

Programación de código seguro

José María Alonso Cebrián
Jordi Gay Sensat
Antonio Guzmán Sacristán
Pedro Laguna Durán
Alejandro Martín Bailón
Jordi Serra Ruiz
Josep Vañó Chic

PID_00208374

Material docente de la UOC

José María Alonso Cebrián

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 tienen tres personas en España. Escribe habitualmente en revistas tecnológicas sobre seguridad informática y es ponente en conferencias nacionales como la Gira de Seguridad de Microsoft, Masters, el Technet Security Day o el Asegur@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".

Jordi Gay Sensat

Ingeniero informático por la Universidad Politécnica de Cataluña. Ha ejercido como profesor en la Universidad de Girona. Ha participado en diversos retos de *hacking* como Izhai, Boinas negras (I y II), Hackerslab o NGsec. Actualmente es el jefe del departamento de tecnología del Centro de Convenciones Internacional de Barcelona.

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 y profesor del Área de Arquitectura y Tecnología de Computadores de la Universidad Rey Juan Carlos desde el año 2000. Coordinador de las asignaturas de Arquitectura de Computadores y Seguridad Informática en la titulación de Ingeniería Informática. Ha participado en 10 proyectos de investigación de diferente alcance, ha impartido cerca de 200 créditos en programas de grado y posgrado 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 Microsoft da a los estudiantes que destacan por su labor en 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/wbfingerprinting> y <http://www.informatica64.com/thumbando/>. Investiga temas 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. Director de desarrollo de soluciones en Informática 64 y especialista en seguridad en redes inalámbricas, temas sobre los que ha publicado múltiples artículos en revistas y congresos y sobre los que ha impartido conferencias en congresos como FIST o Asegur@IT.

Jordi Serra Ruiz

Doctor ingeniero informático por la UOC. Ingeniero informático por la Universidad Autónoma de Barcelona (UAB). Máster en Informática Industrial por la UAB. Profesor del Departamento de Informática de la UAB hasta 2002. Actualmente, es profesor de la Universitat Oberta de Catalunya (UOC) y director académico del máster de Seguridad informática de la UOC.

Josep Vañó Chic

Ingeniero en Informática y máster en Dirección y gestión de sistemas y tecnologías de la información, por la UOC. Profesional en el área de desarrollo de software desde 1985, inicialmente en el ámbito de la empresa privada y actualmente en la Administración pública, combinando esta tarea con la de consultor de la UOC en el máster interuniversitario de Seguridad de las tecnologías de la información y las comunicaciones.

El encargo y la creación de este material docente han sido coordinados por el profesor: Jordi Serra Ruiz para el programa del Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones –MISTIC– (2013).



Segunda edición: septiembre 2013

© José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán, Pedro Laguna Durán,

Alejandro Martín Bailón, Jordi Serra Ruiz, Josep Vañó Chic

Todos los derechos reservados

© de esta edición, FUOC, 2013

Av. Tibidabo, 39-43, 08035 Barcelona

Diseño: Manel Andreu

Realización editorial: Eureka Media, SL

Depósito legal: B-19.918-2013

Módulos 1, 2, 3, 6, 7 y 8 bajo licencia *Copyright*

Ninguna parte de esta publicación, incluido el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares del copyright.

Módulos 4 y 5 bajo licencia *Creative Commons*



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>

Contenidos

Módulo didáctico 1

Introducción

José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán, Pedro Laguna Durán, Alejandro Martín Bailón y Jordi Serra Ruiz

1. Introducción
2. Gestión de memoria
3. Conceptos básicos de lenguaje máquina

Módulo didáctico 2

Ejecución de procesos

José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán, Pedro Laguna Durán, Alejandro Martín Bailón y Jordi Serra Ruiz

1. Código
2. Área de datos dinámicos (*heap*)
3. Área de datos estáticos (*bss*)
4. Pila
5. Espacio de usuario y espacio de sistema

Módulo didáctico 3

Herramientas

José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán, Pedro Laguna Durán, Alejandro Martín Bailón y Jordi Serra Ruiz

1. *Debuggers*
2. Compiladores/Lenguajes

Módulo didáctico 4

Diseño de aplicaciones seguras

Josep Vañó Chic

1. Ciclo de vida del desarrollo de software seguro
2. Evaluación de riesgos
3. Modelado de amenazas
4. Técnicas de seguridad

Módulo didáctico 5

Testing y buenas prácticas

Josep Vañó Chic

1. Técnicas de código seguro
2. Revisión de código seguro
3. Pruebas de seguridad
4. Buenas prácticas

Módulo didáctico 6

Código seguro

José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán,
Pedro Laguna Durán, Alejandro Martín Bailón y Jordi Serra Ruiz

1. *Integer Overflow*
2. *Stack Overflow*
3. *Heap overflow*

Módulo didáctico 7

Shellcodes

José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán,
Pedro Laguna Durán, Alejandro Martín Bailón y Jordi Serra Ruiz

1. Escritura de *Shellcodes*
2. *Shellcodes* por entrada estándar
3. *Shellcodes* alfanuméricas
4. Un ejemplo de *Shellcode*
5. Dirección de la función a llamar
6. La *shellcode* en ensamblador
7. La *shellcode* en binario
8. El *exploit* con la *shellcode*

Módulo didáctico 8

Exploits remotos y locales

José María Alonso Cebrián, Jordi Gay Sensat, Antonio Guzmán Sacristán,
Pedro Laguna Durán, Alejandro Martín Bailón y Jordi Serra Ruiz

1. *Exploits* Remotos
2. *Exploits* Locales

Bibliografía

AT&T. <http://www.att.com/>

Codegear *Borland C++ compiler.* <http://www.codegear.com/downloads/free/cppbuilder>

CVE.Mitre. *Common Vulnerabilities and Exposures.* <http://cve.mitre.org/cve/>

GCC. GNU. *GCC online documentation.* <http://gcc.gnu.org/onlinedocs/>

GCC. GNU. *The GNU Compiler Collection.* <http://gcc.gnu.org/>

GNU. *GDB: The GNU Project Debugger.* <http://www.gnu.org/software/gdb/>

GNU. *GNU Binutils (Objdump y otras aplicaciones).* <http://www.gnu.org/software/binutils/>

IBM. *Linux / Inside memory management: Garbage Collection.* <http://www.ibm.com/developerworks/linux/library/l-memory/#N103DD>

Inline Assembly. http://www.delorie.com/djgpp/doc/brennan/brennan_att_inline_djgpp.html

Insight: The GDB GUI. <http://sources.redhat.com/insight/>

Intel. *Intel 64 and IA-32 Architectures Software Developer's Manuals.* <http://www.intel.com/products/processor/manuals/index.htm>

Intel. *Intel 64 and IA-32 Architectures Software Developer's Manuals.*

Intel *Intel 64 and IA-32 Architectures Software Developer's Manuals. Volume 2A: Instruction Set Reference, A-M.* <http://download.intel.com/design/processor/manuals/253666.pdf>

Intel *Intel 64 and IA-32 Architectures Software Developer's Manuals. Volume 2A: Instruction Set Reference, N-Z.* <http://download.intel.com/design/processor/manuals/253667.pdf>

Intel. <http://www.intel.com/>

Kernel *Linux.* <http://www.kernel.org/>

Microsoft *Debugging tools for Windows.* <http://www.microsoft.com/whdc/devtools/debugging/default.msp>

Microsoft *Windows.* <http://www.microsoft.com/WINDOWS/>

MSDN *Microsoft Visual Studio 2008/.NET: Garbage Collection.* <http://msdn.microsoft.com/en-us/library/0xy59wtx.aspx>

NASM *The Netwide Assembler.* <http://www.nasm.us/>

OllyDbg. <http://www.ollydbg.de/>

Secunia. <http://secunia.com/advisories/>

SecurityFocus. <http://www.securityfocus.com/bid>

Sourcerware. *Debugging with GDB.* <http://sourcerware.org/gdb/download/onlinedocs/gdb.html>

Sourcerware *GNU Binary Utilities (Documentación de Objdump y otras aplicaciones).* <http://sourcerware.org/binutils/docs-2.19/binutils/index.html>

Sourcerware *AS Documentation (part of Binutils).* <http://sourcerware.org/binutils/docs-2.19/as/>

Sourcerware *AT&T Syntax versus Intel Syntax.* http://sourcerware.org/binutils/docs/as/i386_002dSyntax.html#i386_002dSyntax

Unix. <http://www.unix.org/>

Volume 1: *Basic Architecture.* <http://download.intel.com/design/processor/manuals>