

OWASP LatamTour
Rep Dom. 2016

Su aplicación es segura? Demuéstraselo al auditor

ASVS: Application Security Verification Standard

Saira Isaac



OWASP
The Open Web Application Security Project



OWASP
LATAM
2016
LATIN AMERICA TOUR

Introducción




OWASP
The Open Web Application Security Project



Saira Isaac Hernández
Consultor | Enterprise Risk Services
(ERS)
Deloitte RD, S.R.L.


Email: Saisaac@Deloitte.com
Ingsairaisaac@gmail.com



OWASP
The Open Web Application Security Project

Temario

- Introducción
- ASVS
- Niveles de Verificación
 - Nivel 0
 - Nivel 1
 - Nivel 2
 - Nivel 3
- Conclusiones



OWASP
The Open Web Application Security Project

QUE ES OWASP ?

OWASP: Open Web Application Security Project

Proyecto abierto de seguridad para aplicaciones Web.

“Proyecto libre que crea y divulga metodologías, estándares y herramientas opensource para usarlas gratuitamente”




OWASP
The Open Web Application Security Project

QUE ES ASVS ?

ASVS: Application Security Verification Standard

Un estándar de OWASP, que documenta y organiza un checklist de 179 verificaciones de seguridad.

“Requisitos a cumplir”, para medir y certificar el nivel de seguridad de una aplicación.



OWASP
The Open Web Application Security Project

QUE ES ASVS ?


ASVS: Documenta 179 verificaciones de seguridad !

...y para que sirve eso ?

ASVS permite evaluar objetivamente los niveles de:

- Alcance (sólo código propio o también DLL externas?)
- Cobertura (sólo los módulos críticos?)
- Grado de rigurosidad aplicable (re-certificar o no ?)

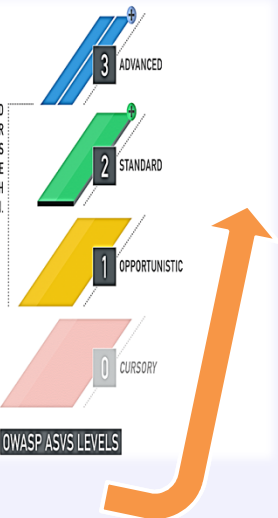
ASVS

 **OWASP**
The Open Web Application Security Project

ASVS define niveles de seguridad que una aplicación puede lograr...

Si cumple los requisitos del nivel !!

ASVS DEFINES DETAILED VERIFICATION REQUIREMENTS FOR LEVELS 1 AND ABOVE; WHEREAS LEVEL 0 IS MEANT TO BE FLEXIBLE AND IS CUSTOMIZED BY EACH ORGANIZATION.



OWASP/ASVS/LEVELS

 **OWASP**
The Open Web Application Security Project

Niveles de Certificación

 0 Superficial

1 Oportunista

2 Estándar

3 Avanzado

Niveles de Verificación



OWASP
The Open Web Application Security Project




Nivel 0

Indica que la aplicación tuvo algún tipo de verificación.

- La organización puede definir sus propios criterios mínimos
- Útil para organizaciones con gran número de apps, y que quieren auto-exigirse un “nivel mínimo inicial”.
- No es Pre-Requisito... podría saltarse directo al N1.
- Se recomienda que cada requisito auto-definido, sea documentado de forma similar a los requisitos de niveles 1-2-3 (claro , realista y verificable)

Niveles de Verificación




OWASP
The Open Web Application Security Project

Nivel 1

“Oportunista”, la app se defiende adecuadamente contra vulnerabilidades fáciles de identificar.


- Incluye vulnerabilidades que un verificador debería poder identificar con un mínimo de esfuerzo.
- Apropiado para aplicaciones donde se requiera cierta confianza
- Vulnerabilidades del tipo “Fácil de hallar” y “Fácil de explotar”



OWASP
The Open Web Application Security Project

Nivel 2 “Estándar”, hay una defensa adecuada de la app contra vulnerabilidades de seguridad que tienen riesgo moderado a grave.

- Asegura que los controles de seguridad evaluados existen, se aplican y son eficaces.
- Nivel de Seguridad “deseable” de alcanzar en la industria.
- Apropiado para aplicaciones que usan transacciones Business-to-Business.
- Las amenazas de seguridad serán del tipo “oportunistas” y del tipo “Atacantes decididos”.



OWASP
The Open Web Application Security Project

Nivel 3 “Avanzado”, la app se defiende bien de las vulnerabilidades de seguridad más avanzadas y posee un buen diseño de seguridad.

- Requiere una inspección del diseño de la aplicación.
- Apropiado para aplicaciones críticas que se relacionan con riesgo de vida y seguridad de “bienes sensibles”.
- Todo control de seguridad debe ser centralizado.
- Todos los datos enviados por interpretes de SQL deben utilizar interfaces parametrizadas.
- Los controles de validación deben utilizar listas blancas (“comparación positiva”).

OWASP

The Open Web Application Security Project


Categorías de Verificación


Diagrama de niveles de certificación OWASP:

- Nivel 3: 3 requisitos
- Nivel 2: 2 requisitos
- Nivel 1: 1 requisito
- Nivel 0: 0 requisitos

Categorías	Cantidad Requisitos	Level 1	Level 2	Level 3
V1: Arquitectura, diseño y modelado de amenazas	10	1	6	10
V2: Los requisitos de verificación de autenticación	26	17	24	26
V3: Requisitos de verificación de gestión sesión	13	10	12	13
V4: Los requisitos de verificación de Control de acceso	12	7	11	12
V5: Entrada maliciosa manejo de los requisitos de verificación	21	10	20	21
V7: Criptografía en los requisitos de verificación del resto	10	2	7	10
V8: Error manejo y registro de los requisitos de verificación	12	1	7	12
V9: Requisitos de verificación de protección de datos	11	4	8	11
V10: Requisitos de verificación de seguridad de las comunicaciones	13	7	8	13
V11: Requisitos de verificación de seguridad HTTP	8	6	8	8
V13: Los requisitos de verificación de los controles maliciosos	2	0	0	2
V15: Requisitos de verificación de lógica de negocio	2	0	0	2
V16: Archivos y los requisitos de verificación de recursos	9	7	9	9
V17: Requisitos de verificación para mobile	11	6	9	11
V18: Requisitos de verificación para Web Services	10	7	10	10
V19: Configuración	9	1	5	9
Total general	179	86	144	179

OWASP The Open Web Application Security Project		Ejemplo Proceso de Verificación		
Requisitos verificación de la protección de Datos.		Niveles		
		1	2	3
Verificar que todas las formas que contienen información confidencial han desactivado cliente caché de lado, incluyendo características de autocompletar.		x	x	x
Verificar que la lista de datos procesados por esta aplicación se identifica, y que existe una política explícita de cómo acceder a estos datos debe ser controlado, y cuando estos datos deben ser encriptados (tanto en reposo como en tránsito). Verifique que esta política se aplique correctamente.				x
Comprobar que todos los datos delicados se envía al servidor en el cuerpo del mensaje HTTP (es decir, parámetros de URL no se utilizan para enviar datos confidenciales).		x	x	x
Verificar que todas las copias en caché o temporales de los datos confidenciales enviados al cliente están protegidas de accesos no autorizados o purgado/invalidado después de que el usuario autorizado acceda a los datos confidenciales (por ejemplo, se fijan las cabeceras de Cache-Control apropiadas no-cache y no la tienda).			x	x

Ejemplo Proceso de Verificación			
 OWASP The Open Web Application Security Project			
Requisitos verificación de la protección de Datos.	Niveles		
	1	2	3
Verificar que todas las formas que contienen información confidencial han desactivado cliente caché de lado, incluyendo características de autocompletar.	x	x	x
Verificar que la lista de datos procesados por esta aplicación se identifica, y que existe una política explícita de cómo acceder a estos datos debe ser controlado, y cuando estos datos deben ser encriptados (tanto en reposo como en tránsito). Verifique que esta política se aplique correctamente.			x
Comprobar que todos los datos delicados se envía al servidor en el cuerpo del mensaje HTTP (es decir, parámetros de URL no se utilizan para enviar datos confidenciales).	x	x	x
Verificar que todas las copias en caché o temporales de los datos confidenciales enviados al cliente están protegidas de accesos no autorizados o purgado/invalidado después de que el usuario autorizado acceda a los datos confidenciales (por ejemplo, se fijan las cabeceras de Cache-Control apropiadas no-cache y no la tienda).		x	x

Ejemplo Proceso de Verificación			
 OWASP The Open Web Application Security Project			
Requisitos verificación de la protección de Datos.	Niveles		
	1	2	3
Verifique que todas las copias en caché o temporales de los datos confidenciales almacenados en el servidor protegidas de accesos no autorizados o purgado/invalidado después de que el usuario autorizado acceda a los datos confidenciales		x	x
Verifique que no hay un método para eliminar cada tipo de datos confidenciales de la aplicación al final de su período de retención requerido.			x
Verificar que la aplicación minimiza el número de parámetros enviados a sistemas no confiables, tales como campos ocultos, variables de Ajax, cookies y valores de encabezado.			x
Verificar que la aplicación tiene la capacidad de detectar y alerta sobre un número anormal de solicitudes de información o de procesamiento de transacciones de alto valor para ese rol de usuario, tales como pantalla raspado, automatizado uso de prevención de pérdida de datos o mediante extracción de servicio web. Por ejemplo, el usuario promedio no debe ser capaz de acceder a registros más de 5 por hora o 30 por día, o añadir a 10 amigos a una red social por minuto.			x

