



# OWASP

## LATIN AMERICA

## TOUR 2012



# OWASP Testing Guide

John Vargas

Open-Sec Senior Security Consultant

OWASP Perú Chapter Leader

[John.Vargas@owasp.org](mailto:John.Vargas@owasp.org)

@John\_Vargas / @OWASP\_Peru

**The OWASP Foundation**

<http://www.owasp.org>



## **Derechos de Autor y Licencia**

Copyright © 2003 – 2012 Fundación OWASP

Este documento es publicado bajo la licencia Creative Commons Attribution ShareAlike 3.0. Para cualquier re-utilización o distribución, usted debe dejar en claro a otros los términos de la licencia sobre este trabajo.

**The OWASP Foundation**  
**<http://www.owasp.org>**

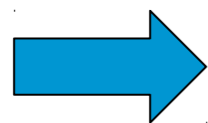


# ¿Guía de Pruebas? Testing Guide?



# Guía de Pruebas de OWASP

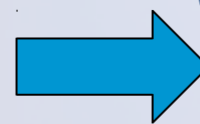
Qué es?



Un documento donde se establecen controles de seguridad como marco base para la realización de pruebas de penetración en las aplicaciones web.

De una manera sencilla se explica el

Que  
Porque  
Cuand  
o  
Como



probar las aplicaciones web y no tan solo proveer un simple checklist.

La intención es que puedan poner en práctica esta guía en sus propias organizaciones.



# Historia

- Julio 14, 2004

"OWASP Web Application Penetration Checklist",  
Versión 1.1

- Diciembre 25, 2006

"OWASP Testing Guide",  
Versión 2.0

- Diciembre 16, 2008

"OWASP Testing Guide", Versión 3.0 – Liberado en el  
OWASP Summit 08

[http://www.owasp.org/index.php/Category:OWASP\\_Testing\\_Project](http://www.owasp.org/index.php/Category:OWASP_Testing_Project)



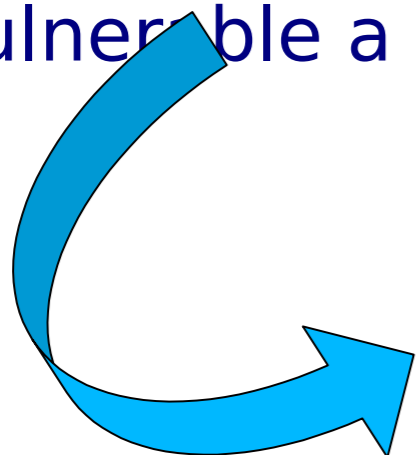
¿Quienes  
deberían  
usarla?



# Para quienes?

## Desarrolladores de Software

Usar la guía para asegurarse que el código que se entrega no es vulnerable a ataque



**No** se puede confiar solo en los testers o grupos de seguridad para que hagan esto por usted



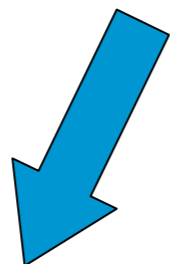
Estos grupos nunca entenderán su aplicación tan bien como **usted**, y por lo tanto nunca será capaz de probar su aplicación tan efectivamente como **usted** puede.

¡La responsabilidad de la seguridad de su código es enfáticamente suyo!



# Para quienes?

## Testers de Software



Deberían usar esta guía para mejorar sus habilidades de evaluación

Pruebas de seguridad han sido artes oscuras?



Las pruebas en esta guía no son complicados y no requieren habilidades especiales o herramientas.

OWASP esta trabajando duro para hacer este conocimiento gratuito y abierto

<http://www.owasp.org>



# Para quienes?

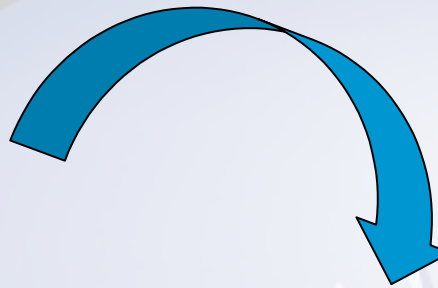
## Especialistas de Seguridad



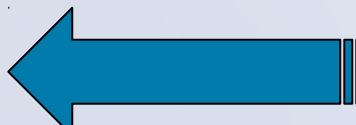
Asegurar que las aplicaciones no se publiquen con vulnerabilidad

Su trabajo es verificar la seguridad de la aplicación completa.

Puede usar esta guía para ayudar a ayudarse en asegurar un nivel de cobertura y rigor



No sea **víctima** de la trampa de simplemente buscar algunas vulnerabilidades básicas



Recomendamos ampliamente usar el Estándar de Seguridad en Aplicaciones de OWASP (ASVS) como una guía también.



# ¿Que contiene?



# Estructura

1. Prólogo
  2. Introducción
  3. Marco de pruebas de OWASP
  4. Pruebas de Penetración en Aplicaciones Web
  5. Redacción de informes: Valorando el riesgo real
- Apéndice A: Herramientas de Comprobación
- Apéndice B: Lecturas recomendadas
- Apéndice C: Vectores Fuzzing
- Apéndice D: Inyección codificada



# Estructura

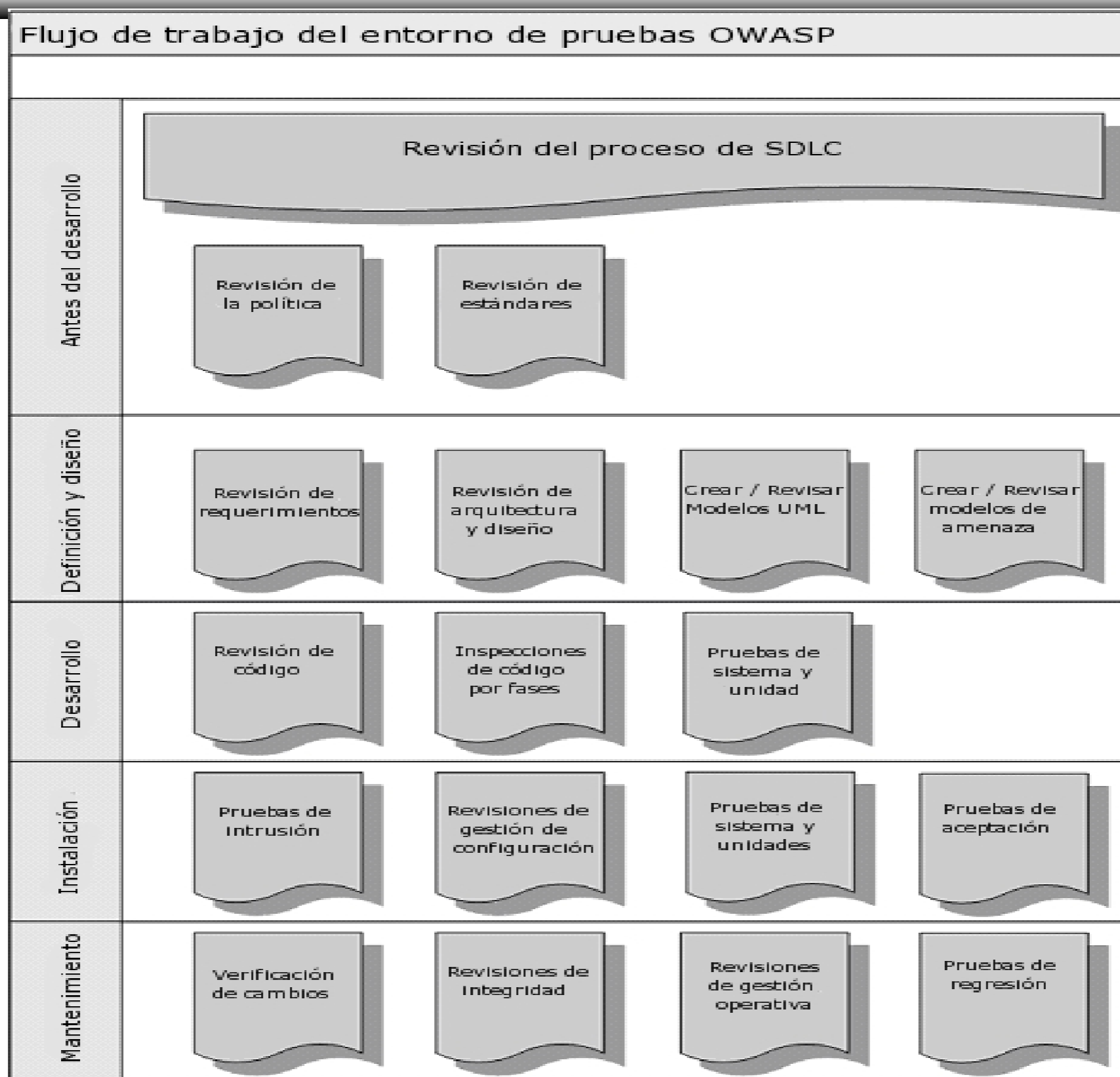
V2 → 8 sub-categorías (48 controles)

V3 → 10 sub-categorías (66 controles)

- Testing Principles
- Testing Process
- Custom Web Applications
  - Black Box Testing
  - Grey Box Testing
- Risk and Reporting
- Appendix: Testing Tools
- Appendix: Fuzz Vectors
- Appendix: Encoded Injection
- Information Gathering
- Configuration Management Testing
- Authentication Testing
- Session Management
- Authorization Testing
- Data Validation Testing
- Business logic testing
- Denial of Service Testing
- Web Services Testing
- Ajax Testing



# Estructura





# Nuevos controles

- 4.1.1 Testing Checklist
- 4.2.3 Identify application entry points
- 4.3.3 Infrastructure Configuration Management Testing
- 4.5.1 Credentials transport over an encrypted channel
- 4.5.2 Testing for user enumeration
- 4.5.8 Testing for CAPTCHA
- 4.5.9 Testing Multiple Factors Authentication
- 4.6.1 Testing for path traversal
- 4.6.2 Testing for bypassing authorization schema
- 4.6.3 Testing for Privilege Escalation
- 4.7.1 Testing for Session Management Schema
- 4.7.2 Testing for Cookies attributes
- 4.8.1 Testing for Reflected Cross Site Scripting
- 4.8.2 Testing for Stored Cross Site Scripting
- 4.8.3 Testing for DOM based Cross Site Scripting
- 4.8.4 Testing for Cross Site Flashing
- 4.8.5.4 MS Access Testing
- 4.8.5.5 Testing PostgreSQL (from OWASP BSP)
- 4.9.1 Testing for SQL Wildcard Attacks
- 4.10.1 WS Information Gathering
- 4.10.2 Testing WSD



# Reportes

Categoría	Número de ref.	Nombre	Elementos afectados	Conclusión	Comentarios/Solución	Riesgo
Recopilación de información	OWASP-IG-001	Robots, Crawlers y Arañas				
	OWASP-IG-002	Motores de Búsqueda Descubrimiento/Reconocimiento				
	OWASP-IG-003	Identificando puntos de entrada en la aplicación				
	OWASP-IG-004	Probando por la firma digital de la aplicación Web				
	OWASP-IG-005	Descubrimiento de aplicación				
	OWASP-IG-006	Análisis de Códigos de Error				
	OWASP-CM-001	Pruebas de SSL/TLS (Versión SSL, Algoritmos, Tamaño de Clave, Validez del Certificado Digital)				
	OWASP-CM-002	Prueba del Listener de la Base de				



# Reportes

## Brief Summary

Describe in "natural language" what we want to test. The target of this section is non-technical people (e.g.: client executive)

## Description of the Issue

Short Description of the Issue: Topic and Explanation

Black Box testing and example

How to test for vulnerabilities:

Result Expected:

...

Gray Box testing and example

How to test for vulnerabilities:

Result Expected:

...

References

Whitepapers

Tools





# ¿Y Como lo implemento?

# Attacker Tactics

From "Open Source Information Gathering" by Chris Gates, Brucon 2009

## Real World Hacking Methodology

carnal0wnage

Discover  
What  
Makes The  
Company  
Money

Discover  
What Is  
Valuable  
To The  
Attacker

Do  
Whatever  
It Takes...

Steal It

<http://carnal0wnage.attackresearch.com/>



# ¿Problemática?

## **Pentesters vs Atacantes**

- Pentesters cuentan con Tiempo/Alcance Limitado
- Pentesters debemos escribir un informe

## **Aplicaciones más complejas**

A mayor complejidad, Mayor tiempo para realizar una evaluación apropiadamente.

Los clientes rara vez están dispuestos a:  
"Pagar lo suficiente / Manejar tiempos razonables"

## **Necesidad de Eficiencia:**

- Debemos buscar vulnerabilidad con mayor rapidez.
- Debemos ser mas eficientes... o los "chicos malos" las encontraran

# Podemos ser mas eficientes?

**¿Es posible que las herramientas, el conocimiento y el análisis humano tengan una coordinación adecuada?**



Imagen: <http://rohaut.blogspot.com/>



# OWTF?

## Offensive (WEB) Testing Framework



# ¿Posibles Soluciones?



Offensive (Web) Testing Framework: An OWASP+PTES-focused try to unite great tools and make pen testing more efficient @owtfp  
<http://owtf.org>  
Author: Abraham Aranguren <name.surname@gmail.com> - <http://7-a.org> - Twitter: @7a\_  
OWTF Version: 0.14 "London"

Current Path: owtf.py

Syntax: owtf.py [ options ] <target1 target2 target3 ...> where target can be: <target URL / hostname / IP>  
NOTE: targets can also be provided via a text file

-l <web/net/aux>: list available plugins in the plugin group (web, net or aux)  
-f: force plugin result overwrite (default is avoid overwrite)  
-i <yes/no> interactive: yes (default, more control) / no (script-friendly)  
-e <except plugin1,2,...> comma separated list of plugins to be ignored in the test  
-o <only plugin1,2,...> comma separated list of the only plugins to be used in the test  
-p (ip:)port setup an inbound proxy for manual site analysis  
-x ip:port send all owtf requests using the proxy for the given ip and port  
-s Do not do anything, simply simulate how plugins would run

<https://github.com/7a/owtf> Abraham Aranguren  
<http://blog.7-a.org> @7a\_  
abraham.aranguren@gmail.com  
<http://7-a.org>



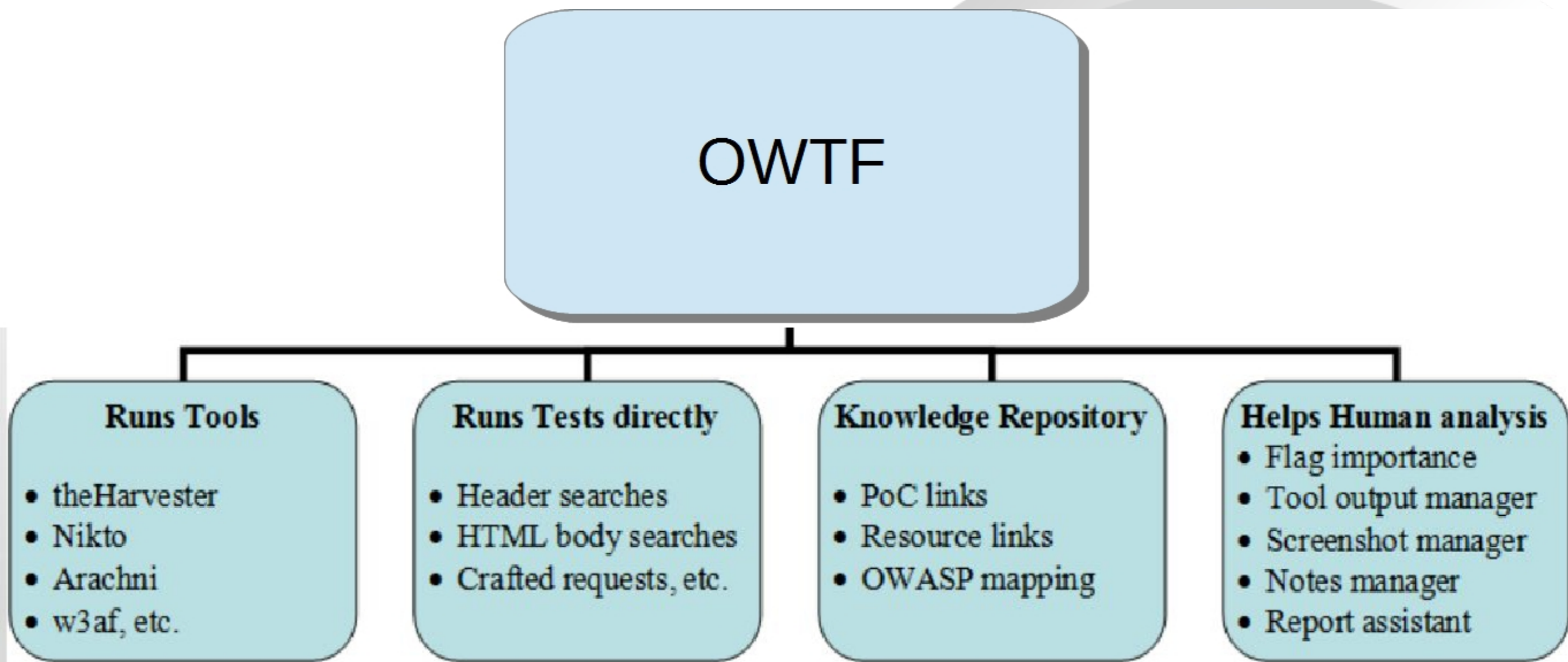
# ¿Posibles Soluciones?

## Maneras de vencer algunas limitantes

- Pruebas Anticipadas (Silenciosas y programadas)
- Automatizar tanto como sea posible (Scripting).
- Pruebas Eficientes (Scripting / Análisis)
- Elaboración de informes eficiente (Plantillas o Scripting)

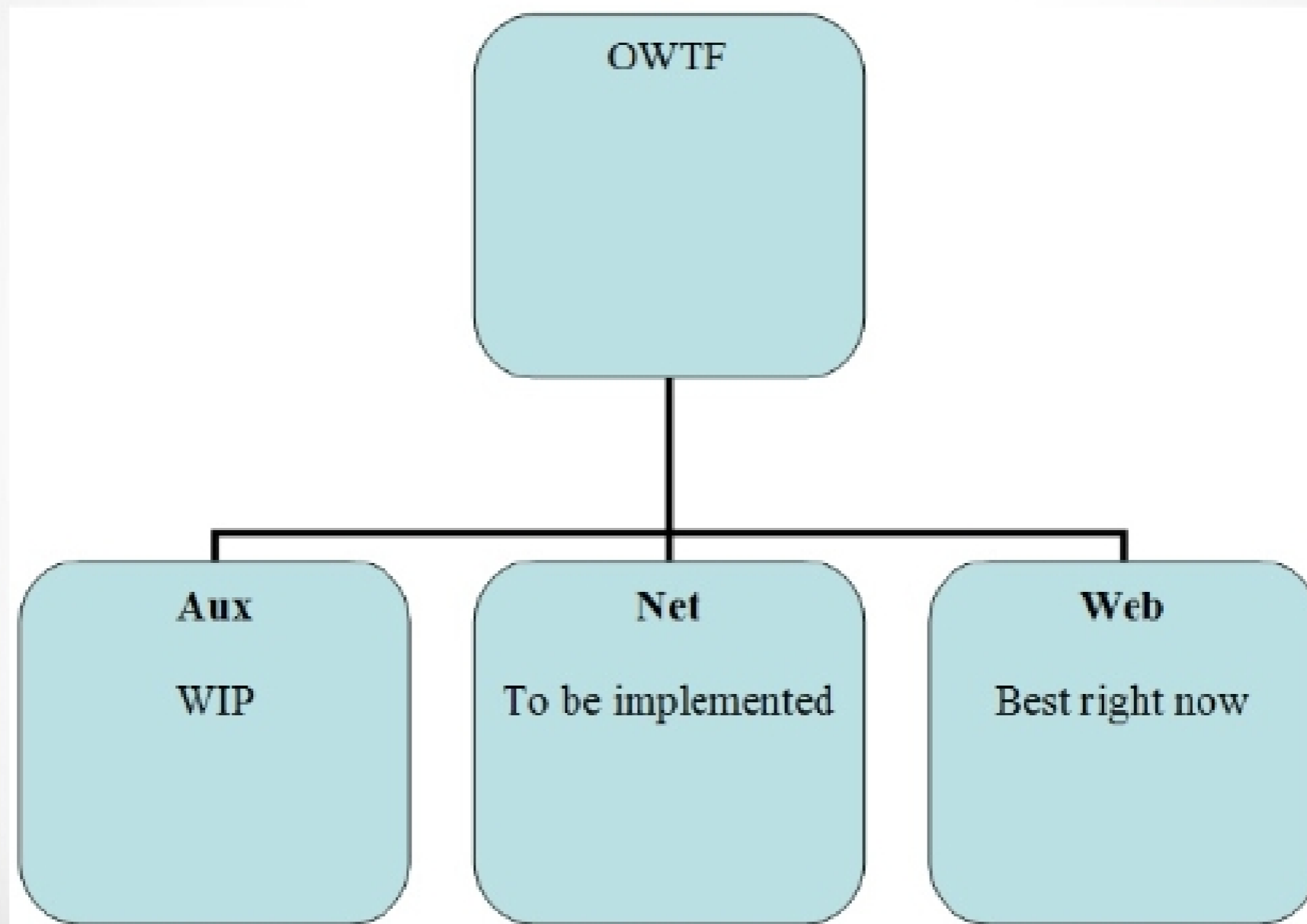


# OWTF





## OWTF Plugin Groups





## **OWFT vs Método Tradicional :**

### **Herramientas existentes:**

- Cumplen de manera efectiva con las actividades puntuales
- Resuelven algunos problemas complejos.
- Sus autores son personas muy inteligentes.
- Hacen posible OWTF.

### **Método Tradicional**

Recordar las pruebas a realizar

Recordar las herramientas /webs utilizadas para cada prueba.

Recordar el mejor orden para ejecutar las herramientas

Muchas herramientas son necesarias y requieren de ejecución manual.



## OWTF

Pruebas son ejecutadas de manera automática

Utiliza las mejores herramientas seleccionada + websites

Llama a las herramientas + webs en un orden recomendado.

Puede implementar otras herramientas para la realización de pruebas.

Todas la herramientas las ejecutan automáticamente por ustedes.

Puedes ejecutar herramientas o controles puntuales

Usarlo por default ejecuta todos los controles

Alineado al OWASP Testing Guide

Alineado a PTES

Puedes obtener un reporte previo casi inmediato. Centralizado del resultado de las herramientas.



# Links de Interes

## **OWASP TESTING PROJECT**

**[https://www.owasp.org/index.php/Category:OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/Category:OWASP_Testing_Project)**

## **Proyectos de OWASP**

**[https://www.owasp.org/index.php/Category:OWASP\\_Project](https://www.owasp.org/index.php/Category:OWASP_Project)**

## **MANTRA**

**<https://getmantra.org>**

## **ENTRENAMIENTOS OWASP**

**[http://www.owasp.org/index.php/OWASP\\_Training](http://www.owasp.org/index.php/OWASP_Training)**

**<http://code.google.com/p/owasp-training/downloads/list>**

## **OWASP WTE**

**<http://appseclive.org>**

## **OWASP BROKENAPPS**



# OWASP

## LATIN AMERICA

### TOUR 2012



# Preguntas?

**John Vargas**

Open-Sec Senior Security Consultant

OWASP Perú Chapter Leader

[John.Vargas@owasp.org](mailto:John.Vargas@owasp.org)

@John\_Vargas / @OWASP\_Peru

**The OWASP Foundation**

<http://www.owasp.org>



# OWASP

## LATIN AMERICA

### TOUR 2012



# OWASP Testing Guide

**John Vargas**

Open-Sec Senior Security Consultant

OWASP Perú Chapter Leader

[John.Vargas@owasp.org](mailto:John.Vargas@owasp.org)

@John\_Vargas / @OWASP\_Peru

**The OWASP Foundation**

<http://www.owasp.org>