



La necesidad de construir software seguro

Vicente Aguilera Díaz

vicente.aguilera@owasp.org

OWASP Spain Chapter Leader

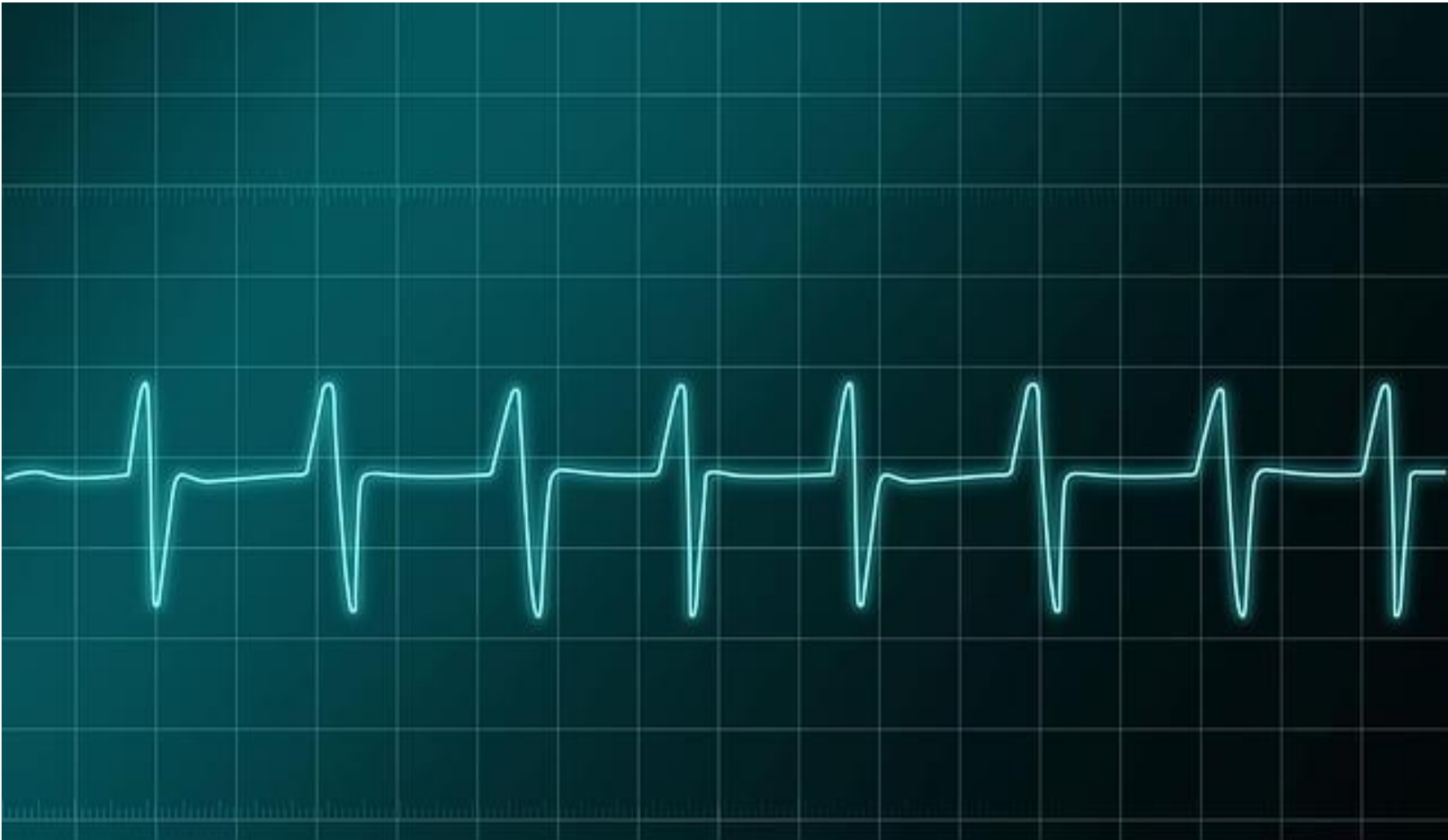
Socio de Internet Security Auditors

IBM Software Summit #START013. Madrid 06/11/2012.

Agenda

- Dependencia del software
- Construcción de software seguro
- OWASP
- Conclusiones y recomendaciones

Dependencia del software



Dependencia del software

- Es crítico crear software seguro:
 - Conectividad
 - Complejidad
 - Extensibilidad
 - ... y requerimientos normativos

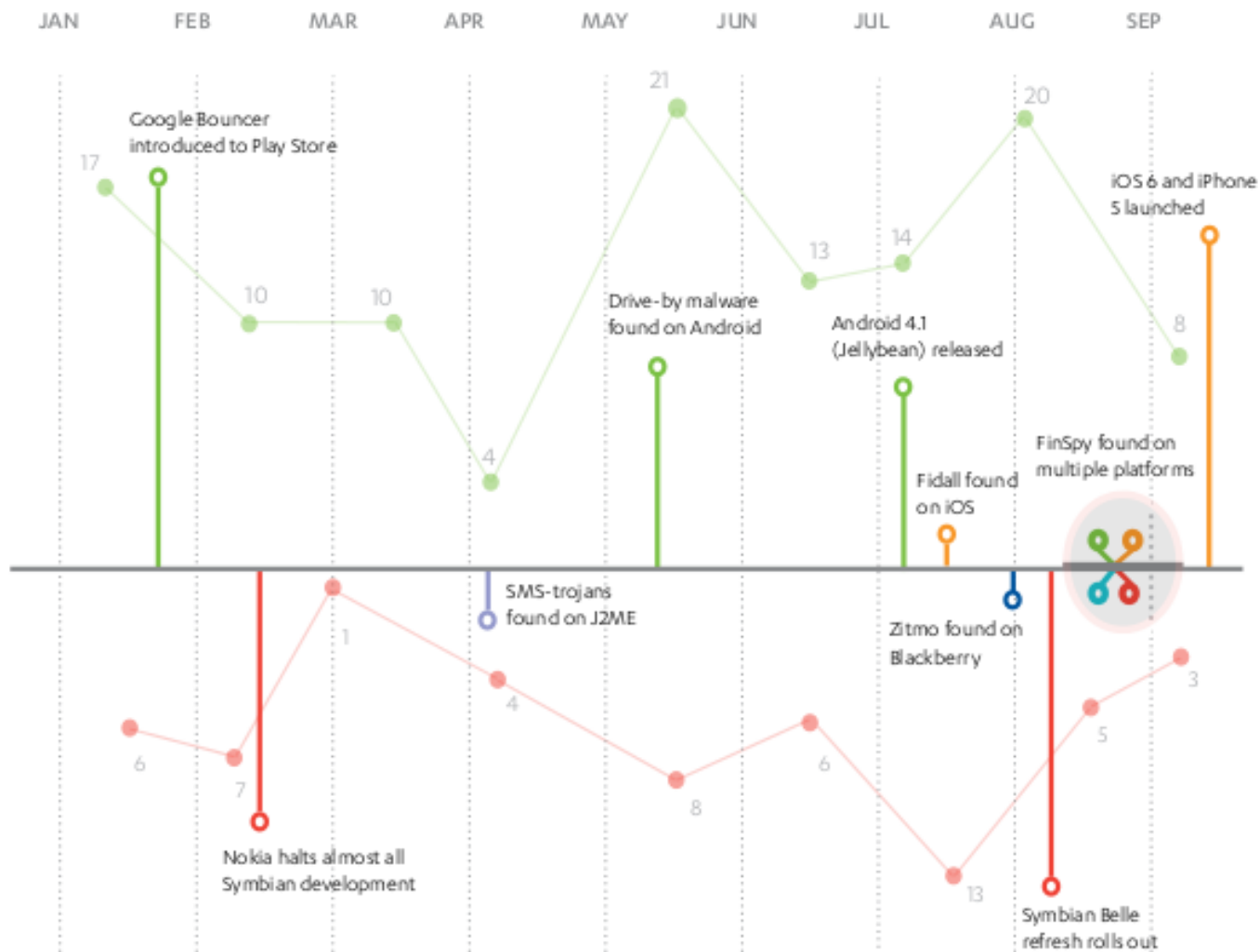
Dependencia del software

- ¿Y el mundo de los dispositivos móviles?



Dependencia del software

2012 MOBILE LANDSCAPE CALENDAR



Construcción de software seguro



Construcción de software seguro

- ¿Qué entendemos como software seguro?
 - Diseñado, construido y probado para su seguridad
 - Continúa ejecutándose correctamente bajo ataque
 - Diseñado con el fallo en mente


Construcción de software seguro

- ¿Porqué ha cobrado tanta relevancia?
 - Proliferación de modelos de negocio en la web
 - Las aplicaciones resultan muy atractivas
 - Auge de los dispositivo móviles
 - La mayoría de aplicaciones son vulnerables
 - Nuevos requerimientos normativos

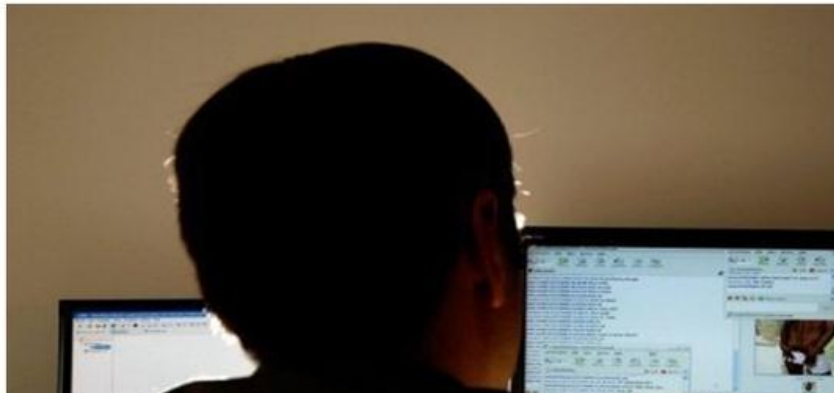
Construcción de software seguro

- ¿Porqué ha cobrado tanta relevancia?

Philippines appeals to hackers to cease attacks

Recomendar  7 personas han recomendado esto. Sign Up para ver qué recomiendan tus amigos.

By Agence France-Presse
Saturday, October 6, 2012 19:00 EDT



Bank Cyber Attacks Originated From Hacked Data Centers, Not Large Botnet

05 Oct 2012 / Comments Off / in News / by Sera-Brynn

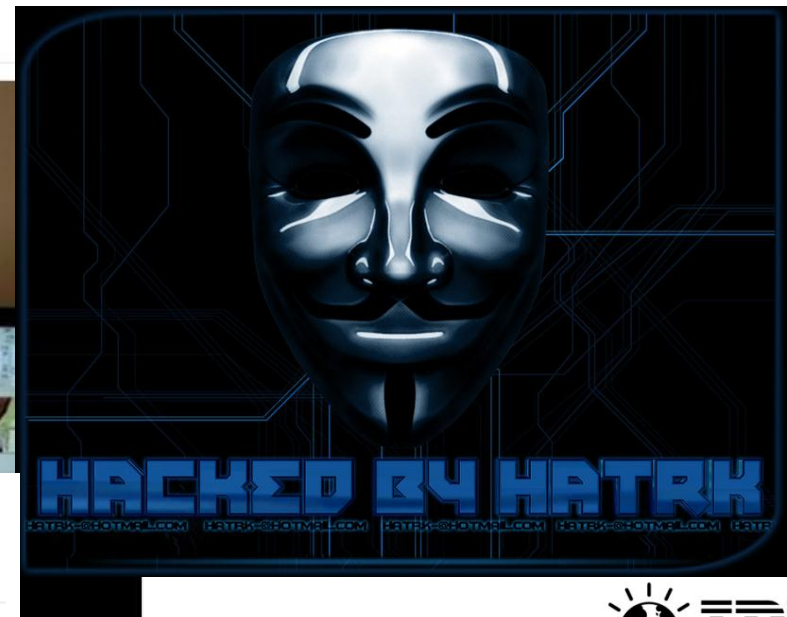
THE CYBERCRIME ECONOMY

'Massive' credit card data breach involves all major brands

By Julianne Pepitone and Leigh Remizowski @CNMoneyTech April 2, 2012: 6:53 AM ET

CNNMoney

603 comments



Construcción de software seguro

- Todo es posible en la web

Inglaterra subasta el portaaviones “HMS Invincible” en internet

El Ministerio acepta pujas por el Invencible, que participó en la guerra de las Malvinas de 1982, en su página web de “servicios de disposición” (www.edisposals.com), creada para vender equipo militar excedente.



The screenshot shows the edisposals.com website interface. At the top, there is a navigation bar with links for 'View Shopping Cart', 'Buyer ID', 'Password', 'Login', and 'Registration'. Below this is a search bar and a 'GO Advanced Search' button. The main content area features a large image of the HMS Invincible aircraft carrier. To the right of the image, there is a detailed description of the ship, including its specifications and a 'Contact Details' section. The 'Contact Details' section lists the address, phone, fax, email, and homepage of the Disposal Services Authority. The bottom of the page includes a footer with 'Foto 2 de 2' and a small IBM logo.

edisposals.com View Shopping Cart Buyer ID: Password: Login Registration

Search: GO Advanced Search

Home | News | About Us | How to use the DSA | Contact Us | FAQs | Your Disposal Services

de&s
DSA

e-Government
National Awards
WINNER 2008

Categories

- Aeronautics
- Building GRADS 2 Services
- Building and Facilities
- Landfill
- Metals and Dental
- Miscellaneous
- Other Services
- Paper
- Textiles
- Vehicles

Auction Categories

- General Services

Disposal Services

You are here: [Tenders](#) > [Sale by Tender](#) > [HMS Invincible](#)

Sale by Tender - HMS Invincible

HMS Invincible is for sale by tender. Last down in 1972 at Vickers Shipbuilding, Barrow-in-Furness, she was completed in 1950. She is currently stable for sale, subject to buyer confirmation.

Displacement - Current 17000 Tonnes
Estimated metal % - 95% mild steel
Length - OA 220m, WL 192m
Draught - Fed 5.2m, Mid 5.6m, AH 5.6m
Beam - Extreme 35m, Ex-walkways 32m, WL 27.53m
Height - 45m (estimated at current draught)

Engines - 4 x removed
Generators and Pumps - Generally unserviceable or not working

For fuller information, please see the General Particulars.

For items without a price please contact the supplier using the details below

Contact Details

Address: Disposal Services Authority
Building 169
Ploughley Road
Lower Amcott
Bicester
Oxon
OX25 2LD
Phone: 01869 256 827
Fax: 01869 256 076
Email: enquiry@edisposals.com
Homepage: www.edisposals.com

Product ID: **Sale by Tender - HMS Invincible**
Manufacturer: **Vickers Shipbuilding**
Availability: **In stock**

Our Price: **N/A**

[Add to Wishlist](#) [Compare](#)

Product Details **Notification Agent** **Additional Specifications**

Closing Date - 10:00am Wednesday 05th January 2011
Further Information - [Click Additional Specifications](#)
Location - HM Naval Base Portsmouth
Point of Contact Details - Janet Kynman 01869 256017 or email dsdsa-mst1a2@med.uk
Viewing Details - All viewings are by appointment only, between 29th Nov 2010 and 10th Dec 2010

Foto 2 de 2

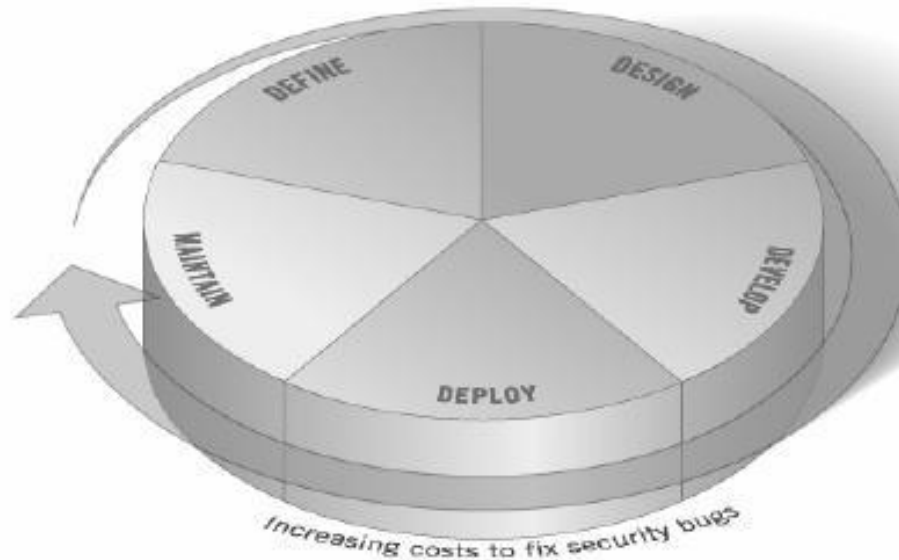


Construcción de software seguro

- ¿Cómo conseguir crear software seguro?
 - Adoptar un modelo de madurez
 - La seguridad debe ser considerada desde el inicio
 - S-SDLC es la clave

Construcción de software seguro

- Secure SDLC es la clave
 - SDLC basado en principios de seguridad
 - No existe una fórmula única para su implementación
 - Implica a personas, procesos y tecnología



Construcción de software seguro

- Iniciativas de seguridad en el desarrollo de software:
 - Microsoft SDL
 - OWASP CLASP
 - Digital Software Security Touchpoints
 - OWASP OpenSAMM
 - BSIMM
 - SSE CMM

Construcción de software seguro

- Ejemplos de actividades de seguridad:
 - Clasificar datos y aplicaciones según su riesgo
 - Desarrollar y mantener guías de cumplimiento
 - Realizar formación en seguridad para cada rol
 - Elaborar modelos de amenaza
 - Identificar patrones de seguridad en el diseño
 - Realizar revisiones de código
 - Realizar pruebas de seguridad en las aplicaciones
 - Establecer hitos para la revisión del diseño
 - Crear procedimientos de gestión de cambio



OWASP



OWASP

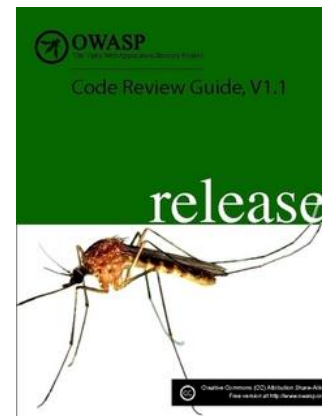
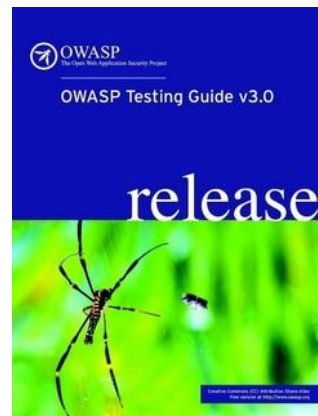
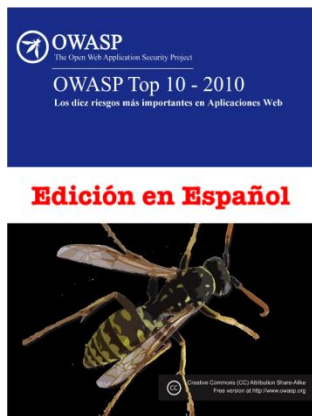
The Open Web Application Security Project

OWASP

- Comunidad libre y abierta sobre seguridad en aplicaciones
- Búsqueda y lucha contra las causas de software inseguro
- Creación de herramientas, documentación y estándares
- Conferencias
- Recursos gratuitos y de código abierto
- 10.000 miembros y 250 capítulos locales en el mundo
- Más de 200 proyectos
- www.owasp.org

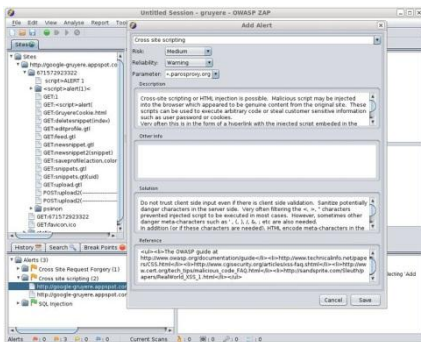
OWASP

- Principales proyectos a nivel de documentación:
 - Top 10
 - Guía de pruebas
 - Guía de desarrollo
 - Guía de revisión de código
 - ASVS

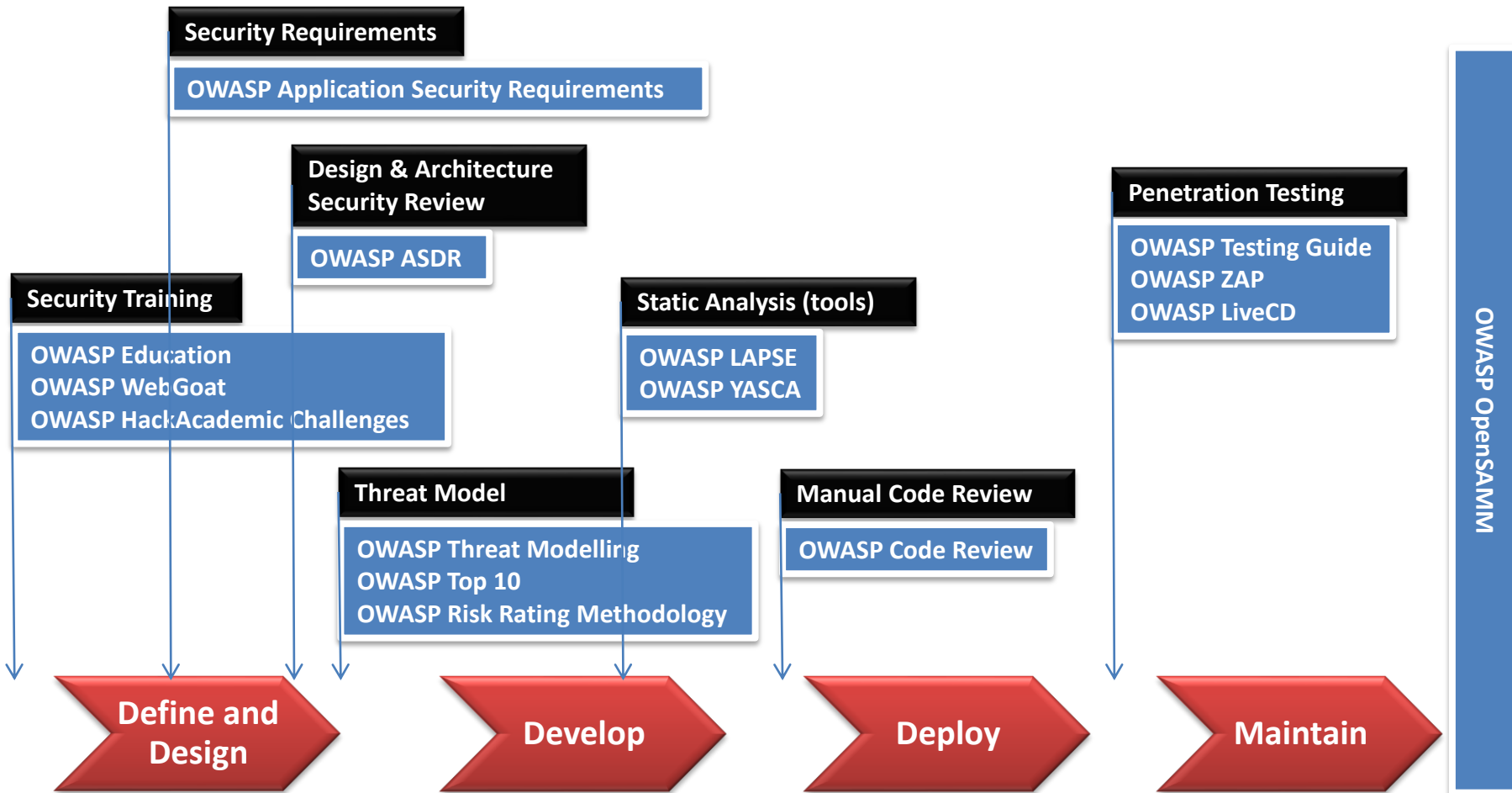


OWASP

- Principales proyectos a nivel de herramientas:
 - ZAP
 - WebGoat
 - ESAPI
 - Live CD



OWASP



Conclusiones y recomendaciones



Conclusiones

- Necesitamos crear software seguro
- Debemos conocer todos los riesgos y cómo mitigarlos
- Necesitamos invertir más en la seguridad del software
- Software seguro \neq código seguro

Recomendaciones

- Clasificar las aplicaciones y definir niveles de seguridad
- Verificar la adopción de los requerimientos de seguridad
- Crear el software pensando en los casos de abuso
- Huir de la solución “todo en uno”
- Seguir el principio de defensa en profundidad
- Identificar los marcos regulatorios y su cumplimiento
- Equiparar requerimientos de seguridad a los funcionales
- Estar informado sobre las amenazas existentes
- No despreciar soluciones open-source
- Potenciar la cultura de la seguridad en la organización



dudas / comentarios/ sugerencias

¡Muchas gracias!