Introducción OWASP TESTING GUIDE 4

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

3 Agosto 2015

Pretende alentar a las personas a evaluar y tomar una medida de la seguridad a través de todo el proceso de desarrollo.

Presenta una metodología que recorre de forma organizada y sistemática todas las posibles áreas que supongan vectores de ataque a una aplicación web.

Organiza la auditoria en etapas según el estado de madurez en el desarrollo de la aplicación.

Propone un framework de pruebas donde se identifican y detallan los puntos de control sobre los que se aplicarán los tests correspondientes.

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

3 Agosto 2015

En Castellano versión 3.0 (2009)

Acuerdo Colaboración c

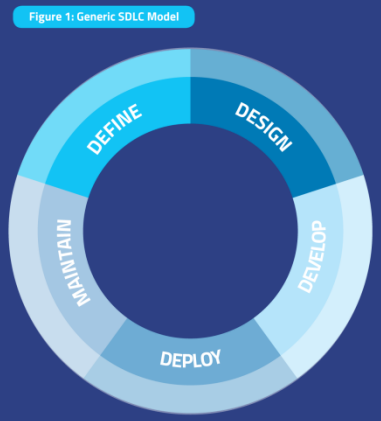
UNIVERSIDAD PABLO DE OLAVIDE SEVILLA

OWASP Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

CICLO DE VIDA Y FRAMEWORK DE PRUEBAS



PERSONAS, PROCESOS y TECNOLOGÍA

3 PRINCIPIOS DEL TESTING

No existe una bala de plata
Pensar estratégicamente, no tácticamente
El SDLC es el rey
Prueba de detección temprana y la prueba de frecuencia
Comprender el alcance de la seguridad
Entender la situación
Utilice las herramientas adecuadas
El diablo está en los detalles
Usa Código Fuente si está disponible
Desarrolla métricas
Documentar los resultados de la prueba

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

TESTING FRAMEWORK WORK FLOW

Esta sección describe un marco de p ruebas típico que pueden ser desarrollado dentro de una organización.

Fase 1: Antes de que comience el desarrollo

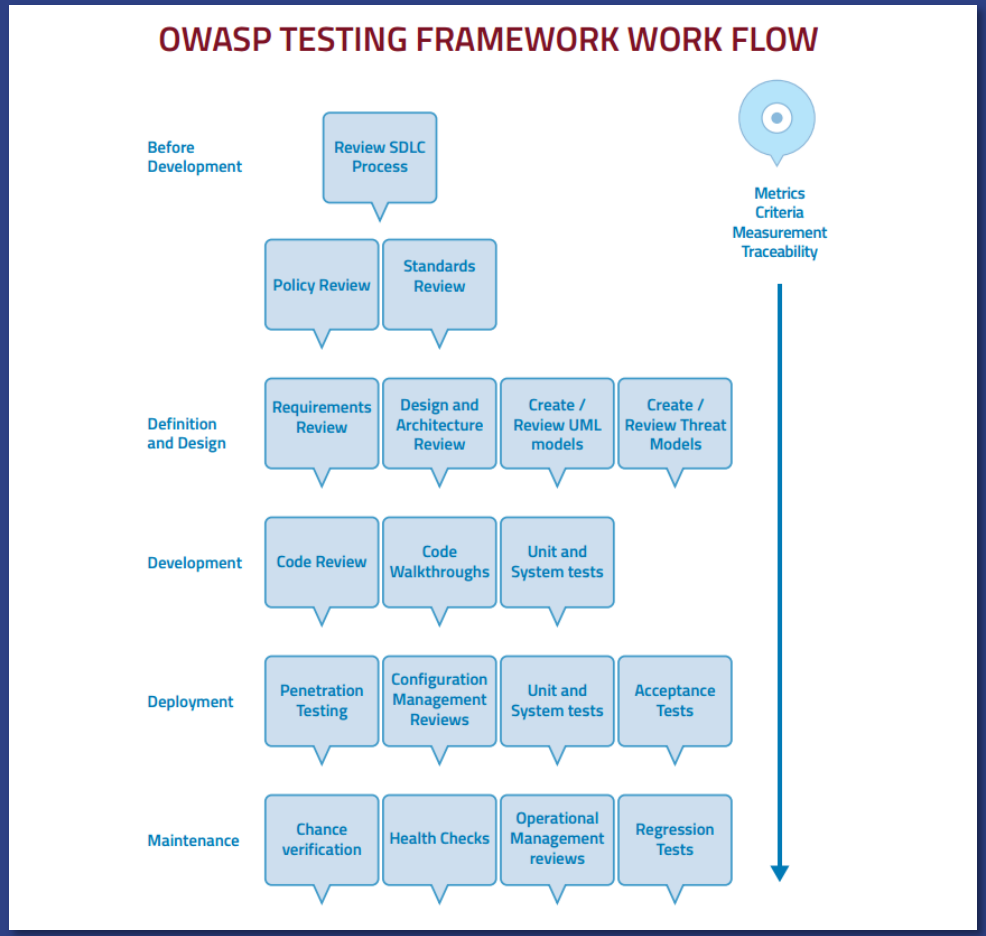
- ↘ Revisar SDLC (Systems Development Life Cycle)
- ↘ Desarrollar métricas y asegurar Trazabilidad

Fase 2: Durante el diseño y definició n

- ↘ Revisión de requisitos de seguridad.
- ↘ Revisión de diseño y arquitectura
- ↘ Crear y revisar modelos UML (Leng. Unif. Modelad)
- ↘ Crear y revisar modelos de amenaza

Fase 3: Durante el desarrollo

- ↘ Code Walkthrough (itinerario proceso de revisión)



OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Information Gathering	Config. & Deploy Management
Identity Management Testing	Authentication Testing
Authorization Testing	Session Management Testing
Input Validation Testing	Error Handling
Cryptography	Business Logic Testing
Client Side Testing	ENJOY ;)

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Information Gathering	
OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage
OTG-INFO-002	Fingerprint Web Server
OTG-INFO-003	Review Webserver Metafiles for Information Leakage
OTG-INFO-004	Enumerate Applications on Webserver
OTG-INFO-005	Review Webpage Comments and Metadata for Information Leakage
OTG-INFO-006	Identify application entry points
OTG-INFO-007	Map execution paths through application
OTG-INFO-008	Fingerprint Web Application Framework
OTG-INFO-009	Fingerprint Web Application
OTG-INFO-010	Map Application Architecture

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Configuration and Deploy Management Testing	
OTG-CONFIG-001	Test Network/Infrastructure Configuration
OTG-CONFIG-002	Test Application Platform Configuration
OTG-CONFIG-003	Test File Extensions Handling for Sensitive Information
OTG-CONFIG-004	Backup and Unreferenced Files for Sensitive Information
OTG-CONFIG-005	Enumerate Infrastructure and Application Admin Interfaces
OTG-CONFIG-006	Test HTTP Methods
OTG-CONFIG-007	Test HTTP Strict Transport Security
OTG-CONFIG-008	Test RIA cross domain policy

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Identity Management Testing	
OTG-IDENT-001	Test Role Definitions
OTG-IDENT-002	Test User Registration Process
OTG-IDENT-003	Test Account Provisioning Process
OTG-IDENT-004	Testing for Account Enumeration and Guessable User Account
OTG-IDENT-005	Testing for Weak or unenforced username policy
OTG-IDENT-006	Test Permissions of Guest/Training Accounts
OTG-IDENT-007	Test Account Suspension/Resumption Process

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Authentication Testing	
OTG-AUTHN-001	Testing for Credentials Transported over an Encrypted Channel
OTG-AUTHN-002	Testing for default credentials
OTG-AUTHN-003	Testing for Weak lock out mechanism
OTG-AUTHN-004	Testing for bypassing authentication schema
OTG-AUTHN-005	Test remember password functionality
OTG-AUTHN-006	Testing for Browser cache weakness
OTG-AUTHN-007	Testing for Weak password policy
OTG-AUTHN-008	Testing for Weak security question/answer
OTG-AUTHN-009	Testing for weak password change or reset functionalities
OTG-AUTHN-010	Testing for Weaker authentication in alternative channel

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Authorization Testing	
OTG-AUTHZ-001	Testing Directory traversal/file include
OTG-AUTHZ-002	Testing for bypassing authorization schema
OTG-AUTHZ-003	Testing for Privilege Escalation
OTG-AUTHZ-004	Testing for Insecure Direct Object References

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Session Management Testing	
OTG-SESS-001	Testing for Bypassing Session Management Schema
OTG-SESS-002	Testing for Cookies attributes
OTG-SESS-003	Testing for Session Fixation
OTG-SESS-004	Testing for Exposed Session Variables
OTG-SESS-005	Testing for Cross Site Request Forgery
OTG-SESS-006	Testing for logout functionality
OTG-SESS-007	Test Session Timeout
OTG-SESS-008	Testing for Session puzzling

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

WEB APPLICATION SECURITY TESTING

Input Validation Testing	
OTG-INPVAL-001	Testing for Reflected Cross Site Scripting
OTG-INPVAL-002	Testing for Stored Cross Site Scripting
OTG-INPVAL-003	Testing for HTTP Verb Tampering
OTG-INPVAL-004	Testing for HTTP Parameter pollution
OTG-INPVAL-006	Testing for SQL Injection
	Oracle Testing
	SQL Server Testing
	Testing PostgreSQL
	MS Access Testing
	Testing for NoSQL injection
OTG-INPVAL-007	Testing for LDAP Injection
OTG-INPVAL-008	Testing for ORM Injection
OTG-INPVAL-009	Testing for XML Injection
OTG-INPVAL-010	Testing for SSI Injection
OTG-INPVAL-011	Testing for XPath Injection
OTG-INPVAL-012	IMAP/SMTP Injection
OTG-INPVAL-013	Testing for Code Injection
	Testing for Local File Inclusion
	Testing for Remote File Inclusion
OTG-INPVAL-014	Testing for Command Injection
OTG-INPVAL-015	Testing for Buffer overflow
	Testing for Heap overflow
	Testing for Stack overflow
	Testing for Format string
OTG-INPVAL-016	Testing for incubated vulnerabilities
OTG-INPVAL-017	Testing for HTTP Splitting/Smuggling

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Testing Guide 4.0

Error Handling	
OTG-ERR-001	Analysis of Error Codes
OTG-ERR-002	Analysis of Stack Traces

Testing Guide 4.0

Cryptography	
OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection
OTG-CRYPST-002	Testing for Padding Oracle
OTG-CRYPST-003	Testing for Sensitive information sent via unencrypted channels

Testing Guide 4.0

Business Logic Testing	
OTG-BUSLOGIC-001	Test Business Logic Data Validation
OTG-BUSLOGIC-002	Test Ability to Forge Requests
OTG-BUSLOGIC-003	Test Integrity Checks
OTG-BUSLOGIC-004	Test for Process Timing
OTG-BUSLOGIC-005	Test Number of Times a Function Can be Used Limits
OTG-BUSLOGIC-006	Testing for the Circumvention of Work Flows
OTG-BUSLOGIC-007	Test Defenses Against Application Mis-use
OTG-BUSLOGIC-008	Test Upload of Unexpected File Types
OTG-BUSLOGIC-009	Test Upload of Malicious Files

OWASP
Open Web Application Security Project
Sevilla CHAPTER

Testing Guide 4.0

Client Side Testing	
OTG-CLIENT-001	Testing for DOM based Cross Site Scripting
OTG-CLIENT-002	Testing for JavaScript Execution
OTG-CLIENT-003	Testing for HTML Injection
OTG-CLIENT-004	Testing for Client Side URL Redirect
OTG-CLIENT-005	Testing for CSS Injection
OTG-CLIENT-006	Testing for Client Side Resource Manipulation
OTG-CLIENT-007	Test Cross Origin Resource Sharing
OTG-CLIENT-008	Testing for Cross Site Flashing
OTG-CLIENT-009	Testing for Clickjacking
OTG-CLIENT-010	Testing WebSockets
OTG-CLIENT-011	Test Web Messaging
OTG-CLIENT-012	Test Local Storage

OWASP
Open Web Application Security Project

Sevilla CHAPTER

Conduct search engine discovery/reconnaissance for information leakage (OTG-INFO-001)

Hay elementos directos e indirectos para el descubrimiento con motores de búsqueda:

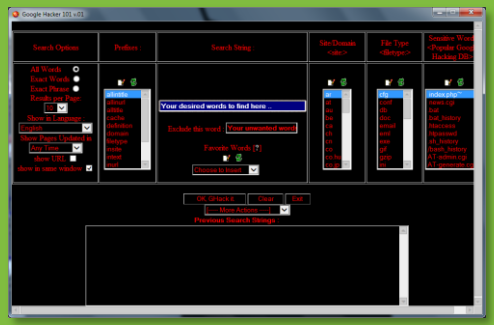
- ↘ Métodos directos se refieren a los índices de la búsqueda y el contenido asociado de cachés.
- ↘ Métodos indirectos se refieren a información sensible del diseño y configuración, buscando foros, grupos de noticias y otros sitios web.

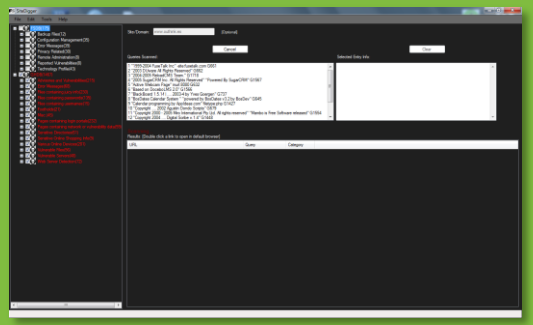
Una vez que un robot del motor de búsqueda ha terminado de recórrela, comienza la indexación de la página web basada en etiquetas y atributos asociados, con el fin de devolver los resultados de búsqueda relevantes. Si el archivo robots.txt no se actualiza durante la vida útil del sitio web y es posible que los índices de contenido de la web, incluyan archivos no deseados.

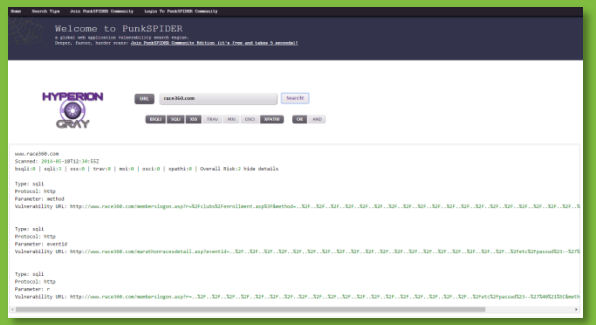
Conduct search engine discovery/reconnaissance for information leakage (OTG-INFO-001)

Tools:

- ↘ FoundStone SiteDigger
- ↘ Google Hacker
- ↘ Stach & Liu's Google Hacking Diggity Project
- ↘ PunkSPIDER







Fingerprint Web Server (OTG-INFO-002)

Obtener las Huellas de un Servidor Web es una tarea fundamental para un test de penetración. Conocer la versión y el tipo de un servidor web en ejecución permite analistas determinar vulnerabilidades conocidas y las técnicas apropiadas para usar durante la prueba.

Esta información puede obtenerse enviando al servidor web comandos específicos y analizando la salida, cada versión del software del servidor web puede responder diferente a estas consultas.

```
$ nc 202.41.76.251 80
HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Mon, 16 Jun 2003 02:53:29 GMT
Server: Apache/1.3.3 (Unix) (Red Hat)
Last-Modified: Wed, 07 Oct 1998
11:18:14 GMT
ETag: "1813-49b-361b4df6"
Accept-Ranges: bytes
Content-Length: 1179
Connection: close
Content-Type: text/html
```

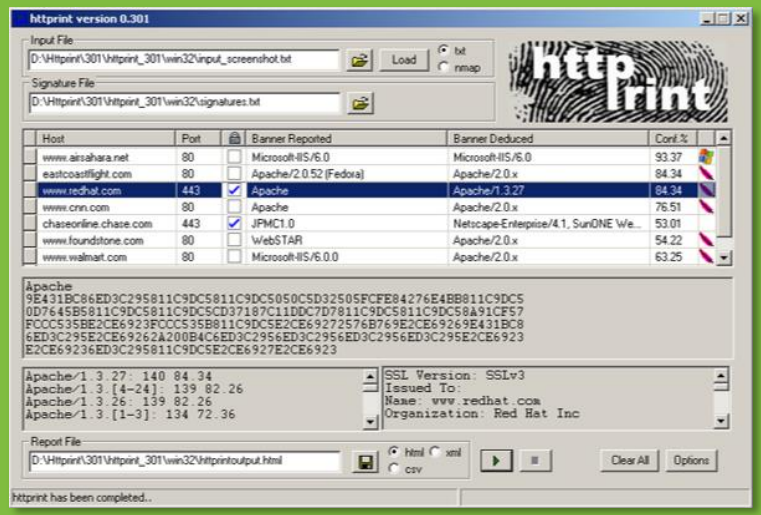
```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Expires: Yours, 17 Jun 2003
01:41: 33 GMT
Date: Mon, 16 Jun 2003 01:41:
33 GMT
Content-Type: text/HTML
Accept-Ranges: bytes
Last-Modified: Wed, 28 May 2003
15:32: 21 GMT
ETag: b0aac0542e25c31: 89d
Content-Length: 7369
```

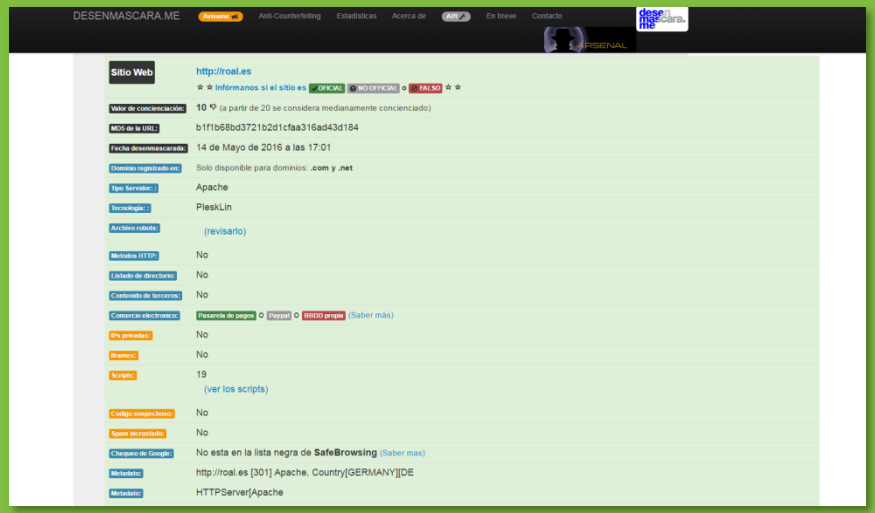
```
HTTP/1.1 200 OK
Server: Sun-ONE-Web-Server/6.1
Date: Tue, 16 Jan 2007 14:53:45
GMT
Content-length: 1186
Content-type: text/html
Date: Tue, 16 Jan 2007 14:50:31
GMT
Last-Modified: Wed, 10 Jan 2007
09:58:26 GMT
Accept-Ranges: bytes
Connection: close
```

Fingerprint Web Server (OTG-INFO-002)

Tools:

- ↘ httprint
- ↘ httprecon
- ↘ Netcraft
- ↘ Desenmascarame





Review Webserver Metafiles for Information Leakage (OTG-INFO-003)

El archivo robots.txt se utiliza para bloquear el acceso a determinados directorios de spiders, robots o crawlers.Esta sección describe cómo probar el archivo robots.txt para evitar fugas de información de la ruta o rutas directorio o carpeta de la aplicación web

```
User-agent: *
Disallow:
Disallow: /_*/
Disallow: /ES/FamiliaReal/Urdangarin/
Disallow: /CA/FamiliaReal/Urdangarin/
Disallow: /EU/FamiliaReal/Urdangarin/
Disallow: /GL/FamiliaReal/Urdangarin/
Disallow: /VA/FamiliaReal/Urdangarin/
Disallow: /EN/FamiliaReal/Urdangarin/
Sitemap: http://www.casareal.es/sitemap.xml
```

```
Disallow: /apuestas/
Disallow: /especiales/urdangarin/
Disallow: /especiales/sucesion-papa/
Disallow: /especiales/caso-barcenas/

Disallow: /especiales/motogp/

Disallow: /especiales/renta-2012/
Disallow: /especiales/turismo/
Disallow: /especiales/tour-francia/
Disallow: /especiales/vuelta-espana/
Disallow: /especiales/esqui/
Disallow: /especiales/declaracion-renta/
Disallow: /especiales/coche-del-anyo/
```

```
User-Agent: *
Disallow: /music/+noredirect/
Disallow: /*/music/+noredirect/
Disallow: /user/*/library/music/
Disallow: /*/user/*/library/music/
Disallow: /*/+wiki/diff

Disallow: /debug
Disallow: /*/debug

# AJAX content
Disallow: /search/autocomplete
Disallow: /*/search/autocomplete
Disallow: /player
Disallow: /*/player

Disallow: /harming/humans
Disallow: /ignoring/human/orders
Disallow: /harm/to/self
```


Everybody needs a hacker