

امنیت در

ASP.NET 2.0

مهندس وحید نصیری



شرکت ناقوس اندیشه
(سهامی خاص)

سرشناسه

: تصیری، وحید، ۱۳۶۱

عنوان و پدیدآور

: امنیت در ASP.NET 2.0 / وحید نصیری.

مشخصات نشر

: تهران: کتاب مرو: شرکت ناقوس اندیشه، ۱۳۸۶.

مشخصات ظاهری

: ۲۱۶ ص: مصور.

شابک

: ۳۵۰۰۰ ریال: ۵-۱-۹۶۷۸۳-۹۶۴-۹۷۸

وضعیت فهرست‌نویسی: فیا

آوانویسی عنوان

: امنیت در ای.اس.پی. نت ۲.۰

موضوع

: صفحه‌های مرور فعال.

موضوع

: وب -- سایت‌ها -- طراحی.

رده بندی کنگره

: ۷ص/ ۸۸۸۵/ TK ۵۱۰۵

رده بندی دیویی

: ۲۷۶/ ۰۰۵

شماره کتابخانه ملی

: ۵۰۸۲۸-۸۵



www.naghoospress.ir



چاپ اول

: امنیت در ASP.NET 2.0

نام کتاب

: کتاب مرو

ناشر

: شرکت ناقوس اندیشه

ناشر همکار

: وحید نصیری

مؤلف

: ۱۳۸۶

چاپ اول

: ۲۰۰۰ جلد

تیراژ

: غرازنکر

لبن‌گرافی

: سعیدی

چاپ

۵۵۶۵۹۹۶۸



: صفحه‌پرداز

صحافی

: حروفچینی و صفحه‌آرایی: واحد تولید

: مریم رضایی

حروف‌نگار

: ۳۵۰۰۰ ریال

قیمت

: ۵-۱-۹۶۷۸۳-۹۶۴-۹۷۸

شابک

: 978-964-96783-5-1

ISBN

کلیه حقوق برای ناشر محفوظ است. تکثیر تمامی یا قسمتی از این اثر به‌صورت حروفچینی یا چاپ مجدد، چاپ افست، پلی‌کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مرکز پخش: شرکت ناقوس اندیشه

تهران: خیابان انقلاب، خیابان ۱۲ فروردین، کوچه نوروژ، پلاک ۲۷

تلفن: ۶۶۴۱۱۷۱۵-۶۶۹۶۶۷۵۰-۶۶۹۶۶۷۳۹

فهرست

۷	مقدمه مؤلف
۹	فصل اول: مقابله با خطاها و اهمیت آنها در تأمین امنیت سایت
۱۰	استفاده از فایل web.config
۱۱	مقابله با خطاهای مدیریت نشده
۱۳	فصل دوم: تعیین اعتبار ورودی کاربر
۱۴	مدیریت ورودی‌های خطرناک مهاجمان
۱۶	اطمینان نکردن به کنترل‌های تعیین اعتبار در ASP.NET
۱۶	محافظت از برنامه‌های خود در مقابل SQL Injection
۱۸	روش محافظت در برابر تزریق عبارتی که از or و Single quote marks استفاده می‌نمایند
۱۹	روش محافظت در برابر تزریق SQL در Query String
۲۰	از user با کمترین حد دسترسی هنگام اتصال به SQL Server استفاده نمایید
۲۲	تأجایی که می‌توانید از رویه‌های ذخیره شده استفاده کنید
۲۲	به کاربر اجازه انشا نوشتن ندهید!
۲۲	چگونه می‌توان متوجه شد که برنامه، تحت حملات تزریق SQL آسیب‌پذیر است؟
۲۲	نوشتن توابعی برای جلوگیری از تزریق SQL
۲۵	توجه داشتن به معادل‌های عبارات unicode و امثال آن
۲۹	سرریز بافر (buffer overflow)
۳۰	محافظت در برابر حملات Canonicalization
۳۱	آشنایی با برنامه FxCop
۳۳	فصل سوم: hash کردن اطلاعات در ASP.NET
۳۳	مقدمه
۳۳	کریپتوگرافی
۳۴	مبانی کریپتوگرافی
۳۵	استفاده از الگوریتم MD5 برای رمزگذاری پسوندهای ذخیره شونده در بانک اطلاعاتی
۳۵	خلاصه‌ای در مورد الگوریتم MD5
۳۶	استفاده از MD5 برای رمزگذاری پسوندها و ذخیره کردن آنها

۳۳	فصل چهارم: انتخاب پسوردهای قوی
۴۴	وادر کردن کاربران به انتخاب پسوردهای قوی در ASP.NET 1.x
۴۵	وادر کردن کاربران به انتخاب پسوردهای قوی در ASP.NET 2.x
۳۷	فصل پنجم: ذخیره‌سازی اطلاعات حساس در ASP.NET
۴۷	رمزنگاری و رمزگشایی قسمت‌های مختلف فایل Webconfig از طریق برنامه نویسی
۴۸	استفاده از ابزار خط فرمان aspnet_regiis.exe جهت رمزنگاری فایل webconfig
۵۱	فصل ششم: محافظت از سورس
۵۳	معرفی تعدادی از ابزارهای محافظت از سورس
۵۹	فصل هفتم: امنیت View State در ASP.NET
۶۰	مقایسه Session State و View State
۶۳	فصل هشتم: امنیت Up Load فایل در ASP.NET
۶۳	تنظیمات سطح دسترسی کاربر ASP.NET
۶۴	محدود کردن نوع فایل‌های قابل Up Load
۶۶	یک تجربه تلخ با php !
۶۶	مخفی کردن مسیر ذخیره شدن فایل‌ها
۷۱	ملاحظات در مورد حملات (DoS) Denial of Service
۷۳	فصل نهم: امنیت Cookies در ASP.NET
۷۹	فصل دهم: مبحث Authentication در ASP.NET
۷۹	مقدمه
۷۹	توضیحاتی در مورد دو واژه متداول
۸۰	مراحل یک Forms Authentication به صورت زیر است
۸۰	تنظیمات مربوط به Forms Authentication
۸۸	نحوه تعیین اعتبار یک کاربر با استفاده از بانک اطلاعاتی SQL Server
۹۱	فصل یازدهم: امنیت Sessions در ASP.NET
۹۲	طراحی یک Token امن
۹۴	انتخاب مکانیزم مناسب Token
۹۵	Token‌هایی بر مبنای فرم
۹۶	حالت‌های مختلف ذخیره‌سازی سشن بر روی server
۹۶	امن کردن حالت In-Process
۹۶	امن کردن حالت ASP.NET State Service
۹۸	امن کردن حالت SQL Server State Management
۹۹	بهبود مدیریت حالت در ASP.NET
۹۹	ایجاد tokenها

۱۰۲	انقیاد به Client (Binding to the Client)
۱۰۳	خاتمه دادن به یک سشن
۱۰۵	نحوه حذف token سشن از referrer ها
۱۰۷	فصل دوازدهم: بازنویسی URL
۱۰۷	مقدمه
۱۰۷	The ASP.NET v1.1 Hack
۱۰۸	بازنویسی URL در ASP.NET v2.0
۱۰۹	فصل سیزدهم: بالا بردن میزان امنیت سرویس دهنده وب
۱۰۹	مقدمه
۱۰۹	طول و یا اندازه درخواست (Request Length)
۱۱۰	مشخص کردن کاراکترهای مجاز
۱۱۱	برنامه UrlScan
۱۱۱	برنامه ISS Lockdown
۱۱۱	برنامه Microsoft Baseline Security Analyzer
۱۱۲	محدود کردن IPها و دومین‌های مجاز
۱۱۳	فعال سازی logging در IIS
۱۱۵	فصل چهاردهم: امنیت در کنترل‌های Site Navigation در ASP.NET 2.0
۱۲۳	فصل پانزدهم: مبحث عضویت و نقش‌ها در ASP.NET 2.0
۱۲۳	مقدمه
۱۲۳	کلاس Membership
۱۲۴	تأمین کننده‌های منابع داده جهت membership و roles
۱۲۸	استفاده از Security Web Controls
۱۲۸	کنترل login
۱۲۹	کنترل LoginView
۱۳۰	کنترل PasswordRecovery
۱۳۱	کنترل LoginStatus
۱۳۲	کنترل LoginName
۱۳۲	کنترل CreateUserWizard
۱۳۵	کنترل ChangePassword
۱۳۶	معرفی متدهای کلاس Membership
۱۳۹	مدیریت نقش‌ها
۱۴۰	بررسی متدهای کلاس Roles
۱۴۴	آشنایی با WindowsTokenRoleProvider

۱۴۵	آشنایی با AuthorizationStoreRoleProvider
۱۴۷	آشنایی با Web Site Administration Tool
۱۴۹	فصل شانزدهم: استفاده از تصاویر امنیتی در کنترل Login
۱۴۹	معرفی کنترل CAPTCHA
۱۵۵	فصل هفدهم: استفاده از Active directory جهت تعیین اعتبار کاربران
۱۵۶	تعریف کانکشن استرینگ مخصوص Active directory
۱۵۶	تعریف قسمت عضویت مخصوص Active directory
۱۵۷	آشنایی با ADAM
۱۶۰	تنظیمات ActiveDirectoryMembershipProvider
۱۶۱	فصل هجدهم: جلوگیری از Loginهای متعدد
۱۶۱	سیستم اجبار به Login غیرهمزمان
۱۶۷	فصل نوزدهم: نگهداری تاریخچه کلمات عبور کاربران
۱۷۷	فصل بیستم: استفاده از Database Access جهت مبحث عضویت
۱۷۷	ایجاد Access Database
۱۷۷	ایجاد یک تأمین کننده سفارشی
۱۸۴	The ASP.NET Provider Toolkit
۱۸۴	تبدیل کدها به زبانهای مختلف .Net Frame Work
۱۸۵	فصل بیست و یکم: پیادهسازی Automatic Unlocking
۱۸۵	مقدمه
۱۸۵	پیادهسازی تأمین کننده سفارشی فعالسازی خودکار Account
۱۸۹	فصل بیست و دوم: راه اندازی SSL جهت شبکه داخلی
۱۹۰	تعریف SSL (Secure Sockets Layer)
۱۹۱	مراحل ایجاد یک ارتباط امن SSL
۱۹۳	تنظیم کردن server و همچنین web server جهت استفاده از SSL
۲۰۲	نکاتی در مورد استفاده از SSL در ASP.NET
۲۰۳	سوئچ کردن بین پروتکل های مختلف
۲۰۳	نحوه به دست آوردن اطلاعات مجوز یک Client
۲۰۵	فصل بیست و سوم: Impersonation
۲۱۱	فصل بیست و چهارم: امنیت در هاستینگ چندین برنامه وب ASP.NET
۲۱۲	قفل کردن تنظیمات Webconfig برنامه های host های مختلف
۲۱۵	منابع و مأخذ

مقدمه مؤلف

"تمامی مقالات موجود در بانک اطلاعاتی سایت امروز، به طرز مشکوکی پاک شده‌اند!"

"تمام فایل‌های Up Load شده سایت بدون هک شدن server پاک شده‌اند!"
"امروز گزارش کاملی از قسمت مدیریتی و محافظت شده سایت در بسیاری از سایت‌ها منتشر شده است!"
و ...

عبارات فوق را به وفور در سایت‌های مرتبط با برنامه نویسی وب می‌توان یافت. بسیاری از سایت‌ها هم شبانه روز با پشتکاری وصف ناپذیر در جهت انتشار کدهای مخرب در تلاشند. در این میان کمتر به مباحث امنیتی و نه ضد امنیتی با محتوا و با رویکرد ASP.NET می‌توان دست یافت. هدف این کتاب، بر شمردن مشکلات امنیتی عمده سایت‌های پویای موجود، بدون دید تخریبی و توسعه کدهای مخرب، به همراه ارائه راهحل‌های امنیتی مرتبط است.

بسیاری از برنامه‌نویس‌ها به تجربه دریافته‌اند، که مبحث امنیت باید از مراحل طراحی برنامه در نظر گرفته شود و نباید تا مرحله توسعه به تعویق افتد. بهترین برنامه‌های وب از نظر امنیتی برنامه‌هایی هستند که بتوانند بیشتر در برابر انواع حملات مقاومت کنند و باید این نکته را در نظر داشت، که این امنیت در دو سطح سیستمی و برنامه باید اعمال گردد تا بتوان به بهترین نتایج دست یافت.

ASP.NET با فراهم آوردن زیر ساخت محافظت از دسترسی غیرمجاز به صفحات مختلف وب، امکان برنامه‌نویسی امنی را به سادگی فراهم آورده است، اما این تنها یک روی سکه است. با مطالعه فصول مختلف این کتاب، علاوه بر آموختن مباحث پایه‌ای امنیتی موجود در ASP.NET، با انواع حملات متداول به سایت‌های پویای وب و نحوه مقابله مؤثر با آنها نیز آشنا خواهید شد.

سه لایه امنیتی جهت برنامه‌های ASP.NET قابل تعریف هستند: لایه IIS، لایه ASP.NET worker process و لایه Application. به عنوان یک برنامه نویس، می‌توان بر روی دو لایه اول نیز تأثیرگذار بود و آنها را تنظیم نمود، اما بیشترین مسئولیت یک برنامه‌نویس وب، متوجه لایه سوم اشاره شده می‌باشد و این لایه امنیتی محور اصلی کتاب جاری است.