Usando OWASP para cumplir PCI-DSS

Mauro Flores
OWASP Global Industry Committee
OWASP PCI Project
OWASP Uruguay Chapter Co-Leader
Mauro.flores@owasp.org

@mauro_fcib

AppSec Latam '11

The OWASP Foundation

http://www.owasp.org

Motivación

- ✓ PCI es un medio para acercar la OWASP a la industria
- X OWASP tiene más de 200 proyectos
- X Usabilidad de la Wiki
- X Es difícil saber que materiales del OWASP pueden ser utilizados para la PCI

Introducción

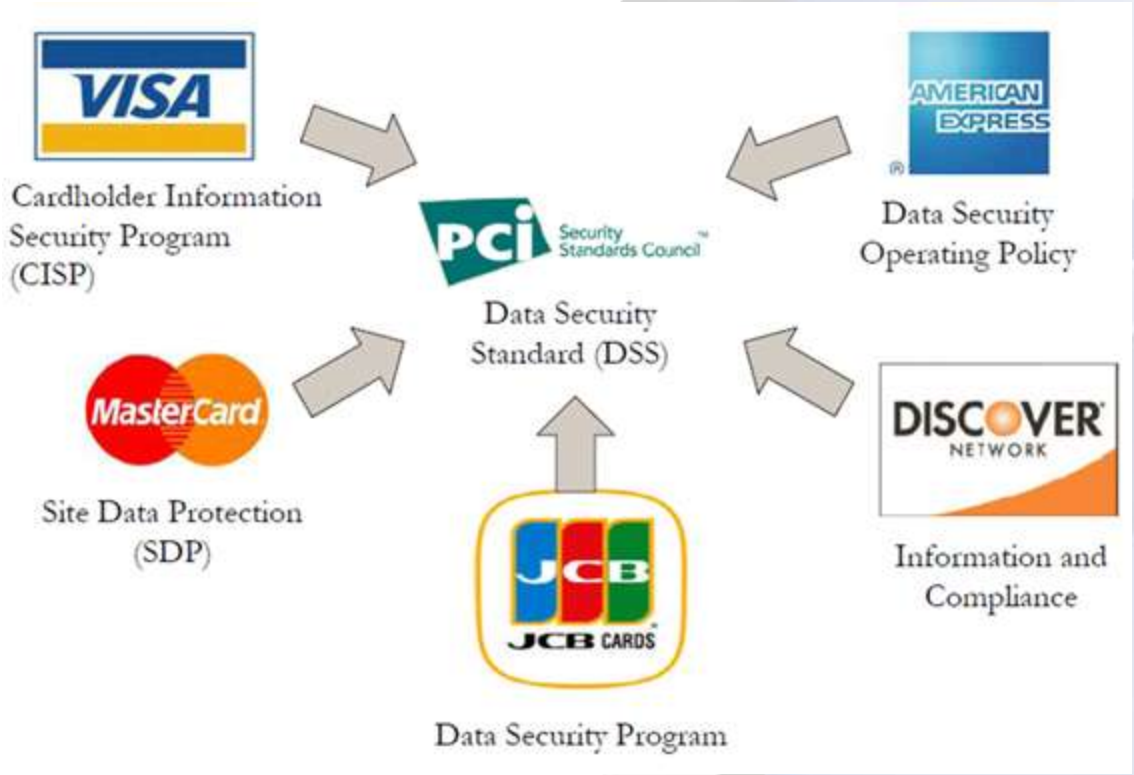
- Payment Card Industry (PCI) Data Security Standard (DSS)

Objetivo 

- Ayudar a las organizaciones que utilizan tarjetas de crédito y debito a proteger los datos sensibles asociados a las cuentas de los clientes.

Introducción

Surge como síntesis de distintos programas que las marcas de tarjetas utilizaban para proteger la información:



Introducción

Contempla

- Requerimientos de gestión de la seguridad
- Políticas
- Procedimientos
- Arquitectura de red
- Diseño y desarrollo de software
- Medidas de protección a datos críticos

288 puntos organizados en 6 requerimientos

Requerimientos

1. Desarrollar y mantener una Red Segura
2. Proteger los datos del titular de la tarjeta
3. Programa de administración de vulnerabilidades
4. Implementar medidas solidas de control de acceso
5. Supervisar y evaluar las redes con regularidad
6. Mantener un política de seguridad de la información

Proyectos aplicables a la PCI

Comité de educación

- Lecciones de estudio disponibles 24/7
- Cursos on-line

Comunidad de Expertos dispuestos a evaluar dudas (Mailing List)

Proyectos aplicables a la PCI

Proyectos aplicables a la PCI

OWASP Backend Security Project

OWASP Backend Security Project (Hardening)

- Oracle Hardening
- SQL Server Hardening
- DB2 Hardening
- MySQL Hardening
- PostgreSQL Hardening
- Hardening de configuración SAP HTTP & WebServices

Incluye:

- Instalación
- Administración
- Cifrado

http://www.owasp.org

Proyectos aplicables a la PCI

OWASP Backend Security Project

OWASP Backend Security Project (Testing)

Documentos

- DBMS Fingerprinting
- Testing Oracle
- Testing SQL Server
- Testing MySQL
- Testing PostgreSQL
- LDAP security testing

Herramientas

- SQL Ninja
- SQL Map
- OWASP SQLiX
- Scuba
- Squid SQL Injection Digger
- SQLDumper
- SQL Power Injector
- BobCat

Proyectos aplicables a la PCI

Transport Layer Protection Cheat Sheet

Providing Transport Layer Protection with SSL/TLS

- Benefits
- SSL vs. TLS
- Secure Server Design
- Server Certificate & Protocol Configuration
- Client (Browser) Configuration
- Additional Controls

Providing Transport Layer Protection for Back End and Other Connections

Proyectos aplicables a la PCI

Guía de Criptografía

Asegura que se usa la criptografía para proteger la seguridad de la integridad y confidencialidad de la información confidencial del usuario.

Usos

- Autenticación
- No Repudio
- Confidencialidad
- Integridad

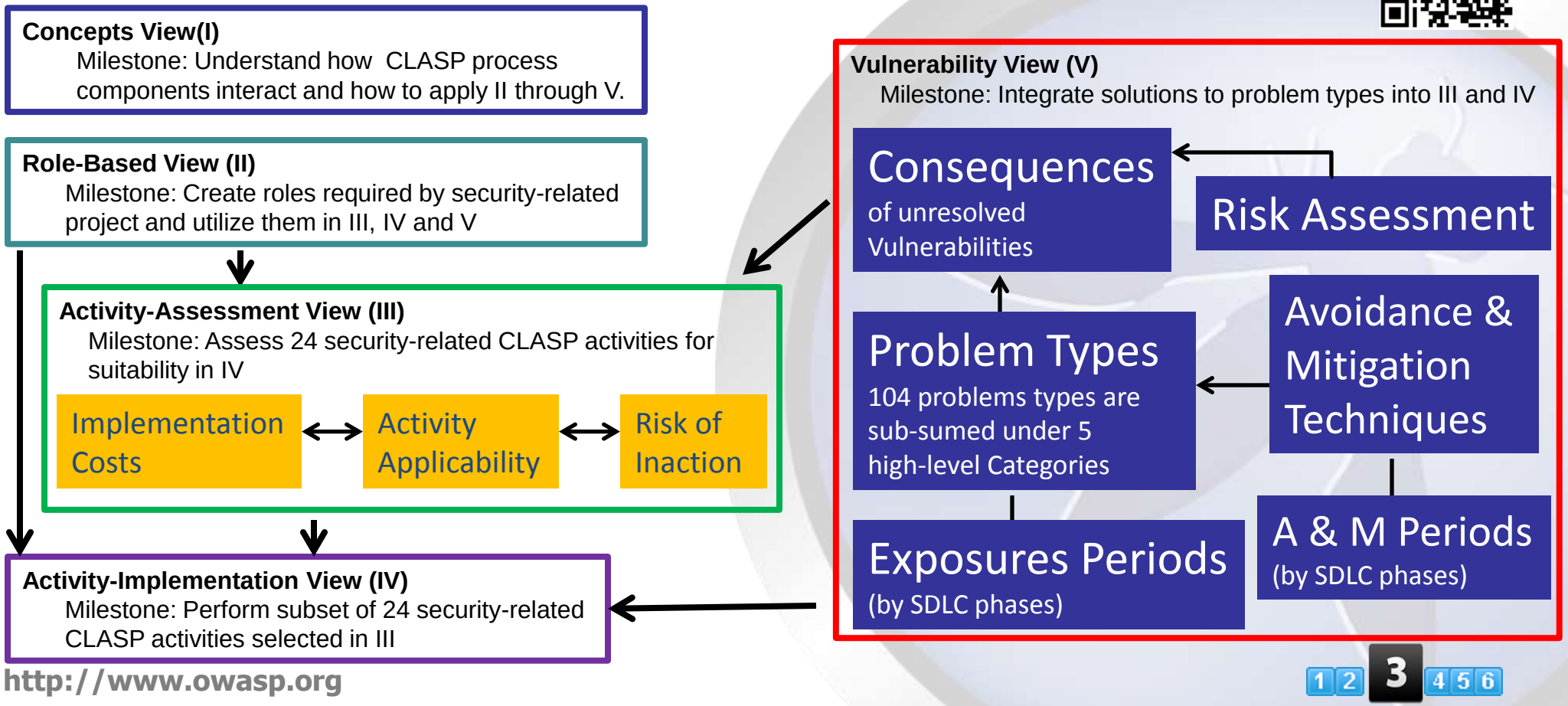
Algoritmos Criptográficos

Almacenamiento de Claves

- Transmisión segura de datos
- Uso de tokens en los procesos de autenticación
- Generación segura de UUID

Proyectos aplicables a la PCI

CLASP (Comprehensive, Lightweight Application Security Process)



http://www.owasp.org

Proyectos aplicables a la PCI

OWASP Secure Coding Practices – Quick Reference Guide Project

Contiene un mapeo general sobre practicas de desarrollo seguro de software.
Utiliza un formato de checklist lo que permite de manera fácil integrarlo al ciclo de vida de desarrollo del proyecto.

Se enfoca en garantizar la definición de adecuados requerimientos de seguridad, en lugar de la identificación de vulnerabilidades o ataques. Incluye una introducción a los principios de software de seguridad y un glosario de términos clave.

Proyectos aplicables a la PCI

OWASP Guide Project

Permitir a empresas, desarrolladores, diseñadores y arquitectos generar aplicaciones web seguras.

Si se incorpora desde las primeras etapas, el costo de desarrollar aplicaciones seguras no diverge mucho del de desarrollar aplicaciones inseguras. Este proyecto genera su máxima rentabilidad en el largo plazo.

- Inyecciones SQL
- Manipulaciones de tarjetas de crédito
- Ataques de Phishing
- Fijación de sesiones
- Cross-Site Request Forgeries
- Cumplimiento y temas de privacidad

http://www.owasp.org

Proyectos aplicables a la PCI

ESAPI (Enterprise Security API):

Proyecto enfocado a los desarrolladores, permite crear aplicaciones de bajo nivel de riesgo.

Contiene bibliotecas que están diseñadas para facilitar la reconversión de la seguridad en las aplicaciones existentes. Contienen también sólidos fundamentos para nuevos desarrollos.

Dentro de las diferentes versiones de ESAPI, se mantiene una estructura básica:

- Existe un conjunto de interfaces de control de seguridad
- Hay una implementación de referencia para cada control de seguridad
- Se definen implementaciones propias para cada control de seguridad

Proyectos aplicables a la PCI

OWASP Backend Security Project

OWASP Backend Security Project (Development)

- JAVA Backend Security programming
- PHP Backend Security programming
- .Net Backend Security programming

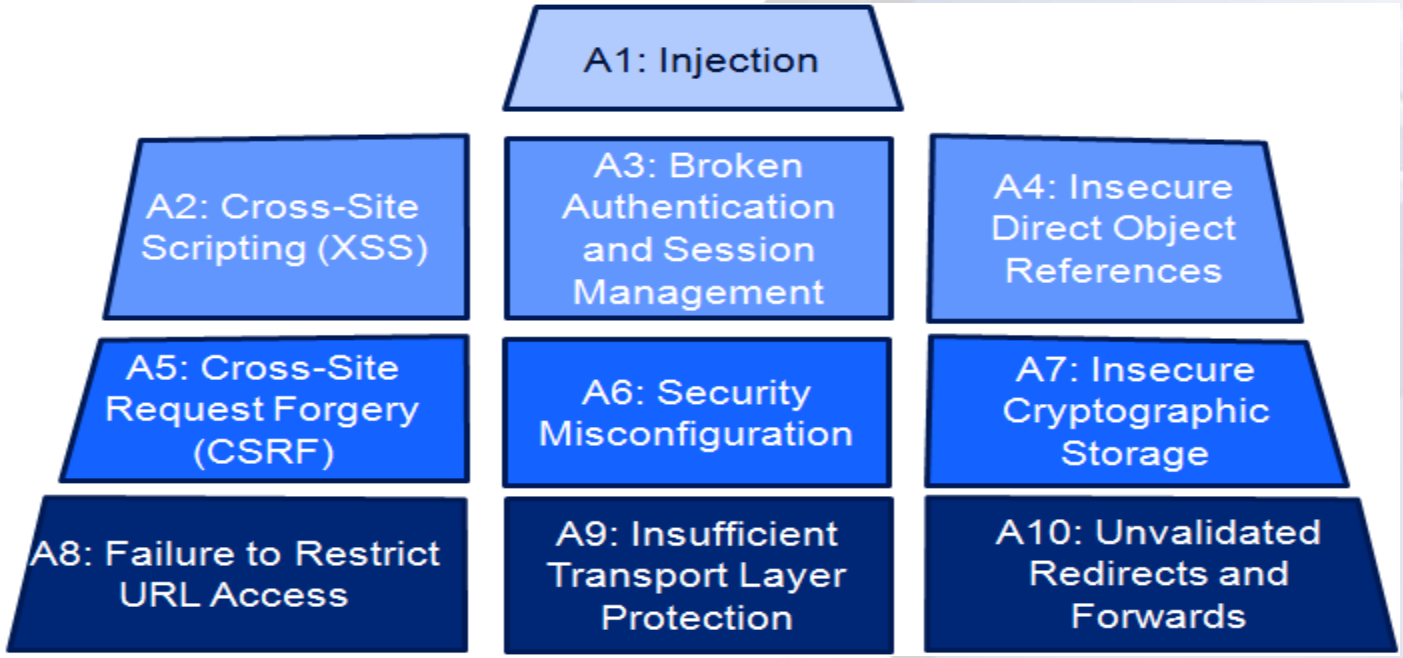
Incluyen:

- Ejemplos de códigos vulnerables
- Como prevenir las vulnerabilidades
- Detección de intrusos

Proyectos aplicables a la PCI

Top 10:

Ranking de las 10 vulnerabilidades más críticas.
Se detalla cada una de ella explicando donde se pueden encontrar, el impacto que estas pueden tener, maneras de mitigar la amenaza, etc.



http://www.owasp.org

Proyectos aplicables a la PCI

OWASP Mobile Security Project

Ayudar a la comunidad a entender mejor los riesgos presentes en las aplicaciones móviles, y aprender a defenderse de ellos

- For Security Testers
- Secure Development Guidelines
- Top Ten Mobile Risks
- Top Ten Mobile Controls
- GoatDroid Project: Es el equivalente para Android del proyecto iGoat

http://www.owasp.org

Proyectos aplicables a la PCI

OWASP Code Review Guide

Contenido

- Security Code Review in the SDLC
- Code review and PCI DSS
- Reviewing by technical control: Authentication, Authorization, Session Management, etc
- Metodología
- Crawling Code
- Revisiones de código y PCI
- Ejemplos por Técnica
- Ejemplos por Vulnerabilidad
- Buenas practicas para lenguajes específicos
- Ejemplos de informes
- Automatización de códigos

http://www.owasp.org

Herramientas:

- Yasca Analisys Tool
- OWASP O2 Platform
- LAPSE+

Proyectos aplicables a la PCI

ASVS (Application Security Verification Standard):

Estándar que proporciona una base para las pruebas de seguridad de las aplicaciones, que se invocan para proteger contra las vulnerabilidades como Cross-Site Scripting (XSS) y la inyección de SQL.
Este estándar se puede utilizar para establecer un nivel de confianza en la seguridad de las aplicaciones Web.

Objetivos

- Utilizar como una métrica
- Usar como guía
- Uso durante la contratación

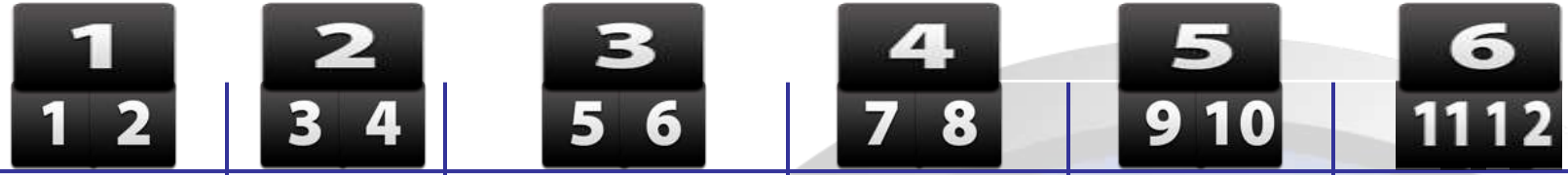
Conclusiones

Matriz de Proyectos vinculados

	Desarrollar y mantener una red segura	Proteger los datos del titular de la tarjeta	Programa de administración de vulnerabilidades	Implementar medidas solidas de control de acceso	Supervisar y evaluar las redes con regularidad	Mantener una política de seguridad de la información
Backend Security Project (Hardening)	2.1 2.2 2.3					
Backend Security Project (Testing)	1.2 2.1 2.3		6.2 6.5 6.6			
Transport Layer Protection Cheat Sheet	1.1 2.3	4.1 4.2	6.6			
Guía de Criptografía	2.3	3.4 3.6 4.1 4.2	6.5	8.3		
CLASP			6.3 6.5			

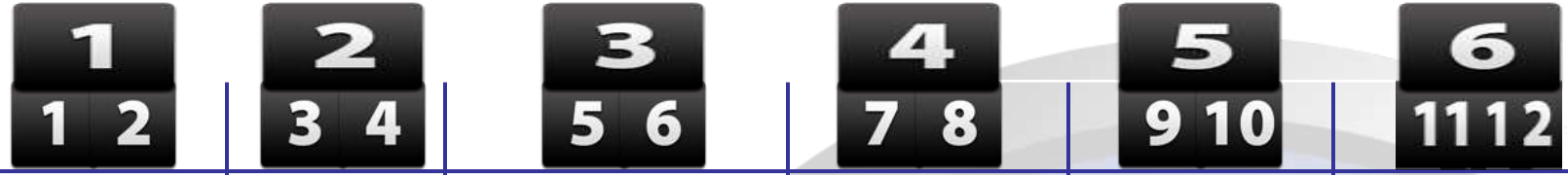
http://www.owasp.org

Matriz de Proyectos vinculados



	Desarrollar y mantener una red segura	Proteger los datos del titular de la tarjeta	Programa de administración de vulnerabilidades	Implementar medidas solidas de control de acceso	Supervisar y evaluar las redes con regularidad	Mantener una política de seguridad de la información
OWASP Sec. Coding Practice			6.5			
OWASP Sec. Coding Practice			6.5			
OWASP Guide Project			6.5			
ESAPI			6.5 6.6			
Backend Security Project (Development)			6.3 6.5			

Matriz de Proyectos vinculados



	Desarrollar y mantener una red segura	Proteger los datos del titular de la tarjeta	Programa de administración de vulnerabilidades	Implementar medidas solidas de control de acceso	Supervisar y evaluar las redes con regularidad	Mantener una política de seguridad de la información
Top 10			6.1 6.2 6.6			11.3
Mobile Security Project			6.1 6.2 6.6			11.3
OWASP Code Review Guide			6.3 6.5 6.6			
ASVS			6.6			11.3

¿Preguntas?

Muchas gracias

Mauro Flores
mauro.flores@owasp.org

@mauro_fcib