Autoritat de Certificació
de la Comunitat Valenciana

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

I Ciclo de Conferencias ISACA - CV "Rafael Bernal"

Auditoría, Seguridad y Gobierno de las TIC

Autoritat de Certificació de la Comunitat Valenciana

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

AUDITORÍA WEB

D. Ángel Alonso Párrizas CISM, CISSP, GCIH, GCIA, CCNA

Ingeniero de Seguridad

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

Índice

I Ciclo de Conferencias
ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

Se puede enfocar desde una perspectiva:

- Legal / jurídico (cumplimiento de LSSICE Y LOPD)
- Accesibilidad (obligada para las AAPP)
- Seguridad (se puede incluir en una auditoría de instrusión)
- Otros aspectos: Usabilidad, Fiabilidad, diseño, posicionamiento, etc.

Web Accessibility Certification AAA

Euracert
European eAccessibility Certification

eurocert eAccessibility AA

LOPD - LSSI
Ley de protección de datos y ley de servicios de la información.

Marco Jurídico

- LSSICE (Ley de Servicios de la Sociedad de la Informacion y Comercio Electrónico) y LOPD en su caso
- Nombre de dominio, marcas, patentes, copyright, condiciones generales, políticas de contratación, pago y devoluciones, prestación de servicios online, etc
- "*El presente certificado reconoce que este Sitio Web cumple los requisitos legales de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE) de España. ECONFIA se otorga tras un riguroso análisis Legal garantizando la ADECUACIÓN del Sitio, así como lo referente a:*

  Condiciones de Contratación

  Protección de Datos

  Propiedad Intelectual

  Demás aspectos regulados por dicha ley."

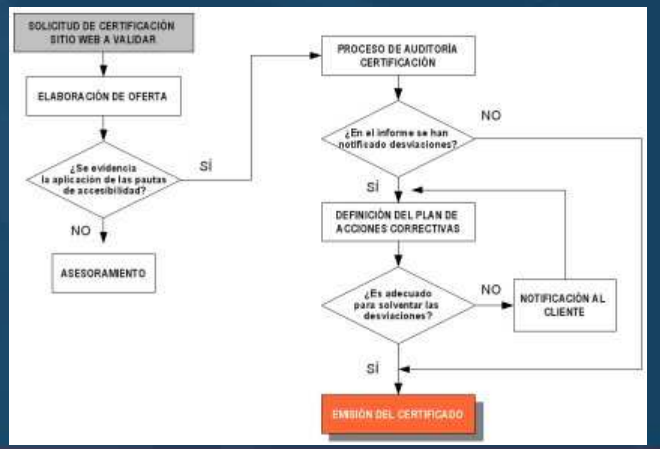
Accesibilidad

"Accesibilidad Web es el arte de garantizar que la información y servicios en Internet están disponibles para todas las personas, independientemente de sus capacidades personales y tecnológicas" **Tim Berners-Lee**

EURACERT http://www.euracert.org/

Directrices europeas sobre accesibilidad, que ha sido diseñada bajo las bases:

- recomendaciones internacionales (WCAG 1.0, WAI)
- una metodología de evaluación (UWEM)
- un esquema de evaluación de la conformidad

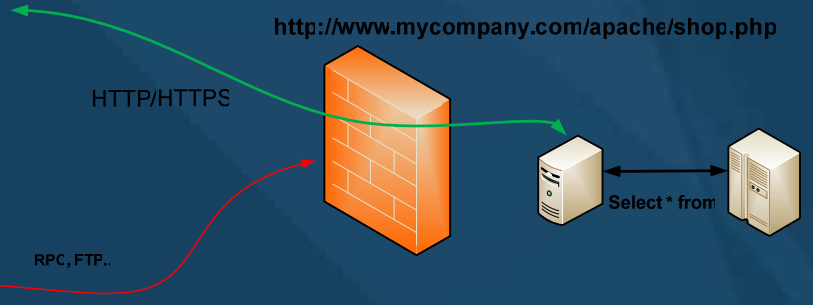


http://www.technosite.es/ ONCE

I Ciclo de Conferencias ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

Auditoría de seguridad I: generalidades

- Aplicaciones más complejas a través de HTTP/S y mayor presencia
- Diseño cada vez más robusto de la seguridad perimétrica
- Los servicios de red filtrados por FWs y muy permisivos con el tráfico HTTP/HTTPS.
- La Web como objetivo y como plataforma de ataque.
  - http://isc.sans.org/diary.html?storyid=3621 (40.000 Webs infectadas)
- Metodologías específicas de auditoria: OWASP, OSSTMM, ISSAF



Auditoría de seguridad II: Toolkit

- Herramientas automáticas: Nessus, Nikto, WebInspect.. iiiy *scripting*!!!
- Navegador con *plugins* adecuados (convert base64, edit forms, cookies..)
- Proxy: Paros, WebScarab, Aquilles
- SwitchProxy Tool: Conmutacion Proxy.
- ¡¡Google Hacking!! http://www.sans.org/GoogleCheatSheet.pdf
- … y puede que.. decompiladores (.JAR)

I Ciclo de Conferencias ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

Auditoría de seguridad III: identificación

- Identificación de los servicios
- Detección del *fingerprint* del servidor WEB y la capa SSL.
- ¿Hay una BBDD que se pueda identificar?
- Tecnologías de programación (JSP, PHP, .NET, XML..)

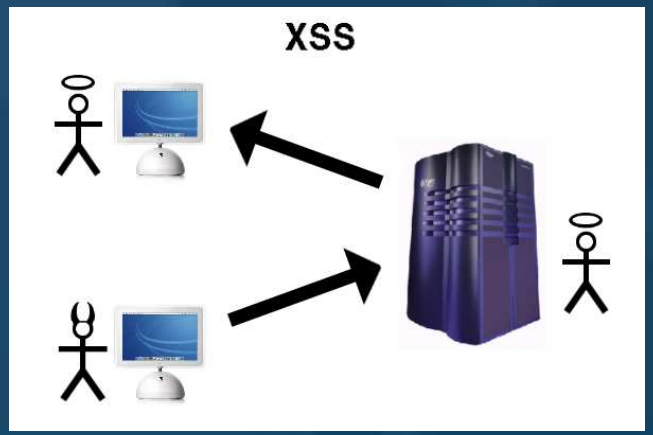
Auditoría de seguridad IV: Seguridad del servidor

- Contenido por defecto, configuración por defecto (métodos TRACE, directorios por defecto..), parches..
- Ataques al sistema: ejecución de comandos, Path Trasversal..
- Configuración de SSL/TLS: fortaleza, análisis CA, Validez del certificado

Auditoría de seguridad V: Vulnerabilidades / Ataques

- OWASP http://www.owasp.com y WAS http://www.webappsec.org
- Robo de identidad, integridad de los datos, phising, compromiso del sistema..
- TOP Ten 2007 (según OWASP): http://www.owasp.org/index.php/Top_10_2007

"XSS e Injection flaws"



I Ciclo de Conferencias ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

Auditoría de seguridad VI: Informe de resultados

- Verificación de los resultados
- Estructura del documento
  - Informe Ejecutivo (CEO, CISO..)
  - Matriz de riesgo
  - Mejores prácticas
  - Informe final

Bibliografía

http://www.w3.org/TR/WCAG10/
http://www.w3.org/WAI/
http://www.euracert.org/es/
http://www.w3c.es/
http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf
http://www.owasp.com
http://www.accesibilidad.com
http://www.sans.edu/resources/securitylab/audit_web_apps.php
http://www.securityfocus.com/infocus/1864
https://www2.sans.org/top20/#c1
http://www.slideshare.net/iwmw/trends-in-web-attacks/
http://www.iec.csic.es/gonzalo/Conferencias.aspx

Autoritat de Certificació de la Comunitat Valenciana

ISACA
Al servicio de los profesionales encargados de la gobernabilidad de la informática
Valencia Chapter

I Ciclo de Conferencias ISACA - CV "Rafael Bernal"
Auditoría, Seguridad y Gobierno de las TIC

¡GRACIAS POR VUESTRA ATENCIÓN!

aalonso@accv.es