

Contenido

<i>Introducción</i>	<i>xvii</i>
Parte I. Técnicas de desarrollo	1
Capítulo 1. Cifrado	3
Archivos de prácticas	4
Resúmenes hash	5
Cifrado de clave privada	10
Cómo mantener seguras las claves privadas	14
Cifrado de clave pública	16
Cómo ocultar la información innecesaria	18
Cifrado en el mundo real	20
Resumen	21
Capítulo 2. Autorización basada en roles	23
Ejercicio de autorización basada en roles	25
Seguridad integrada en Windows	27
Autenticación y autorización en ASP.NET	31
Autorización basada en roles en el mundo real	33
Resumen	35
Capítulo 3. Seguridad de acceso al código	37
¿Por qué se consideran las acciones seguras o inseguras?	38
¿Cómo se puede evitar la ejecución de código dañino?	38
Activación predeterminada	39
Funciones de seguridad y el Diseñador de Visual Basic .NET	39
Seguridad de acceso al código frente a seguridad basada en roles de las aplicaciones	39
La seguridad de acceso al código es prioritaria frente a la seguridad basada en roles de las aplicaciones	40
Cómo ejecutar el código en diferentes zonas de seguridad	40
Qué va a proteger la seguridad de acceso al código	44
Permisos: La base de lo que puede hacer el código	44
Cómo puede asegurarse que su código se ejecutará con seguridad	52

Cooperación con el sistema de seguridad	53
Seguridad de acceso al código en el mundo real	56
Resumen	57
Capítulo 4. Autenticación ASP.NET	59
Archivos de prácticas EmployeeManagementWeb	60
Autenticación por formularios	60
Autenticación de seguridad integrada en Windows	66
Autenticación Passport	70
Instalación del SDK de Passport	71
Autenticación ASP.NET en el mundo real	78
Resumen	78
Capítulo 5. Cómo garantizar la seguridad de las aplicaciones Web	79
Secure Sockets Layer (SSL)	82
Cómo funciona SSL	82
Cómo garantizar la seguridad de los servicios Web	85
Implementación de un seguimiento de auditoría	90
Cómo garantizar la seguridad de las aplicaciones Web en el mundo real	91
Resumen	92
Parte II. Cómo obtener código resistente a los ataques	93
Capítulo 6. Ataques a las aplicaciones y cómo evitarlos	95
Ataques de Denegación de servicio (DoS)	95
Técnicas de defensa para los ataques DoS	96
Ataques basados en archivo o en directorio	99
Técnicas de defensa para los ataques basados en archivo o en directorio	100
Ataques de inyección SQL	102
Técnicas de defensa para los ataques de inyección SQL	104
Ataques de programación de sitio cruzado	108
Cuando la inyección de archivos de comandos HTML se convierte en un problema	112
Técnicas de defensa para los ataques de programación de sitio cruzado	114
Ataques de aplicaciones hijas	117
Técnicas de defensa para los ataques de aplicaciones hijas	117
Defensa contra los ataques en el mundo real	119
Resumen	119
Capítulo 7. Validación de la entrada	121
Empleo de los tipos de entrada y de las herramientas de validación	122
Entradas directas del usuario	122
Herramientas generales de validación de lenguaje	127
Entradas en aplicaciones Web	133
Entradas no realizadas por el usuario	134
Entradas a subrutinas	136
Resumen	139
Capítulo 8. Control de excepciones	141
Dónde se producen las excepciones	142
Control de excepciones	143

Controladores globales de excepciones	148
Control de excepciones en el mundo real	151
Resumen	151

Capítulo 9. Prueba del código resistente a los ataques 153

Plan de ataque: El plan de pruebas	154
Tormenta de ideas: Generación de escenarios relacionados con la seguridad	155
Cómo centrarse: Asignación de prioridades a los escenarios	158
Generar pruebas	159
Ataque: Ejecutar el plan	161
Técnicas de pruebas	161
Herramientas de pruebas	165
Pruebas en el entorno objetivo	168
Convertir en prioritarias las pruebas de seguridad	168
Errores frecuentes cometidos en las pruebas	169
Probar poco y tarde	169
Fracasar en las pruebas de seguridad	169
Fracasar a la hora de estimar el coste de las pruebas	170
Esperar demasiado de la información obtenida con la versión beta	170
Suponer que los componentes desarrollados por terceros son seguros	170
Probar en el mundo real	170
Resumen	171

Parte III. Implementación y configuración 173

Capítulo 10. Cómo asegurar su aplicación para la implementación 175

Técnicas de implementación	176
Implementación basada en XCopy	176
Implementación automática	176
Implementación mediante Windows Installer	177
Implementación de archivos Cabinet	177
Implementación y seguridad de acceso mediante código	177
Implementación y ejecución de sus aplicaciones en el entorno de seguridad de .NET	179
Certificados y firmas	180
Certificados digitales	180
Firma con Authenticode	182
Firma con nombre seguro	184
Firma con Authenticode frente a firma con nombre seguro	187
Ejercicios con nombres seguros, certificados y firmas	188
Implementación de las actualizaciones de la directiva de seguridad de .NET	196
Actualización de la directiva de seguridad empresarial de .NET	197
Implementación de las actualizaciones de la directiva de seguridad empresarial de .NET	201
Cómo proteger su código: ofuscamiento	204
Oscuridad y seguridad	205
Lista de comprobación de la implementación	206
Implementación en el mundo real	207
Resumen	207

Capítulo 11. Protección de Windows, Internet Information Services y .NET . 209

"Ya estoy protegido, tengo un cortafuegos"	210
Principios fundamentales del bloqueo	210
Herramientas automatizadas	212

Bloqueo de clientes de Windows	213
Cómo dar formato a unidades de disco utilizando NTFS	213
Desactivación del inicio de sesión automático	214
Activación de la auditoría	214
Desactivación de los servicios innecesarios	214
Desactivación de los recursos compartidos no necesarios	215
Empleo de contraseñas en el protector de pantallas	215
Eliminación de software de compartición de archivos	215
Definición de una contraseña para proteger el BIOS	216
Desactivación del arranque desde la unidad de disquete	216
Bloqueo de servidores de Windows	216
Cómo aislar un controlador de dominio	216
Desactivación y eliminación de las cuentas innecesarias	216
Instalación de un cortafuegos	216
Bloqueo de IIS	217
Desactivación de los servicios de Internet que no sean necesarios	217
Desactivación de los script maps que no sean necesarios	217
Eliminación de ejemplos	217
Activación del registro IIS	217
Restricción de IUSR_<nombre_equipo>	217
Instalación de URLScan	217
Bloqueo de .NET	218
Resumen	218

Capítulo 12. Cómo garantizar la seguridad de las bases de datos 219

Conceptos de seguridad de las bases de datos	220
Autenticación de SQL Server	220
Quién ha iniciado una sesión	223
Cómo asigna privilegios SQL Server	224
Autorización de SQL Server	225
Autenticación y autorización de Microsoft Access	226
Modelos de seguridad a nivel de usuario de Microsoft Access	227
Bloqueo de Microsoft Access	230
Bloqueo de SQL Server	230
Resumen	232

Parte IV. Seguridad a nivel empresa 235

Capítulo 13. Diez pasos para diseñar un sistema empresarial seguro 237

Desafíos del diseño	238
Paso 1: Crea que puede ser atacado	239
Paso 2: Diseña e implementa la seguridad desde el principio	239
Paso 3: Forme al equipo	239
Paso 4: Diseño de una arquitectura segura	240
Canalizaciones con nombre frente a TCP/IP	242
Si no hace nada más	242
Paso 5: Modelo de riesgos de las vulnerabilidades	243
Paso 6: Empleo de las funciones de seguridad de Windows	243
Paso 7: Diseña para simplificar y facilitar su empleo	243
Paso 8: Eliminación de las puertas traseras	244
Paso 9: Cómo asegurar la red con un cortafuegos	245
Paso 10: Diseñar pensando en el mantenimiento	246
Resumen	247

Capítulo 14. Amenazas: análisis, prevención, detección y respuesta 249

Análisis de amenazas y vulnerabilidades 250
 Identificar y asignar prioridades 250
 Evitar ataques disminuyendo las amenazas 254
 Disminución de las amenazas 254
 Detección 254
 Detección temprana 254
 Cómo detectar que un ataque se ha producido o que se está ejecutando 257
 Cómo responder a un ataque 258
 Cómo prepararse para responder 259
 Amenazas de seguridad en el mundo real 260
 Resumen 260

Capítulo 15. Ejercicio de análisis de amenazas 263

Análisis de amenazas 263
 Dedicar tiempo 263
 Planificar y documentar su análisis de amenazas 264
 Crear una lista de amenazas 264
 Asignar prioridades a las amenazas 266
 Responder a las amenazas 269
 Resumen 271

Capítulo 16. Tendencias futuras 273

La carrera armamentística de los hackers 273
 Ningún sistema operativo es seguro 275
 Ciberterrorismo 275
 ¿Qué pasará en el futuro? 277
 Cómo responder a las amenazas de seguridad 278
 Privacidad frente a seguridad 278
 El Protocolo Internet versión 6 (IPv6) 280
 Iniciativas de la Administración 281
 Iniciativas de Microsoft 281
 Resumen 282

Apéndice A. Guía de los ejemplos de código 283

Sistema de administración de empleados 283
 Web de administración de empleados 286
 Demostración de cifrado 288
 Utilidad TogglePassportEnvironment 290
 Estructura de la base de datos Employee 291
 Cómo migrar la base de datos Employee a SQL Server 2000 291

Apéndice B. Contenido de SecurityLibrary.vb 295

Resúmenes hash 295
 Cifrado de clave privada 295
 Cifrado DPAPI 295
 Cifrado de clave pública 296
 Registro de excepciones 296
 Seguridad basada en roles 296
 Validación de la entrada 297

Índice 299