ملاحظات امنیتی در توسعه نرم‌افزار:

آموزش با نمونه‌های عملی

www.ketab.ir

نویسندگان:

محمد پیشدار

سمانه ربیعی

حمیدرضا حمیدی

سرشناسه	:	پیشدار، محمد، ۱۳۷۰-
عنوان و نام پدیدآور	:	ملاحظات امنیتی در توسعه نرم‌افزار: آموزش با نمونه‌های عملی/ نویسندگان محمد پیشدار، سمانه ربیعی، حمیدرضا حمیدی.
مشخصات نشر	:	قزوین: دانشگاه بین‌المللی امام خمینی(ره)، انتشارات، ۱۳۹۹.
مشخصات ظاهری	:	۳۸۶ ص.: مصور، جدول.
شابک	:	978-622-6898-45-4
وضعیت فهرست نویسی	:	فیپا
عنوان دیگر	:	ecurity bugs in software development :training with practical examples
موضوع	:	نرم‌افزار کاربردی -- طراحی و توسعه
موضوع	:	Application software -- Development
موضوع	:	نرم‌افزار کاربردی -- تدابیر ایمنی
موضوع	:	Application software -- Security measures
شناسه افزوده	:	ربیعی، سمانه، ۱۳۶۱-
شناسه افزوده	:	حمیدی، حمیدرضا، ۱۳۵۰-
شناسه افزوده	:	دانشگاه بین‌المللی امام خمینی(ره). انتشارات
رده بندی کنگره	:	AQ ۷۶/۷۶
رده بندی دیویی	:	۳/۰۰۵
شماره کتابشناسی ملی	:	۷۵۰۵۱۶۳
وضعیت رکورد	:	فیپا

عنوان : **ملاحظات امنیتی در توسعه نرم‌افزار: آموزش با نمونه‌های عملی**

نویسندگان : **محمد پیشدار، سمانه ربیعی و حمیدرضا حمیدی**

ناظر فنی : **حمید کلهر**

شابک : **۹۷۸-۶۲۲-۶۸۹۸-۴۵-۴**

نوبت چاپ : **اول ۱۳۹۹**

قیمت : **۵۰ هزار تومان**

شمارگان : **۵۰۰ جلد**

ناشر : **انتشارات دانشگاه بین‌المللی امام خمینی(ره)**

قزوین، دانشگاه بین‌المللی امام خمینی(ره)، تلفن ۳۳۹۰۱۴۲۶ - ۰۲۸

کلیه حقوق برای ناشر محفوظ است.

مسئولیت حقوقی و قانونی محتوای کتاب بر عهده صاحبان اثر است

www.ketab.ir

پیشگفتار

آموزش دانشگاهی و آموزشگاهیِ طراحی و توسعه نرم‌افزار با تاکید بسیار بر سرعت در تولید محصول است. هدف این آموزش‌ها افزایش مهارت دانشجویان و کارآموزان در کُدنویسی و بکارگیری چارچوب‌های برنامه نویسی است. آزمون نرم‌افزار نیز با تاکید بسیار بر صحت عملکرد تجاری محصول است و حتی کاربری نرم‌افزار از منظر کاربر نهایی مورد کم توجه‌ای واقع می‌شود. در ابتدای دوره بهره‌برداری از محصول نرم‌افزاری، صحت عملکرد محصول مورد توجه است. از آنجاکه تعداد کاربران و گستره دسترسی به نرم‌افزار به آرامی افزایش می‌یابد، منظر امنیتی محصول کمتر مورد توجه قرار می‌گیرد. عموماً رویکرد عملی طراحان نرم‌افزار درخصوص تهدیدهای امنیتی، برخورد با تهدید بعد از بروز مشکل است.

این کتاب با هدف آموزش کاربردی ملاحظات امنیتی در طراحی و توسعه نرم‌افزار تهیه شده است و مخاطب اصلی کتاب را دانشجویان، مهندس‌های طراح نرم‌افزار و کُدنویسان تشکیل می‌دهند. تلاش کرده‌ایم مشهورترین و پرتکرارترین نواقص امنیتی را از طریق مثال‌های برنامه‌نویسی شرح دهیم و چگونگی رفع این نواقص را بیان کنیم.

www.ketab.ir

مقالات بگونه‌ای ساماندهی شده‌اند که می‌توان کتاب را همچون یک کتاب درسی و یا کمک آموزشی از ابتدا به انتها مورد مطالعه و تدریس قرار داد. همچنین در خارج از دوره‌های آموزشی، مخاطبِ کتاب می‌تواند بسته به نیاز هر مقاله را بصورت مستقل مورد مطالعه قرار دهد و الزامی به طی نمودن ترتیبی مقالات نیست. تلاش کرده‌ایم که هر مقاله از مراجع مناسب گزارش شود و برای آشنایی بیشتر خوانندگان، توضیحات فنی و عمومی مناسب نیز به هر مقاله اضافه شود. روان نویسی و تلاش برای قابل فهم بودن مطالب و رعایت اصول نگارش فارسی، مورد توجه ویژه بوده است. هرچند در بین افراد متخصص، معمولا اصطلاحات فنی به زبان انگلیسی بیان و نوشته می‌شود اما تلاش شد تا آنجاکه مناسب است از معادل فارسی استفاده کنیم و درصورتیکه معادل فارسی گویا نباشد، با حروف فارسی نوشته شود. همچنین این اصطلاحات از طریق پاورقی بصورت انگلیسی نیز ذکر شده‌اند. مراجع اصلی ملاحظات امنیتی به شرح زیر است:

اووَسپ : پروژه اووَسپ[1] یا پروژه امنیت نرم‌افزاری تحت وب، یک سازمان غیر انتفاعی است که بر روی ارتقای امنیت نرم‌افزارها کار می‌کند. این بنیاد در اول دسامبر ۲۰۰۱ راه اندازی و در ۲۱ آوریل ۲۰۰۴ به عنوان یک موسسه غیرانتفاعی در ایالات متحده ثبت شد. از جمله اقدامات این سازمان می‌توان به موارد زیر اشاره کرد:

- ایجاد پروژه‌های متن‌باز[2] در حوزه امنیت نرم‌افزار.
- تولید بیش از ۲۷۵ فصل موضوع آموزشی رایگان در حوزه امنیت نرم افزار.
- ایجاد انجمن‌های تخصصی.
- برگزاری کنفرانس ها و آموزش‌های پیشرفته صنعتی در حوزه امنیت نرم‌افزار.

سامانه سی.وی.ای.[3] : سامانه ثبت و تایید آسیب‌پذیری‌های عمومی و بهره‌برداری از آنها یا به اختصار سی.وی.ای. یک روش مرجع برای انتشار اطلاعات شناسه‌دار در مورد آسیب‌پذیری‌های امنیت سایبری است. شرکت میتره[4] به عنوان یکی از مراکز تحقیق و توسعه با بودجه فدرال آمریکا مسئولیت اداره این سامانه را بر عهده دارد. البته تامین مالی اصلی این موسسه توسط وزارت امنیت داخلی آمریکا صورت می‌گیرد. این سامانه در سپتامبر ۱۹۹۹ بصورت رسمی برای عموم راه اندازی شده است.

www.ketab.ir

نِت.اِسپارکِر[5] : نِت.اِسپارکِر یک ابزار پویشگر امنیتی خودکار برای برنامه‌های کاربردی تحت وب (با هر زبان یا بستری) است. این ابزار تنها پویشگر موجود با توانایی بهره‌گیری[6]

---

[1] OWASP (The Open Web Application Security Project)

[2] متن‌باز، منبع‌باز (به انگلیسی: Open source) یک کُد منبع است که برای اصلاح و توزیع مجدد احتمالی آزادانه در دسترس قرار می‌گیرد.

[3] CVE (Common Vulnerabilities and Exposures)

[4] MITRE

[5] Netsparker

[6] بهره‌جو، Exploit، برنامه‌ها و کُدهایی هستند که توسط یک یا چند هکر یا محقق امنیتی برای اثبات یا استفاده از آسیب‌پذیری امنیتی خاصی در یک نرم‌افزار، سیستم‌عامل یا سخت‌افزار خاص نوشته می‌شوند.

از آسیب‌پذیری‌ها در شرایط فقط خواندنی[1] و امن است. در سامانه مربوط به این ابزار یک نوع دانشنامه نیز وجود دارد که اطلاعات مفیدی را نسبت به آسیب‌پذیری‌ها و تهدیدات امنیتی منتشر می‌کند.

در پایان نویسندگان کتاب از خوانندگان محترم درخواست می‌کنند تا آنها را از نقد سازنده خود بهره‌مند سازند.

www.ketab.ir

[1] فقط خواندنی به داده، پرونده، پوشه یا هر شی دیگری که قابلیت ویرایش‌شدن و تغییر یافتن نداشته باشد، گفته می‌شود.

فهرست مطالب

مقدمه‌ای بر چرخه توسعه امن نرم‌افزار ۱۷

۱. چرخه توسعه امن (اس.دی.ال.): ۱۷

فصل اول : نقص در استفاده از حافظه ۲۵

۱-۱. سرریز بافر ۲۷

۱-۲. استفاده ازحافظه آزاد شده ۳۵

۱-۳. نشت حافظه ۳۹

۱-۴. آزادسازی مجدد حافظه ۴۴

۱-۵. کانال پنهان ذخیره‌سازی ۵۰

فصل دوم : بررسی نادرست ورودی ۵۷

۲-۱. قالب کنترل نشده رشته‌ها ۵۹

۲-۲. اسکریپت نویسی بین وبگاهی ۶۷

۲-۳. پردازش یک موجودیت خارجی ایکس.اِم.اِل ۷۵

۲-۴. تزریق سی.اس.وی ۸۰

۲-۵. تزریق کُدهای پی.اِچ.پی. ۸۸

۲-۶. تزریق زبانِ بیان ۹۷

۲-۷. تزریق سی.آر.اِل.اف. ۱۰۲

۲-۸. تزریق اِس.کیو.اِل ۱۰۸

فصل سوم : اعتبارسنجی نادرست ۱۱۷

۳-۱. اعتبارسنجی نادرست ورودی‌ها ۱۱۹

۳-۲. خطا محدودیت مسیر ۱۲۶

www.ketab.ir

۳-۳. درج فایل ۱۳۴
۳-۴. دسترسی ناامن شخص ثالث به دامنه یک سامانه ۱۴۰
۳-۵. اعتبارسنجی نکردن ایکس.ام.ال ۱۴۴
۳-۶. ملاحظات پرسش و پاسخ امنیتی ۱۴۹
فصل چهارم : ملاحظات امنیتی کُد نویسی ۱۵۳
۴-۱. نقص قابلیت حمل ۱۵۵
۴-۲. ملاحظات امنیتی کُدنویسی متحرک ۱۶۰
۴-۳. رابط بومی نا امن جاوا ۱۶۴
۴-۴. استفاده ناامن از بازتاب در برنامه‌نویسی ۱۷۰
۴-۵. خطای پایان‌دهی رشته ۱۷۵
۴-۶. استفاده از توابع منسوخ ۱۷۹
۴-۷. آزاد نکردن منابع ۱۸۴
۴-۸. برگردان سریال‌سازی داده غیر قابل اعتماد ۱۸۹
۴-۹. استفاده از اشارهگر تهی ۱۹۵
۴-۱۰. بررسی نکردن مقدار بازگشتی ۲۰۱
۴-۱۱. تفریق نامناسب اشارهگر ۲۰۷
۴-۱۲. تولید ناامن اعداد تصادفی ۲۱۱
۴-۱۳. سوء استفاده از عدم تایید ارجاع‌ها در سی.ال.آر ۲۱۵
۴-۱۴. فقدان رسیدگی به خطا ۲۲۱
فصل پنجم : ملاحظات امنیتی ارتباطات ۲۲۹
۵-۱. انتقال ناامن ۲۳۱
۵-۲. استفاده از رمزنگاری شکسته‌شده ۲۳۵
۵-۳. شناسه نشست کوتاه ۲۴۳

www.ketab.ir

۵-۴. آشفتگی متغیر نشست ۲۴۷
۵-۵. خونریزی قلبی ۲۵۲
۶-۵. ضعف در برابر محروم‌سازی از سرویس ۲۵۸
فصل ششم : ملاحظات امنیتی در مدیریت نرم‌افزار ۲۶۵
۶-۱. انقضاء دامنه ها یا حسابها ۲۶۷
۶-۲. ملاحظات امنیتی «نقص حریم خصوصی» ۲۷۰
۶-۳. ملاحظات «حفاظت از داده حساس» ۲۷۳
۶-۴. ملاحظات «مدیریت رمز عبور» ۲۷۹

www.ketab.ir