

# Seguridad en bases de datos

José María Alonso Cebrián  
Vicente Díaz Sáez  
Antonio Guzmán Sacristán  
Pedro Laguna Durán  
Alejandro Martín Bailón

PID\_00191660

Material docente de la UOC

**José María Alonso Cebrián**

Es ingeniero informático por la Universidad Rey Juan Carlos, de Madrid, donde está terminando su tesis doctoral sobre seguridad en aplicaciones web. Ha sido premiado con el título de Most Valuable Professional por Microsoft en el área de seguridad informática desde el año 2004, distinción que, a día de hoy, sólo ostentan tres personas en España. Escritor habitual en revistas tecnológicas sobre seguridad informática y ponente en conferencias nacionales como la Gira de Seguridad de Microsoft, Masters, el Technet Security Day o el Asegúr@IT, además de participar en conferencias internacionales como Blackhat, Defcon, ToorCon o ShmooCon. Trabaja como consultor de seguridad en Informática 64 y escribe un blog sobre seguridad informática titulado "Un Informático en el lado del mal".

**Vicente Díaz Sáez**

Ingeniero superior en Informática por la UPC, doctorando del programa de Inteligencia Artificial. Más de 5 años trabajando en seguridad informática y experto en bases de datos. En la actualidad, *manager* en el Departamento de crime de S21sec.

**Antonio Guzmán Sacristán**

Doctor en Informática desde 2006 por la Universidad Rey Juan Carlos (URJC), de Madrid, donde desarrolla prácticamente toda su labor docente e investigadora. Cofundador del grupo de investigación en arquitecturas de altas prestaciones, es profesor del área de Arquitectura y tecnología de computadores de la URJC desde el año 2000. Es el coordinador de las asignaturas Arquitectura de computadores y Seguridad informática en la titulación de Ingeniería informática. Ha participado en 10 proyectos de investigación de diferente envergadura e impartido cerca de 200 créditos en programas de grado y postgrado oficiales, y está especialmente involucrado en proyectos de innovación educativa. Tiene publicaciones en las conferencias internacionales Blackhat, Defcon, Toorcon y ShmooCon.

**Pedro Laguna Durán**

Trabaja como consultor de seguridad en Informática 64. Ha sido premiado con el título de MSP (Microsoft Student Partner) que MS otorga a los estudiantes que destacan por su labor en las comunidades técnicas. Es ponente habitual en conferencias de seguridad y está especializado en técnicas XSS. Ha sido el creador de WebBrowsing Fingerprinting y Thumbando, herramientas para el análisis de navegadores y de ficheros de miniaturas. <http://www.informatica64.com/wb-fingerprinting> y <http://www.informatica64.com/thumbando/>. Es investigador de seguridad y reporta bugs habitualmente en servicios basados en web.

**Alejandro Martín Bailón**

Ingeniero informático por la Universidad de Salamanca y máster en Tecnologías de la información y sistemas informáticos por la Universidad Rey Juan Carlos, de Madrid. Es director de desarrollo de soluciones en Informática 64 y está especializado en seguridad en redes inalámbricas, temáticas sobre las que ha publicado múltiples artículos en revistas e impartido conferencias en congresos como FIST o Asegúr@IT.

El encargo y la creación de este material docente los ha coordinado el profesor Jordi Serra Ruiz para el programa del Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones –MISTIC– (2012).



Primera edición: septiembre 2012

© José María Alonso Cebrián, Vicente Díaz Sáez, Antonio Guzmán Sacristán, Pedro Laguna Durán, Alejandro Martín Bailón

Todos los derechos reservados

© de esta edición, FUOC, 2012

Av. Tibidabo, 39-43, 08035 Barcelona

Diseño: Manel Andreu

Realización editorial: Eureca Media, SL

Depósito legal: B-22.601-2012



Los textos e imágenes publicados en esta obra están sujetos –excepto que se indique lo contrario– a una licencia de Reconocimiento-NoComercial-SinObraDerivada (BY-NC-ND) v.3.0 España de Creative Commons. Podéis copiarlos, distribuirlos y transmitirlos públicamente siempre que citéis el autor y la fuente (FUOC. Fundación para la Universitat Oberta de Catalunya), no hagáis de ellos un uso comercial y ni obra derivada. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es>

## Objetivos

Al finalizar la lectura de este material habréis alcanzado las siguientes competencias:

1. Conocer el funcionamiento de la estructura de las aplicaciones web.
2. Saber hacer los ataques de inyección de *scripts*.
3. Saber hacer ataques de inyección de código y *LDAP Injection*.
4. Conocer el *Xpath Injection*.
5. Saber crear ataques de *Path Transversal* y ataques de inyección de ficheros.
6. Conocer la ruptura de sesión.
7. Saber hacer *Fuzzing* de aplicaciones web.
8. Conocer la arquitectura de las bases de datos.

## Contenidos

### Módulo didáctico 1

#### **Introducción**

Vicente Díaz Sáez

1. Seguridad en bases de datos y aplicaciones web
2. Evolución de los ataques
3. Perspectivas
4. Arquitectura de aplicaciones web
5. Arquitectura de bases de datos

### Módulo didáctico 2

#### **Ataques a aplicaciones web**

José María Alonso Cebrián, Antonio Guzmán Sacristán, Pedro Laguna Durán y Alejandro Martín Bailón

1. Ataques de inyección de *scripts*
2. Ataques de inyección de código
3. Ataques de Path Transversal
4. Ataques de inyección de ficheros
5. Google Hacking
6. Seguridad por ocultación

### Módulo didáctico 3

#### **Ataques a BB. DD., SQL Injection**

José María Alonso Cebrián, Antonio Guzmán Sacristán, Pedro Laguna Durán y Alejandro Martín Bailón

1. SQL Injection
2. Blind SQL Injection
3. Blind SQL Injection basándose en tiempos
4. Arithmetic Blind SQL Injection
5. Ficheros remotos en SQL Inyection
6. Consejos en SQL Injection

### Módulo didáctico 4

#### **Auditoría y desarrollo seguro**

José María Alonso Cebrián, Vicente Díaz Sáez, Antonio Guzmán Sacristán, Pedro Laguna Durán y Alejandro Martín Bailón

1. Introducción
2. Auditorías
3. Fortificación: servicios, permisos y contraseñas
4. Desarrollo seguro