



A real ZAP Story

Mateo Martínez, CISSP
OWASP Uruguay

 **OWASP**
The Open Web Application Security Project

 **McAfee**
An Intel Company



OWASP APPSEC LATAM 2012

NOV 18-21 / VENUE: ANTEL / MONTEVIDEO / URUGUAY

Gold Sponsor 


Silver Sponsors  

Conference Room Sponsor 

Venue Sponsor 

Academic Supporters  

Organizational Supporters  



OWASP
The Open Web Application Security Project


A real ZAP story

The OWASP Zed Attack Proxy



OWASP
The Open Web Application Security Project

¿Real?



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Practical Identification of SQL Injection Vulnerabilities

Chad Dougherty

Background and Motivation


The class of vulnerabilities known as SQL injection continues to present an extremely high risk in the current network threat landscape. In 2011, SQL injection was ranked first on the MITRE



OWASP
The Open Web Application Security Project

ZAP

www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project



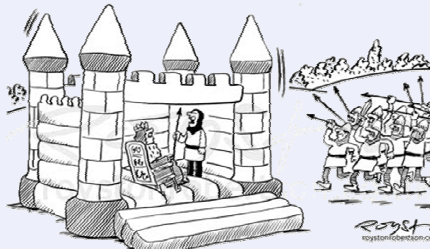
OWASP
The Open Web Application Security Project

Introducción

El enunciado
No se pueden desarrollar aplicaciones seguras si no sabemos como atacarlas

El problema
Para muchos programadores, (y gerentes) hablar de "penetration testing" o "ethical hacking" es hablar de un arte oscuro


La solución
Enseñar técnicas básicas de pentesting a los programadores



"This was fine for your nephew's fifth, Sire, but I fear it is set for a sterner test."

Thanks to Royston Robertson www.roystonrobertson.co.uk for permission to use his cartoon!

Advertencia




OWASP
The Open Web Application Security Project

Esto es solo un adicional a:


- ◆ Enseñar técnicas de codificación segura
- ◆ Enseñar sobre las vulnerabilidades y riesgos más comunes (ej: OWASP top 10)
- ◆ Seguridad en el Ciclo de Vida de Desarrollo de Software
- ◆ Análisis de seguridad del código fuente
- ◆ Pentesting realizado por profesionales

The Zed Attack Proxy



OWASP
The Open Web Application Security Project

- ◆ Lanzado en septiembre de 2010
- ◆ Facilidad de uso
- ◆ Páginas de ayuda muy simples
- ◆ Libre y abierto (Open source)
- ◆ Multi-plataforma
- ◆ Un “fork” del conocido **Paros Proxy**
- ◆ Comunidad de programadores muy activa
- ◆ Adoptado por OWASP en octubre de 2010



En poco tiempo...













OWASP ZAP <http://crowdin.net/project/owasp-zap>

Translations for the OWASP Zed Attack Proxy: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

If you'd like to translate ZAP to a language not on the list then let us know and we'll add it.


Choose the language you want to translate to. The original language is English, United Kingdom.

Needs Translation


 French 13% completed	 Spanish 31% completed	 Danish 25% completed	 German 87% completed	 Greek 43% completed
 Japanese 27% completed	 Polish 11% completed	 Russian 12% completed	 Chinese Simplified 15% completed	 Portuguese, Brazilian 26% completed
 Bahasa Indonesia 25% completed	 Persian 28% completed			

◆ Paros code: ~30% Zap Code: ~70%

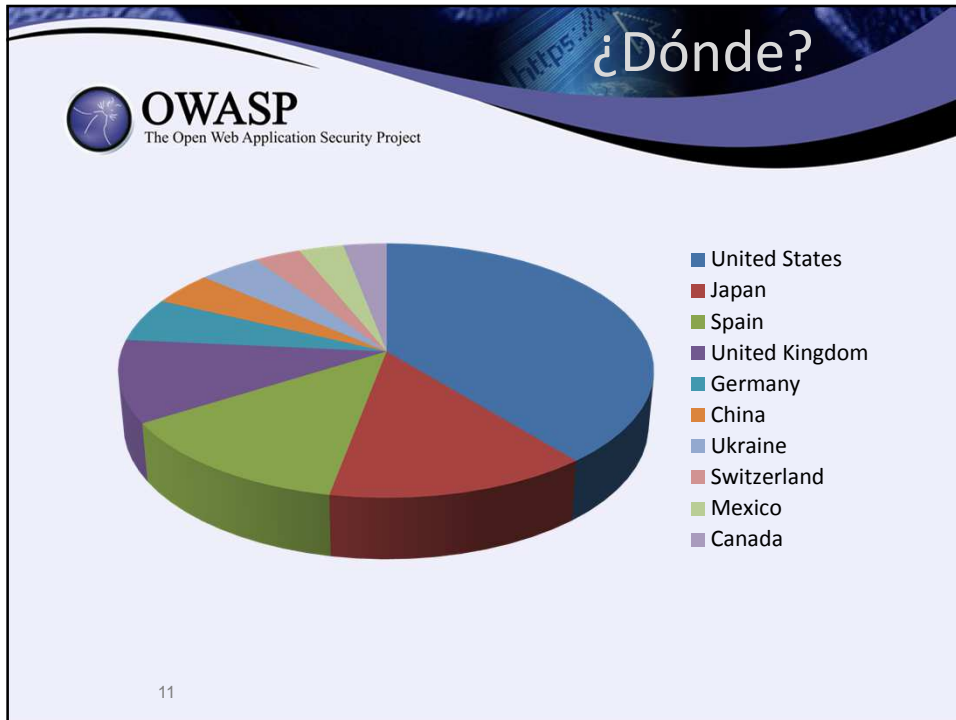
Los pilares


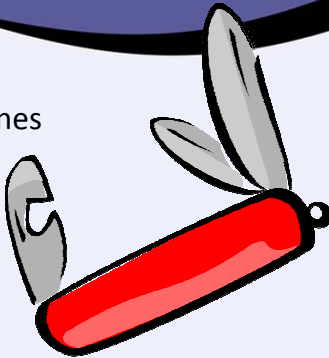
 **OWASP**
The Open Web Application Security Project

- ◆ Libre, Open source
- ◆ Multi-plataforma
- ◆ Fácil de usar
- ◆ Fácil de instalar
- ◆ Internacionalizable
- ◆ 100% Documentado
- ◆ Desarrollo activo
- ◆ Reutilización de componentes




CoolClips.com




- ## Funcionalidades
- 
- OWASP**
The Open Web Application Security Project
- 
- ◆ Lo esencial para testing de aplicaciones
 - ◆ Intercepting Proxy
 - ◆ Informes
 - ◆ Escaner automático
 - ◆ Escaner Activo y Pasivo
 - ◆ Escaner de Fuerza bruta
 - ◆ Spider
 - ◆ Fuzzer
 - ◆ Certificados SSL Dinámicos
 - ◆ API
- 12

Funcionalidades (2)




OWASP
The Open Web Application Security Project

- ◆ Auto tagging
- ◆ Port scanner
- ◆ Smart card support
- ◆ Session comparison
- ◆ Invoke external apps
- ◆ BeanShell integration
- ◆ API + Headless mode
- ◆ Anti CSRF token handling




13

Lo nuevo en v1.4




OWASP
The Open Web Application Security Project

- ◆ Syntax highlighting
- ◆ Fuzzdb integration
- ◆ Parameter analysis
- ◆ Enhanced XSS scanner
- ◆ Pluggable extensions
- ◆ Reveal hidden fields
- ◆ Some of the Watcher checks
- ◆ Lots of bug fixes!




14

Extensiones ZAP



OWASP
The Open Web Application Security Project


- ◆ Invoking applications directly
- ◆ REST API
- ◆ Filters
- ◆ Active Scan Rules
- ◆ Passive Scan Rules
- ◆ Full Extensions



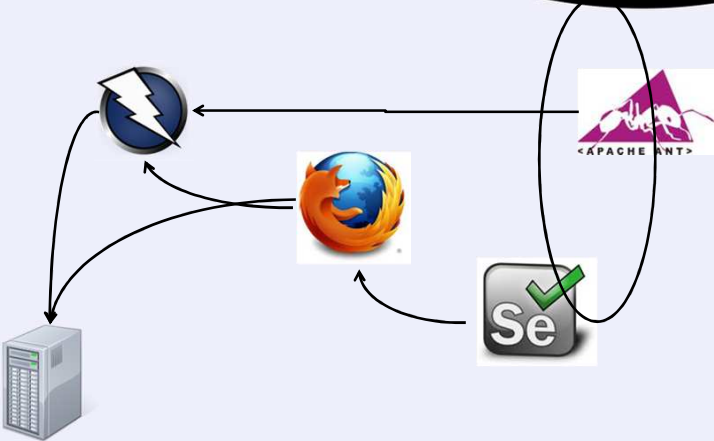
<https://code.google.com/p/zap-extensions/>

15

Security Regression Tests




OWASP
The Open Web Application Security Project



<http://code.google.com/p/zaproxy/wiki/SecRegTests>

16



OWASP
The Open Web Application Security Project


API

The ZAP API

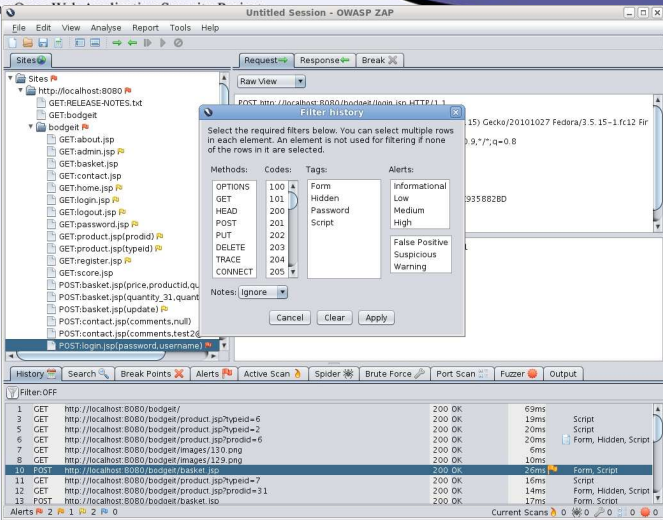
ZAP tiene una API abierta

¿Cómo habilitar la API?
Tools / Options... / API

La API es muy utilizada en los [Security Regression Tests](#)



Demo/Video




The screenshot shows the OWASP ZAP interface. A 'Filter history' dialog box is open, allowing the user to select filters for the current request. The dialog has three columns: Methods, Codes, and Alerts. The 'Methods' column includes OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, and CONNECT. The 'Codes' column includes 100, 101, 200, 201, 202, 203, 204, and 205. The 'Alerts' column includes Form, Hidden, Password, Script, Informational, Low, Medium, High, False Positive, Suspicious, and Warning. The 'Notes' dropdown is set to 'Ignore'. Below the dialog, the 'History' pane shows a list of requests with columns for Method, URL, Status, Time, and Alerts. The current request is a POST to http://localhost:8080/bodget/basket.jsp.

Method	URL	Status	Time	Alerts
1	CET http://localhost:8080/bodget/	200 OK	69ms	
3	CET http://localhost:8080/bodget/product.jsp?productId=6	200 OK	19ms	Script
5	CET http://localhost:8080/bodget/product.jsp?productId=2	200 OK	20ms	Script
6	CET http://localhost:8080/bodget/product.jsp?productId=6	200 OK	20ms	Form, Hidden, Script
7	CET http://localhost:8080/bodget/images/13.0.png	200 OK	6ms	
8	CET http://localhost:8080/bodget/images/13.9.png	200 OK	10ms	
10	POST http://localhost:8080/bodget/basket.jsp	200 OK	20ms	Form, Script
11	CET http://localhost:8080/bodget/product.jsp?productId=7	200 OK	16ms	Script
12	CET http://localhost:8080/bodget/product.jsp?productId=3.1	200 OK	14ms	Form, Hidden, Script
13	POST http://localhost:8080/bodget/basket.jsp	200 OK	17ms	Form, Script


Alerts: 2 1 2 0

Próximos pasos




OWASP
The Open Web Application Security Project

- ◆ Mejorar los escaneos de vulnerabilidades
- ◆ Extender la API y mejorar integración
- ◆ Análisis de Fuzzing
- ◆ Más fácil de usar, más documentación
- ◆ Parametrización
- ◆ Detección de tecnologías
- ◆ ¿Algo más? Todos pueden ser parte 😊



19

Resumen




OWASP
The Open Web Application Security Project

ZAP es:

- ◆ Fácil de usar (para ser una pentest tool)
- ◆ Ideal para los que comienzan en seguridad en aplicaciones
- ◆ Ideal para entrenamientos
- ◆ Utilizada también por Pen Testers profesionales
- ◆ Se puede contribuir fácilmente
- ◆ Mejora día a día, rápidamente

20

Resumen (2)



OWASP
The Open Web Application Security Project

ZAP tiene:

- ◆ Una comunidad activa de desarrolladores
- ◆ Usuarios internacionales
- ◆ El potencial de llegar a personas nuevas en OWASP y en Seguridad, especialmente desarrolladores y testers funcionales

ZAP es un proyecto clave dentro de OWASP

21



¿Preguntas?

http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
Mateo Martínez
mateo.martinez@owasp.org