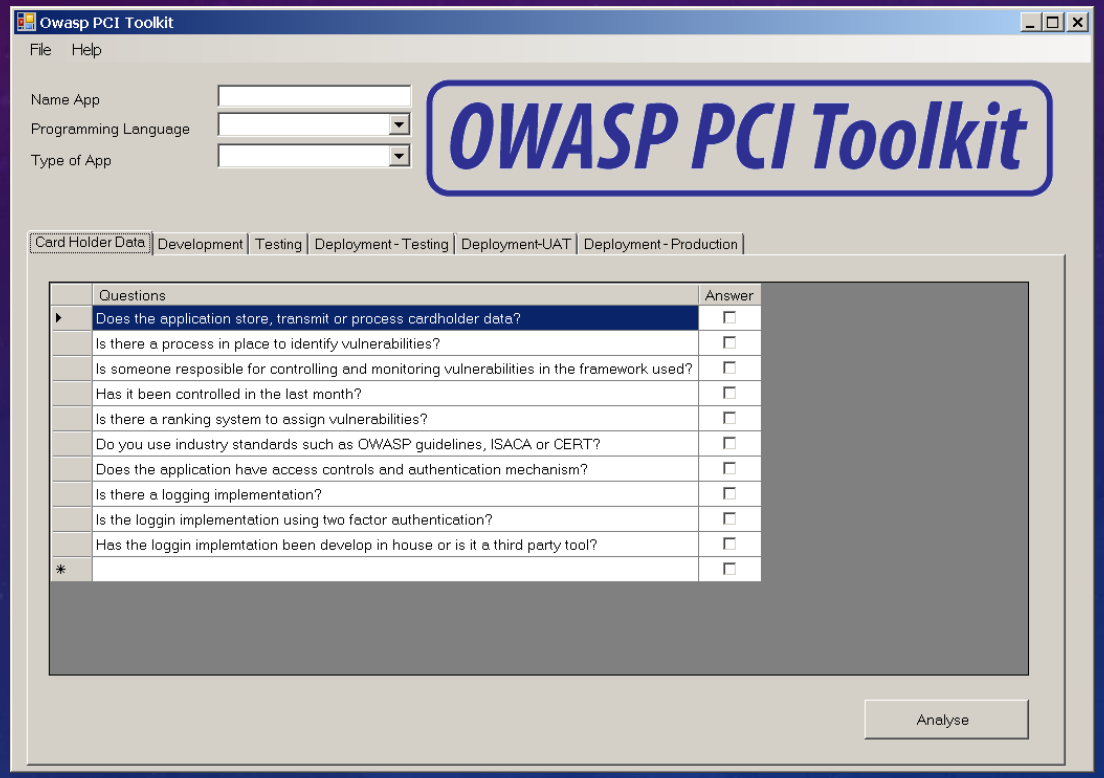
COMMITMENT IS EVERYTHING AND THEN THE SCOPE

- Management commitment is essential at all levels (financially, Operational and morally!)
- Scope is the second step. Divide and conquer
- Training and awareness: Join an OWASP chapter! Information is free of cost!

SCOPE: OWASP PCI TOOLKIT AND MORE

- Start with an inventory of :
- Network (and virtual) components,
- Applications internal or externally developed➔ Requirement 6
- Server & machines
- Remember: CARD HOLDER DATA ➔ Where is it?
- OWASP PCI toolkit: Help scope Web Apps and understand OWASP industry standards to PCI-DSS

OWASP PCI TOOLKIT



HOW DOES IT WORK

- Create a list or inventory of all web apps in your organization
- Are you using a complete development process? (Develop, Test, Deploy, standards)
- Answer the questions based on your process of development of apps per app
- Final analysis will determine if the app falls within the scope and which OWASP tools do you need to use per process

CONCLUSIONS

- Scoping is about deciding which applications are part or not of the PCI scope
- If part of the scope: are you using Industry standards?
- Knowing and understanding the standards is essential
- Knowing which tools you can use makes your life easier for compliance
- Achieve compliance faster
- Questions?