OWASP

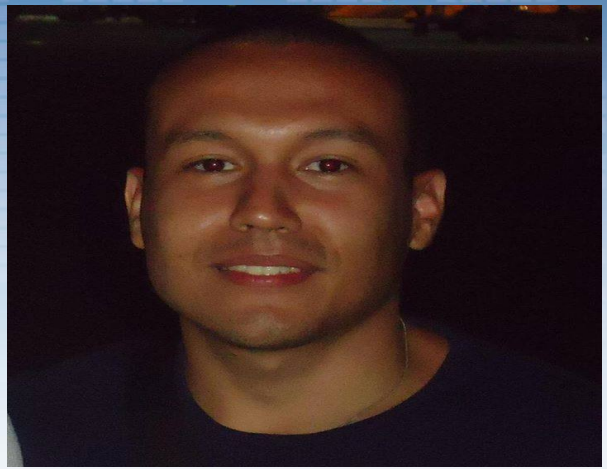
Open Web Application Security Project

# No es culpa del Desarrollador, es de Proceso de entrega S-SDLC.

# Presentador


Gustavo Nieves Arreaza

Titulado: Ingeniero de Sistemas



- Consultor de seguridad
- Certificados : CCNA y CCIA Cisco
- Cursos de programación en .Net y Java( IBM y Microsoft )
- Líder de proyecto en Owasp
- Jefe de proyectos Black Cap ( Seguridad Aplicativos )

Email:Seguridadaplicativos@gmail.com
Pagina web : www.seguridadaplicativos.com

# Estadísticas

OWASP
Open Web Application Security Project

Al preguntar a 12.000 profesionales de la seguridad para nombrar cual es la principal amenaza de seguridad para su organización, el 69% dijo que las vulnerabilidades de la capa de aplicaciones * - sin embargo, menos de un 10% asegura que todas sus aplicaciones críticas de negocio son revisados por la seguridad antes y durante la producción.

Dropbox: 68 millones de cuentas

Ashley Madison: + de 30 millones

Linkedin: 164 millones

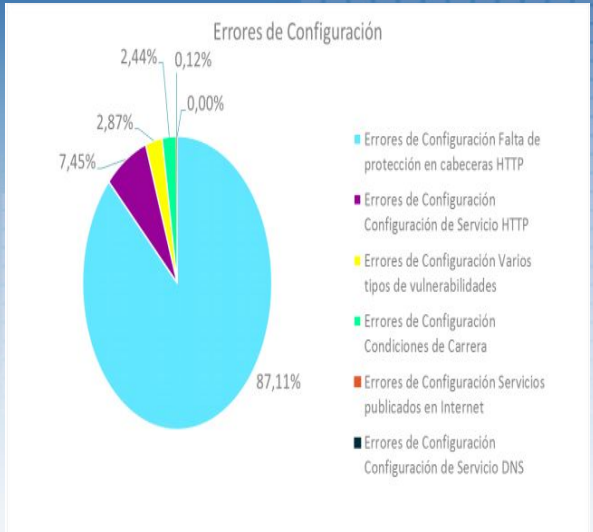
Yahoo + 500 millones

Panama Papers

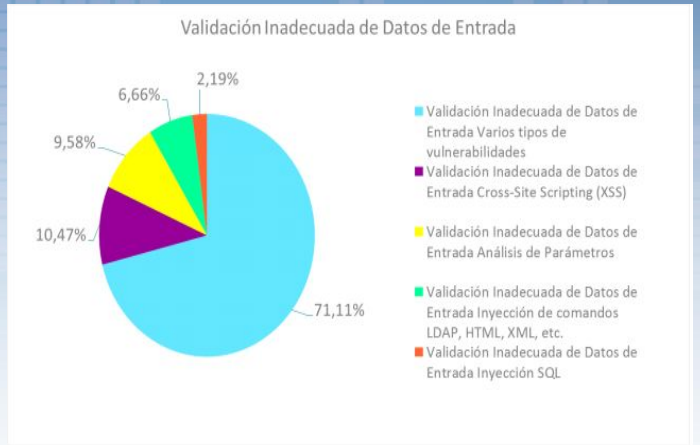
https://tcinet.ru/en/press-centre/technology-news/3863/

# Estadísticas


Configuración:
Aquellos como los que dejan, ficheros de libre acceso o servidores web no actualizados

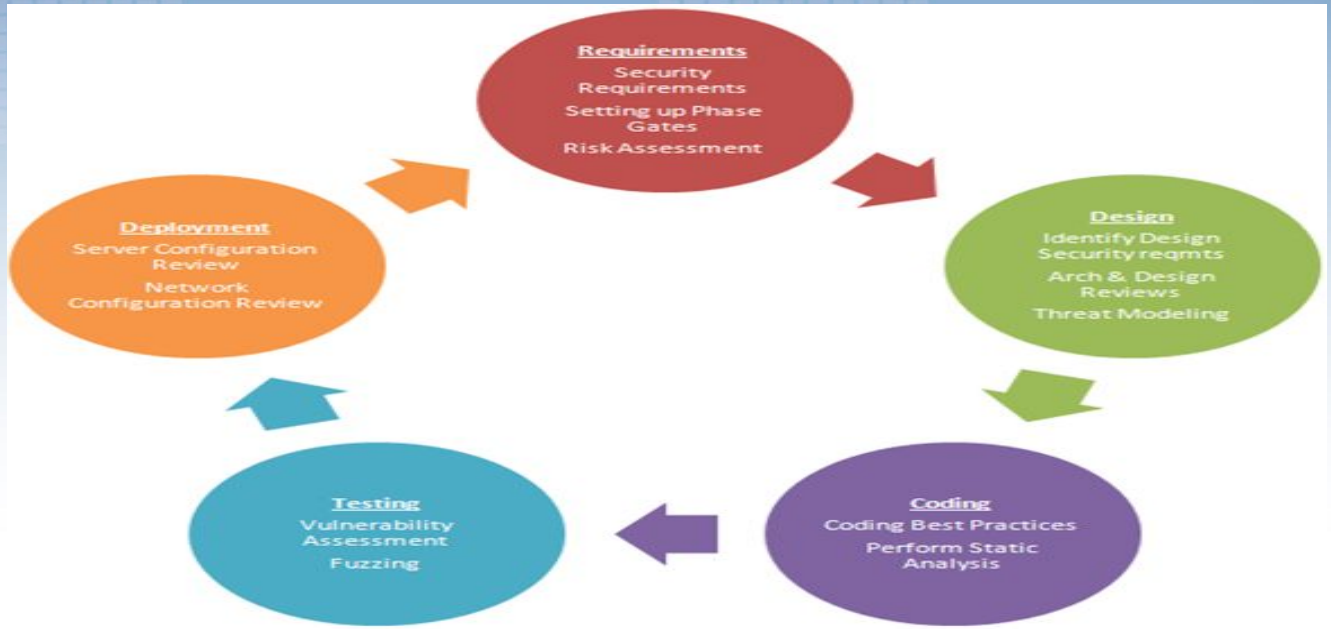



Criptográficos:
Falta de certificados SSL, certificados con Débil encriptación




Cadenas de entrada:
Aquellas que no validan ingresos de datos, ni subida de ficheros

# S-SDLC(Secure Systems Development Life Cycle)

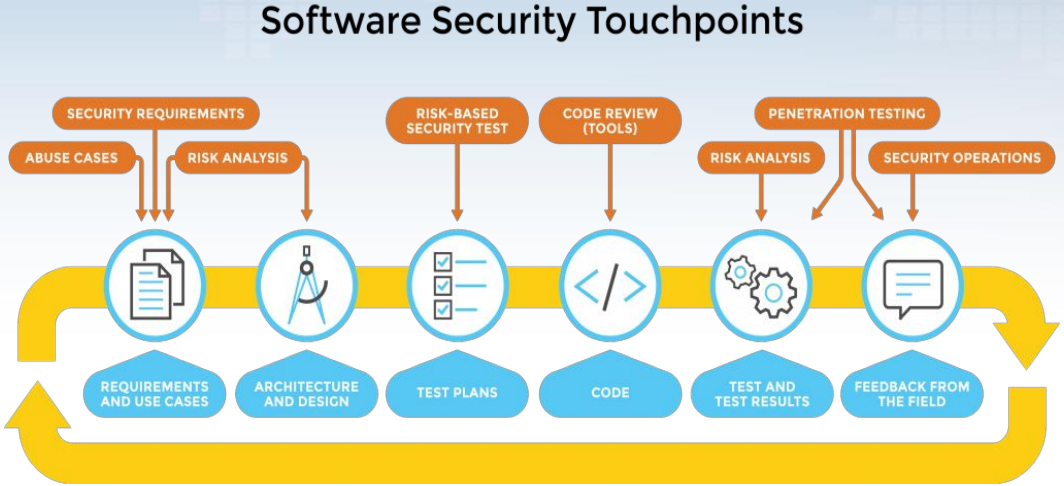


# Modelos de S-SDLC: Security touchpoint

OWASP
Open Web Application Security Project

Propuesto por Gary McGraw en Building Security . Estos puntos de contacto, como se muestra a continuación, presentan un enfoque centrado en el artefacto (diseñado para operar en documentos, diagramas, código, etc.) en lugar de un enfoque centrado en el proceso. Esto, a su vez, hace que el modelo de análisis de seguridad SDLC sea agnóstico.

- Revision de Codigo
- Análisis de riesgo arquitectónico
- Pruebas de penetración
- Pruebas de seguridad basadas en Pruebas de seguridad
- Casos de abuso
- Seguridad de Operaciones
- Requerimientos de seguridad



# Modelos de S-SDLC: MS SDL

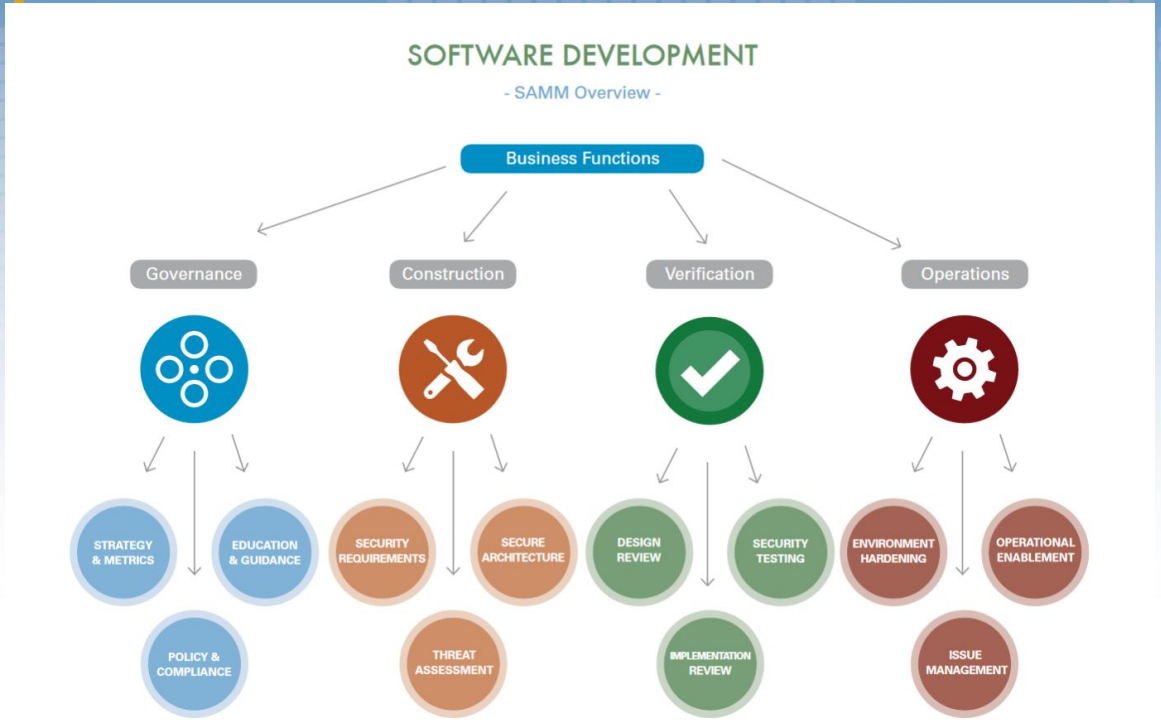
OWASP
Open Web Application Security Project

Ciclo de vida de MS Security Development (MS SDL): Uno de los primeros de su tipo, MS SDL fue propuesto por Microsoft de acuerdo a las fases de un SDLC

| 1. TRAINING | . REQUIREMENTS | 3. DESIGN | 4. IMPLEMENTATION | 5. VERIFICATION | 6. RELEASE | 7. RESPONSE |
|---|---|---|---|---|---|---|
| 1. Core Security Training | 2. Establish Security Requirements | 5. Establish Design Requirements | 8. Use Approved Tools | 11. Perform Dynamic Analysis | 14. Create an Incident Response Plan | Execute Incident Response Plan |
| | 3. Create Quality Gates/Bug Bars | 6. Perform Attack Surface Analysis/ Reduction | 9. Deprecate Unsafe Functions | 12. Perform Fuzz Testing | 15. Conduct Final Security Review | |
| | 4. Perform Security and Privacy Risk Assessments | 7. Use Threat Modeling | 10. Perform Static Analysis | 13. Conduct Attack Surface Review | 16. Certify Release and Archive | |

# S-SDLC Owasp SAMM

SAMM(Software Assurance Maturity Model)



# Entrenamiento

OWASP
Open Web Application Security Project

1.Validación de entrada
2. codificación de salida
3. Autenticación y gestión de contraseñas (incluye el manejo seguro de las credenciales
4. de los servicios / scripts externos)
5. Administración de sesiones
6. Control de acceso
7. Prácticas criptográficos
8. Tratamiento de errores y registro
9. Protección de Datos
10. Seguridad de comunicación
11. Configuración del sistema
12. Seguridad de base de datos
13. Gestión de archivos
14.Gestión de la memoria
15. Prácticas de codificación generales

# Entrenamiento

OWASP
Open Web Application Security Project

## Key references

- Stopping XSS in your web application: OWASP
  - XSS (Cross Site Scripting) Prevention Cheat Sheet
- General information about injection:
  - Top 10 2013-A1-Injection

## Key tools

- OWASP Java Encoder Project
- Microsoft .NET AntiXSS Library
- OWASP ESAPI
- OWASP Encoder Comparison Reference Project

**Proactive: Información general,herramientas que puedes usar**

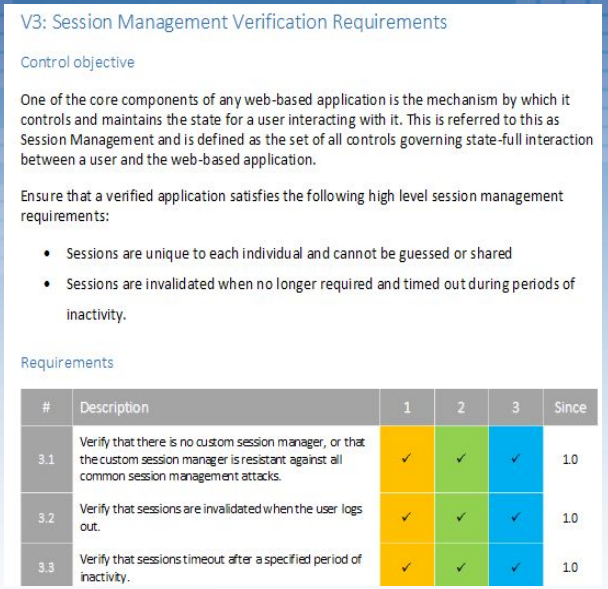
**Web Goat: Prácticas como explotar vulnerabilidades**

# Diseño

OWASP
Open Web Application Security Project

## ASVS

**Estandar de verificación de seguridad aplicaciones**



V3: Session Management Verification Requirements

Control objective

One of the core components of any web-based application is the mechanism by which it controls and maintains the state for a user interacting with it. This is referred to this as Session Management and is defined as the set of all controls governing state-full interaction between a user and the web-based application.

Ensure that a verified application satisfies the following high level session management requirements:

- Sessions are unique to each individual and cannot be guessed or shared
- Sessions are invalidated when no longer required and timed out during periods of inactivity.

Requirements

| # | Description | 1 | 2 | 3 | Since |
|---|---|---|---|---|---|
| 3.1 | Verify that there is no custom session manager, or that the custom session manager is resistant against all common session management attacks. | ✓ | ✓ | ✓ | 1.0 |
| 3.2 | Verify that sessions are invalidated when the user logs out. | ✓ | ✓ | ✓ | 1.0 |
| 3.3 | Verify that sessions timeout after a specified period of inactivity. | ✓ | ✓ | ✓ | 1.0 |

## Threat Modeling:

**Saber que tengo**

Nombre de aplicación: el nombre de La aplicación.
-Versión de la aplicación: la versión De la aplicación.
-Descripción - Una descripción de alto nivel de la aplicación.
-Document Owner - El propietario del documento de modelado de amenazas.

**Risk Ranking: Para establecer el riesgo de una vulnerabilidad**

| Overall Risk Severity | | | | |
|---|---|---|---|---|
| Impact | HIGH | Medium | High | Critical |
| | MEDIUM | Low | Medium | High |
| | LOW | Note | Low | Medium |
| | | LOW | MEDIUM | HIGH |
| | Likelihood | | | |

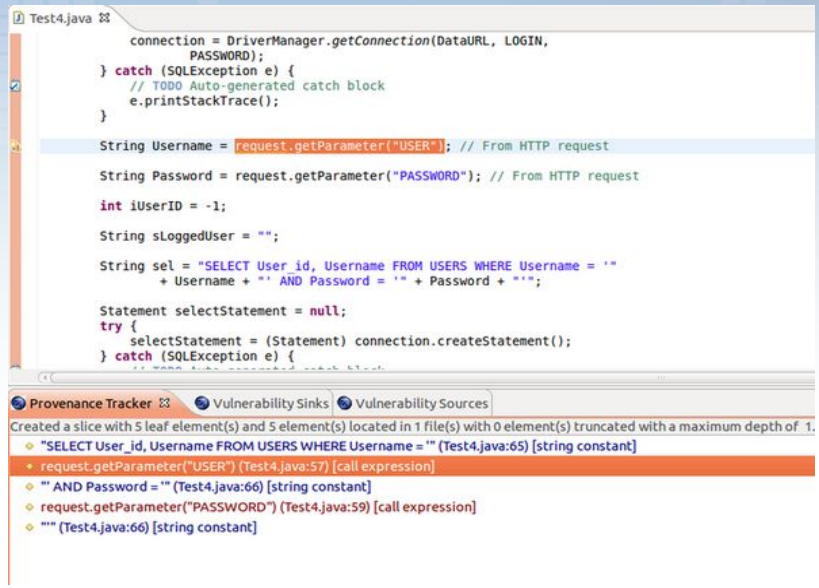
# Desarrollo


ESAPI (The OWASP Enterprise Security API)


Herramienta de análisis de código

Estatico,que Nos permite Medir como vamos

Owasp Lapse




## Response Headers

- HTTP Strict Transport Security (HSTS)
- Public Key Pinning Extension for HTTP (HPKP)
- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- Content-Security-Policy
- X-Permitted-Cross-Domain-Policies

# Verificación

OWASP
Open Web Application Security Project

## ASVS

### Estándar de verificación de seguridad aplicaciones

V3: Session Management Verification Requirements

Control objective

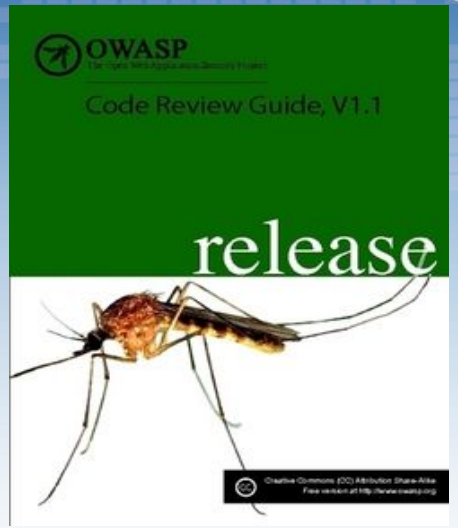
One of the core components of any web-based application is the mechanism by which it controls and maintains the state for a user interacting with it. This is referred to this as Session Management and is defined as the set of all controls governing state-full interaction between a user and the web-based application.

Ensure that a verified application satisfies the following high level session management requirements:

- Sessions are unique to each individual and cannot be guessed or shared
- Sessions are invalidated when no longer required and timed out during periods of inactivity.

Requirements

| # | Description | 1 | 2 | 3 | Since |
|---|---|---|---|---|---|
| 3.1 | Verify that there is no custom session manager, or that the custom session manager is resistant against all common session management attacks. | ✓ | ✓ | ✓ | 1.0 |
| 3.2 | Verify that sessions are invalidated when the user logs out. | ✓ | ✓ | ✓ | 1.0 |
| 3.3 | Verify that sessions timeout after a specified period of inactivity. | ✓ | ✓ | ✓ | 1.0 |



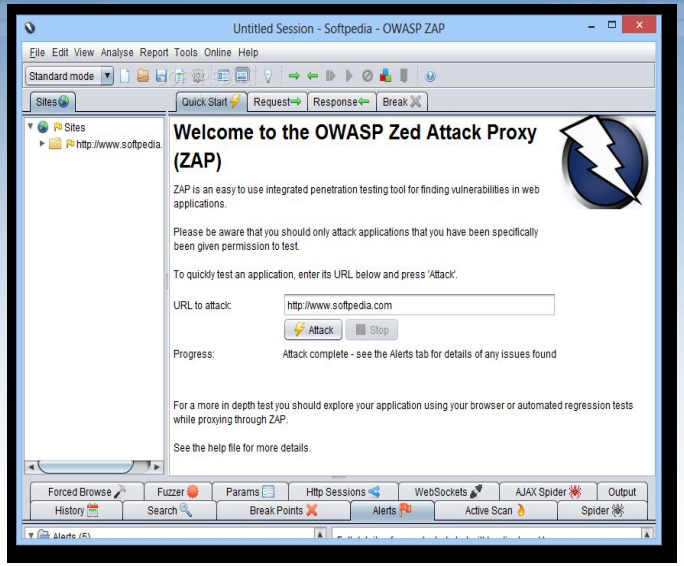

**Code Review Guide:**
Establece parámetros y estándares de soluciones

that allows only users with administrator privileges to access the content.

Figure A5.11
Authorization configuration in IIS

```
<configuration>
  <system.webServer>
    <security>
      <authorization>
        <remove users="*" roles="" verbs="" />
        <add accessType="Allow" users="" roles="Administrators" />
      </authorization>
    </security>
  </system.webServer>
</configuration>
```

# Mantenimiento




Auditar cada entregable

Auditar el proyecto de la raíz del proyecto, separado de los entregables

OWASP
Open Web Application Security Project

# Futuro del SDLC…….

Asegurar la casa desde los cimientos

# References

OWASP
Open Web Application Security Project


https://www.owasp.org/index.php/File:OWASP_CRG_BetaReview.docx
https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf
https://www.owasp.org/index.php/File:OWASP_CRG_BetaReview.docx
https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf
https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
https://www.owasp.org/images/0/07/OWASP_Proactive_Controls_v1.pdf