

INDICE

Introducción	XVII
PARTE I. TECNICAS DE DESARROLLO	1
Capitulo 1. Cifrado	3
Archivos de Practicas	4
Resúmenes Hash	5
Cifrado de Clave Privado	10
Como Mantener Seguras las Claves Privadas	14
Cifrado de Clave Publica	16
Como Ocultar Información Innecesaria	18
Cifrado en el Mundo Real	20
Resumen	21
CAPITULO 2. AUTORIZACION BASADA EN ROLES	23
Ejercicio de Autorización basada e roles	25
Seguridad Integrada en Windows	27
Autenticación y Autorización en ASP. NET	31
Autorización Basada en Roles en el Mundo Real	33
CAPITULO 3. SEGURIDAD DE ACCESO AL CODIGO	37
Por que se Consideran las Acciones Seguras o Inseguras?	38
Como 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
Como Ejecutar el Código de Diferentes Zonas de Seguridad	40
Que va a Proteger la Seguridad de Acceso de Código	44
Permisos: La Base de lo que Puede Hacer el Código	44
Como Puede Asegurar que su Ejecutara con Seguridad	52
Cooperación con el Sistema de Seguridad	53
Seguridad de Acceso al Código en el Mundo Real	56
Resumen	57
CAPITULO 4. AUTENTICACION ASP. NET	59
Archivos de Practicas Employee Management Wet	60
Autenticación por Formularios	60
Autenticación de Seguridad Integrada en Windows	66
Autenticación Passport	70
Instalación ASP. NET en el Mundo Real	78
Resumen	78
CAPITULO 5. COMO GARANTIZAR LA SEGURIDAD DE LAS APLICACIONES WED	79
Secure Sockets Layer (SSL)	82
Como Funciona SSL	82
Como Garantizar la Seguridad de los Servicios Web	85
Implementación de un Seguimiento de Auditoria	91
Como Garantizar la Seguridad de las Aplicaciones Web en el Mundo Real	91
Resumen	92

PARTE II. COMO OBTENER CODIGO RESISTENTE A LOS ATAQUES	93
Capitulo 6. Ataques a las Aplicaciones y Como 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 Basados en Archivo o en Directorio	100
Ataques de Inyección SQL	102
Técnicas Defensa para los Ataques de Inyección SQL	104
Ataques de Programación de Sitio Cruzado	108
Cuando la Inyección de Archivos de Comandos HTML se Convierten en un Problema	112
Técnicas de Defensa ara los Ataques de Programación de Sitio Cruzado	114
Ataques de Aplicación Hijas	117
Técnicas de Defensa para los Ataques de Aplicaciones Hijas	117
Defensa Contra los Ataques en el Mundo Real	119
Resumen	119
CAPITULO 7. VALIDACION 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
Entrada en Aplicación Web	133
Entradas no Realizadas por el Usuario	134
Entradas a Subrutinas	136
Resumen	139
CAPITULO 8. CONTROL DE EXCEPCION	141
Donde se Producen las Excepciones	142
Control de Excepciones	143
Controladores Globales de Excepciones	148
Control de Excepciones en el Mundo Real	151
Resumen	151
CAPITULO 9. PRUEBA DEL CODIGO RESISTENTE A LOS ATAQUES	153
Plan de Ataque: El Plan de Pruebas	154
Tormenta de Ideas: Generación de Escenarios Relacionados con la Seguridad	155
Como 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 Prioridades 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 Obtenidas 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. IMPLEMENTACION Y CONFIGURACION	173
Capitulo 10. Como Asegurar su Aplicación para la Implementación	175
Técnicas de Implementación	176
Implementación Basada en XCopy	176
Implementación Automática	176
Implementación Mediante Windorw Installer	177
Implementación de Archivos Cabinet	177
Implementación y Seguridad de Acceso Mediante Código	177
Implementación y Ejecución Aplicaciones en el Entorno de Seguridad de NET	179
Certificados y Firmas	180
Certificados Digitales	180
Firmas con Authenticode	182
Firma con Nombre Seguro	184
Firma con Authenticode Frente a Firma con Nombre Seguro	187
Ejercicios con Nombre 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
Como Proteger su Código: Ofuscamiento	204
Oscuridad y Seguridad	205
Lista de Comprobación de la Implementación	206
Implementación en el Mundo Real	207
Resumen	207
CAPITULO 11. PROTECCION DE WINDOWS, INTERNET INFORMATION SERVICES Y NET	209
Ya Estoy Protegido, Tengo un Cortafuegos	210
Principios Fundamentales del Bloqueo	210
Herramientas Automatizadas	212
Bloque de Clientes de Windows	213
Como Dar Formato a Unidades de Disco Utilizando NTFS	213
Desactivación del Inicio de Sesión Automático	214
Activación de la Auditoria	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 Contraseñas para Proteger el BIOS	216
Desactivación del Arranque Desde la Unidad de Disquete	216
Bloqueo de Servidores de Windows	216
Como 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 URLS can	217
Bloqueo de NET	218
Resumen	218
CAPITULO 12. COMO GARANTIZAR LA SEGURIDAD DE LAS BASES DE DATOS	219
Conceptos de Seguridad de las Bases de Datos	220
Autenticación de SQL Server	220
Quien ha Iniciado una Sesión	223
Como Asigna Privilegios SQL Server	224
Autorización de SQL Server	225
Autenticación y Autorización de Microsoft Access	226
Modelo 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
CAPITULO 13. DIEZ PASOS PARA DISEÑAR UN SISTEMA EMPRESARIAL SEGURO	237
Desafíos del Diseño	238
Paso 1: Crea que Puede Ser Atacado	239
Paso 2: Diseño e Implemente 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 Mas	242
Paso: 5 Modelo de Riesgos de las Vulnerabilidades	243
Paso. 6 Empleo de las Funciones de Seguridad de Windows	243
Paso: 7 Diseño para Simplificar y Facilitar su Empleo	243
Paso: 8 Eliminación de las Puertas Traseras	244
Paso: 9 Como Asegurar la Red con un Cortafuegos	245
Paso: 10 Diseñar Pensando en el Mantenimiento	246
Resumen	247
CAPITULO 14. AMENAZAS: ANALISIS, PREVENCION, DETECCION 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
Como detectar que un Ataque se ha Producido o que se Está Ejecutando	257
Como Responder a un Ataque	258

Como Prepararse para Responder	259
Amenazas de Seguridad en el Mundo Real	260
Resumen	260
CAPITULO 15. EJERCICIO DE ANALISIS 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
CAPITULO 16. TENDENCIAS FUTURAS	273
La Carrera Armamentística de los hackers	273
Ningún Sistema Operativo es Seguro	275
Ciberterrorismo	275
Que Pasara en el Futuro?	277
Como Responder a las Amenazas de Seguridad	278
Privacidad Frente a Seguridad	278
El Protocolo Internet Versión 6 (IP v6)	280
Iniciativas de la Administración	281
Iniciativa de Microsoft	281
Resumen	282
APENDICE A. GUIA DE LOS EJEMPLOS DE CODIGO	283
Sistema de Administración de Empleados	283
Web de Administración de Empleados	286
Demostración de Cifrado	288
Utilidad Toggle PassportEnvironment	290
Estructura de la Base de Datos Employee	291
Como Migrar la Base de Datos Employee a SQL Server 2000	291
APENDICE B. CONTENIDO DE SECURITY LIBRARY.VB	295
Resúmenes Hash	295
Cifrado de Clave Privado	295
Cifrado DPAPI	295
Cifrado de Clave Publica	296
Registro de Excepciones	296
Seguridad Basada en Roles	297
Validación de la Entrada	297
Índice	299