

**1. Conserve  
la calma**



**2. Elimine fuente  
de incendio**



**3. Retirase de  
ventanas y  
objetos que  
pueden caer**



**4. No use  
elevadores**



**5. Ubicarse en  
zonas seguras**



**6. Localice la ruta  
de evacuación**





**APAGA TU**  
**CELULAR**  
**TURN OFF**  
**YOUR CELLPHONE**

**GRACIAS**  
**THANK YOU**



**OWASP**  
Open Web Application  
Security Project



# OWASP LATAM 2017

LATIN AMERICA TOUR





# UTEC

UNIVERSIDAD DE INGENIERÍA  
Y TECNOLOGÍA



**OWASP**  
Open Web Application  
Security Project



# OWASP

Open Web Application  
Security Project

Perú Chapter



OWASP  
Open Web Application  
Security Project

# Sobre el OWASP LATAM TOUR

- Conferencias Gratuitas de Seguridad
- 16 países recorridos durante el mes de abril
- Realizado en Perú desde el 2011
- <https://www.owasp.org/index.php/LatamTour2017>
- @appseclatam - @owasp\_peru
- #OWASPLatamTour2017





# OWASP





# 16

Años de servicio a la comunidad







**OPEN  
INNOVATION  
GLOBAL  
INTEGRITY**

**ADN OWASP**

# 200

## Proyectos Activos







# 250

## Capítulos Activos



60,000+

Participantes en listas de correos



A close-up, vertical view of several old book spines. The spines are made of dark, worn leather with gold-colored lettering and decorative bands. The text on the spines is partially legible, including the word 'LEIS'. The lighting is warm and focused on the central spines, creating a sense of depth and history.

# 100+

Referencias de gobiernos e industrias!



100+

Soportes Académicos



# Sobre OWASP Perú

- Web: <https://www.owasp.org/index.php/Peru>
- Twitter: @owasp\_Peru
- Reuniones: Ultimo Miércoles de cada mes
- > Talleres gratuitos (Mayo)
- OWASP Day (Agosto)
- Conferencia OWASP Latam Tour
- 2 Entrenamientos - OWASP Perú



**OWASP**  
Open Web Application  
Security Project

OWASP

# FLAGSHIP - TOOLS

mature projects

**OWASP Zed Attack Proxy**

**OWASP Web Testing Environment Project**

**OWASP OWTF**

**OWASP Dependency Check**



**OWASP**  
Open Web Application  
Security Project



History Search Alerts Output Spider Active Scan +

New Scan : Progress: 0: http://owasp.org

Id	Req. Timestamp	Resp. Timestamp	Method
21	06/04/17 06:57:35	06/04/17 06:57:36	GET
22	06/04/17 06:57:35	06/04/17 06:57:36	GET
23	06/04/17 06:57:35	06/04/17 06:57:36	GET
24	06/04/17 06:57:35	06/04/17 06:57:36	GET
25	06/04/17 06:57:35	06/04/17 06:57:36	GET

Attack

- Include in Context
- Flag as Context
- Run application
- Exclude from Context
- Resend...
- New Alert...
- Show in History Tab
- Open URL in Browser
- Copy URLs to Clipboard
- Exclude from
- Delete
- Break...
- Alerts for This Node
- Generate Anti-CSRF Test FORM
- Invoke with script...
- Add to Zest Script

Spider... Active Scan... Forced Browse site Forced Browse directory Forced Browse directory (and children) AJAX Spider... Fuzz...

URL to attack: http://misitio.com.uy

Attack Stop

[https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)

OWASP

# FLAGSHIP - CODE

mature projects

**OWASP ModSecurity Core Rule Set Project**

**OWASP CSRFGuard Project**

**OWASP AppSensor Project**



**OWASP**  
Open Web Application  
Security Project



The Core Rule Set provides protection against many common attack categories, including:

SQL Injection (SQLi)  
Cross Site Scripting (XSS)  
Local File Inclusion (LFI)  
Remote File Inclusion (RFI)  
Remote Code Execution (RCE)  
PHP Code Injection  
HTTP Protocol Violations

HTTPoxy  
Shellshock  
Session Fixation  
Scanner Detection  
Metadata/Error Leakages  
Project Honey Pot Blacklist  
GeoIP Country Blocking

[https://www.owasp.org/index.php/Category:OWASP\\_ModSecurity\\_Core\\_Rule\\_Set\\_Project](https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project)



## Chapter 19 : AppSensor and PCI DSS for Ecommerce Merchants

### Introduction

Merchants with web-facing ecommerce applications need to protect cardholder data, whether or not a hosted payment page solution has been implemented.

### Requirement 6.6

The Payment Card Industry (PCI) Security Standards Council requires in-scope public facing web applications to address new threats and vulnerabilities on an ongoing basis PCI Data Security Standard (DSS) in requirement 6.6. One of the two options to meet this requirement is to undertake reviews using manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. The other option is to detect and prevent attacks continuously. In PCI DSS version 2.0 (issued October 2010), this method was worded as follows:

[https://www.owasp.org/index.php/OWASP\\_AppSensor\\_Project](https://www.owasp.org/index.php/OWASP_AppSensor_Project)



**OWASP**  
Open Web Application  
Security Project



OWASP

# FLAGSHIP - DOCs

mature projects

**OWASP ASVS**

**OWASP Software Assurance Maturity Model**

**OWASP AppSensor Project**

**OWASP Top Ten Project**

**OWASP Testing Guide Project**



**OWASP**  
Open Web Application  
Security Project



[https://www.owasp.org/index.php/OWASP\\_SAMM\\_Project](https://www.owasp.org/index.php/OWASP_SAMM_Project)

# )release(



Project Leaders: Matteo Meucci and Andrew Muller

Creative Commons (CC) Attribution Share-Alike  
Free version at <http://www.owasp.org>

## How to test

Testing for access to administrative functions

For example, suppose that the 'AddUser.jsp' function is part of the administrative menu of the application, and it is possible to access it by requesting the following URL:

```
https://www.example.com/admin/addUser.jsp
```

Then, the following HTTP request is generated when calling the AddUser function:

```
POST /admin/addUser.jsp HTTP/1.1
```

```
Host: www.example.com
```

```
[other HTTP headers]
```

```
userID=fakeuser&role=3&group=grp001
```

What happens if a non-administrative user tries to execute that request? Will the user be created? If so, can the new user use their privileges?



**OWASP**

The Open Web Application Security Project

# OWASP Top 10 - 2017 rc1

The Ten Most Critical Web Application Security Risks

**Release Candidate**

Comments requested per instructions within

# release



Creative Commons (CC) Attribution Share-Alike  
Free version at <https://www.owasp.org>

[https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

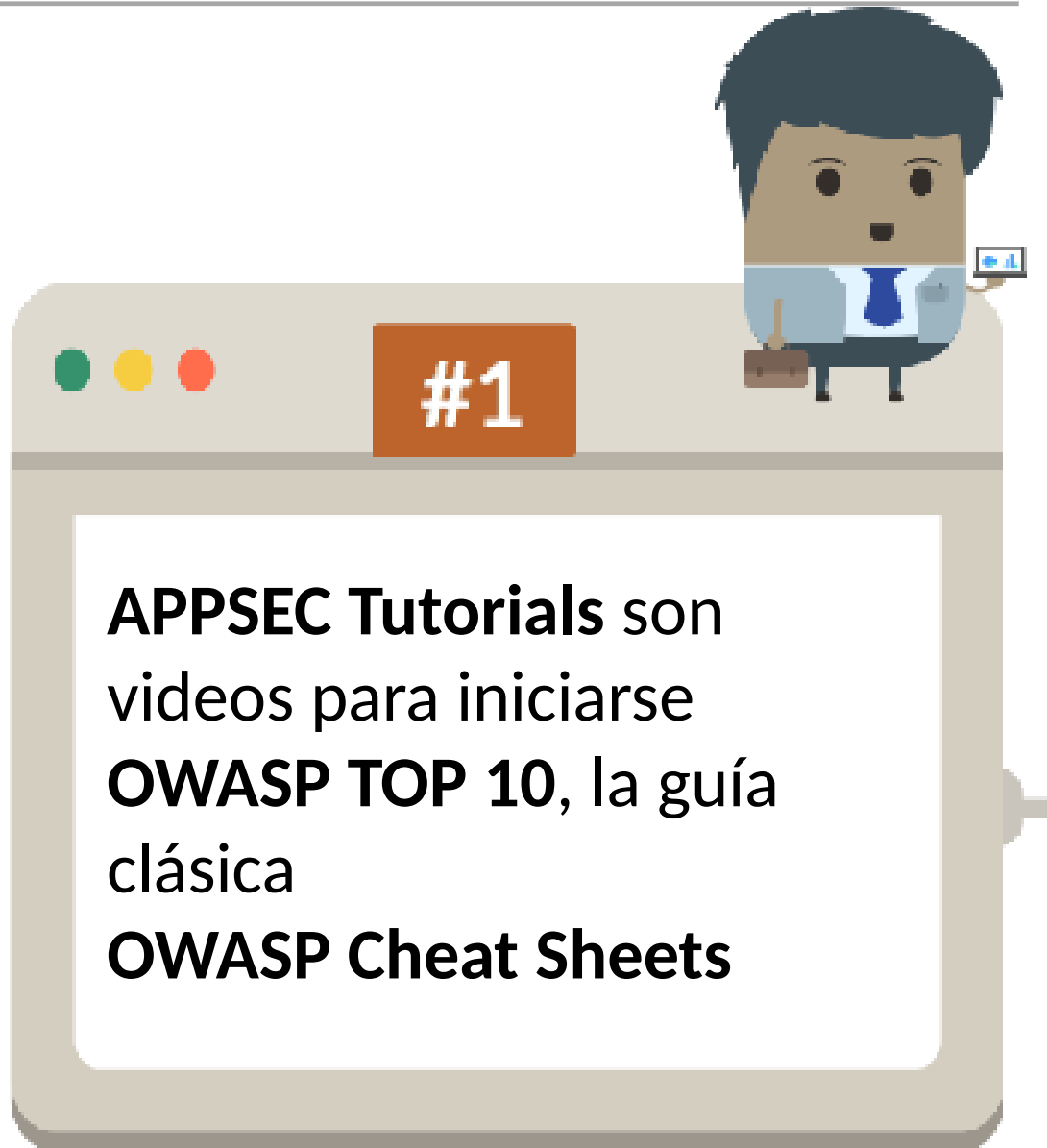


**OWASP**

Open Web Application  
Security Project



# Soy nuevo en esto, ¿por dónde puedo empezar?



[https://www.owasp.org/index.php/OWASP\\_Project\\_Inventory](https://www.owasp.org/index.php/OWASP_Project_Inventory)

# Quiero entender y analizar vulnerabilidades



**Security Shepherd**, juego CTF para aprender  
**WebGoat**, sitio vulnerable Java y .Net con lecciones para programadores  
**OWASP Bricks**, un sitio web PHP vulnerable con lecciones

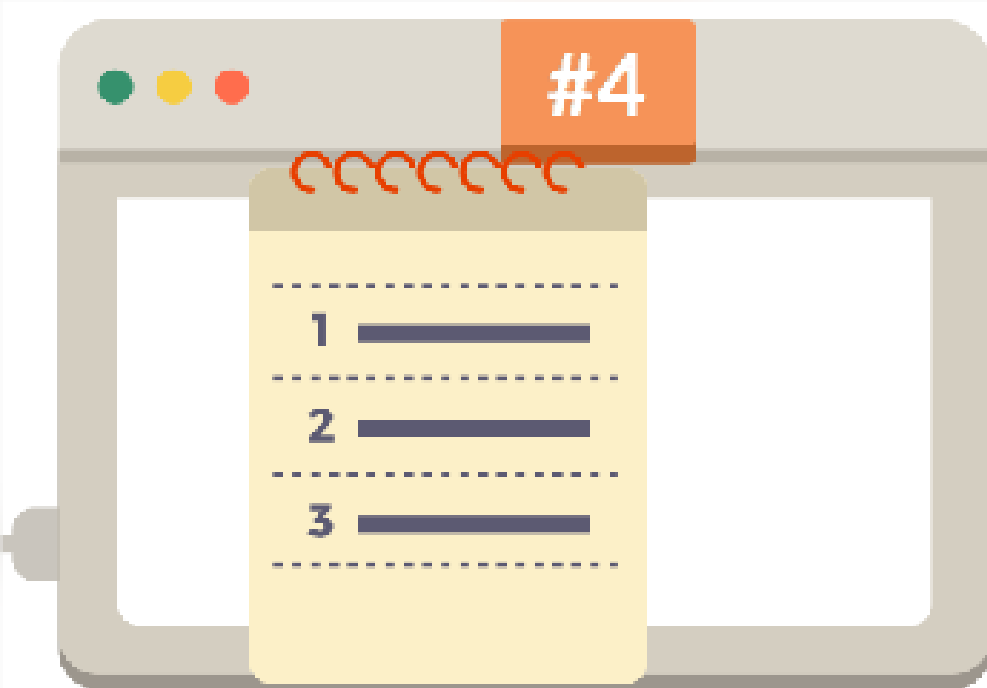
# Quiero utilizar herramientas de pentesting y hacer pruebas



**OWASP ZAP**, es un proxy de ataque, “creme de la creme” tool para hackear tu propio sitio

**OWTF**, un framework completo de pentesting alineado a los últimos estándares de seguridad

**Xenotix Exploit**, para experimentar con XSS

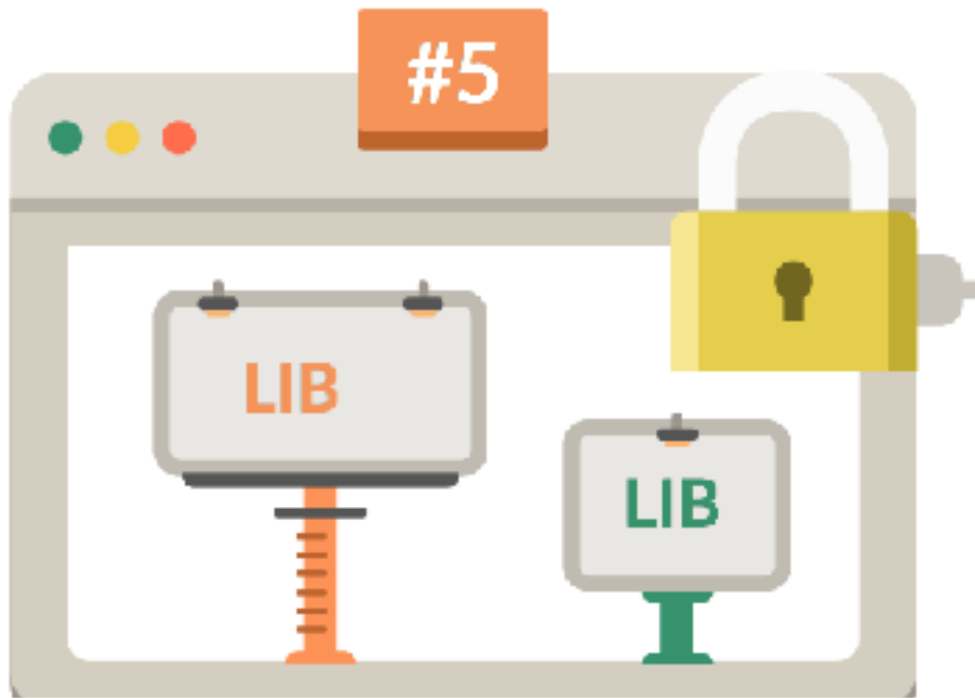


## Quiero entender y analizar vulnerabilidades

**OWASP ASVS** es “La Lista” para aplicar al proceso de desarrollo. Son controles técnicos de seguridad.

**Secure Coding Practices Quick Reference Guide** es una checklist para integrar en el SDLC con prácticas y requerimientos de seguridad





## Quiero Asegurar mi sitio web

**APPSENSOR** es un detector de intrusos en su sitio  
**OWASP HTML Sanitizer** permite incorporar código HTML de terceros pero manteniendo la protección contra XSS.  
**CRSFGuard**, protege su sitio contra ataques de CRSF.



**Dependency-Check** es una herramienta que identifica dependencias y valida si ha vulnerabilidades conocidas. Dependencias en Java, .Net y Python se encuentran soportadas.



¿Existe alguna guía para programadores?

**OWASP Developer Guide** es el proyecto original de OWASP, publicado por primera vez en 2002.



**Me gustaría poder analizar código fuente con más detalle**

**CODE REVIEW GUIDELINES** indican como validar y revisar el código fuente en búsqueda de vulnerabilidades

**O2 PLATFORM** permite un análisis estático robusto junto con ser una herramienta poderosa para prototipos y desarrollo ágil en .Net



# Otros proyectos de OWASP

- OWASP Application Security Guide For CISOs Project
- OWASP Cornucopia
- OWASP Proactive Controls
- OWASP Broken Web Applications Project





# OWASP

Open Web Application  
Security Project

Perú Chapter





# OWASP

Open Web Application  
Security Project

## Guía de Seguridad en Aplicaciones para CISOs

El **Guía de Seguridad en Aplicaciones para CISOs versión 1.0** documento es una traducción al español del documento oficial en inglés "[Application Security Guide For CISOs](#)" de OWASP.

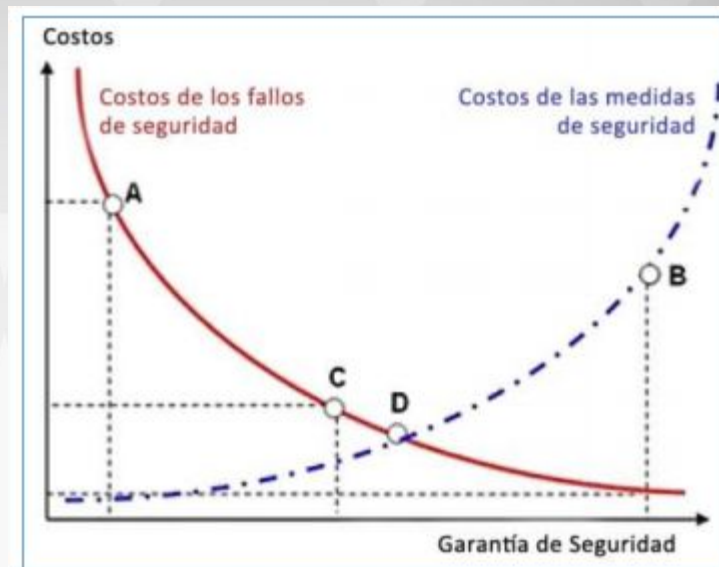


Figura 3 - Costo de los fallos vs los costos de las medidas de seguridad

Parte I: Razones para invertir en Seguridad de Aplicaciones.....	12
Parte II: Criterios para gestionar riesgos de seguridad en aplicaciones .....	35
Parte III: Programa de Seguridad de Aplicaciones .....	67
Parte IV: Métricas para Gestionar Riesgos e Inversiones en Aplicaciones de Seguridad .....	88


[https://www.owasp.org/index.php/Application\\_Security\\_Guide\\_For\\_CISOs](https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs)



OWASP  
Open Web Application  
Security Project



# AGENDA

DETALLES DE LA JORNADA		
Horario	Tema	Ponente
9:00 am	Acreditación	OWASP PERU
10:00 am	Presentación del evento - Proyectos OWASP	<a href="#">John Vargas</a> 
10:30 am	Atacando servicios web en el mundo real	Luis Quispe
11:30 am	Retos de la ciberseguridad en la transformación digital	Jorge Córdova
12:30 pm	Iniciandome en el Desarrollo Seguro ¿Por dónde empiezo?	Gabriel Robalino
15:00 pm	Prácticas seguras de criptografía en aplicaciones web	Henry Sanchez
16:00 pm	SQL Injection Deep Dive	Mateo Martínez [Uruguay]



# OWASP

Open Web Application  
Security Project

¡Muchas Gracias!

Capítulo OWASP Perú

Abril 2017