بسم الله الرحمن الرحیم

مهندسی آزمون امنیت، اعتبار سنجی و تست نرم افزار

انتشارات مهرگان قلم

سرشناسه	:	مدیری، ناصر، ۱۳۴۱ -
عنوان و نام پدیدآور	:	مهندسی آزمون امنیت، اعتبارسنجی و تست نرم‌افزار/ ناصر مدیری، طاهره نیری‌فرد.
مشخصات نشر	:	تهران: مهرگان قلم، ۱۳۹۳.
مشخصات ظاهری	:	۲۰۴ ص.: مصور، جدول، نمودار.
شابک	:	978-600-6236-67-4
وضعیت فهرست نویسی	:	فیپا
موضوع	:	آزمایش نفوذ (ایمن‌سازی کامپیوتر) -- آزمون‌ها
موضوع	:	کامپیوترها -- ایمنی اطلاعات -- آزمون‌ها
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی -- آزمون‌ها
موضوع	:	نرم‌افزار -- آزمایش
شناسه افزوده	:	نیری‌فرد، طاهره، ۱۳۶۳ -
رده بندی کنگره	:	۱۳۹۳ ۳۷ن۹ک/ QA۷۶/۹
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۳۶۳۰۴۶۷

وب سایت: www.mehreganeghalam.com

نام کتاب: مهندسی آزمون امنیت , اعتبار سنجی و تست نرم افزار

مولف: دکتر ناصر مدیری , طاهره نیری فرد

ناشر: مهرگان قلم

نوبت چاپ اول: ۱۳۹۳

شابک : ۹۷۸-۶۰۰-۶۲۳۶-۶۷-۴

تیراژ : ۵۰۰

قیمت: ۱۳۰۰۰ تومان

مرکز پخش

انتشارات مهرگان قلم:

تهران، میدان انقلاب، خیابان کارگر جنوبی، بعد از وحید نظری، کوچه گشتاسب، پلاک ۷، طبقه ۲

تلفن: ۵-۶۶۴۷۷۲۲۴ - ۶۶۴۷۶۲۱۷- ۰۹۱۲۳۱۴۶۰۵۸

پیشگفتار

شکر و سپاس و منّت و عزّت خدای را پروردگار خلق و خداوند کبریا

اول، به نام الله آغاز می کنیم که آغاز هر انجام است. شکر و سپاس بر خداوند جهانیان که ما را توفیق انجام وظیفه با قلم خویش داد. هم او که انسان را از «خون بسته» آفرید و به او یاد داد آنچه را که نمی‌دانست.

مشکل نرم افزار نام امن، شاید مهمترین چالش فنی در زمان ما است. در حال حاضر امنیت، عامل محدود کننده اصلی در مورد آنچه که ما قادر به ایجاد با فن آوری اطلاعات هستیم می باشد. امنیت نرم افزار نظامی است که خصوصیات امنیتی نرم افزار را در مراحل طراحی، آزمایش، پیاده سازی و بکارگیری، مورد خطاب قرار می‌دهد یعنی در دوره زمانی تولید نرم‌افزار یا چرخه حیات گسترش نرم افزار، و شامل فعالیت های امنیتی زیادی مانند مدل کردن تهدید، مدیریت خطر و تست های امنیتی است. به سبب پیچیدگی روزافزون برنامه های کاربردی وب، روش سنتی تست امنیتی عملکرد که فقط مکانیزم امنیت نرم افزار را تست و اعتبار سنجی می کند در نمایان کردن نقص های امنیتی پنهان نرم افزار ناکارآمد شده است.

متاسفانه تولید و توسعه نرم‌افزار امن هنوز تبدیل به دانش نشده است یا قوانین سخت‌گیرانه‌ای تبیین نشده است و فرایند توسعه به صورت عمده برای کمینه کردن آسیب‌پذیری‌هایی که منجر به حملات می‌شوند، کنترل نمی‌شود. سامانه‌های رایانه‌ای و شبکه‌ها به صورت فزاینده‌ای توسط کیفیت و امنیت نرم‌افزارشان محدود شده‌اند. نقایص و آسیب‌پذیری‌های امنیتی در نرم‌افزار متداول شده‌اند و هنگامی که با حملات مخرب مورد استفاده قرار گیرند می‌توانند به مخاطرات جدی منجر شوند.

پژوهش‌ها نشان می دهد که بر طرف کردن اشکالات امنیتی در مراحل اولیه و با استفاده از روش های نوین، بسیار مؤثرتر و کارآمدتر از برطرف کردن آنها در مراحل پیشرفته تر و با استفاده از روش هایی سنتی می باشد. بدیهی است که نمی توان نرم‌افزار امن را بدون انجام تست های امنیتی بر روی آن ایجاد کرد. با این حال بسیاری از سازمان های توسعه‌دهنده نرم افزار، تست امنیت را به عنوان بخشی از فرآیند استاندارد توسعه نرم افزار خود قرار نمی دهند. تست نرم‌افزار، تنها قدرت منحصر به فردی است که میتواند متقاعد کند که مشکل وجود دارد.

در این راستا، کتاب پیش رو در شش فصل تألیف و تدوین شده است:

فصل اول- تست نرم افزار: این بخش به آشنایی کلی با مقوله تست نرم‌افزار می پردازد. در واقع اولین و مهمترین گام در جهت رسیدن به هدف این کتاب که همان تست امنیت نرم افزار می باشد، آشنایی با مفهوم تست است که بسیار ضروری می‌نماید. در این فصل چرخه حیات تست نرم افزار بررسی و سپس به معرفی انواع روش ها، استراتژی ها و سطوح مختلف آزمون پرداخته شده است. مطالعه این فصل دید جامعی نسبت به موضوع تست نرم افزار برای خوانندگان فراهم خواهد کرد.

فصل دوم- تست امنیت نرم افزار: می توان گفت مهمترین مسئله در بحث امنیت، درک مفهوم آن و درک مشکلات امنیتی موجود است. در واقع تا نقاط حساس و نقاط ضعف شناسایی نشوند، نمی توان در این حوزه به درستی گام برداشت. این فصل به معرفی عوامل مهم و مؤثر در امنیت نرم افزار می پردازد. همچنین مهمترین خطرات نرم افزاری و راه حل های رفع یا کاهش آن ها بررسی و در ادامه به معرفی انواع روش های تست امنیت پرداخته شده است.

فصل سوم- استاندارد تست نرم افزار OWASP: در این فصل به معرفی و بررسی استاندارد OWASP پرداخته ایم. پروژه آزادی که به منظور بالا بردن سطح امنیت برنامه های کاربردی تحت وب توسعه یافته است. شاید یکی از اصلی ترین سوالات در ذهن خوانندگان کتاب این باشد که چرا OWASP؟ در جواب این پرسش می توان گفت که بیشتر راهنماهای امنیتی موجود، فقط افراد را در مورد مشکل موجود نگران می کنند بدون اینکه اطلاعات کافی برای پیدا کردن، تشخیص و حل مشکلات امنیتی ارائه کنند. پروژه OWASP مهارت و تبحر در این زمینه را در اختیار افرادی که به آن نیاز دارند، قرار می دهد. پروژه OWASP در تلاش است تا جهان را مکانی بسازد که در آن نرم افزار های نا امن، غیر عادی و نا به هنجار هستند.

فصل چهارم- روش تست نرم افزار ASVS: امنیت برنامه‌های کاربردی تحت وب از اهمیت زیادی برخوردار است. به این دلیل، تولیدکنندگان و استفاده‌کنندگان از آن‌ها نیاز به استانداردی دارند تا از آن به عنوان معیاری مشترک برای رسیدن به درجه‌ای از اطمینان در امنیت یک برنامه کاربردی تحت وب استفاده کنند. در این فصل، استاندارد وارسی امنیت در برنامه های کاربردی معرفی می شود که چهار سطح برای وارسی امنیت برنامه‌های کاربردی تحت وب تعریف می‌کند و در هر سطح نیازمندی‌هایی را تعیین می‌کند که برای داشتن برنامه کاربردی امن باید آن‌ها را برآورده کرد.

فصل پنجم- تست برنامه های کاربردی وب بر اساس OWASP: این فصل به چگونگی به کارگیری ASVS در چرخه حیات نرم افزار و معرفی فازهای تست نرم افزار بر اساس چارچوب OWASP می پردازد و کنترل های تست ارائه شده توسط این استاندارد بررسی می‌شود.

فصل ششم- آزمایشگاه تست امنیت نرم افزار: به منظور انجام تست صحیح، انجام این پروسه در یک روال مشخص شده الزامی است. در این فصل، پس از معرفی چند آزمایشگاه مطرح در این زمینه، فرآیندهای مورد نیاز برای آزمایشگاه تست امنیت نرم افزار معرفی شده اند. همچنین آشنایی با ابزارهای تست نفوذ با قابلیت های مختلف به منظور به کارگیری عملی ارائه گردیده است.

در دنیای نرم افزار های امن، داشتن گام های صحیح در این راستا الزامی است. در نگاهی سطح بالا این گام ها را می‌توان بدین ترتیب بیان داشت:

گام اول: تست معمول و پایه که در این گام باید کاستی های سیستم شناسایی و کشف شود که چه فرآیندهایی صحیح انجام نشده. بررسی اینکه آیا کیفیت برآورده شده است یا نه در این گام باید مورد توجه قرار گیرد.

گام دوم: تست نفوذ در این مرحله باید ریسک های امنیتی بررسی شده و کاستی ها از منظر امنیتی مورد توجه قرار گرفته و تست نفوذ پذیری در قبال آسیب پذیری ها انجام شود.

گام سوم: رزمایش سایبری پس از گذر از گام های اول و دوم و با شناسایی راه های نفوذ و آسیب پذیری های امنیتی، حال این موضوع حیاتی می شود که آیا آمادگی مقابله با مشکلات شناسایی شده را داریم؟ در واقع با ورود به این حوزه و انجام رزمایش سایبری میزان آمادگی خود در برابر کاستی ها و نقاط مورد سوء استفاده را بررسی کنیم.

با توجه به اهداف این تألیف و معرفی فصول ذکر شده، این کتاب در پیشبرد اهداف امن کردن برنامه های کاربردی، در جایگاه دوم از گام های ذکر شده قرار خواهد گرفت. امیدواریم در تلاش برای نیل به این مقصود موفق بوده و این کتاب مورد استفاده دانشجویان و علاقمندان موضوع قرار گیرد.

از تمامی عزیزانی که در تهیه این کتاب به نحوی یاری رساندند، تشکر و قدردانی می نماییم. با امید به دریافت

فهرست مطالب

۱ تست نرم‌افزار

۲ تست امنیت نرم‌افزار

۴ روش تست نرم‌افزار: ASVS