UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Seguridad en aplicaciones Web: un enfoque práctico en el entorno universitario

Evangelino Valverde Álvarez
Área de Tecnología y Comunicaciones UCLM

Marzo de 2008
VI Foro de Seguridad RedIRIS: Seguridad en Web

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Contexto

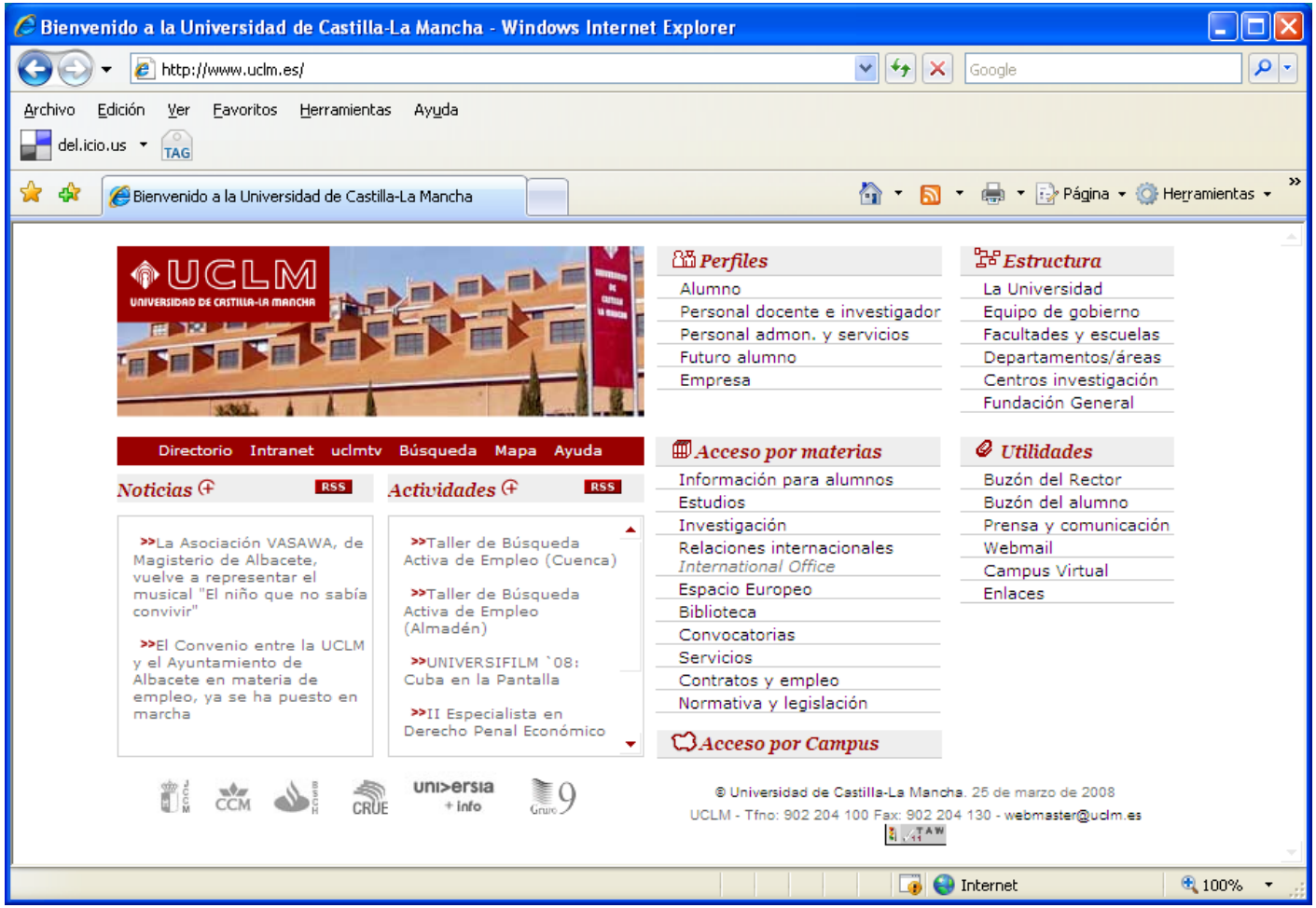
- 4 campus
  - Ciudad Real, Albacete, Cuenca, Toledo
- Presencia en 8 localidades
  - 48 edificios
- 30.000 estudiantes
- 11.000 nodos
- Área Tecnología y Comunicaciones
  - Unidad de Sistemas y Redes
    - Equipo de Seguridad

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

No somos un banco pero…

- Las universidades ofrecemos
  - Servidores y ancho de banda
  - Datos personales
  - Gestión académica
  - Productos: matrículas, ¿comercio-e?
  - Resultados de investigación
  - ¡Los navegadores de nuestros visitantes!
- Todo vía Web
- Motivación
  - Económica
  - Otras: "académica", conflictos, diversión…

¿Me puede pasar a mí?



UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Análisis del incidente

- Técnicas usadas para el ataque:
  - Forzar errores no capturados para conocer la estructura

```
id=0having 1
Column 'columna1' is invalid in the select list because it
is not contained in an aggregate function and there is no
GROUP BY clause.
id=0group by columna1 having 1=1
Column 'columna2' is invalid in the select list because it
is not contained in an aggregate function and there is no
GROUP BY clause.
id=0group by columna1, columna2 having 1=1
```

  - Inyección de una hoja de estilos CSS en el rotor de noticias:

```
id=0update TABLA set
campo = '<link href=url type=text/css rel=stylesheet>'
```

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Análisis del incidente (II)

- Sobre el módulo afectado
  - Atacado meses antes con SQLi para saltar la autenticación
  - Desarrollo subcontratado 7 años antes
  - Autenticación local sobre BD para los administradores
  - Enlace de administración desde la interfaz de lectura
- Problemas detectados
  - Seguimiento insuficiente del primer incidente
  - Falta de control sobre los desarrollos externos
  - Especificación de requisitos incompleta (autenticación LDAP)
  - Diseño inseguro (enlace de administración)

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Otros incidentes

- Phishing de Wells Fargo
  - Vulnerabilidad en PHP
  - Hosting del Área para un centro de investigación
- Phishing de eBay
  - Vulnerabilidad en Mambo
  - Web operado por una delegación de alumnos
- Falta de confidencialidad de un programador
  - Operación de la aplicación delegada en una empresa externa
- Problemas detectados
  - Parcheo de servidores, aplicaciones, etc.
  - Límites en la responsabilidad
  - Control de los contratos de servicio

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Problemática general

Seguridad

- Requisitos
- Diseño
- Codificación
- Pruebas
- Despliegue
- Operación

Diversidad de perfiles

- Desarrollos internos
- Desarrollos externos
- Aplicaciones empaquetadas
- Software como servicio

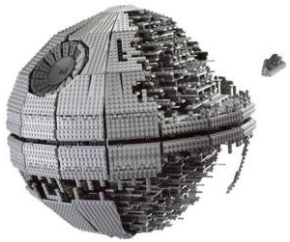
Regulaciones

Gestión distribuida

Google Sites

Basecamp

flickr



Dispositivos embebidos

Raúl Siles …

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Enfoque de la UCLM

Gestión de la seguridad por perfiles

Buscar puntos de control de la seguridad

Perfil	Selección	Contratación	Desarrollo	Explotación	Eval.
Desarrollo interno	X		X	X	X
Desarrollo externo	X	X		X	X
Ap. Empaquetada	X			X	X
Sw. como servicio	X	X			X

X: punto de control

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Selección y contratación

- Selección
  - Cumplimiento de los requisitos de seguridad
  - Valoración de la seguridad del producto
    Características, historial de vulnerabilidades y correcciones, etc.
  - Valoración de la seguridad del servicio
    ASP Security Standars (SANS)
  - Evaluación de la empresa
    Financiera, certificaciones (ISO 27001, CMMI, SPICE, etc.)
- Contratación
  - Cláusulas de seguridad del servicio
    Deber de secreto, LOPD, etc.
  - Cláusulas de seguridad para el desarrollo
    Secure Software Development Contract Annex (OWASP)

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Desarrollo, explotación y eval.

- Desarrollo
  - Requisitos metodológicos y organizativos
  - "Secure Software Development Contract Annex" (OWASP)
- Explotación
  - Requisitos metodológicos y organizativos
  - ISO/IEC 27002 (ISO/IEC 17799), ITIL, etc.
  - "A Guide to Building Secure Web Applications and Web Services" (OWASP)
- Evaluación
  - Requisitos metodológicos y organizativos
  - Contenido del informe de evaluación
  - Métricas requeridas (cuáles y cómo medir)
  - "OWASP Testing Guide"

Plan de mejora

Plan de mejora de la seguridad en aplicaciones Web

Ámbito: aplicaciones Web corporativas

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

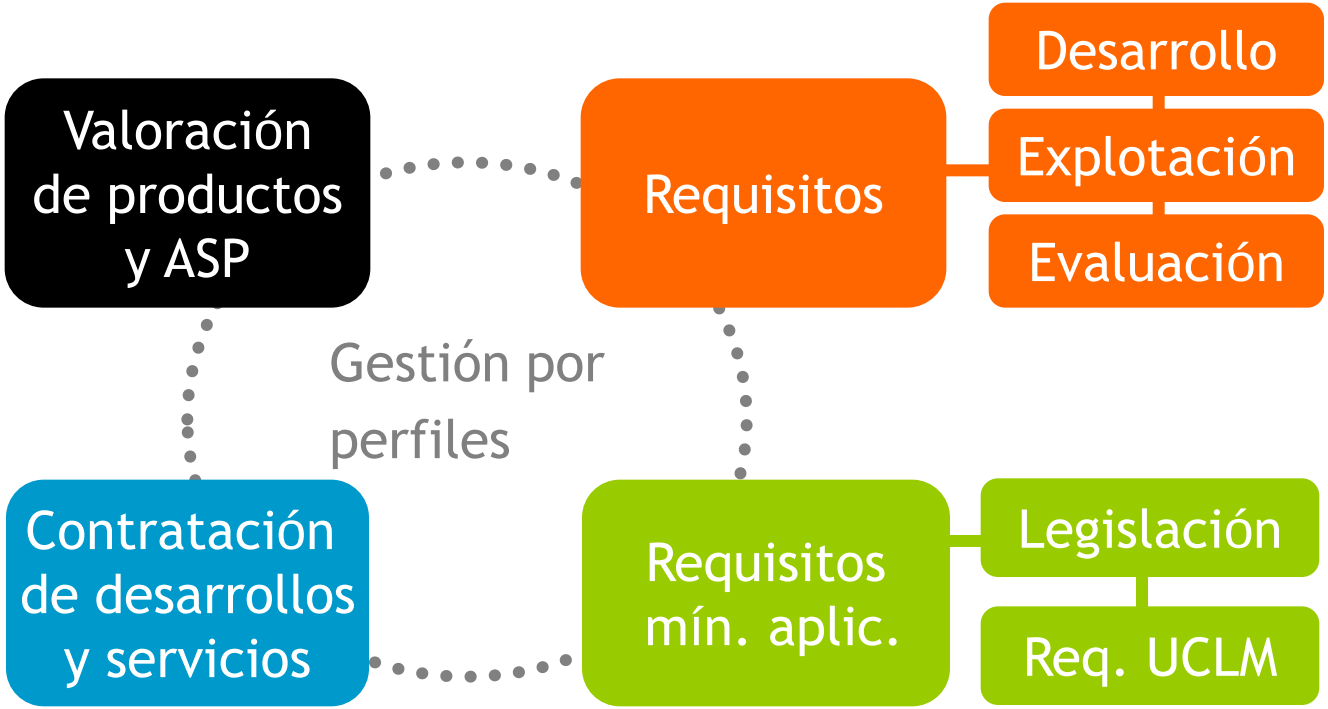
Formación inicial

- "Seguridad en Aplicaciones Web", Raúl Siles
  - 21 horas x curso, 2 ediciones x 15 personas
  - Perfiles: desarrollo y sistemas
- Contenido:
  - Visión completa
  - Laboratorios PHP + ASP.NET + Herramientas
- Objetivos
  - Dotar de conocimientos específicos
  - Concienciar y motivar
  - Eliminar barreras desarrollo/sistemas

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Marco normativo

"Directrices de Seguridad para las Aplicaciones Web de la UCLM"



UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Marco normativo (II)

Requisitos de seguridad mínimos para las aplicaciones:

- Los impuestos por la legislación
  - Derivados del reglamento LOPD
- Normativa interna
  - Política de Seguridad de Red (arquitectura)
- Autenticación externa compatible LDAP
- Generación de logs
  - Eventos de acierto y fallo, campos
- TOP 10 OWASP
  - Evitar la aparición de vulnerabilidades específicas

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Análisis de la situación

- Diferencias entre las directrices y la situación de partida
- Cuestiones
  - Personal y organización
  - Políticas (logs, red, incidentes)
  - Procedimientos y métodos (parcheo, cambios, etc.)
  - Entorno (red, servicios, etc.)
- Inventarios
  - Aplicaciones, bases de datos, servidores y personal
  - Herramientas, lenguajes, librerías, frameworks

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Adaptación: desarrollo

- Guía de diseño seguro
  - Debe dar respuesta a los requisitos de la UCLM (OWASP/MS)
- Selección de librerías
- Metodología
  - Catálogo de patrones + recortes de código
  - Threat modeling (MS) o CLASP (OWASP)
- Herramientas durante el desarrollo
  - Paros Proxy o WebScarab
  - Análisis del código (RATS, HP DevInspect, etc.)
- Gestión del desarrollo
  - Gestión de proyectos, versiones, vulnerabilidades, doc., etc.
  - Probablemente GForge (forja.rediris.es)

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Adaptación: explotación

- Guías de seguridad para red, S.O., S. Web, S. Aplic., BD
  - Guías CIS adaptadas a la UCLM
- Plantillas de configuración
- Herramientas de comprobación de la conformidad (CIS)
- Web Application Firewall
  - Criterios de evaluación del WASC
- Programa de gestión de parches y vulnerabilidades
  - NIST SP 800-40
- Política de gestión de incidentes
- Política de gestión de logs

the CENTER for INTERNET SECURITY

Web Application Security Consortium

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Adaptación: evaluación

- Guías de evaluación y revisión de código
  - OWASP Testing Guide
  - OWASP Code Review Guide
- Informe tipo y métricas
- Herramientas
  - WASS (Watchfire, Acunetix, SPI Dynamics, etc.)
  - Análisis de código (RATS, HP DevInspect, etc.)
- Balance entre recursos internos/externos
- ¿Servicios tipo Sentinel de WhiteHat Security?
  - SaaS para pruebas de caja negra

acunetix

watchfire
an IBM company

SPI DYNAMICS
Start Secure. Stay Secure.

WhiteHat
SECURITY

Adaptación: apoyos

- Comunidad
  - Wiki, lista de distribución
  - Asignación de tareas (implicación)
- Formación
  - Con monitores externos, intensiva
  - Interna: 30 minutos, viernes de 9:30 a 10:00

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Plan de choque

- Priorizar las aplicaciones
  - Las de mayor riesgo primero
- Revisión de desarrollos (caja blanca)
  - Conformidad con los requisitos
  - Revisión de la funcionalidad
  - Revisiones de código
- Revisión de despliegues (caja gris)
  - Pruebas de intrusión, revisión de configuraciones, etc.
- Revisión de contratos
  - Adecuación a las cláusulas para servicios y desarrollos externos

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Futuro

- Convertir las directrices de seguridad en una normativa para todas las aplicaciones de la UCLM, aprobada en Consejo de Gobierno
- Aplicación a todos los contratos y adquisiciones

¿Posibilidad de proyectos de colaboración en la comunidad RedIRIS?

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Referencias

- Open Web Application Security Project (OWASP)
  - http://www.owasp.org
- Web Application Security Consortium (WASC)
  - http://www.webappsec.org
- Center for Internet Security (CIS)
  - http://www.cisecurity.org

Plan de Seguridad Informática